Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ....7
Αποφάσεις του ΕΔΔΑ σχετικά με τις αρχές που διέπουν το διαδίκτυο - Το διαδίκτυο ως μέσο έκφρασης....10
ΠΡΩΤΟ ΚΕΦΑΛΑΙΟ: Διαδίκτυο των Πραγμάτων....14
1 Ζητήματα ασφαλείας....20
2 Το Διαδίκτυο των Πραγμάτων (IoT) σε σχέση με την προστασία των δεδομένων και την Κυβερνοασφάλεια....24
3 Εφαρμογές του διαδικτύου των Πραγμάτων....32
3.1 Μη επανδρωμένα αεροσκάφη (Drones)....40
3.1.1 Χρήσεις....41
3.1.2 Προστασία της ιδιωτικής ζωής....44
4 Διαδίκτυο των πραγμάτων και ιδιωτικότητα....47
5 Διαδίκτυο των σκέψεων....52
ΔΕΥΤΕΡΟ ΚΕΦΑΛΑΙΟ: Κρυπτονομίσματα....56
1 Εισαγωγικά....56
2 Κρυπτονομίσματα και τρίτοι: χρηματιστήριο, χρηματοπιστωτικά ιδρύματα κι επενδυτές....58
3 Προβλήματα από τη χρήση των κρυπτονομισμάτων....61
4 Ειδικότερα θέματα κατά τη χρήση των κρυπτονομισμάτων....65
5 Είδη κρυπτονομισμάτων....71
5.1 Bitcoin....71
5.2 Ethereum - Ether....85
5.3 Ripple....86
5.4 KodakCoin....87
5.5 Petro....88
6 Τεχνολογία blockchain....89
6.1 Εφαρμογές της τεχνολογίας blockchain....94
6.2 Νομικά ζητήματα της τεχνολογίας blockchain....96
7 Θέματα φορολόγησης....105
7.1 Η φορολόγηση σε σχέση με την τεχνολογία blockchain και το διαμοιρασμένο δημόσιο καθολικό (shared public ledger)....108
7.2 Η φορολόγηση σε σχέση με την ICO (Initial Coin Offering)....110
7.3 Η φορολόγηση των κρυπτονομισμάτων....112
8 Τα κρυπτονομίσματα στην ελληνική πραγματικότητα και η φορολόγησή τους....123
ΤΡΙΤΟ ΚΕΦΑΛΑΙΟ: Εικονική κι Επαυξημένη Πραγματικότητα....127
1 Εισαγωγικά....127
2 Εφαρμογές των τεχνολογιών εικονικής κι επαυξημένης πραγματικότητας....132
3 Κοινωνικός εγκλιματισμός στις νέες τεχνολογίες....140
4 Εικονική πραγματικότητα....143
4.1 Εικονικοί Κόσμοι: έννοια....146
4.2 Ιδιομορφίες και νομικοί προβληματισμοί επί των εικονικών κόσμων....148
4.2.1 Προστασία της ιδιωτικής ζωής στον εικονικό κόσμο....150
4.2.2 Κυριότητα εικονικών κινητών πραγμάτων....151
4.2.3 Φορολόγηση των παιχνιδιών στους εικονικούς κόσμους....153
4.2.4 Αδικοπραξίες εντός των εικονικών κόσμων....154
4.2.5 Δικαίωμα στη δημοσιότητα και ελευθερία έκφρασης....155
4.2.6 Σωματικές βλάβες και τόπος τέλεσης του αδικήματος....156

4.2.7 Όροι χρήσης....157
4.3 Εφαρμογές των εικονικών κόσμων....158
5 Επαυξημένη πραγματικότητα....162
5.1 Εφαρμογές της επαυξημένης πραγματικότητας....165
5.1.1 Μουσεία....167
5.1.2 Τα γυαλιά της Google....168
5.1.3 PokemonGo....176
5.2 Επαυξημένη Πραγματικότητα και ηλεκτρονικό εμπόριο....187
6 Ζητήματα ασφάλειας των δεδομένων κατά τη χρήση των νέων τεχνολογιών και των ψηφιακών εφαρμογών....188
7 Νέες τεχνολογίες: ζητήματα προστασίας κι εφαρμοστέο δίκαιο....192
7.1 Πνευματική Ιδιοκτησία....192
7.2 Προστασία της ιδιωτικότητας....195
7.3 Ασφάλεια....197
7.4 Προστασία της ελευθερίας λόγου κι έκφρασης....199
7.5 EULAS (End-User License Agreement)....201
7.6 ToS (Terms of Service)....203
7.7 Εγκυρότητα των δικαιοπραξιών....204
7.8 Αδικοπραξίες....204
7.9 Ειδικά ζητήματα κυριότητας....205
7.10 Δικαίωμα στην ιδιωτική ζωή....207
7.11 Εφαρμοστέο Δίκαιο....210
ΤΕΤΑΡΤΟ ΚΕΦΑΛΑΙΟ: Τεχνητή Νοημοσύνη....217
1 Εισαγωγικά....217
2 Ορισμοί....219
3 Τεχνητή νοημοσύνη και ανθρώπινη αυτονομία....224
4 Νομικό πλαίσιο....227
5 Εφαρμογές της Τεχνητής Νοημοσύνης....240
5.1 Αναγνώριση προσώπου (facial recognition)....244
5.2 Ειδικά ζητήματα για τις εφαρμογές της τεχνητής νοημοσύνης....251
5.3 Ειδικά ζητήματα για τις εφαρμογές της ρομποτικής....261
6 Κενά και προκλήσεις....270
ΣΥΜΠΕΡΑΣΜΑΤΑ....277
Παράρτημα Α΄....295
Παράρτημα Β΄....306
Βιβλιογραφία – Αρθρογραφία....307

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ



ΤΜΗΜΑ ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΜΟΥΣΕΙΟΛΟΓΙΑΣ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ ΜΕ ΘΕΜΑ:

Δίκαιο και Δεοντολογία στις εφαρμογές της Επαυξημένης Πραγματικότητας. Τεχνολογικές προεκτάσεις και προβληματισμοί.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΑΝΑΣΤΑΣΙΑ ΜΙΧΑΗΛΑΚΗ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ: ΜΑΡΙΑ ΚΑΝΕΛΛΟΠΟΥΛΟΥ – ΜΠΟΤΗ (επιβλέπουσα)

ΓΕΩΡΓΙΟΣ ΓΙΑΝΝΟΠΟΥΛΟΣ

ΕΜΜΑΝΟΥΗΛ ΜΑΓΚΟΣ

ΜΑΡΤΙΟΣ 2021

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Συντομογραφίες

ΑΕΙ:	Ανώτατα Εκπαιδευτικά Ιδρύματα
ΑΚ:	Αστικός Κώδικας
ΓΚΠΔ:	Γενικός Κανονισμός για την Προστασία των Δεδομένων
ΔτΠ:	Διαδίκτυο των Πραγμάτων
ΕΔΔΑ:	Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου
ΕΕ:	Ευρωπαϊκή Ένωση
ΕΕΤΤ:	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΚ:	Ευρωπαϊκό Κοινοβούλιο
ΕΚΠΑ:	Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών
ΕΜΠ:	Εθνικό Μετσόβιο Πολυτεχνείο
επ.:	επόμενα
ΕΣΔΑ:	Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου
Η/Υ:	Ηλεκτρονικός Υπολογιστής
ΗΠΑ:	Ηνωμένες Πολιτείες Αμερικής
ΚΦΕ:	Κώδικας Φορολογίας Εισοδήματος
ΜΚΟ:	Μη Κυβερνητικές Οργανώσεις
ΟΠΙ:	Οργανισμός Πνευματικής Ιδιοκτησίας
ΦΠΑ:	Φόρος Προστιθέμενης Αξίας
2D:	two-dimensional
3D:	three-dimensional
AI:	Artificial intelligence
app:	application
ATM:	Automated Teller Machine
BAA:	Business Associate Agreement
BBC:	British Broadcasting Corporation
BrainNet:	Brain network
CCBE:	Council of Bars and Law Societies of Europe
CCTV:	Closed-circuit television
CEPEJ:	European Commission for the Efficiency of Justice
CFAA:	Computer Fraud and Abuse Act
COVID-19:	Corona virus disease 2019

DAO:	Decentralized Autonomous Organization
Darknet:	Dark network
DDoS:	Distributed Denial-of-Service
DApps:	Decentrilized Applications
DEFeND :	Data govErnance For supportiNg gDpr
DNA:	Deoxyribonucleic acid
DPA:	Data Protection Act
eIDAS:	electronic IDentification, Authentication and trust Services
ENISA:	European Network and Information Security Agency
EULA:	End-user License Agreement
FBI:	Federal Bureau of Investigation
FOMO:	Fear Of Missing Out
FTC:	Federal Trade Commission
GBC:	Global Business Company
GDPR:	General Data Protection Regulation
GPS:	Global Positioning System
HMDs:	Head-Mounted Displays
HIPAA:	Health Insurance Portability and Accountability Act
hodl:	hold on for dear life
ICCPR:	International Covenant on Civil and Political Rights
ICO:	Information Commissioner's Office
ICO:	Initial Coin Offering
ICESCR:	International Covenant on Economic, Social and Cultural Rights
ICT:	Information and communications technology
IDS:	Intrusion Detection System
IoT:	Internet of Things
IPO:	Initial Public Offering
IRS:	Internal Revenue Service
LCD:	Liquid Crystal Displays
LED:	Light-Emitting Diode
MIT:	Massachusetts Institute of Technology
MoMA:	Museum of Modern Art
NCRFRILS:	National Capital Region Facial Recognition Investigative Leads System

NIST:	National Institute of Standards and Technology
PerC:	Pervasive Computing
PTSD:	Post-traumatic stress disorder
QR:	Quick Response
RFID:	Radio-frequency identification
SIENNA:	Stakeholder-Informed Ethics for New technologies with high socio-ecoNomic and human rights impAct
TCP/IP:	Transmission Control Protocol/Internet Protocol
ToS:	Terms of Service
UAV:	Unmanned Aerial Vehicles
UDHR:	Universal Declaration of Human Rights
UNISEF:	United Nations International Children's Emergency Fund
vDPA:	virtual Data Path Acceleration
VR:	Virtual Reality
WiFi:	Wireless Fidelity
WRO:	World Robot Olympiad

ΕΙΣΑΓΩΓΗ

Το 1987, το Ανώτατο Δικαστήριο των Ηνωμένων Πολιτειών της Αμερικής, στην απόφασή του *Daniel vs Dow Jones*[1] υπογράμμιζε χαρακτηριστικά ότι «για αιώνες οι τελάληδες μετέφεραν τα νέα στους κατοίκους κάθε πόλης και ύστερα οι εφημερίδες ευρείας κυκλοφορίας κατέστησαν τους τελευταίους περιττούς. Στις αρχές του [20ού] αιώνα η έγκαιρη ενημέρωση επιτυγχανόταν με ειδικές εκδόσεις των εφημερίδων και συνδρομητικές ραδιοφωνικές ή τηλεφωνικές υπηρεσίες. Η τηλεόραση και το ραδιόφωνο ευρείας εμβέλειας επέτρεψαν στο κοινό την πρόσβαση στην είδηση μέσα σε λίγα λεπτά από το συμβάν. Τα τελευταία χρόνια η πληροφόρηση είναι στιγμιαία γι' αυτόν που διαθέτει στο σπίτι του ηλεκτρονικό υπολογιστή κι έχει πρόσβαση σε τηλεφωνική γραμμή». Παρά την προφητική αυτή δήλωση, το Ανώτατο Δικαστήριο δεν ήταν σε θέση να προβλέψει την έκρηξη του διαδικτύου που θα σημειωνόταν τις επόμενες δεκαετίες, με τις διασυνδεδεμένες συσκευές σε αυτό να φτάνουν μέχρι το έτος 2030 τα 50δις[2].

Οι λόγοι αυτής της «πανδημίας» συνδέσεων είναι πολλοί, με κυριότερους τη φτηνή «πρώτη ύλη», καθώς για τη σύνδεση απαιτείται ένας υπολογιστής και πολλές φορές δεν είναι απαραίτητη ούτε η τηλεφωνική γραμμή, ενώ από την άλλη η απουσία τρίτων το διαφοροποιεί από τα άλλα μέσα ενημέρωσης, καθιστώντας το αποκεντρωμένο σύστημα διάχυσης της πληροφορίας, άνευ χωρικών ή χρονικών ορίων. Η διαφοροποίηση αυτή επιτυγχάνεται επίσης και με τη δυνατότητα διατήρησης της πληροφορίας στο διηνεκές, αλλά και με την ασύγχρονη πρόσβαση σε αυτή, χαρακτηριστικά που αποτελούν τόσο πλεονεκτήματα, όσο και μειονεκτήματα του μέσου. Αλλά αυτά τα ίδια χαρακτηριστικά του είναι που το καθιστούν και την

1 «*Daniel v. Dow Jones & Co*, Inc, 520 N.Y.S 2d 334, 335, 137 Misc. 2d 94, 94-95 (N.Y.Civ. Ct. 1987) σε Παναγιώτης Βογιατζής, «Η Ελευθερία της Έκφρασης στο Διαδίκτυο: ένας θαυμαστός, καινούριος κόσμος» στη νομολογία του ΕΔΔΑ, *ΔiΜΕΕ,* τ. 3, (2016): 371-384.

2 Στα τέλη του 2018 ήταν συνδεδεμένες στο διαδίκτυο 22 δισεκατομμύρια συσκευές, ενώ οι ειδικοί εκτιμούν ότι ο αριθμός των συνδεδεμένων στο διαδίκτυο συσκευών θα αγγίξει τα 38,6 δις μέχρι το 2025 και τα 50 δις έως το 2030. Βλ. σχετικά https://zarifopoulos.com/ecosystem-internet-things-numbers/.

«πιο συμμετοχική μορφή άσκησης της ελευθερίας του λόγου σε παγκόσμια κλίμακα»[3].

Ήδη από τα τέλη της δεκαετίας του ’60 οι κοινωνικοί επιστήμονες που εξέταζαν τη μεταβιομηχανική εποχή, μίλησαν για την περίφημη «κοινωνία της πληροφορίας[4]», η οποία, στην τρίτη δεκαετία πλέον του 21ου αιώνα, αποτελεί πια μία παγκόσμια πραγματικότητα. Σύμφωνα με τον Antony Giddens, όλες οι ανθρώπινες κοινωνίες υπήρξαν ανέκαθεν «κοινωνίες της πληροφορίας». Αυτή ήταν που αποτελούσε δίαυλο προόδου και ευημερίας. Από τον Γουτεμβέργιο έως το σιδηρόδρομο, τον τηλέγραφο και το τηλέφωνο, είχαμε διαδοχικές τεχνολογικές επαναστάσεις, οι οποίες προκάλεσαν αναστάτωση, τριβές κι εντάσεις, οδήγησαν όμως τελικά τον κόσμο προς τα εμπρός[5]. Κατά την παρουσίαση επένδυσης της εταιρίας Microsoft στην Ελλάδα τον Οκτώβριο του 2020 επισημάνθηκε ότι «η εντυπωσιακή ανατροπή της δικής μας «εποχής της γνώσης» είναι ότι η ίδια η πληροφορία και η τεχνολογία γίνονται, πια, μέσα παραγωγής. Συνεπώς η ανάπτυξή τους συνιστά ένα βήμα συλλογικής οικονομικής ανάπτυξης. Ενώ κάθε μέτρο που τις κάνει πιο προσιτές στους πολίτες συνιστά και δημοκρατική τομή».[6]

---

3 Eric Barendt, «Freedom of Speech», (δεύτερη έκδοση), Oxford University Press, (2005): 451 σε Παναγιώτης Βογιατζής, «Η Ελευθερία της Έκφρασης στο διαδίκτυο: ένας θαυμαστός, καινούριος κόσμος στη νομολογία του ΕΔΔΑ», *ΔiΜΕΕ,* τ. 3, (2016): 371-384.

4 Πρόκειται για μια κοινωνία στην οποία «η πληροφορική τεχνολογία κυριαρχεί και προκαλεί σημαντικές κοινωνικές αλλαγές, όπου η ανάπτυξη της πληροφορικής τεχνολογίας αντιμετωπίζεται ως το αίτιο για την κοινωνική αλλαγή που οδηγεί από τη βιομηχανική κοινωνία σε ένα νέο τύπο κοινωνίας, την Κοινωνία της Πληροφορίας και της Γνώσης». βλ. σχετικά Γιάννης Κάλλας, «Η Κοινωνία της Πληροφορίας και ο νέος ρόλος των Κοινωνικών Επιστημών», εκδόσεις Νεφέλη (2006).
Η κοινωνία της πληροφορίας θέτει αναμφίβολα νέες προκλήσεις και ζητήματα στο δίκαιο - και για το δίκαιο. Η πρώτη - και ίσως η πλέον προφανής – πρόκληση αφορά την εφαρμογή και εφαρμοσιμότητα των κανόνων και γενικότερα την επιβολή του δικαίου. Τα χρονικά και εδαφικά όρια που συνιστούν παραδοσιακές βάσεις του δικαίου ανατρέπονται από το πλαίσιο της κοινωνίας της πληροφορίας που χαρακτηρίζεται από την απουσία ορίων και τον άυλο χαρακτήρα των επικοινωνιών. Στο διαδίκτυο οι εδαφοχρονικές συνιστώσες αποτελούν ένα διαρκές πρόβλημα. Το ισχύον (εθνικό) δίκτυο έχει ως σημείο αναφοράς το έδαφός του, καθώς τα εδαφικά όρια προσδιορίζουν το πεδίο εφαρμογής του. Η σχέση μεταξύ φυσικών συνόρων και ορίων του νόμου αντικατοπτρίζει μια βαθιά ριζωμένη σχέση ανάμεσα στη φυσική εγγύτητα και τις (έννομες) συνέπειες της ιδιαίτερης συμπεριφοράς. Βλ. σχετικά Λίλιαν Μήτρου, «Το δίκαιο στην κοινωνία της πληροφορίας», εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη (2002): 24-25.

5 Βλ. σχετικά «Αντονι Γκίντενς: Επαναστατικό φαινόμενο η παγκοσμιοποίηση», (2007), διαθέσιμο σε https://m.naftemporiki.gr/story/155396 .

6 Βλ. σχετικά «Παρουσίαση της νέας επένδυσης της Microsoft στην Ελλάδα από τον Πρωθυπουργό Κυριάκο Μητσοτάκη και τον Πρόεδρο της εταιρείας, Brad Smith», (2020), διαθέσιμο σε

Είναι γεγονός ότι «η αξία βρίσκεται στην πληροφορία. Όπως ακριβώς τα υλικά αγαθά έχουν οικονομική αξία, έτσι και η ψηφιακή πληροφορία αποκτά οικονομική αξία. Το bit, η ελάχιστη μονάδα ψηφιακής απεικόνισης των «0» και «1», του δυαδικού συστήματος, μετασχηματίζεται σε νέο είδος ατόμου, στοιχειώδους δομικού στοιχείου που επηρεάζει τις κοινωνικές και οικονομικές δομές, κατά τον ίδιο επαναστατικό τρόπο που η ανακάλυψη στην πυρηνική φυσική των αναλογικών ατόμων επηρέασε τη γνώση μας για το σύμπαν. Το πρακτικό γεγονός, πάντως είναι ότι εδώ και καιρό οι υλικοί φορείς ψηφιακών δεδομένων έχουν μηδαμινή αξία σε σχέση με τις αποθηκευμένες πληροφορίες, τα bits»[7].

Το Μάιο του 2020, το Γερμανικό Συνταγματικό Δικαστήριο αποφάνθηκε ότι οι εξουσίες παρακολούθησης της διαδικτυακής κίνησης δεδομένων (internet trac) αλλοδαπών υπηκόων στο εξωτερικό από την πλευρά της γερμανικής υπηρεσίας πληροφοριών είναι αντισυνταγματικές και επισημάνθηκε ότι η πρακτική που ακολουθεί η γερμανική υπηρεσία πληροφοριών παραβιάζει την ελευθερία του Τύπου, όπως αυτή κατοχυρώνεται στο γερμανικό Σύνταγμα. Η σημαντική αυτή απόφαση, η οποία εκδόθηκε έπειτα από προσφυγή μίας γερμανικής ΜΚΟ, της Society for Civil Rights και πέντε δημοσιογραφικών οργανισμών, αποτελεί την πρώτη δικαστική απόφαση με αντικείμενο τις δραστηριότητες παρακολούθησης της γερμανικής υπηρεσίας πληροφοριών, μετά από τουλάχιστον 20 χρόνια. Σημαντικό είναι επίσης το γεγονός ότι για πρώτη φορά το Γερμανικό Συνταγματικό Δικαστήριο αποφαίνεται ότι η γερμανική υπηρεσία πληροφοριών υπόκειται στο γερμανικό Σύνταγμα, ακόμα και στην περίπτωση που οι δραστηριότητές της διεξάγονται εκτός συνόρων.[8]

https://primeminister.gr/2020/10/05/24950 .

7 Γεώργιος Γιαννόπουλος, «Εισαγωγή στη Νομική Πληροφορική», Νομική Βιβλιοθήκη, Αθήνα, 2018.

8 Ειδικότερα, το Γερμανικό Συνταγματικό Δικαστήριο έκρινε (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 - Rn. 1-332) ότι, δυνάμει του άρθρου 1 παρ. 3 του Γερμανικού Συντάγματος, η άσκηση των γερμανικών κρατικών εξουσιών διέπεται από τα θεμελιώδη δικαιώματα που κατοχυρώνονται στο Σύνταγμα, όχι μόνο εντός της γερμανικής επικράτειας. Οι διατάξεις του άρθρου 10 παρ. 1 (θεμελιώδες δικαίωμα στην ιδιωτικότητα των τηλεπικοινωνιών) και του άρθρου 5 παρ. 1, εδ. β΄ (ελευθερία του Τύπου), οι οποίες προβλέπουν την προστασία από την παρακολούθηση των τηλεπικοινωνιών, ως δικαιώματος που αντιτίθεται στην κρατική παρέμβαση, παρέχουν επίσης προστασία στους αλλοδαπούς υπηκόους σε άλλες χώρες. Αυτό εφαρμόζεται ανεξαρτήτως από το εαν η παρακολούθηση διεξάγεται από τη Γερμανία ή από το εξωτερικό. Εντούτοις, σύμφωνα με το Γερμανικό

Αποφάσεις του ΕΔΔΑ σχετικά με τις αρχές που διέπουν το διαδίκτυο - Το διαδίκτυο ως μέσο έκφρασης.

Η ελευθερία της έκφρασης καλύπτει όχι μόνο το περιεχόμενο των ιδεών και των πληροφοριών, αλλά και το μέσο με το οποίο δίνεται βήμα για να εκφραστούν αυτές[9]. *Κατ' επέκταση, και οι απόψεις και οι πληροφορίες που διαδίδονται μέσω του διαδικτύου εμπίπτουν στο πεδίο εφαρμογής του άρθρου 10 ΕΣΔΑ*[1011]. «Χάρη στην

Συνταγματικό Δικαστήριο, η στρατηγικής σημασίας παρακολούθηση τηλεπικοινωνιών αλλοδαπών σε άλλες χώρες είναι, καταρχήν, συμβατή με τα θεμελιώδη δικαιώματα που κατοχυρώνονται στο Γερμανικό Σύνταγμα, υπό τον όρο ότι ο σχεδιασμός της πληροί τις απαιτήσεις της αρχής της αναλογικότητας. Βλ. σχετικά Janosch Delcker, «Top German court deems spying on foreigners' internet traffic is unconstitutional», (2020), διαθέσιμο σε https://www.politico.eu/article/top-german-court-deems-spying-on-foreigners-internet-traffic-is-unconstitutional/.

9 ΕΔΔΑ, *Jersild κατά Δανίας* (τμήμα ευρείας σύνθεσης), 22-09-1994, παρ. 31, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= .Ο προσφεύγων, ο οποίος ήταν δημοσιογράφος, γύρισε ένα ντοκιμαντέρ που περιείχε αποσπάσματα από μια τηλεοπτική συνέντευξη την οποία είχε πάρει ο ίδιος από τρία μέλη μιας ομάδας νέων, αυτοαποκαλούμενων «τα πράσινα σακάκια», οι οποίοι εξέφρασαν προσβλητικά και υποτιμητικά σχόλια εις βάρος μεταναστών και εθνοτικών ομάδων που είχαν εγκατασταθεί στη Δανία. Ο προσφεύγων καταδικάστηκε για συνέργεια στη διάδοση ρατσιστικών σχολίων. Ισχυρίστηκε ότι παραβιάστηκε το δικαίωμά του στην ελευθερία έκφρασης. Το Δικαστήριο διέκρινε μεταξύ, αφενός, των μελών της ομάδας «τα πράσινα σακάκια», τα οποία εξέφρασαν προδήλως ρατσιστικά σχόλια, και, αφετέρου, του προσφεύγοντος, ο οποίος επιχείρησε να παρουσιάσει, να αναλύσει και να εξηγήσει την ιδιαίτερη αυτή ομάδα νέων και να ασχοληθεί με συγκεκριμένες εκφάνσεις ενός ζητήματος που ήδη τότε απασχολούσε έντονα το κοινό. Το ντοκιμαντέρ, συνολικά θεωρούμενο, δεν αποσκοπούσε στη διάδοση ρατσιστικών ιδεών και απόψεων, αλλά στην πληροφόρηση του κοινού σχετικά με ένα κοινωνικό ζήτημα. Συνεπώς το Δικαστήριο έκρινε ότι υπήρξε παραβίαση του Άρθρου 10 (ελευθερία έκφρασης) της Σύμβασης.

10 Άρθρο 10 ΕΣΔΑ

11 ΕΔΔΑ, *Ahmet Yildirim κατά Τουρκίας*, 18-12-2012, παρ. 48, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= Στην υπόθεση αυτή, το Δικαστήριο κλήθηκε να εξετάσει τη νομιμότητα μίας δικαστικής απόφασης περί της παρεμπόδισης (block) της πρόσβασης σε όλες τις ιστοσελίδες που δημιουργήθηκαν με Google Sites. Το Google Sites είναι ένα εργαλείο δημιουργίας ιστοσελίδων, στο οποίο και ο προσφεύγων είχε δημιουργήσει δική του ιστοσελίδα όπου δημοσίευε το ακαδημαϊκό του έργο. Επειδή μία από τις ιστοσελίδες που δημιουργήθηκαν μέσω του Google Sites προσέβαλε τη μνήμη του Κεμάλ - πράξη που θεωρείται ποινικό αδίκημα στην Τουρκία, τουρκικό εθνικό δικαστήριο απέκλεισε την πρόσβαση σε όλες τις ιστοσελίδες που δημιουργήθηκαν μέσω του Google Sites, με αποτέλεσμα ο προσφεύγων, ο οποίος δεν είχε καμία σχέση με την εν λόγω προσβολή, να μην μπορεί να έχει πρόσβαση στο προσωπικό του site.Το ΕΔΔΑ αναγνώρισε ότι δεν υπάρχει καθολική απαγόρευση, αλλά περιορισμός στην πρόσβαση στο Ίντερνετ, ο οποίος όμως δεν είναι ήσσονος σημασίας εφόσον «*το ίντερνετ έχει γίνει σήμερα ένα από τα κύρια μέσα με τα οποία τα άτομα εξασκούν το δικαίωμά τους στην ελευθερία έκφρασης και πληροφόρησης, καθώς παρέχει τα απαραίτητα εργαλεία για τη συμμετοχή σε δραστηριότητες και συζητήσεις που αφορούν πολιτικά θέματα και θέματα γενικού ενδιαφέροντος*». Εν συνεχεία, το Δικαστήριο διέγνωσε την παραβίαση του άρθρου 10 ΕΣΔΑ, καθώς το εθνικό δικαστήριο δε στήριξε την απόφασή του σε ένα συμπαγές νομικό πλαίσιο που θα μπορούσε να αποσοβήσει αυθαιρεσίες, αλλά βασίστηκε σε μία γνώμη της Διεύθυνσης Τηλεπικοινωνιών, δεν εξέτασε την πιθανότητα υιοθέτησης ενός ηπιότερου μέτρου και απέτυχε να σταθμίσει τα διάφορα συμφέροντα που διακυβεύονταν, καθιστώντας τελικά έναν μεγάλο όγκο πληροφοριών απρόσιτο, θίγοντας έτσι τα δικαιώματα των χρηστών του διαδικτύου με παράπλευρες συνέπειες.

προσβασιμότητα σε αυτό και τη δυνατότητά του να αποθηκεύει και να διακινεί τεράστιες ποσότητες δεδομένων, το διαδίκτυο διαδραματίζει σημαντικό ρόλο στην ενίσχυση της πρόσβασης του κοινού σε ειδήσεις και διευκολύνει τη διάδοση των πληροφοριών γενικότερα. Η διατήρηση των αρχείων στο διαδίκτυο είναι μία κρίσιμη πτυχή αυτού του ρόλου και, ως εκ τούτου, το Δικαστήριο κρίνει ότι τα εν λόγω αρχεία εμπίπτουν στο πεδίο εφαρμογής της προστασίας που παρέχεται από το άρθρο 10»[12]. Περαιτέρω, αποδεικνύεται ότι η ισχύς του νέου μέσου επικοινωνίας είναι σημαντικά μεγαλύτερη από τα παραδοσιακά, ειδικότερα σε ό,τι έχει να κάνει με την προσβολή της προσωπικότητας. «Το διαδίκτυο αποτελεί πληροφοριακό και επικοινωνιακό εργαλείο, ιδιαίτερα διακριτό από τον Τύπο και συγκεκριμένα σε ό,τι αφορά τη δυνατότητα αποθήκευσης και διακίνησης πληροφοριών. Το ηλεκτρονικό δίκτυο, το οποίο εξυπηρετεί δισεκατομμύρια χρήστες παγκοσμίως, δεν είναι, κι ενδεχομένως δεν θα αποτελέσει ποτέ, αντικείμενο των ίδιων ρυθμίσεων κι ελέγχου [με τον Τύπο]. Ο κίνδυνος προσβολής στην άσκηση και απόλαυση δικαιωμάτων κι ελευθεριών από δημοσιεύματα κι επικοινωνία στο διαδίκτυο, ιδιαίτερα σε ό,τι αφορά το σεβασμό της ιδιωτικής ζωής, είναι αναμφισβήτητα υψηλότερος απ΄ ό,τι μέσω του Τύπου»[13]. Σχετικά με το περιεχόμενο όσων διακινούνται στο διαδίκτυο – πληροφορίες και ιδέες, σύμφωνα με την πάγια νομολογία του ΕΔΔΑ, κάθε είδος λόγου προστατεύεται από το άρθρο 10 της Σύμβασης[14]. Εξαιρείται ο ρατσιστικός και

12 ΕΔΔΑ, *Times Newspapers Ltd, (nos 1 et 2) κατά Ηνωμένου Βασιλείου*, 10-03-2009, παρ. 27, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= . Το Δικαστήριο έκρινε, εν προκειμένω, ότι «η σύσταση αρχείων στο Διαδίκτυο, καθόσον αποτελεί ουσιώδη πτυχή του ρόλου που διαδραματίζουν οι διαδικτυακοί τόποι», εμπίπτει στο πεδίο εφαρμογής του άρθρου 10 της ΕΣΔΑ.

13 ΕΔΔΑ, *Editorial Board of Pravoye Delo και Shtekel κατά Ουκρανίας*, 05-05-2011, παρ. 63, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= . Το ΕΔΔΑ αναγνώρισε για πρώτη φορά την υποχρέωση δημιουργίας ενός κατάλληλου κανονιστικού πλαισίου για την προστασία της ελευθερίας της έκφρασης των δημοσιογράφων στο διαδίκτυο.

14 ΕΔΔΑ, *Ashby Donald και λοιποί κατά Γαλλίας*, 10-01-2013, παρ. 34, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= . Οι προσφεύγοντες είναι φωτογράφοι μόδας, οι οποίοι καταδικάστηκαν για παραβίαση του νόμου για το copyright, διότι δημοσίευσαν φωτογραφίες στον ιστότοπο του διαδικτύου εταιρείας μόδας των πρώτου και δεύτερου εξ αυτών, χωρίς την άδεια των δικαιούχων οίκων μόδας. Επικαλούμενοι το άρθρο 7 της ΕΣΔΑ (καμιά ποινή χωρίς νόμο), υποστηρίζουν ότι το Ακυρωτικό Δικαστήριο της Γαλλίας, με το να αρνηθεί μια εξαίρεση στον νόμο για το copyright που παρείχε κάποιο άρθρο του Κώδικα Πνευματικής Ιδιοκτησίας, παραβίασε την αρχή ότι ο ποινικός νόμος πρέπει να ερμηνεύεται στενά. Επίσης, παραπονούνται και για παραβίαση των δικαιωμάτων τους για ελεύθερη έκφραση από το άρθρο 10 της ΕΣΔΑ. Το Ευρωπαϊκό Δικαστήριο

μισαλλόδοξος λόγος[15]. Παράλληλα, όμως, δεν προστατεύονται με τον ίδιο τρόπο όλα τα είδη λόγου. Για παράδειγμα, ο πολιτικός λόγος και ο λόγος που άπτεται του δημοσίου συμφέροντος απολαμβάνουν ευρύτερης, αν όχι απόλυτης προστασίας[16]. Περαιτέρω, εάν έχουμε άσκηση δημοσιογραφικής ελευθερίας, εναπόκειται στον Τύπο η διάδοση ειδήσεων και ιδεών δημοσίου ενδιαφέροντος και με αυτόν τον τρόπο εκπληρώνει το ρόλο του ως δημόσιος φρουρός (public watchdog)[17]. Επίσης η πρόσφατη νομολογία του ΕΔΔΑ μεταχειρίζεται προνομιακά την ερευνητική δημοσιογραφία (investigative journalism), τα αποτελέσματα της οποίας στη συνέχεια δημοσιοποιούνται[18]. Τέλος, αναφορικά με τους ιστότοπους οι οποίοι λειτουργούν ως πλατφόρμες συζήτησης και ανταλλαγής απόψεων, θεωρείται ότι η κριτική που

σχετικά με την επικαλούμενη παραβίαση του άρθρου 7 της ΕΣΔΑ αποφαίνεται ότι τα εθνικά δικαστήρια ερμηνεύουν τα ίδια τους δικούς τους νομικούς κανόνες και αυτό παρεμβαίνει μόνο όταν τα αποτελέσματα μιας ερμηνείας παραβιάζουν ατομικά δικαιώματα και ελευθερίες που προστατεύονται από την ΕΣΔΑ, πράγμα που δεν συμβαίνει εν προκειμένω. Επίσης, το Ευρωπαϊκό Δικαστήριο υπενθυμίζει ότι το άρθρο 10 της ΕΣΔΑ εφαρμόζεται και στο μέσο του διαδικτύου. Συνεπώς, η δημοσίευση των επίδικων φωτογραφιών σε έναν ιστότοπο αυτού που προτείνει στο κοινό εικόνες μόδας συνάπτεται προς το δικαίωμα της ελεύθερης έκφρασης και συνεπώς η καταδίκη των προσφευγόντων αποτελεί επέμβαση στο δικαίωμα αυτό. Αναγνωρίζεται όμως στις εθνικές αρχές ένα περιθώριο να κρίνουν κάθε φορά που συγκρούονται δικαιώματα και ελευθερίες που προστατεύονται από την ΕΣΔΑ και τα Πρωτόκολλα, όπως εδώ το δικαίωμα ελευθερίας έκφρασης και αυτό της προστασίας των δικαιωμάτων του δημιουργού.

15 Ιωάννης Ιγγλεζάκης, «Ελευθερία της έκφρασης και μισαλλόδοξος λόγος», σε Σπυρίδων - Ηρακλής Ακτύπης, Philippe Jougleux και Τατιάνα - Ελένη Συνοδινού, «Ελευθερία έκφρασης δημοσιογράφων και σκιτσογράφων», Σάκκουλας, 2016, σελ. 170.

16 ΕΔΔΑ, *Sürek κατά Τουρκίας* (No 1), (τμήμα ευρείας σύνθεσης), 08-07-1999, παρ. 62, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= . Ο προσφεύγων ήταν ιδιοκτήτης ενός εβδομαδιαίου περιοδικού, στο οποίο δημοσιεύθηκαν δύο επιστολές αναγνωστών, οι οποίες καταδίκαζαν με σφοδρότητα τις στρατιωτικές επιχειρήσεις των Αρχών στη νοτιοανατολική Τουρκία, κατηγορώντας τες για βίαιη καταστολή του αγώνα του κουρδικού πληθυσμού για ανεξαρτησία και ελευθερία. Ο προσφεύγων καταδικάστηκε για «διάδοση προπαγάνδας εναντίον του αδιαιρετου του Κράτους και για παρακίνηση του λαού στην εχθρότητα και το μίσος». Ο προσφεύγων ισχυρίστηκε ότι παραβιάστηκε το δικαίωμά του στην ελευθερία έκφρασης. Το Δικαστήριο έκρινε ότι δεν υπήρξε καμία παραβίαση του Άρθρου 10 (ελευθερία έκφρασης) της Σύμβασης. Διαπίστωσε ειδικότερα ότι οι επίμαχες επιστολές ισοδυναμούσαν με έκκληση για αιματηρή εκδίκηση και ότι μία από αυτές κατονόμαζε πρόσωπα, υποκινούσε μίσος εναντίον τους και τα εξέθετε σε ενδεχόμενο κίνδυνο σωματικής βίας. Κατά το Δικαστήριο, μολονότι ο προσφεύγων δεν υποστήριζε προσωπικά τις απόψεις που εκφράζονταν στις επιστολές, παρείχε εντούτοις στους συντάκτες τους ένα μέσο για την υποκίνηση μίσους και βίας. Το Δικαστήριο εκτίμησε ότι ο προσφεύγων, ως ιδιοκτήτης του περιοδικού, υπόκειτο εμμέσως στα καθήκοντα και τις υποχρεώσεις που υπέχουν οι συντάκτες και οι δημοσιογράφοι κατά τη συλλογή και διάδοση πληροφοριών στο κοινό, ρόλος ο οποίος αποκτά αυξημένη σπουδαιότητα σε περιπτώσεις διαμάχης και έντασης.

17 ΕΔΔΑ, Times Newspapers Ltd, (nos 1 et 2), παρ. 40, ό.π. υποσημείωση 10.

18 ΕΔΔΑ, *Mosley κατά Ηνωμένου Βασιλείου*, 10-05-2011, παρ. 129, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c= . Στην έννοια της σωματικής, ηθικής ή ψυχολογικής ακεραιότητας δύναται να συμπεριλαμβάνεται και η γενετήσια ζωή.

ασκείται είναι αποδεκτή, όταν έχει αντικείμενο ζητήματα γενικού ενδιαφέροντος και προέρχεται από επαγγελματίες δημοσιογράφους[19] οι οποίοι είναι γνωστοί στο ευρύ κοινό. Καταλήγοντας, και σύμφωνα με το άρθρο 10 παρ. 2 ΕΣΔΑ, το ΕΔΔΑ σημειώνει ότι «σε έναν κόσμο όπου ο ιδιώτης έρχεται αντιμέτωπος με τεράστιες ποσότητες πληροφοριών που διακινούνται μέσω των παραδοσιακών και των ηλεκτρονικών μέσων και συνεπάγονται έναν ολοένα και μεγαλύτερο αριθμό παικτών, ο έλεγχος τήρησης της δημοσιογραφικής δεοντολογίας αποκτά επιπρόσθετη σημασία»[20].

19 Φερενίκη Παναγοπούλου-Κουτνατζή, «Οι ιστότοποι Κοινωνικής Δικτυώσεως», Σάκκουλας, 2010.

20 ΕΔΔΑ, *Stoll κατά Ελβετίας*, (Τμήμα ευρείας σύνθεσης), 10-12-2007, παρ. 104, διαθέσιμο σε https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=. Στο πλαίσιο των διαπραγματεύσεων ανάμεσα στο Παγκόσμιο Εβραϊκό Κογκρέσο και τις ελβετικές τράπεζες, αναφορικά με τις αποζημιώσεις των θυμάτων του Ολοκαυτώματος για την απώλεια των κεφαλαίων τους που ήταν τοποθετημένα σε λογαριασμούς ελβετικών τραπεζών, ο Πρέσβης της Ελβετίας στις Ηνωμένες Πολιτείες απέστειλε στις ελβετικές αρχές ένα απόρρητο έγγραφο σχετικά με τη στρατηγική που θα έπρεπε, κατά τη γνώμη του, να ακολουθήσει η ελβετική κυβέρνηση στο συγκεκριμένο θέμα. Ένα αντίγραφο του απόρρητου αυτού εγγράφου περιήλθε στην κατοχή τού προσφεύγοντος δημοσιογράφου, ο οποίος δημοσίευσε δύο άρθρα σε εβδομαδιαία εφημερίδα ασκώντας έντονη κριτική στον Πρέσβη και κατηγορώντας τον για τη χρήση αντισημιτικών εκφράσεων. Οι εθνικές αρχές καταδίκασαν το δημοσιογράφο επιβάλλοντάς του χρηματική ποινή για τη δημοσιοποίηση μυστικών επίσημων διαβουλεύσεων σύμφωνα με το άρθρο 293 του ελβετικού Ποινικού Κώδικα. Κατόπιν τούτου, ο δημοσιογράφος προσέφυγε ενώπιον του ΕΔΔΑ για παραβίαση της ελευθερίας της έκφρασης του άρθρου 10 της Σύμβασης. Η ιδιαιτερότητα της συγκεκριμένης υπόθεσης εντοπίζεται στο γεγονός ότι αμφότερα τα αντικρουόμενα έννομα συμφέροντα διέθεταν δημόσιο χαρακτήρα. Δεδομένου ότι οι διαδικασίες που κινήθηκαν σε βάρος του δημοσιογράφου δεν αφορούσαν στη δυσφήμηση του Πρέσβη ή στην προσβολή της ιδιωτικής του ζωής, η στάθμιση στην οποία το ΕΔΔΑ προέβη στη συγκεκριμένη περίπτωση ήταν ανάμεσα στο συμφέρον του κοινού προς ενημέρωση και στο συμφέρον των ελβετικών αρχών προς διασφάλιση της ομαλής και επιτυχούς ολοκλήρωσης των διπλωματικών διαπραγματεύσεων με την εβραϊκή πλευρά. Σύμφωνα με το σκεπτικό του Δικαστηρίου, παρά τη δυνατότητα των δημοσιευμάτων να συμβάλουν σε μια δημόσια συζήτηση για το θέμα των αποζημιώσεων και παρά το γεγονός ότι ο εμπιστευτικός χαρακτήρας των διπλωματικών εγγράφων δε μπορεί να προστατεύεται με κάθε κόστος σε βάρος του ρόλου του τύπου ως δημόσιου επιτηρητή, στη συγκεκριμένη περίπτωση αναγνωρίζεται το προβάδισμα στο δημόσιο συμφέρον διατήρησης της εμπιστευτικότητας της επιστολής του Πρέσβη, δεδομένου ότι ενδεχόμενη δημοσίευση της επιστολής θα μπορούσε να καταστήσει τον Πρέσβη ανεπιθύμητο στη χώρα υποδοχής του ενώ, παράλληλα, θα μπορούσε να προκαλέσει ιδιαίτερα σοβαρή βλάβη στα κρατικά συμφέροντα της Ελβετίας, υπονομεύοντας το κλίμα διακριτικότητας που απαιτείται στις διπλωματικές σχέσεις και επηρεάζοντας αρνητικά τις εν εξελίξει διαπραγματεύσεις της χώρας. Σχετικά με τη συμπεριφορά του δημοσιογράφου και το βαθμό συμμόρφωσής του προς τις επιταγές της δημοσιογραφικής ηθικής, το ΕΔΔΑ εξέτασε αφενός τον τρόπο με τον οποίο απέκτησε το απόρρητο έγγραφο και αφετέρου τη μορφή και το περιεχόμενο των άρθρων που συνέταξε βάσει αυτού. Αρχικά, το Δικαστήριο τόνισε ότι η μη παράνομη συμπεριφορά του δημοσιογράφου κατά το στάδιο συλλογής των πληροφοριών μέσω της απόκτησης του εγγράφου από τρίτο πρόσωπο δεν αποτελεί απαραιτήτως αποφασιστικό παράγοντα ως προς τη συμμόρφωσή του προς τα «καθήκοντα και ευθύνες» τού άρθρου 10 § 2 της ΕΣΔΑ, δεδομένου ότι, ως δημοσιογράφος, δε θα μπορούσε να ισχυριστεί καλή τη πίστει ότι αγνοούσε το αξιόποινο της δημοσίευσης του συγκεκριμένου απόρρητου εγγράφου βάσει του άρθρου 293 του ελβετικού Ποινικού Κώδικα. Παράλληλα, το ΕΔΔΑ επεσήμανε ότι η μορφή και το περιεχόμενο των υπό εξέταση

ΠΡΩΤΟ ΚΕΦΑΛΑΙΟ: Διαδίκτυο των Πραγμάτων

> *Στις 22 Μαρτίου του έτους 1876, η εφημερίδα New York Times παρουσίασε μία νέα «καυτή» τεχνολογία, το τηλέφωνο, το οποίο θα σηματοδοτούσε την έναρξη μίας εποχής όπου οι άνθρωποι δεν θα χρειαζόταν να βγουν από τα σπίτια τους ποτέ. «Φέρνοντας η συσκευή του τηλεφώνου τη μουσική και τους ιερείς μέσα σε κάθε σπίτι, θα άδειαζε τις αίθουσες συναυλιών και τις εκκλησίες» παρατήρησαν οι New York Times.*
> *Τα πράγματα δεν εξελίχθησαν ακριβώς έτσι, αλλά σχεδόν 150 έτη αργότερα, η ιδέα ότι η τεχνολογία μας ενθαρρύνει να αποσυρθούμε από τον αληθινό κόσμο, ακόμη και αν προσκολληθούμε κάπου αλλού, δεν μοιάζει τόσο αμφίβολη. Ούτως ή άλλως, μπορεί κάποιος να έχει τα πάντα από τον καναπέ του σπιτιού του, συμπεριλαμβανομένης της μουσικής και της πνευματικής καθοδήγησης. Το μόνο που χρειάζεται είναι ένα «έξυπνο τηλέφωνο»* [1].

Η επαυξημένη πραγματικότητα αποτελεί το συνδυασμό της εικονικής πραγματικότητας και της πραγματικής, την τεχνολογία που επαυξάνει αληθινά μέρη, ανθρώπους και πράγματα με πλούσιες εικονικές εμπειρίες. Πρόκειται για μία ενισχυμένη εκδοχή της πραγματικότητας, όπου ζωντανές άμεσες ή έμμεσες όψεις του περιβάλλοντος του φυσικού – πραγματικού κόσμου επαυξάνουν – ανυψώνονται με υπερτεθειμένες εικόνες που έχουν δημιουργηθεί από τον υπολογιστή πάνω στην οπτική που έχει ο χρήστης για τον πραγματικό κόσμο, ενισχύοντας έτσι την τρέχουσα

δημοσιευμάτων δεν εστίαζαν στην ανάδειξη του θέματος των αποζημιώσεων αλλά στη μείωση της προσωπικότητας του Πρέσβη. Εκτιμώντας τα μέτρα που έλαβαν οι εθνικές αρχές σε βάρος του δημοσιογράφου, το ΕΔΔΑ διαπίστωσε ότι τα εθνικά δικαστήρια έλαβαν υπόψη το συμβατό με τις επιταγές της ΕΣΔΑ ουσιαστικό περιεχόμενο της έννοιας της εμπιστευτικότητας του εγγράφου, δίχως να επηρεάζονται κατά τη στάθμιση των διακυβευόμενων έννομων συμφερόντων από τη στενή γραμματική ερμηνεία της επίσημης έννοιας του απορρήτου, στην οποία βασίζεται το άρθρο 293 του ελβετικού Ποινικού Κώδικα. Ενόψει των ανωτέρω παρατηρήσεων, το ΕΔΔΑ διαπίστωσε ότι οι εθνικές αρχές δεν παραβίασαν στη συγκεκριμένη περίπτωση την ελευθερία της έκφρασης του δημοσιογράφου, όπως αυτή κατοχυρώνεται στο άρθρο 10 της ΕΣΔΑ, μέσω των κυρώσεων που του επέβαλαν για τη δημοσιοποίηση της εμπιστευτικής επιστολής του Πρέσβη. Βλ. σχετικά Κωνσταντίνος Λύρας-Χατζής, «Η παράνομη δημοσιογραφική έρευνα στη νεότερη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου», ΠΜΣ στην «Επικοινωνία και τα Μέσα Μαζικής Ενημέρωσης», Σχολή Οικονομικών και Πολιτικών Επιστημών, Τμήμα Επικοινωνίας και Μέσων Μαζικής Ενημέρωσης, 2019.

1 Αναστασία Μιχαηλάκη, «Επαυξημένη ή Ενισχυμένη Πραγματικότητα (mixed or augmented reality). Εφαρμογές της και αντιμετώπισή της απο την πλευρά του δικαίου» (2014).

αντίληψή του για την πραγματικότητα. Το διαδίκτυο συγχωνεύεται με το φυσικό κόσμο γύρω μας[2]: ο αληθινός κόσμος υπερσυνδέεται και ευρετηριάζεται, ενώ μέχρι τώρα το διαδίκτυο συνέδεε και ευρετηρίαζε την ανθρώπινη γνώση και την έκανε αναζητήσιμη[3].

Καθώς η επαυξημένη πραγματικότητα οδήγησε τον υπολογιστή στον έξω κόσμο και τον έκανε να εμφανίζεται παντού, δημιουργήθηκε ένας καινούριος όρος, η έννοια της συνεχούς ή διάχυτης χρήσης του υπολογιστή - του «ubiquitous computing» ή «ubicomp» ή «pervasive computing»[4]. Η γραμμή που διαχωρίζει τον κυβερνοχώρο από την πραγματικότητα έχει καταστεί εξαιρετικά δύσκολο να οριοθετηθεί και σύντομα η οριοθέτηση αυτή θα καταστεί αδύνατη. Η διάδοση της συνεχούς ή διάχυτης χρήσης του υπολογιστή (PerC) θα εγκαταστήσει το διαδίκτυο για πάντα γύρω μας, παρέχοντάς μας συνεχείς πληροφορίες στον αληθινό κόσμο όπου πλοηγούμαστε. Επιπρόσθετα, με την ενσωμάτωση του υπολογιστή στο φυσικό κόσμο, η συνεχής ή διάχυτη χρήση του υπολογιστή (PerC) θα μεταφέρει τις αρετές του κυβερνοχώρου στον υλικό κόσμο. Θα ενεργοποιήσει την, ίσως αυτόνομη,

2 Βλ. σχετικά https://www.realitytechnologies.com.

3 Joshua Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal*, Vol. 27:55 (2012).

4 Jerry Kang και Dana Cuff, «Pervasive Computing: Embedding the Public Sphere», *62 Wash. & Lee L. Rev. 93* (2005). Η έννοια της συνεχούς ή διάχυτης χρήσης του υπολογιστή (Pervasive computing -- ubiquitous computing) αφορά στην ολοένα και αυξανόμενη τάση της ενσωμάτωσης της υπολογιστικής ικανότητας (με τη μορφή των μικροεπεξεργαστών) στα αντικείμενα της καθημερινότητάς μας, με στόχο να αποκτήσουν την δυνατότητα της αποτελεσματικής επικοινωνίας και της εκτέλεσης χρήσιμων εργασιών, με τέτοιο τρόπο ώστε να ελαχιστοποιείται η ανάγκη του τελικού χρήστη να αλληλεπιδρά με τους υπολογιστές ως υπολογιστής. Οι διάχυτες υπολογιστικές συσκευές είναι συνδεδεμένες σε δίκτυο και συνεχώς διαθέσιμες. Αντίθετα με το σταθερό υπολογιστή (desktop computing), η υπολογιστική διάχυση μπορεί να προκύψει με κάθε είδους συσκευή, σε οποιονδήποτε χρόνο και με κάθε μορφή δεδομένων, μέσω οποιουδήποτε δικτύου και έχει τη δυνατότητα να εκτελεί εντολές από τον έναν υπολογιστή στον άλλο, όπως για παράδειγμα όταν ένας χρήστης κινείται από το αυτοκίνητό του προς το γραφείο του. Κατά συνέπεια, οι συσκευές διάχυτης χρήσης του υπολογιστή έχουν εξελιχθεί στο να συμπεριλαμβάνουν όχι μόνο φορητούς υπολογιστές ή «έξυπνα» τηλέφωνα, αλλά και συσκευές που μπορούν να φορεθούν, συστήματα φωτισμού, συσκευές και αισθητήρες κλπ. Ο στόχος της διάχυτης χρήσης του υπολογιστή είναι να καταστήσει τις συσκευές «έξυπνες», δηλαδή να δημιουργήσει ένα δίκτυο αισθητήρων ικανό να συγκεντρώνει, να επεξεργάζεται και να αποστέλλει δεδομένα και το σημαντικότερο, να επικοινωνεί ως μέσο προσαρμογής στο περιβάλλον και τη δραστηριότητα των δεδομένων. Στην ουσία, πρόκειται για ένα δίκτυο το οποίο μπορεί να κατανοεί το περιβάλλον του και να βελτιώνει την ανθρώπινη εμπειρία και την ποιότητα της ζωής. Οι εφαρμογές της διάχυτης χρήσης του υπολογιστή μπορεί να καλύπτουν τους τομείς της ενέργειας, της ασφάλειας, των καταναλωτών, της υγείας, της παραγωγής κλπ. Βλ. σχετικά https://internetofthingsagenda.techtarget.com.

ανταπόκριση του κυβερνοποιημένου περιβάλλοντος (cyberized environment[5]) στα δεδομένα, τα οποία μέχρι σήμερα δεν είχαν συλλεχθεί και δεν ήταν δυνατόν να συλλεχθούν. Ας φανταστούμε όχι ένα ρομπότ[6], ούτε μία απομονωμένη και μη αναγνωρίσιμη συσκευή, αλλά έναν κόσμο κορεσμένο με δικτυωμένη ευφυΐα[7].

Χάρη στα μοναδικά χαρακτηριστικά του δυναμικού περιβάλλοντος της τεχνολογίας της διάχυτης ή συνεχούς χρήσης του υπολογιστή, όπως είναι η χαλαρότητα των φυσικών ορίων και η ad-hoc διάδραση με συσκευές αδιευκρίνιστης εμπιστοσύνης, οι καταναλωτές, συμπεριλαμβανομένων και των εταιριών και των οργανισμών, θα θέτουν ως προαπαιτούμενο τη διασφάλιση της ασφάλειας, με τρόπους όπως η επαλήθευση των μηνυμάτων και των οντοτήτων, ο έλεγχος πρόσβασης και η εμπιστευτικότητα και η προστασία της ακεραιότητας του διαύλου επικοινωνίας. Επίσης, η προστασία των προσωπικών δεδομένων όπως η ταυτότητα και οι

5 Ο όρος «κυβερνοποίηση» (cyberization) αναφέρεται στη χρήση των τεχνολογιών επικοινωνίας και υπολογιστών προς διασύνδεση των υπολογιστών και των διαφόρων ηλεκτρονικών τερματικών συσκευών που είναι διαμοιρασμένες σε διάφορες τοποθεσίες. Επιτρέπει στους χρήστες να μοιράζονται λογισμικό, εξαρτήματα hardware και πόρους δεδομένων, σύμφωνα με συγκεκριμένα πρωτόκολλα δικτύου. Η κυβερνοποίηση έχει βελτιώσει σημαντικά την πρακτική χρησιμότητα των υπολογιστών κι εφαρμόζεται ευρέως στις μεταφορές, την οικονομία, τη διοίκηση επιχειρήσεων, την εκπαίδευση, τις τηλεπικοινωνίες , το εμπόριο και κατ' επέκταση την καθημερινότητα των ατόμων. Xiaokang Zhou, Flavia C. Delicato, Kevin I-Kai Wang και Runhe Huang, «Smart computing and cyber technology for cyberization», *World Wide Web* Vol. 23 (2020): 1089–1100.

6 Σύμφωνα με τον ορισμό του Ινστιτούτου Ρομπότ των ΗΠΑ, «ρομπότ είναι μια επαναπρογραμματιζόμενη πολυλειτουργική χειριστική διάταξη, σχεδιασμένη για τη μετακίνηση υλικών, εξαρτημάτων, εργαλείων και εξειδικευμένων διατάξεων, μέσω μεταβλητών, προγραμματισμένων κινήσεων για την εκτέλεση μιας σειράς εργασιών». Ένα ρομπότ συγκροτείται από δύο συστήματα, το μηχανικό (στο οποίο περιλαμβάνεται το σύστημα κίνησης) και το ηλεκτρονικό (στο οποίο υπάγεται και η επαναπρογραμματιζόμενη μνήμη του). βλ. σχετικά http://users.sch.gr

7 Μία νέα, σημαντική πλευρά της τεχνολογίας της συνεχούς ή διάχυτης χρήσης του υπολογιστή (PerC) είναι το γεγονός ότι οχυρώνει τις αισθητήριες, επικοινωνιακές και επεξεργάσιμες δυνάμεις του προσώπου, οι οποίες θα παρέχουν αυτό που κάποιοι έχουν ονομάσει «Επαυξημένη Πραγματικότητα». Ο στόχος της τεχνολογίας της διάχυτης ή συνεχούς χρήσης του υπολογιστή (PerC) δεν είναι μία ακόμη πιο ρεαλιστική εικονική πραγματικότητα που θυμίζει Matrix, όπου βυθιζόμαστε σε έναν προσομοιωτή της πραγματικότητας, κατασκευασμένο από έναν διακομιστή και αναπαραγόμενο στις αισθήσεις μας μέσω γυαλιών, ακουστικών και αναδραστικών στολών. Αντιθέτως, ο στόχος είναι ο ακριβώς αντίθετος: να ενσωματωθεί ο υπολογιστής στην πραγματικότητα και να δημιουργηθεί η μορφή της «ενσωματωμένης εικονικότητας». Σε αυτόν τον κόσμο ο υπολογιστής βρίσκεται στον αέρα, στους τοίχους, στα γυαλιά μας. Σε μία ιδανική αποτύπωση της τεχνολογίας της συνεχούς ή διάχυτης χρήσης του υπολογιστή (PerC), ουδείς περιηγείται με μία φορητή συσκευή αναζητώντας βύσμα εξόδου ή δεδομένα. Αντιθέτως, ο υπολογιστής είναι απλά διαθέσιμος, ως ψηφιακό οξυγόνο, με άνευ κόπου, αόρατη, φαινομενικά φυσική ικανότητα πρόσβασης στα δεδομένα και την πληροφόρηση. Αναστασία Μιχαηλάκη, «Επαυξημένη ή Ενισχυμένη Πραγματικότητα (mixed or augmented reality). Εφαρμογές της και αντιμετώπισή της από την πλευρά του δικαίου» (2014).

πληροφορίες τοποθεσίας αποτελούν ένα σημαντικό κριτήριο για τη μεγάλης κλίμακας ανάπτυξη της σχετικής τεχνολογίας. Με τον ερχομό των κατάλληλων συσκευών και τεχνολογιών, όπως είναι οι ασύρματοι αισθητήρες και η τεχνολογία RFID[8], οι χρήστες ήδη ανησυχούν για την εμφάνιση τεχνολογιών «Μεγάλου Αδελφού» που θα καταγράφουν τις συναλλαγές τους χωρίς τη συναίνεσή τους. Για παράδειγμα, μπορεί να αποκαλυφθεί η ταυτότητα ενός χρήστη που συμμετέχει σε μία θεωρητικά ανώνυμη συναλλαγή ή μπορεί να ταυτοποιηθούν διαφορετικές συναλλαγές από το χρήστη στο ίδιο σύστημα, με στόχο τη δημιουργία ενός προφίλ. Πρόκειται ξεκάθαρα για μία εγγενή ανταλλαγή ανάμεσα στην ιδιωτικότητα – απόρρητο και την πρόσβαση της τεχνολογίας της διάχυτης χρήσης του υπολογιστή, σύμφωνα με την οποία (ανταλλαγή), από την πλευρά του χρήστη, κανένας δεν θα έπρεπε να έχει τη δυνατότητα να ανακαλύψει την πραγματική ταυτότητα αυτού, να συνδέσει περισσότερες συνεδρίες του χρήστη στο σύστημα ή να αποκτήσει πληροφορίες για το περιεχόμενο αυτών, όπως την τοποθεσία, την ώρα και τη διάρκεια, το είδος της υπηρεσίας κ.ο.κ. Από την άλλη πλευρά, η ανάγκη ελέγχου της πρόσβασης μεγεθύνεται. Οι πάροχοι υπηρεσιών χρειάζονται την πιστοποίηση ενός μηνύματος, μιας οντότητας ή του ίδιου του περιεχομένου, με στόχο την παροχή εξουσιοδότησης πρόσβασης σε μία υπηρεσία για την αποτροπή καταχρηστικών ενεργειών ή για την προστασία των πληρωμών ή την παροχή προσωποποιημένων και σχετικών με το περιβάλλον υπηρεσιών ή τέλος για να αποκρυπτογραφήσουν την ταυτότητα του προσώπου για λόγους λογοδοσίας ή ευθύνης, σε περιπτώσεις κατάχρησης των υπηρεσιών, για την ανάκληση προνομίων ή για παράνομες ενέργειες. Για την ισορροπία των ανωτέρω, κρίθηκε ότι η ανωνυμία στην τεχνολογία

8 Η συντομογραφία RFID προέρχεται από την αγγλική φράση «Radio Frequency Identification». Πρόκειται για μικρά ηλεκτρονικά κυκλώματα, συχνά στο μέγεθος ενός κόκκου ρυζιού, τα οποία φέρουν κάποιου είδους ψηφιακή πληροφορία και χρησιμοποιούνται για κάποιου είδους αναγνώριση. Δηλαδή ένα συγκεκριμένο κύκλωμα επικοινωνεί με κάποιον δέκτη και δίνει πληροφορίες για ένα συγκεκριμένο αντικείμενο ή μια συγκεκριμένη ενέργεια. https://www.lightgear.gr/blog/ti-einai-h-prostasia-rfid/ .

της διάχυτης χρήσης του υπολογιστή πρέπει να είναι υπό όρους και μόνο υπό πολύ καλά προσδιορισμένες προϋποθέσεις πρέπει να εκτίθεται η ταυτότητα του χρήστη[9].

Αντίθετα με άλλες τεχνολογίες, η διάχυτη χρήση του υπολογιστή μπορεί να προκύψει με οποιαδήποτε συσκευή, σε κάθε τοποθεσία και με οποιαδήποτε μορφή. Ο χρήστης αλληλεπιδρά με τον υπολογιστή, ο οποίος εμφανίζεται σε διάφορες μορφές, όπως τα φορητά (laptop και tablets), τα τερματικά (terminals) και τα τηλέφωνα. Όταν οι έννοιες αυτές εμπλέκουν και αντικείμενα, είναι επίσης γνωστές και ως «physical computing» ή «Διαδίκτυο των Πραγμάτων» (Internet of things)[10]. Το διαδίκτυο των πραγμάτων αφορά πολλά αντικείμενα καθημερινής χρήσης, τα οποία έχουν τη δυνατότητα να στέλνουν και να δέχονται δεδομένα μέσω διαδικτύου[11]. Συσκευές που μπορούν να φορεθούν και συγκεντρώνουν δεδομένα (σχετικά με το βηματισμό του

9 Emmanouil Magkos, Panayiotis Kotzanikolaou, «Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments», σε The Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems - MOBISEC 2010, Catania, Sicily. LNICST, Springer, 2010.

10 Ο όρος «Διαδίκτυο των πραγμάτων» έχει λάβει διάφορες ερμηνείες. Κατά μία ευρεία έννοια περιλαμβάνει ο,τιδήποτε είναι διασυνδεδεμένο με το διαδίκτυο, κάτι που κυρίως χρησιμοποιείται για συσκευές οι οποίες μιλάνε μεταξύ τους. Άλλη, πιο απλή ερμηνεία αποτελεί η σκέψη ότι διασυνδέει με το διαδίκτυο οποιαδήποτε συσκευή έχει on και off. Το λεξικό της Οξφόρδης περιγράφει τον όρο ως η διασύνδεση μέσω του διαδικτύου υπολογιστικών συσκευών, ενσωματωμένων σε καθημερινά αντικείμενα, επιτρέποντάς τους να αποστείλουν ή να δεχθούν δεδομένα. Άλλοι περιγράφουν το διαδίκτυο των πραγμάτων ως την ικανότητα μιας συσκευής να συνδεθεί με άλλες μέσω ασύρματης υποδομής δεδομένων ή ένα σύστημα από συσκευές και αντικείμενα στα οποία έχουν εμφυτευθεί αισθητήρες, λογισμικό και ηλεκτρονικά για την διευκόλυνση της ανταλλαγής και περισυλλογής δεδομένων και πληροφοριών. Βλ. σχετικά Φερενίκη Παναγοπούλου – Κουντατζή, «Διαδίκτυο των πραγμάτων και προστασία της ιδιωτικότητας», *ΔιΜΕΕ* τ. 3, (2014): 346-358. Βλ. επίσης https://internetofthingsagenda.techtarget.com, Matt Burgess, «What Is the Internet of Things?», διαθέσιμο σε http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot (2017), Jacob Morgan, «A Simple Explanation of The Internet of Things», διαθέσιμο σε https://www.forbes.com/sites/jacobmorgan/2014/05/13/simpleexplanation-internet-things-that-anyone-can-understand (2014), Internet of Things, Oxford Dictionaries, https://en.oxforddictionaries.com/definition/Internet_of_things, Nikole Davenport, «Smart Washers May Clean Your Clothes, but Hacks Can Clean out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line», *32 J. Marshall J. Info. Tech. & Privacy L.* 259, (2016) και Vikas Agarwal, «10 Real Life Examples of Internet of Things», διαθέσιμο σε http://circuitdigest.com/ten-examples-of-internet-of-things-iot (2017) σε Hillary Brill και Scott Jones, «Little Things And Big Challenges: Information Privacy And The Internet Of Things», *American University Law Review*, Vol. 66, (2017):1183 – 1184.

11 Κατά το έτος 2008 ο αριθμός των συσκευών των συνδεδεμένων με το διαδίκτυο ήταν μεγαλύτερος από τον αριθμό των ατόμων που έκαναν χρήση του διαδικτύου. Σύμφωνα με τις στατιστικές σήμερα υπάρχουν περισσότερα από 10εκ. συνδεδεμένα αντικείμενα και μέχρι το έτος 2020 προβλέπεται αυτός ο αριθμός να φτάσει στα 50εκ.

χρήστη, την ποιότητα του ύπνου του, τις καταναλωθείσες θερμίδες, τη γεωγραφική του θέση), τα οποία θα μπορούν να αναλυθούν από τα συγχρονισμένα με αυτές τηλέφωνα ή tablets, δισκία με αισθητήρες τα οποία θα λαμβάνουν πληροφορίες από τον οργανισμό του χρήστη, θα τις υποβάλλουν σε συσκευές, όπως τα «έξυπνα» τηλέφωνα και θα προειδοποιούν στην περίπτωση πιθανών προβλημάτων υγείας, αισθητήρες που θα τοποθετούνται κάτω από τα στρώματα των νηπίων και θα ελέγχουν την υγεία τους (αναπνοή και καρδιακούς παλμούς) είναι κάποιες από τις ρεαλιστικές εκφράσεις του διαδικτύου των πραγμάτων[12].

Όπως μπορεί να γίνει αντιληπτό, ο προσωπικός υπολογιστής έχει γίνει ακόμη πιο προσωπικός – μπορεί να φορεθεί[13]. Ωστόσο, όσες συσκευές μπορούν να φορεθούν σήμερα έχουν τη δυνατότητα να αφουγκράζονται και να επικοινωνούν περισσότερο. Στην πραγματικότητα είναι «ενσωματώσιμα». Επίσης, ο προσωπικός υπολογιστής γίνεται καθημερινά μικρότερος, φθηνότερος και ισχυρότερος[14]. Και ακόμη περισσότερο, τα «έξυπνα» τηλέφωνα τείνουν να αντικατασταθούν από «έξυπνα» ρολόγια, τα οποία πραγματοποιούν τηλεφωνικές κλήσεις, συνδέονται με το διαδίκτυο ή λαμβάνουν φωτογραφίες, στην πραγματικότητα λειτουργούν όπως ένα «έξυπνο» τηλέφωνο ή ένα tablet. Στο άμεσο μέλλον κάθε άνθρωπος θα είναι συνδεδεμένος με τουλάχιστον επτά συσκευές, με επτά «ηλεκτρονικά κατοικίδια», τα οποία θα

12 Bernard Marr, «What The Heck is… The Internet of Things?», (2013), διαθέσιμο σε https://www.linkedin.com/pulse/20131023054859-64875646-what-the-heck-is-the-internet-of-things, .

13 Η ιδέα της επικοινωνίας μέσω αυτών που φοράμε δεν είναι καινούρια. Οι άνθρωποι εκφράζονται μέσα από τατουάζ, τρυπήματα του δέρματος και κοσμήματα, τα οποία συνήθως υποδηλώνουν κάτι για τους ίδιους: την προσωπικότητά τους, την καταγωγή τους ή το επάγγελμά τους. Dave Evans, «The Future of Wearable Technology: Smaller, Cheaper, Faster, and Truly Personal Computing», (2013), διαθέσιμο σε https://blogs.cisco.com/digital/the-future-of-wearable-technology-smaller-cheaper-faster-and-truly-personal-computing .

14 Ο φυσικός όγκος των υπολογιστών μειώνεται κατά 100 φορές ανά δεκαετία. Από τον ENIAC, τον πρώτο υπολογιστή του 1956, ο οποίος κάλυπτε ένα ολόκληρο δωμάτιο, προέκυψε το μικροσκοπικό κύκλωμα μίας μουσικής κάρτας, την οποία μπορεί κάποιος να προμηθευθεί από οπουδήποτε. Ένα «έξυπνο» τηλέφωνο είναι πιο ισχυρό από τους υπολογιστές που ήταν σε χρήση πριν από μία δεκαετία. Η ανθρωπότητα χρειάστηκε 2.000 χρόνια για να παράγει 5δις gigabyte δεδομένων (από παπύρους μέχρι dvd – rom) και το 2014 εκτιμάται ότι παρήχθησαν περίπου 6 zettabyte (έξι εξάκις εκατομμύρια) δεδομένων, ενώ από το 2020 ο αριθμός θα ανέβει στα 20 zettabyte. Dave Evans, «The Future of Wearable Technology: Smaller, Cheaper, Faster, and Truly Personal Computing», (2013), διαθέσιμο σε https://blogs.cisco.com/digital/the-future-of-wearable-technology-smaller-cheaper-faster-and-truly-personal-computing.

«σιτίζονται» καθημερινά με δεδομένα. Στο μέλλον οι οδοντόβουρτσες θα ειδοποιούν για την ανάγκη αντικατάστασής τους, θερμικές κάμερες στα καταστήματα θα αντιλαμβάνονται τα ενδιαφέροντα και τις προτιμήσεις των καταναλωτών, ώστε ο πωλητής να «επεμβαίνει» την κατάλληλη στιγμή, ενώ όλες οι πληροφορίες των προϊόντων, μαζί με διαφημίσεις και ανακοινώσεις προσφορών θα προβάλλονται σε οθόνη.

Το διαδίκτυο των πραγμάτων έχει ήδη λάβει μέρος στις ζωές μας με απεριόριστες μορφές. Κάποιες από αυτές είναι ευπρόσδεκτες, όπως οι εντοπίσιμες συσκευές εκγύμνασης, τα οικιακά προειδοποιητικά συστήματα ασφαλείας ή τα οχήματα με εξ αποστάσεως ξεκλείδωμα κι εκκίνηση. Άλλες είναι ακούσιες και ενδέχεται να προκαλέσουν ανησυχία στους καταναλωτές, όπως τα διασυνδεδεμένα παιχνίδια, τα οποία κατά τη λειτουργία τους παρακολουθούν τα παιδιά ή τεχνολογίες ικανές να εντοπίσουν χωρίς την έγκριση του χρήστη την τοποθεσία του ή τις αγοραστικές του συνήθειες. Καθώς το διαδίκτυο των πάντων (πλέον) ωριμάζει, τα διαφορετικά «έξυπνα» οικιακά και εμπορικά δίκτυα που δημιουργεί θα έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους, παράγοντας «έξυπνα» και πιθανόν πιο ανθεκτικά, πράγματα, πόλεις και κοινωνίες[15].

1 Ζητήματα ασφαλείας

Τον Οκτώβριο του 2016 έλαβε χώρα μία κυβερνοεπίθεση της μορφής «distributed denial of service (DDoS)[16]» από μικρές και φθηνές συσκευές συνδεδεμένες στο

15 Scott Shackelford και Scott O. Bradner, «Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything», *Hastings Law Journal*, Kelley School of Business Research Paper No. 18-60, (2021).

16 Στην πληροφορική με τον όρο «denial-of-service attack» (DoS attack) περιγράφεται η κυβερνοεπίθεση κατά την οποία ο εισβολέας προσπαθεί να καταστήσει έναν πόρο υπολογιστή ή δικτύου ακατάλληλο για τους χρήστες του, διακόπτοντας, προσωρινά ή επ' αόριστον, τις υπηρεσίες του κεντρικού υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο. Αυτό τυπικά επιτυγχάνεται με την υπερχείλιση του μηχανήματος ή του πόρου – στόχου από περιττά αιτήματα, σε μία απόπειρα να υπερφορτωθούν τα συστήματα και να αποτραπεί η ικανοποίηση κάποιων ή όλων των νόμιμων αιτημάτων. Περαιτέρω, στην περίπτωση της κυβερνοεπίθεσης που περιγράφεται με τον όρο «distributed denial-of-service attack» (DDoS attack), η

διαδίκτυο, η οποία συλλογικά έγινε γνωστή ως «Mirai botnet»[17]. Η επίθεση παρέλυσε κυριολεκτικά τους διακομιστές με τους οποίους συνδεόταν στο διαδίκτυο μία τεχνολογική εταιρία με την επωνυμία Dyn. Αυτό από μόνο του δεν θα ήταν σημαντικό, αν δεν αποκαλυπτόταν ότι η συγκεκριμένη εταιρία διαχειριζόταν κρίσιμες διαδικτυακές υποδομές, κάτι που οδήγησε στην επιβράδυνση και διακοπή της πρόσβασης σε σημαντικές διαδικτυακές συσκευές στις περισσότερες από τις ανατολικές Πολιτείες των ΗΠΑ[18]. Η επίθεση αυτή υπήρξε τόσο επιτυχής και αξιοσημείωτη, διότι εκμεταλλεύτηκε τις ευπάθειες της ασφάλειας του διαδικτύου των πραγμάτων και απέδειξε ότι σχεδόν τα πάντα είναι συνδεδεμένα με το διαδίκτυο και ό,τι δεν έχει ακόμα συνδεθεί, θα συνδεθεί στο άμεσο μέλλον[19]. Αρχικά θεωρήθηκε ότι η επίθεση είχε πολιτικά κίνητρα, αλλά από τις έρευνες προέκυψε ότι πίσω από αυτή δεν ήταν κάποιοι επαναστάτες ή κάποια παρακρατική οργάνωση, αλλά τρεις φοιτητές οι οποίοι προσπαθούσαν να κερδίσουν στο διαδικτυακό παιχνίδι Minecraft[20]. Αξιωματούχοι του FBI δήλωσαν ότι οι εισβολείς δεν είχαν συνειδητοποιήσει το μέγεθος της απειλής. Το περιστατικό αυτό καταδεικνύει τις ιδιαιτερότητες στη διαχείριση των πολύπλευρων διαδικτυακών απειλών που

υπερχείλιση προέρχεται από πολλές διαφορετικές πηγές και κατά συνέπεια καθίσταται αδύνατον να διακοπεί η επίθεση με τον αποκλεισμό μίας και μόνης πηγής. Βλ. σχετικά https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

17 Με τον όρο «bot» περιγράφεται ένας υπολογιστής ή μία συσκευή συνδεδεμένη με το διαδίκτυο που έχουν προβληθεί από κακόβουλο λογισμικό και ελέγχονται από έναν κεντρικό διακομιστή «command-and-control C2». Ο όρος «botnet» χρησιμοποιείται για να περιγράψει όλες τις συσκευές που ελέγχονται από έναν διακομιστή C2 και μπορούν να χρησιμοποιηθούν για να πραγματοποιήσουν σε μεγάλη κλίμακα κυβερνοεπιθέσεις τύπου «DDoS» (distributed denial of service attacks) σε βάρος ιστοτόπων, με αποτέλεσμα την υπερφόρτωση της επισκεψιμότητάς τους, καθιστώντας τους άχρηστους. Βλ. Neena Kapur, «The Rise of IoT Botnets», διαθέσιμο σε https://www.americansecurityproject.org/the-rise-of-iot-botnets/ (2017).

18 Josh Fruhlinger, «The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet», (2018), διαθέσιμο σε https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html, Βλ. επίσης «Inside the infamous Mirai IoT Botnet: A Retrospective Analysis», (2017), διαθέσιμο σε https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ και Garrett M. Graff, «How a Dorm Room Minecraft Scam Brought Down the Internet», (2017), διαθέσιμο σε https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet .

19 Daniel Burrus, «The Internet of Things is Far Bigger than Anyone Realizes», (2014), διαθέσιμο σε http://www.wired.com/2014/11/the-internet-of-things-bigger/. Lawrence J. Trautman, «Cybersecurity: What About U.S. Policy?», *Journal of Law, Technology and Policy*, Vol. 2015, 341 (2015).

20 Ben Bours, «How a Dorm Room Minecraft Sam Brought Down the Internet», (2017), διαθέσιμο σε https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

απευθύνονται τόσο στο δημόσιο τομέα, όσο και στον ιδιωτικό. Οι επιθέσεις μέσω του διαδικτύου των πραγμάτων προέρχονται από μη κυβερνητικούς φορείς, όπως άτομα με παραβατικές συμπεριφορές εντός του κυβερνοχώρου, πολιτικά υποκινούμενους ακτιβιστές, εφήβους εν μέσω παιχνιδιών και αποτελούν ασύμμετρες απειλές που μπορούν να χρησιμοποιηθούν με στόχο την προσβολή δικαιωμάτων και κρίσιμων υποδομών. Πλέον επιδιώκονται συνεργασίες ανάμεσα σε φορείς του Δημοσίου και του ιδιωτικού τομέα για την περιχαράκωση του διαδικτύου των πάντων, αλλά δεν είναι ακόμα εμφανές εάν αυτό είναι αρκετό.

Δεδομένου, λοιπόν, ότι οποιεσδήποτε «έξυπνες» ηλεκτρονικές συσκευές - και όχι μόνο οι υπολογιστές ή τα κινητά τηλέφωνα- μπορούν πια να πέσουν θύματα εισβολέα (hacker), είναι δυνατό ακόμα και οι συσκευές της κουζίνας να αξιοποιηθούν από τους τελευταίους ως εργαλεία μιας «κυβερνοεπίθεσης». Το ζήτημα της παραβίασης των πολύ πιο ευάλωτων συσκευών στο «διαδίκτυο των πραγμάτων» έρχεται στο προσκήνιο, καθώς όπως ανακοίνωσε η αμερικανική εταιρία κυβερνο-ασφάλειας Proofpoint, ανακάλυψε για πρώτη φορά ένα ψυγείο, το οποίο έστελνε στο διαδίκτυο ανεπιθύμητα και κακόβουλα ηλεκτρονικά μηνύματα (spam). Στην επιθετική διαδικτυακή «καμπάνια», που ενορχήστρωσαν οι εισβολείς (hackers), το ψυγείο συμμετείχε ανάμεσα σε πάνω από 100.000 άλλες συσκευές που απάρτιζαν το εν λόγω κακόβουλο δίκτυο (botnet). Η επίθεση - πιθανώς η πρώτη αποδεδειγμένη επίθεση που εκμεταλλεύτηκε το «Διαδίκτυο των Πραγμάτων» με τη σχεδόν ανύπαρκτη κυβερνο-ασφάλειά του - είχε ως στόχο ηλεκτρονικούς υπολογιστές, δρομολογητές, «έξυπνες» τηλεοράσεις.[21]. Οι ειδικοί αναλυτές της Proofpoint εκτιμούν ότι τουλάχιστον το 25% αυτών των μηνυμάτων - «δολωμάτων» δεν πέρασαν καθόλου μέσω των παραδοσιακών διαύλων (ηλεκτρονικών υπολογιστών ή

21 Σύμφωνα με το BBC και το Γαλλικό Πρακτορείο, ο καταιγισμός των ανεπιθύμητων μηνυμάτων διήρκεσε μεταξύ 23 Δεκεμβρίου 2013 και 6 Ιανουαρίου 2014. Υπολογίζεται ότι στάλθηκαν περίπου 750.000 κακόβουλα μηνύματα spam, η διαδικτυακή διαδρομή των οποίων πέρασε μέσα από παραβιασμένες συσκευές όπως τα έξυπνα ψυγεία. Βλ. σχετικά «Your Fridge is Full of SPAM: Proof of An IoT-driven Attack», (2014), διαθέσιμο σε https://www.proofpoint.com/us/threat-insight/post/Your-Fridge-is-Full-of-SPAM και «Proofpoint Uncovers Internet of Things (IoT) Cyberattack», (2014), διαθέσιμο σε https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack .

«έξυπνων» τηλεφώνων). Αντίθετα, το κακόβουλο λογισμικό σε μεγάλο βαθμό εγκαταστάθηκε και διοχετεύτηκε μέσω άλλων «έξυπνων» συσκευών, όπως οι «λευκές» συσκευές της κουζίνας και τα συστήματα οικιακών πολυμέσων (home multi-media) που συνήθως είναι συνδεδεμένα με τηλεοράσεις. Οι ιδιοκτήτες αυτών των συσκευών δεν γνώριζαν ότι οι συσκευές τους είχαν ενταχθεί στο κακόβουλο δίκτυο και είχαν «αξιοποιηθεί» από αυτό για την αποστολή των ανεπιθύμητων μηνυμάτων σε άλλους χρήστες και επιχειρήσεις - στόχους. Καμία συσκευή που είχαν παραβιάσει οι εισβολείς (hackers) δεν απέστειλε περισσότερα από δέκα τέτοια μηνύματα, ώστε να γίνει πιο δύσκολο το «μπλοκάρισμα» της κυβερνο-επίθεσης. Ο επικεφαλής ασφαλείας της Proofpoint προειδοποίησε ότι τέτοιες επιθέσεις θα είναι συχνότερες στο μέλλον, καθώς οι συσκευές ενός σπιτιού γίνονται ολοένα πιο «έξυπνες» και διασυνδέονται στο διαδίκτυο[22].

Ένα εξαιρετικά σοβαρό περιστατικό που καταδεικνύει τις τραγικές συνέπειες από τις αδυναμίες της ασφάλειας του κυβερνοχώρου αποτελεί η περίπτωση του Πανεπιστημιακού Νοσοκομείου του Ντίσελντροφ[23]. Έπειτα από επίθεση εισβολέων - hackers το Σεπτέμβριο του 2020, τα ηλεκτρονικά συστήματα του νοσοκομείου νέκρωσαν, με αποτέλεσμα να τεθεί το νοσοκομείο εκτός λειτουργίας και να μην μπορεί να εξυπηρετήσει κανένα περιστατικό. Μια γυναίκα ασθενής που εκείνο το βράδυ διακομίστηκε στα επείγοντα και έπρεπε να εγχειριστεί αμέσως, μεταφέρθηκε στο πλησιέστερο νοσοκομείο, λόγω αδυναμίας να της παράσχουν οποιαδήποτε ιατρική βοήθεια. Παρά το σύντομο της διαδρομής, η ασθενής κατέληξε. Το περιστατικό αυτό αποτελεί πιθανότητα το πρώτο, σε παγκόσμια κλίμακα, κρούσμα κυβερνοεπίθεσης, που είχε παράπλευρη απώλεια. Αυτό που έκανε πιο τραγική τη συγκεκριμένη επίθεση ήταν το γεγονός ότι οι δράστες αποκάλυψαν ότι ο στόχος της επίθεσής τους ήταν το πανεπιστήμιο και όχι το νοσοκομείο και παρότι παρείχαν

22 «Ψυγείο…χάκερ συμμετείχε σε κυβερνοεπίθεση», (2014), διαθέσιμο σε https://www.inewsgr.com/257/psygeiochaker-symmeteiche-se-kyvernoepithesi.htm .

23 «Γερμανία: Θρίλερ στον κυβερνοχώρο με έναν νεκρό», (2020), διαθέσιμο σε https://www.kathimerini.gr/world/561084721/germania-thriler-ston-kyvernochoro-me-enan-nekro .

άμεσα τους κωδικούς για το ξεκλείδωμα των διακομιστών του νοσοκομείου, ήταν ήδη αργά για την ασθενή.

2 Το Διαδίκτυο των Πραγμάτων (IoT) σε σχέση με την προστασία των δεδομένων και την Κυβερνοασφάλεια.

Οι Ηνωμένες Πολιτείες της Αμερικής ως πρωτοπόροι των τεχνολογιών του διαδικτύου, εστίασαν σταδιακά στους κινδύνους των τεχνολογιών του διαδικτύου των πραγμάτων, συμπεριλαμβανομένων και των τρόπων με τους οποίους οι τεχνολογίες αυτές θα μπορούσαν να χρησιμοποιηθούν και ως μέσα εισβολής πολιτικά υποκινούμενων ομάδων. Συγκεκριμένα, καλλιεργήθηκε μία εθελοντική προσέγγιση, τόσο για την κυβερνοασφάλεια, όσο και για την ιδιωτικότητα των δεδομένων, σε αντίθεση με την ολοένα και περισσότερο υποχρεωτική και περιεκτική προσέγγιση που καλλιεργείται στην Ευρωπαϊκή Ένωση, κυρίως ως προς την προστασία των προσωπικών δεδομένων, μέσα από το Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (GDPR)[24], ο οποίος τέθηκε σε εφαρμογή το Μάιο του 2018[25]. Για τους πολίτες των χωρών της Ευρωπαϊκής Ένωσης οι διαδικτυακές αναζητήσεις προστατεύονται ως προσωπικά δεδομένα, ενώ οι πολίτες των Ηνωμένων Πολιτειών δεν απολαμβάνουν αντίστοιχης προστασίας[26]. Επίσης, στις ΗΠΑ, οι διατάξεις για την κυβερνοασφάλεια, ειδικά στο πλαίσιο του διαδικτύου των πραγμάτων, περιλαμβάνουν ένα συνονθύλευμα από ομοσπονδιακούς και

24 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).

25 Meghna Chakrabarti, «Overhauling Digital Privacy in the EU», (2018), διαθέσιμο σε http://www.wbur.org/onpoint/2018/04/24/eu-gdpr-facebook-digital-privacy . Βλ επίσης Scott Shackelford και Scott O. Bradner, «Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything», *Hastings Law Journal*, Kelley School of Business Research Paper No. 18-60, (2021).

26 Βλ. σχετικά Γεώργιος Γιαννόπουλος κλπ, «Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR). Νομική Διάσταση και Πρακτική Εφαρμογή», επιμ. Λεωνίδας Κοτσαλής - Κωνσταντίνος Μενουδάκος, έκδοση 2η, Νομική Βιβλιοθήκη, 2021.

πολιτειακούς νόμους και πολιτικές, οι οποίοι, λόγω του εύρους και της πολυπλοκότητάς τους, σε γενικές γραμμές δεν μπορούν να μετριάσουν τα ζητήματα ασφαλείας που προκύπτουν[27]. Οι ελλείψεις σε επίπεδο ρυθμίσεων παραμένουν, παρά τις φιλότιμες προσπάθειες φορέων όπως η Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission -FTC), η οποία κυρίως προβαίνει σε συστάσεις, οι οποίες δεν είναι υποχρεωτικές[28]. Οι συστάσεις αυτές είναι σύμφωνες τόσο με το Πλαίσιο Κυβερνοασφάλειας του 2014 του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology[29]), όσο και με το Πλαίσιο του διαδικτύου των Πραγμάτων του 2015 του ιδίου φορέα.

Σε αντίθεση με τα ανωτέρω, η Ευρωπαϊκή Ένωση είχε εξαρχής μία διακριτή, υποχρεωτική και πολύ πιο ολοκληρωμένη προσέγγιση τόσο ως προς την κυβερνοασφάλεια, όσο και την ιδιωτικότητα της πληροφορίας, σε σχέση με το καθεστώς που ακολουθείται στις ΗΠΑ[30]. Επίσης, η Ευρωπαϊκή Ένωση έδινε παραδοσιακά έμφαση σε θέματα που προέκυπταν αναφορικά με το διαδίκτυο των πραγμάτων. Συγκεκριμένα, το 2014 η Ευρωπαϊκή Επιτροπή χρηματοδότησε ένα πρόγραμμα με την ονομασία CIPHER, το οποίο είχε ως στόχο να πραγματοποιήσει μία «σε βάθος ανάλυση της πραγματικότητας στην ασφάλεια των ιδιωτικών

27 «FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks», (2015), διαθέσιμο σε https://www.ftc.gov/newsevents/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

28 «Συνίσταται, για την προάσπιση της κυβερνοασφάλειας και των προσπαθειών ανάπτυξης των λογισμικών που αφορούν στους καταναλωτές, μία ολιστική προσέγγιση, η οποία ενσωματώνει μία στρατηγική ιδιωτικότητας από το σχεδιασμό (privacy by design) για την αντιμετώπιση ολόκληρου του κύκλου ζωής της περισυλλογής, χρήσης, πρόσβασης, αποθήκευσης των δεδομένων και τελικά την ασφαλή διαγραφή τους». Βλ. σχετικά «FTC Enters Internet of Things Arena With TRENDnet Proposed Settlement», (2013), διαθέσιμο σε http://www.infolawgroup.com/2013/09/articles/ftc/trendnet-settlement/.

29 Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας ιδρύθηκε το έτος 1901 και αποτελεί τομέα του Αμερικανικού Υπουργείου Εμπορίου. Πρόκειται για ένα από τα αρχαιότερα εθνικά εργαστήρια φυσικών επιστημών. Βλ. σχετικά https://www.nist.gov/about-nist.

30 Ιωάννης Ιγγλεζάκης, «Δίκαιο πληροφορικής», 4η έκδοση, εκδόσεις Σάκκουλα, Αθήνα - Θεσσαλονίκη (2021), Scott J. Shackelford, «Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations», *Seton Hall Journal of Diplomacy and International Relations,* in press (2019).

πληροφοριακών συστημάτων στην Ευρώπη»[31]. Ειδικότερα, το πρόγραμμα CIPHER περιελάμβανε μία απόπειρα να δημιουργηθεί ένας οδικός χάρτης με συστάσεις προς τους ιθύνοντες που θα περιελάμβαναν το διαδίκτυο των πραγμάτων. Περαιτέρω, η Ευρωπαϊκή Επιτροπή ίδρυσε τη Συμμαχία για τις Καινοτομίες του διαδικτύου των Πραγμάτων, η οποία επιφορτίστηκε με την αρμοδιότητα να αναπτύξει ένα πλαίσιο μεγάλης κλίμακας, το οποίο θα αντιμετωπίζει ζητήματα σχετικά με το διαδίκτυο των Πραγμάτων[32]. Η ομάδα αυτή είχε διεθνείς συνεργασίες και δέχθηκε αντιπροσωπείες από όλο τον κόσμο με στόχο τη συζήτηση της διακυβέρνησης του διαδικτύου των πραγμάτων, ενισχύοντας τη θέση της Ευρωπαϊκής Ένωσης ως βασικού κόμβου για την κυβερνοασφάλεια και τη διακυβέρνηση της ιδιωτικότητας. Τέλος, το 2015 η Ευρωπαϊκή Επιτροπή παρουσίασε το πρόγραμμα Horizon 2020, το οποίο περιελάμβανε στόχους για τις «έξυπνες» πόλεις και την ανάπτυξη του διαδικτύου των πραγμάτων[33]. Με λίγα λόγια, η Ευρωπαϊκή Ένωση αγκάλιασε το «Διαδίκτυο των πάντων», του οποίου συσκευές που μπορούν να φορεθούν (wearables) αποτελούνται από ολοκληρωμένες τεχνολογίες – κλειδιά (όπως τα νανο–ηλεκτρονικά ή τα οργανικά ηλεκτρονικά) κι «έξυπνα» συστήματα, τα οποία παρέχουν νέες λειτουργίες σε μία σειρά από καταναλωτικά προϊόντα, όπως ρούχα, υφάσματα, ρολόγια και άλλες συσκευές που μπορούν να φορεθούν στο ανθρώπινο σώμα[34].

Μία βασική πτυχή του πώς διαμορφώνεται η διακυβέρνηση του διαδικτύου των πραγμάτων στην Ευρωπαϊκή Ένωση είναι ο Γενικός Κανονισμός Προστασίας για τα Προσωπικά Δεδομένα[35]. Μολονότι το μεγαλύτερο τμήμα του ΓΚΠΔ έχει εστιάσει

31 «A Cyber Security Framework For Europe, European Commission», (2014). διαθέσιμο σε http://cordis.europa.eu/news/rcn/121360_en.html.

32 Alliance for Internet of Things Innovation, Working Group 3 Report, IoT LSP Standard Framework Concepts, Release 2.0, AIOTI WG03 – loT Standardisation (2015). Βλ. σχετικά https://aioti.eu/aioti-wg03-reports-on-iot-standards/

33 Horizon 2020 Work Programme, European Commission (2015), διαθέσιμο σε http://ec.europa.eu/digitalagenda/sites/digital-agenda/files/discussions/h2020-wp1617-focus_en.pdf.

34 Scott Shackelford και Scott O. Bradner, «Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything», *Hastings Law Journal*, Kelley School of Business Research Paper No. 18-60, (2021).

35 Ιωάννης Ιγγλεζάκης, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019)», Interactive Books, 2020. Βλ. επίσης Λίλιαν Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων», Σάκκουλας, 2017, Ευγενία

στις διατάξεις του σχετικά με την προστασία της ιδιωτικότητας και τα πιθανά μεγάλα πρόστιμα που μπορούν να επιβληθούν στις περιπτώσεις που παραβιάζονται οι κανόνες προστασίας των δεδομένων, ένας σημαντικός στόχος του ΓΚΠΔ είναι να κατακρημνίσει, στο βαθμό που αυτό είναι εφικτό, τα εναπομείναντα νομοθετικά εμπόδια μεταξύ των κρατών – μελών της Ευρωπαϊκής Ένωσης και να προχωρήσει προς μία κοινή Ευρωπαϊκή αγορά[36]. Σε αυτή τη βάση, ο ΓΚΠΔ αποτελεί ένα αναλυτικό ρυθμιστικό καθεστώς με ευρύ φάσμα απαιτήσεων ως προς τη διασφάλιση της φορητότητας των δεδομένων και τη συγκατάθεση[37]. Όσο πρωτοποριακές και αν υπήρξαν αυτές οι ρυθμίσεις, δεν είχαν υπόψη τους το διαδίκτυο των πραγμάτων και αυτό προκύπτει και από τη διαπίστωση του ENISA (European Union Agency for Network and Information Security)[38] το 2017, σύμφωνα με την οποία «δεν υπήρξαν νομικές κατευθυντήριες γραμμές για τις συσκευές του διαδικτύου των πραγμάτων και των υπηρεσιών εμπιστοσύνης (service trust), αλλά ούτε κι ένα ελάχιστο επίπεδο που να προσδιορίζει την ασφάλεια και την ιδιωτικότητα των διασυνδεδεμένων και «έξυπνων» συσκευών»[39].

Ακόμα κι εάν ο Γενικός Κανονισμός αποτελεί μία ριζική αλλαγή με σημαντικά πλεονεκτήματα για τα υποκείμενα των δεδομένων, αποδείχθηκε και σημαντική πρόκληση. Οι οργανισμοί χρειάζεται να προχωρήσουν σε χρονοβόρες και σύνθετες τροποποιήσεις για τις διαδικασίες επεξεργασίας των προσωπικών δεδομένων, προκειμένου να είναι συμβατοί με τον Κανονισμό. Οι πολίτες, ως υποκείμενα δεδομένων αποκτούν νέα δικαιώματα, για τα οποία πρωτίστως θα πρέπει να

Αλεξανδροπούλου – Αιγυπτιάδου, «Προσωπικά Δεδομένα», Νομική Βιβλιοθήκη, 2016 και Φερενίκη Παναγοπούλου - Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ», Σάκκουλας, 2017.

36 European Commission, «Digital Single Market – Bringing down barriers to unlock online opportunities», (2017), διαθέσιμο σε https://www.europeansources.info/record/digital-single-market-bringing-down-barriers-to-unlock-online-opportunities/.

37 «Top Ten Operational Impacts of the GDPR», (2018), διαθέσιμο σε https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/.

38 Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών ιδρύθηκε το 2004 και στόχος τους είναι η ασφάλεια των συστημάτων δικτύων και των πληροφοριών των κρατών – μελών της Ευρωπαϊκής Ένωσης. Βλ. σχετικά https://www.enisa.europa.eu/ .

39 Scott Gordon, «Will we Get a GDPR for the IOT?», (2018), διαθέσιμο σε https://www.scmagazineuk.com/will-we-get-a-gdpr-for-the-iot/article/758037/.

ενημερωθούν και να τα κατανοήσουν. Τέλος, και ο ρόλος των αρχών προστασίας μεταβάλλεται, όπως επίσης και οι απαιτήσεις τους προς τους οργανισμούς. Η συμμόρφωση προς το Γενικό Κανονισμό, αφενός μεν αποτελεί πρόκληση για τα σχετιζόμενα ενδιαφερόμενα μέρη και για το λόγο αυτό προέκυψαν διάφορα ερευνητικά προγράμματα, όπως το ευρωπαϊκό έργο DEFeND (Data govErnance For supportiNg gDpr), του οποίου στόχος είναι η δημιουργία αυτής της πλατφόρμας[40]. Για την επιτυχία του έργου αυτού απαραίτητες προϋποθέσεις είναι η ικανοποίηση των νομικών απαιτήσεων και αυτών που αφορούν στην ιδιωτικότητα, η αποτελεσματική στήριξη των οργανισμών ως προς την συμμόρφωσή τους με το Γενικό Κανονισμό και η παροχή των λειτουργιών που απαιτούν οι υπεύθυνοι επεξεργασίας των δεδομένων προς υποστήριξη της συμμόρφωσης με το Γενικό Κανονισμό. Περαιτέρω, πρέπει να πληρούνται οι κατάλληλες προδιαγραφές, ώστε να διασφαλιστεί ότι οι χρήστες του θα αγκαλιάσουν και θα χρησιμοποιήσουν την πλατφόρμα[41].

Παράλληλα, η Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή εξέδωσε το Σεπτέμβριο του 2018 Γνωμοδότηση σχετικά με την εμπιστοσύνη, την ιδιωτικότητα και την ασφάλεια των καταναλωτών και των επιχειρήσεων στο διαδίκτυο των πραγμάτων[42]. Σύμφωνα με τη Γνωμοδότηση αυτή, «οι καταναλωτές έχουν εξοικειωθεί περισσότερο με την άσκηση ελέγχου επί των προσωπικών τους δεδομένων και των ιδιωτικών τους προτιμήσεων βάσει του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ). Ο χρήστης μιας συσκευής πρέπει να ελέγχει τον τρόπο με τον οποίο γίνεται χρήση των δεδομένων που παράγει και το ποιος έχει

40 Πρόκειται για μία διεθνή συνεργασία που θα έχει ως αποτέλεσμα τη δημιουργία μίας πλατφόρμας που θα ενισχύσει τους οργανισμούς διαφορετικών τομέων στην πρόσβαση και τη συμμόρφωση με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR). Βλ. σχετικά https://www.defendproject.eu/ .

41 Aggeliki Tsohou, Manos Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni και Beatriz Gallego-Nicasio Crespo, «Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform», *Information & Computer Security*, Emerald Insight (υπό έκδοση), 2020.

42 Βλ. σχετικά «Trust, privacy and consumer security in the Internet of Things (IoT) (own-initiative opinion)», OJ C 440, (2018), διαθέσιμο σε https://www.eesc.europa.eu/el/node/59507?fbclid=IwAR28bSm9c9gZzskz_Q_F11CTKsXXhDsSeHOEWnBcZ_6wJNWHis6A8lnqdRM.

τη δυνατότητα πρόσβασης σε αυτά, λαμβανομένου υπόψη ότι η ποικιλία των δεδομένων, καθώς και η συγκέντρωση και η σύνδεσή τους με άλλα δεδομένα, συνεπάγονται σοβαρό κίνδυνο για την ιδιωτικότητα στο οικοσύστημα του ΔτΠ».[43]. Μέσα σε αυτό το πλαίσιο ο Γενικός Κανονισμός τέθηκε σε εφαρμογή το Μάιο του 2018 και οδήγησε στην επανεκτίμηση των κινδύνων που απορρέουν από την επεξεργασία προσωπικών δεδομένων, με βασικό ζητούμενο την ασφάλεια της επεξεργασίας αυτής[44]. Για το λόγο αυτό, γίνονται προσπάθειες εξεύρεσης αντικειμενικών κριτηρίων για το επίπεδο ασφάλειας των προϊόντων, υπηρεσιών κι επεξεργασίας που στηρίζονται στην Τεχνολογία της Πληροφορίας και των Επικοινωνιών (ICT[45]), κριτήρια τα οποία θα δικαιολογήσουν τη χρήση της τεχνολογίας σε περίπτωση σφάλματος. Η ανασφάλεια αυτή υπήρξε ένα από τα ζητήματα που η Ευρωπαϊκή Ένωση προσπάθησε να επιλύσει με τον Κανονισμό για την Κυβερνοασφάλεια[46], ο οποίος τέθηκε σε εφαρμογή την 27η Ιουνίου 2019. Ο Κανονισμός δημιουργεί ένα σχέδιο πιστοποίησης για την Κυβερνοασφάλεια σε όλη την Ευρωπαϊκή Ένωση, στον τομέα της τεχνολογίας των πληροφοριών και των επικοινωνιών. Περαιτέρω, ο Κανονισμός αυτός ανανεώνει και ενισχύει την ENISA, την Ευρωπαϊκή Υπηρεσία για την Κυβεροασφάλεια, καθορίζοντας τον ειδικό ρόλο της και τις αρμοδιότητές της.

43 Βλ. σχετικά παράρτημα Α.

44 Maarten Stassen, «The EU Cybersecurity Act: Addressing the Risks of a Connected Europe», (2019), διαθέσιμο σε https://www.retailconsumerproductslaw.com/2019/08/the-eu-cybersecurity-act-addressing-the-risks-of-a-connected-europe/.

45 Πρόκειται για διευρυμένο όρο της έννοιας «Τεχνολογία της Πληροφορίας» (IT) που τονίζει το ρόλο των ενοποιημένων επικοινωνιών και την ενσωμάτωση των τηλεπικοινωνιών (τηλεφωνικές γραμμές και ασύρματα σήματα) με τους υπολογιστές, όπως επίσης και με τα απαραίτητα εταιρικά λογισμικά, τα μεσαία λογισμικά, την αποθήκευση και τα οπτικοκουστικά συστήματα, τα οποία επιτρέπουν στους χρήστες να έχουν πρόσβαση, να αποθηκεύουν, να μεταφέρουν και να διαχειρίζονται την πληροφορία. Βλ. σχετικά Kirsten Slyter, «What Is Information Technology? A Beginner's Guide to the World of IT», (2019), διαθέσιμο σε https://www.rasmussen.edu/degrees/technology/blog/what-is-information-technology

46 Κανονισμός (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του Κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια).

Όσο λοιπόν, ο Γενικός Κανονισμός για την Προστασία των Δεδομένων εστιάζει στην «Προστασία των Δεδομένων ήδη από το σχεδιασμό» (Data Protection by Design[47]), όπου συναντώνται συστατικά τόσο σχετικά με την ιδιωτικότητα, όσο και με την ασφάλεια, ο Ευρωπαϊκός Κανονισμός για την Κυβερνοασφάλεια εστιάζει στην «Ασφάλεια ήδη εξ ορισμού» (Security by Design[48]), κάτι που απαντάται κυρίως στις ΗΠΑ. Εκεί οι κανόνες για τη διαχείριση του διαδικτύου των Πραγμάτων σε σχέση με τα ζητήματα της κυβερνοασφάλειας και της ιδιωτικότητας εκδόθηκαν από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology – NIST[49]). Οι σχεδιαστές και οι κατασκευαστές των τεχνολογιών των πληροφοριών και των επικοινωνιών έχουν πλέον την ευκαιρία να επωφεληθούν από μία ευρεία ευρωπαϊκή πιστοποίηση ασφαλείας στον κυβερνοχώρο, η οποία θα αυξήσει σημαντικά την εμπιστοσύνη των πολιτών προς τα προϊόντα, τις υπηρεσίες

47 Οι εταιρείες/οργανισμοί ενθαρρύνονται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα, στα αρχικά στάδια του σχεδιασμού των πράξεων επεξεργασίας, με τέτοιον τρόπο ώστε να διασφαλίζονται οι αρχές ιδιωτικού απορρήτου και προστασίας δεδομένων ήδη από την αρχή. Αντίθετα, σύμφωνα με τον όρο «data protection by default» - προστασία των δεδομένων ήδη εξ ορισμού, οι εταιρείες/οργανισμοί θα πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής (π.χ. μόνο τα απαραίτητα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία, σύντομη περίοδος αποθήκευσης, περιορισμένη προσβασιμότητα) έτσι ώστε εξ ορισμού τα δεδομένα προσωπικού χαρακτήρα να μην είναι προσβάσιμα από αόριστο αριθμό φυσικών προσώπων. Βλ. σχετικά https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_el και https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#:~:text=Data%20protection%20by%20design%20is%20ultimately%20an%20approach%20that%20ensures,and%20then%20throughout%20the%20lifecycle .Βλ. επίσης, Γεώργιος Γιαννόπουλος κλπ, «Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR). Νομική Διάσταση και Πρακτική Εφαρμογή», επιμ. Λεωνίδας Κοτσαλής - Κωνσταντίνος Μενουδάκος , έκδοση 2η, Νομική Βιβλιοθήκη, (2021).

48 Οι επιχειρήσεις, οι οργανισμοί και ο δημόσιος τομέας θα πρέπει να διαμορφώνουν τα προϊόντα ΤΠΕ, τις υπηρεσίες ΤΠΕ ή τις διαδικασίες ΤΠΕ που σχεδιάζουν κατά τρόπο που να διασφαλίζει υψηλότερο επίπεδο ασφάλειας το οποίο επιτρέπει στον πρώτο χρήστη να λαμβάνει μια προεπιλεγμένη ρύθμιση με τις πλέον ασφαλείς παραμέτρους («ασφάλεια εξ ορισμού»), μειώνοντας κατ' αυτόν τον τρόπο την επιβάρυνση των χρηστών με την ανάγκη κατάλληλης ρύθμισης προϊόντος ΤΠΕ, υπηρεσίας ΤΠΕ ή διαδικασίας ΤΠΕ. Βλ. σχετικά Κανονισμό (ΕΕ) 2019/881 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 17ης Απριλίου 2019 σχετικά με τον ENISA («Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια») και με την πιστοποίηση της κυβερνοασφάλειας στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών και για την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013 (πράξη για την κυβερνοασφάλεια), διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32019R0881&from=EL .

49 Υπηρεσία του Υπουργείου Εμπορίου των ΗΠΑ που αναπτύσσει και προωθεί τις μετρήσεις, τα πρότυπα και την τεχνολογία. Βλ. σχετικά https://www.nist.gov/ .

και τις διαδικασίες τους. Η πιστοποίηση είναι προαιρετική, εκτός εάν προβλέπεται κάτι διαφορετικό από την εσωτερική νομοθεσία του Κράτους – μέλους. Ορίζεται ρητά ότι η Ευρωπαϊκή Επιτροπή πρέπει να εξετάζει, τουλάχιστον κάθε δύο χρόνια, εάν πρέπει να καταστεί υποχρεωτική κάποια συγκεκριμένη διαδικασια πιστοποίησης – ο πρώτος έλεγχος οφείλει να έχει πραγματοποιηθεί μέχρι την 31 Δεκεμβρίου 2023.

Ο Ευρωπαϊκός Κανονισμός για την Κυβερνοασφάλεια περιέχει τρία επίπεδα ασφαλείας: το βασικό, το ουσιώδες και το υψηλό[50]. Τα επίπεδα αυτά αντικατοπτρίζουν τον κίνδυνο που συνδέεται με την επιδιωκόμενη χρήση των τομέων των τεχνολογιών πληροφοριών κι επικοινωνίας, αναφορικά με την πιθανότητα και τον αντίκτυπο ενός συμβάντος. Κάθε επίπεδο ασφαλείας καθορίζει τις λειτουργίες ασφαλείας που πρέπει να αξιολογηθούν, καθώς και το βαθμό αυστηρότητας και βάθους της αξιολόγησης. Οι κατασκευαστές και οι πάροχοι που παρουσιάζουν χαμηλό κίνδυνο, ο οποίος κατατάσσεται στο βασικό επίπεδο ασφαλείας, μπορούν να εκδώσουν μία δήλωση συμμόρφωσης βασισμένη σε αυτοαξιολόγηση. Όπου δεν υπάρχει τέτοιου είδους αυτοαξιολόγηση ή τα επίπεδα ασφαλείας είναι ουσιώδη ή υψηλά, η διαδικασία πιστοποίησης πρέπει να πραγματοποιηθεί από ανεξάρτητο τρίτο μέρος. Το πλαίσιο της πιστοποίησης θα καθορίζει εάν το τρίτο μέρος θα μπορεί να είναι ιδιώτης ή δημόσιος οργανισμός ή εθνική αρχή πιστοποίησης της κυβερνοασφάλειας. Μολονότι η ανωτέρω πιστοποίηση δεν θα καθιστά τα προϊόντα ή τις υπηρεσίες ή τις διαδικασίες απόλυτα ασφαλή, η αξιολόγηση της συμμόρφωσης θα δηλώνει ότι αυτά έχουν ελεγχθεί και ότι συμφωνούν με συγκεκριμένες απαιτήσεις, όπως τεχνικά χαρακτηριστικά. Επίσης, δεδομένου ότι οι κυβερνοεπιθέσεις εξακολουθούν να υφίστανται και οι κίνδυνοι να υπάρχουν, οι πιστοποιήσεις θα εκδίδονται για περιορισμένες χρονικές περιόδους[51].

50 Maarten Stassen, «The EU Cybersecurity Act: Addressing the Risks of a Connected Europe», (2019), διαθέσιμο σε https://www.retailconsumerproductslaw.com/2019/08/the-eu-cybersecurity-act-addressing-the-risks-of-a-connected-europe/.

51 Αθανάσιος Ν. Σαμαράς, Εμμανουήλ Τάκας και Βάλια Καϊμάκη, «Από την Κυβερνοασφάλεια στα Fake News. Μέσα, Μηνύματα, Στρατηγικές», Βιβλίο Συνόψεων 7ου Επιστημονικού Συνεδρίου, Εργαστήριο Στρατηγικής Επικοινωνίας και Μέσων Ενημέρωσης, 2018.

Για να ισχυροποιηθεί η σχετική νομοθεσία πρέπει τα Ευρωπαϊκά Κράτη – μέλη να επιβάλλουν πρόστιμα για την παραβίαση των ευρωπαϊκών σχεδίων πιστοποίησης της Κυβερνοασφάλειας από τα μέσα του 2021. Τα πρόστιμα αυτά πρέπει να είναι αποτελεσματικά, αποτρεπτικά και αναλογικά. Αυτό που μένει είναι να αποδειχθεί εάν η αγορά του τομέα τεχνολογιών της πληροφορίας και των επικοινωνιών θα αντιδράσει θετικά σε αυτή την πρωτοβουλία, η οποία στοχεύει στη διασφάλιση και την αύξηση της εμπιστοσύνης στα προϊόντα και τις υπηρεσίες της.

3 Εφαρμογές του διαδικτύου των Πραγμάτων

Στο μακρινό παρελθόν, η άφιξη του σιδηρόδρομου και της ατμομηχανής σήμανε την υιοθέτηση αυστηρών κανόνων ευθύνης σε πολλές ευρωπαϊκές νομοθεσίες. Η ίδια ανάγκη νομοθετικής πρόβλεψης παρουσιάζεται και στη σημερινή εποχή, στον υπέρτατο βαθμό, με την εξέλιξη των αυτόνομων τεχνολογικών συστημάτων[52] που αναπτύσσονται μέσω της τεχνητής νοημοσύνης[53]. Η ύπαρξη αυτών των καινοτομιών θα θέσει υπό αμφισβήτηση την ευθύνη των κατασκευαστών, προμηθευτών εξαρτημάτων, ιδιοκτητών και χειριστών τέτοιου είδους μηχανημάτων. Η τεχνολογία

52 «Αυτόνομο σύστημα» (AS) είναι η μονάδα της πολιτικής δρομολογητή (είτε ένα μόνο δίκτυο είτε μια ομάδα δικτύων) που ελέγχεται από έναν κοινό διαχειριστή δικτύου (ή μια ομάδα διαχειριστών) για λογαριασμό μιας ενιαίας διοικητικής οντότητας (όπως το πανεπιστήμιο, μία επιχείρηση ή ένα τμήμα επιχείρησης). Ένα αυτόνομο σύστημα αναφέρεται μερικές φορές και ως τομέας δρομολόγησης. Στο αυτόνομο σύστημα έχει εκχωρηθεί παγκοσμίως ένας μοναδικός αριθμός, αποκαλούμενος και ως αυτόνομος αριθμός συστήματος (ASN). Τα δίκτυα εντός του αυτόνομου συστήματος κοινοποιούν πληροφορίες δρομολόγησης μεταξύ τους χρησιμοποιώντας ένα πρωτόκολλο εσωτερικής πύλης (Interior Gateway Protocol –IGP). Ένα αυτόνομο σύστημα μοιράζεται πληροφορίες δρομολόγησης με άλλα αυτόνομα συστήματα χρησιμοποιώντας το «Border Gateway Protocol» (BGP). Στο μέλλον, το BGP αναμένεται να αντικατασταθεί από το πρωτόκολλο δρομολόγησης μεταξύ τομέων OSI (IDRP). Βλ. σχετικά https://searchnetworking.techtarget.com.

53 «Τεχνητή νοημοσύνη» (AI) είναι ο τομέας της επιστήμης των υπολογιστών στον οποίο δίνεται έμφαση στη δημιουργία έξυπνων μηχανών, οι οποίες λειτουργούν και αντιδρούν όπως οι άνθρωποι. Κάποιες από τις λειτουργίες τους αφορούν την αναγνώριση του λόγου, την εκμάθηση, τον προγραμματισμό (planning) και την επίλυση προβλημάτων. Βλ. σχετικά Λεωνίδας Κανέλλος, «Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο και στη δικαστική πρακτική», Νομική Βιβλιοθήκη, Αθήνα, (2021). Βλ. επίσης «Έρευνα: Η τεχνητή νοημοσύνη και το «Διαδίκτυο των Πραγμάτων» υιοθετείται όλο και περισσότερο οι επιχειρήσεις παγκοσμίως», (2020), διαθέσιμο σε https://www.fortunegreece.com/article/erevna-i-techniti-noimosini-ke-to-diadiktio-ton-pragmaton-iiothetite-olo-ke-perissotero-i-epichirisis-pagkosmios/ .

αυτή διαφέρει σημαντικά από αυτή του διαδικτύου των πραγμάτων (IoT-devices) γιατί πολλά διασυνδεδεμένα προϊόντα είναι διαθέσιμα ήδη στην αγορά, αλλά λειτουργούν με λογισμικό το οποίο δεν επιτρέπει αυτόνομες ενέργειες από την ίδια τη μηχανή[54].

Οι εφαρμογές της τεχνολογίας του διαδικτύου των πραγμάτων συναντώνται πλέον σε πολλούς τομείς της καθημερινότητάς μας. Για παράδειγμα, στον τομέα της ένδυσης ρούχα και αξεσουάρ μπορούν πλέον να κάνουν πολύ περισσότερα από τον αρχικό στόχο παραγωγής τους, ήτοι την κάλυψη της ανάγκης ένδυσης[55]. Ολοένα και περισσότερες εταιρείες κατασκευάζουν «έξυπνα» ρούχα, τα οποία έχουν ενσωματωμένους αισθητήρες τελευταίας τεχνολογίας και έχουν τη δυνατότητα προστασίας της ανθρώπινης ζωής, όπως το «MIMO», φορμάκι για βρέφη που αποτελεί ένα από τα πιο φιλόδοξα προϊόντα, σχεδιασμένο να προειδοποιεί για τον κίνδυνο αιφνιδίου θανάτου του μωρού[56] ή ο αθλητικός στηθόδεσμος που προειδοποιεί για καρκίνο του μαστού[57]. Το πρόγραμμα «Easy - IMP» αφορά στην

54 Βλ. γενικά Gerhard Wagner, «Robot Liability», Humboldt University School of Law; University of Chicago Law School (2018).

55 Τον Οκτώβριο του 2020 η εταιρία Samsonite έκανε γνωστό στο ευρύ κοινό το προϊόν της «Konnect-i backpack», μία έξυπνη τσάντα ώμου που συνδέεται με το κινητό του χρήστη, μέσω της τεχνολογίας Jacquard της Google. Στόχος του προϊόντος αυτού είναι η αλληλεπίδραση του κατόχου της τσάντας με το κινητό του, χωρίς να χρειαστεί να έρθει σε επαφή με αυτό και απευθύνεται σε άτομα πολυάσχολα, που βρίσκονται διαρκώς σε κίνηση ή χρησιμοποιούν τα μέσα μαζικής μεταφοράς. Η τσάντα αυτή αποτελείται από ένα ειδικό έξυπνο αξεσουάρ που επικοινωνεί απευθείας με το έξυπνο τηλέφωνο. Αντίστοιχος είναι και ο χειρισμός του κινητού από τον χρήστη, καθώς οι ιμάντες της τσάντας έχουν μία ειδική επιφάνεια που είναι ευαίσθητη στην αφή και επιτρέπουν την εκτέλεση λειτουργιών, χωρίς την επαφή με το τηλέφωνο. Ο χρήστης μπορεί να προγραμματίσει τις εντολές που θα δίνονται από τους ιμάντες, μέσω μίας συνοδευτικής εφαρμογής. Το ειδικό αξεσουάρ της Google επιτρέπει και την ειδοποίηση του χρήστη με δόνηση και οπτικές ενδείξεις ανάλογα με το εάν πρόκειται για κλήσεις, email κ.ο.κ. «Η Samsonite λανσάρει μία έξυπνη τσάντα ώμου που συνδέεται με το smartphone», (2020), διαθέσιμο σε https://m.naftemporiki.gr/story/1650134/h-samsonite-lansarei-mia-eksupni-tsanta-omou-pou-sundeetai-me-to-smartphone .

56 Αυτό το οργανικό ρούχο διαθέτει έναν αισθητήρα ο οποίος, μεταξύ άλλων, μετρά την αναπνοή και τη θερμοκρασία του μωρού και δίνει πληροφορίες για τη στάση του σώματός του. Με αυτόν τον τρόπο προειδοποιεί τους γονείς του έγκαιρα, για πιθανά συμπτώματα του συνδρόμου αιφνιδίου θανάτου, μέσω της ασύρματης σύνδεσης στο κινητό τους τηλέφωνο. Danny Chrichton, «With Mimo, MIT Alums Are Disrupting the Baby Nursery, Onesie at a Time», https://techcrunch.com/2015/01/27/withmimo-mit-alums-are-disrupting-the-baby-nursery-onesie-at-a-time, σε Hillary Brill και Scott Jones, «Little Things and Big Challenges: Information Privacy and the Internet of Things», *American University Law Review*, Vol. 66 (2017): 1183 – 1184.

57 Αν και κάποιοι ερευνητές έχουν εκφράσει την ανησυχία τους για την ακρίβεια και τη χρησιμότητα του συγκεκριμένου εσωρούχου, ωστόσο ο διευθύνων σύμβουλος της κατασκευάστριας εταιρείας διευκρινίζει

ανάπτυξη ρούχων τα οποία θα μετρούν διάφορες μεταβλητές που σχετίζονται με τον οργανισμό ενός ανθρώπου και θα αποθηκεύουν όλα τα δεδομένα σε κάποιο νέφος (cloud), για να είναι εύκολα προσβάσιμα από εφαρμογές «έξυπνων» κινητών τηλεφώνων. Τα συγκεκριμένα ρούχα θα αφορούν σε διάφορους τομείς, από την ιατρική μέχρι το εμπόριο και τον αθλητισμό. Ήδη εδώ και μερικά χρόνια η Ευρωπαϊκή Ένωση χρηματοδοτεί επιστήμονες για την ανάπτυξη ρούχων με ενσωματωμένους αισθητήρες που θα μετρούν την καρδιακή δραστηριότητα και την αναπνοή ενός ασθενούς, με στόχο την εξ αποστάσεως ιατρική παρακολούθηση[58].

Πρωτοποριακή εφαρμογή αποτελεί ο «έξυπνος» καθρέφτης αυτοκινήτου, ο οποίος κατασκευάστηκε από την εταιρία παραγωγής αυτοκινήτων NISSAN και βραβεύτηκε στο Παγκόσμιο Συμπόσιο Οδικής Ασφάλειας με το βραβείο συνεισφοράς στην οδική ασφάλεια. Το σκεπτικό της βράβευσης έγκειται στο ότι η τεχνολογία αυτή συμβάλει στην επίτευξη ασφαλέστερων οδικών μετακινήσεων. Συγκεκριμένα, ο καθρέφτης αυτός έχει οθόνη τεχνολογίας LCD[59], η οποία του παρέχει πλήρη ορατότητα στο πίσω μέρος του οχήματος, ανεξαρτήτως συνθηκών. Η ψηφιακή εικόνα βελτιώνει την ορατότητα στο σκοτάδι, αλλά και σε συνθήκες βροχόπτωσης ή έντονης ηλιοφάνειας, με παράλληλη άμεση και εύκολη δυνατότητα εναλλαγής στο συμβατικό καθρέφτη[60].

Στον τομέα της υγείας, η εταιρία Google έκανε γνωστό ότι αναπτύσσει πρωτοποριακούς «έξυπνους» φακούς επαφής, που μετρούν το επίπεδο του σακχάρου στα δάκρυα των διαβητικών[61]. Περαιτέρω, οι φαρμακευτικές βιομηχανίες

ότι το εσώρουχο αυτό δεν υποκαθιστά τη μαστογραφία που πρέπει να κάνει μια γυναίκα σε ετήσια βάση, αλλά λειτουργεί συμπληρωματικά με αυτή. Βλ. σχετικά «Αυτό είναι το έξυπνο σουτιέν της Microsoft!», (2013), διαθέσιμο σε https://www.inewsgr.com/61/afto-einai-to-exypno-soutien-tis-Microsoft.htm.

58 «'Smart bra' to detect early-stage breast cancer», (2020), διαθέσιμο σε https://healthcare-in-europe.com/en/news/smart-bra-to-detect-early-stage-breast-cancer.html

59 Οι οθόνες αυτές αποτελούνται από δύο φύλλα υλικού που μπορεί να πολωθεί ηλεκτρικά με ένα ειδικό μείγμα υγρών κρυστάλλων ανάμεσα. Όταν περνάει ρεύμα από το όλο σύστημα, οι κρύσταλλοι παίρνουν συγκεκριμένες θέσεις, έτσι ώστε να επιτρέπει ή μη τη δίοδο του φωτός. Βλ. σχετικά https://www.ired.gr/blog/item/5435-led-or-lcd-tv-specs-explained.html .

60 Βλ. σχετικά http://www.secnews.gr .

61 Η συσκευή περιλαμβάνει ένα μικροσκοπικό ασύρματο δέκτη - τσιπ, μια κεραία και ένα εξίσου μικροσκοπικό αισθητήρα μέτρησης της γλυκόζης, που είναι ενσωματωμένος ανάμεσα στα δύο στρώματα του υλικού του φακού. Η αμερικανική εταιρία ανακοίνωσε ότι εργάζεται ώστε να προσθέσει στον έξυπνο φακό πολύ μικρά λαμπάκια τύπου LED, που θα ανάβουν και θα προειδοποιούν τον ασθενή σε

χρησιμοποιούν το διαδίκτυο των πραγμάτων με την εισαγωγή των «έξυπνων» προϊόντων που ενθαρρύνουν την ακριβή και αποτελεσματική χρήση των προϊόντων τους. Για παράδειγμα, στις περιπτώσεις της συνταγογράφησης φιαλιδίων, υπάρχει πλέον η δυνατότητα να συμπεριλαμβάνεται σε αυτά ένα ασύρματο κύκλωμα (chip), το οποίο θα αποστέλλει υπενθυμίσεις και θα συντονίζει την επανασυμπλήρωση του σκευάσματος, σε συνεργασία με το θεράποντα ιατρό[62]. Επιπλέον, «έξυπνα» δισκία είναι στο στάδιο του ελέγχου ώστε με την κατάποσή τους να μπορούν να ενημερώσουν τον ενδιαφερόμενο σχετικά με το είδος του φαρμάκου, την ώρα λήψης του και το κατά πόσο υπήρξε αποτελεσματικό[63]. Η τρίτη ηλικία είναι ακόμα ένας σημαντικός αποδέκτης των εφαρμογών του διαδικτύου των πραγμάτων, όταν διάφορες εταιρίες κινούνται προς την κατεύθυνση της παραγωγής συστήματος αισθητήρων, το οποίο θα «διαβάζει» απομακρυσμένα τον καρδιακό παλμό και το ρυθμό της αναπνοής, καθώς και το επίπεδο δραστηριότητας του ατόμου. Ο αισθητήρας θα επιτρέπει στην οικογένεια ή το θεράποντα ιατρό να καταγράφει τις ζωτικές ενδείξεις του ασθενή και να καλεί για ιατρική βοήθεια, εάν παραστεί ανάγκη[64]. Αυτές οι εφαρμογές παρέχουν τη δυνατότητα απομακρυσμένης πρόσβασης από τα μέλη της οικογένειας στη ρουτίνα της καθημερινότητας των οικείων τους, προσφέροντάς τους ηρεμία και ασφάλεια, δεδομένου ότι θα λάβουν ειδοποίηση στην περίπτωση που θα παρουσιαστεί σοβαρή διαταραχή στο καθημερινό πρόγραμμα του χρήστη[65].

περίπτωση που το σάκχαρο (γλυκόζη) περάσει ένα συγκεκριμένο όριο. Η νέα τεχνολογία κάνει τη σχετική μέτρηση στα δάκρυα αντί για το αίμα (όπως συνήθως συμβαίνει μέχρι σήμερα με τρύπημα του δάχτυλου). Οι έξυπνοι φακοί επιτρέπουν μάλιστα μια σχεδόν συνεχή μέτρηση της γλυκόζης ανά δευτερόλεπτο. Do Hee Keum, Su-Kyoung Kim, Jahyun Koo, Geon-Hui Lee1, Cheonhoo Jeon, Jee Won Mok, Beom Ho Mun, Keon Jae Lee, Ehsan Kamrani, Choun-Ki Joo, Sangbaie Shin, Jae-Yoon Sim, David Myung, Seok Hyun Yun, Zhenan Bao και Sei Kwang Hahn, «Wireless smart contact lens for diabetic diagnosis and therapy», *Science Advances,* Vol. 6/ 17 (2020) .

62 Nissa Simon, Technology «Puts You in Charge of Your Health», διαθέσιμο σε http://www.aarp.org/health/healthy-living/info-09-2013/health-gadgets.html .

63 Βλ. σχετικά «Proteus Digital Health Announces FDA Clearance of Ingestible Sensor», διαθέσιμο σε http://www.proteus.com/press-releases/proteusdigital-health-announces-fda-clearance-of-ingestible-sensor-2.

64 Brian Dolan, «FDA Clears Cardiac Monitor from Preventice, Mayo Clinic», διαθέσιμο σε http://www.mobihealthnews.com/18407/fdaclears-cardiac-monitor-from-preventice-mayo-clinic.

65 «An Internet of Things», διαθέσιμο σε https://www.postscapes.com/internet-ofthings-examples.

Στη βιομηχανία της γυμναστικής[66], οι πιο κοινά διαδεδομένες «έξυπνες» συσκευές είναι αυτές που μπορούν να φορεθούν (wearables). Οι συσκευές αυτές έχουν αισθητήρες που παρακολουθούν τον καρδιακό παλμό, τα βήματα ή τις συνήθειες κατά τη διάρκεια του ύπνου. Τα «έξυπνα» ρολόγια συγκεντρώνουν παρόμοια δεδομένα και με τη βοήθεια των τεχνολογιών WiFi και GPS, μπορεί κάποιος να ανακαλύψει τι απόσταση διένυσε και πού, πόσα βήματα πραγματοποίησε ή πόσα σκαλοπάτια ανέβηκε. Η πληροφορία που μεταφέρεται μέσω των διαδικτυακών συνδέσεων καταχωρείται με τέτοιο τρόπο, ώστε ο χρήστης να μπορεί να τη διατηρήσει ή να τη διαμοιραστεί.

Στον τομέα του «έξυπνου» σπιτιού, οι οικιακές συσκευές που διασυνδέονται μέσω του διαδικτύου των πραγμάτων περιλαμβάνουν συστήματα παρακολούθησης, «έξυπνες» εφαρμογές και διασυνδεδεμένη ψυχαγωγία. Σήμερα υπάρχει η δυνατότητα να ελέγχει κάποιος και να παρακολουθεί τόσο το εσωτερικό, όσο και το εξωτερικό της οικίας του, μέσω εφαρμογών και συσκευών ενσωματωμένων στο διαδίκτυο των πραγμάτων[67]. Τα οικιακά συστήματα ασφαλείας έχουν εξελιχθεί από εσωτερικούς ανιχνευτές κίνησης και αισθητήρες παραθύρων, σε συσκευές που περιλαμβάνουν, όχι μόνο μία βιντεοκάμερα, αλλά αισθητήρες για την ποιότητα του αέρα, την κίνηση, τον ήχο, τη θερμοκρασία και τους κραδασμούς. Καταγράφουν την κατανάλωση της ενέργειας και χρησιμοποιούν τη μηχανική μάθηση για να μεταφράσουν τις δραστηριότητες των συσκευών, ώστε να ειδοποιήσουν το χρήστη όταν συμβεί κάτι σοβαρό, όπως εάν ένας ηλεκτρικός φούρνος είναι σε λειτουργία περισσότερη ώρα από την προβλεπόμενη[68]. Η παραγωγή του «έξυπνου» καφέ, όπου μπορεί κάποιος να

66 Jessica Twentyman, «Wearable Devices Aim to Reduce Workplace Accidents», διαθέσιμο σε https://www.ft.com/content/d0bfea5c-f820-11e5-96db-fc683b5e52db . Βλ. επίσης Hillary Brill και Scott Jones, «Little Things And Big Challenges: Information Privacy And The Internet Of Things», *American University Law Review*, Vol. 66 (2017): 1183 – 1184.

67 Robert L. Mitchell, «The Internet of Things at Home: 14 Smart Products that Could Change Your Life», διαθέσιμο σε http://www.computerworld.com/article/2474727/consumerization-of-it/consumerization150407-the-internet-of-things.html.

68 Gillian Shaw, «Vancouver Company Helps You Create a Smart Home», διαθέσιμο σε http://www.vancouversun.com/touch/story.html?id=9206731.

ετοιμάσει το ρόφημά του μέσω του τηλεφώνου του[69] ή τα ψυγεία που επιτρέπουν στο χρήστη απομακρυσμένα να δει τι χρειάζεται από το σούπερ μάρκετ, είναι κάποιες από τις οικιακές «έξυπνες» εφαρμογές που συναντώνται πλέον στην καθημερινότητα των ατόμων[70]. Οικιακοί θερμοστάτες και ανιχνευτές καπνού συγκεντρώνουν πληροφορίες για τις οικιακές συνήθειες των χρηστών τους. Συγκεκριμένα ο «έξυπνος» θερμοστάτης χρησιμοποιεί τα δεδομένα θέσης του χρήστη και όταν δεν «αισθάνεται» κίνηση στο σπίτι, σε συνδυασμό με την επιβεβαίωση μέσω του αυτοκινήτου ή του GPS του «έξυπνου» τηλεφώνου ότι ο χρήστης βρίσκεται στον εργασιακό του χώρο, προσαρμόζει τη θερμοκρασία για εξοικονόμηση ενέργειας, την οποία και αυξάνει όταν πλησιάζει η ώρα να επιστρέψει ο χρήστης στο σπίτι[71].

Η διασυνδεδεμένη ψυχαγωγία αποτελεί ακόμα ένα πεδίο του «έξυπνου» σπιτιού. Με σχετική εφαρμογή «έξυπνης» τηλεόρασης στο κινητό του μπορεί κάποιος να χρησιμοποιήσει το «έξυπνο» τηλέφωνό του για να ελέγξει ταυτόχρονα πολλές συσκευές μαζί, αλλά και να καταγράψει τις υγιείς του συνήθειες ή και να ειδοποιήσει τα παιδιά του εάν βρίσκονται πολύ κοντά στην τηλεόραση[72]. Η Alexa της Amazon και το «νέο σπίτι της Google» είναι «έξυπνοι» ομιλητές, οι οποίοι ενημερώνουν τους χρήστες για τον καιρό και τις τελευταίες ειδήσεις, παίζουν μουσική και ελέγχουν άλλες «έξυπνες» οικιακές συσκευές που είναι συνδεδεμένες με τη θέρμανση, τον κλιματισμό, το φωτισμό, την τηλεόραση ή άλλες πηγές διασκέδασης, βασισμένες σε εφαρμογές όπως τα iHeartRadio, Spotify και Audible[73]. Τα «έξυπνα» τηλέφωνα

69 Βλ, σχετικά «Smarter Coffee», σε https://www.firebox.com/Smarter-Coffee/p6991 .

70 Βλ. σχετικά «Family Hub Refrigerator» σε http://www.samsung.com/us/explore/family-hub-refrigerator .

71 Οι επικριτές αυτής της τεχνολογίας υπογραμμίζουν ότι αυτή η αυτοματοποίηση έχει μεγάλο κόστος: η Google και άλλες παρόμοιες εταιρίες που είναι μυημένες στη λήψη δεδομένων που παράγονται από το διαδίκτυο των πραγμάτων θα χρησιμοποιήσουν τη γνώση σχετικά με τις προσωπικές συνήθειες και προτιμήσεις των χρηστών με στόχο το κέρδος. Η εφημερίδα LA Times ανέφερε ότι πολλοί πελάτες της εταιρίας Nest σκόπευαν να επιστρέψουν τις συσκευές τους με το φόβο των διαφημιστικών τακτικών της Google. Jeff, Stibel, «Google Is Already in Our Nests», (2014), διαθέσιμο σε http://www.breakpointbook.com/google-nests-privacy-jeff-stibel/ .

72 Βλ.σχετικά «iiMote, SMARTV», σε http://smartv.hk/iiMote.html .

73 Ry Crist, «Amazon Alexa: Device Compatibility, How-tos and Much More», διαθέσιμο σε https://www.cnet.com/how-to/amazon-alexa-devicecompatibility-how-tos-and-much-more. Βλ. επίσης Andrew Gebhart, «Google Home vs. Amazon Echo», διαθέσιμο σε https://www.cnet.com/news/google-home-vs-amazon-echo και Ryan Knutson και Laura Stevens, «Amazon and Google Consider Turning Smart Speakers into Home Phones», διαθέσιμο σε https://www.wsj.com/articles/amazon-google-dial-up-

παρέχουν ολοκληρωμένες αγορές μέσω των κατάλληλων εφαρμογών, οι οποίες μιμούνται την εμπειρία εντός των καταστημάτων και παρέχουν στους καταναλωτές την ευκολία να αγοράζουν προϊόντα απομακρυσμένα, ενόσω βρίσκονται στο γραφείο τους ή σε κίνηση. Το ίδιο ισχύει και για τις υπηρεσίες μεταφοράς προϊόντων παντοπωλείου, οι οποίες απλά συνδέουν τους χρήστες με μία λίστα αγαθών μέσω των «έξυπνων» κινητών ή των tablets[74]. Αλλά και τα ίδια τα καταστήματα χρησιμοποιούν το διαδίκτυο των πραγμάτων για να δημιουργήσουν διαδραστικές και διασυνδεδεμένες εμπειρίες. Για παράδειγμα καταστήματα καλλυντικών έχουν ειδικούς πίνακες που παρουσιάζουν φωτογραφίες πελατών που έχουν χρησιμοποιήσει τα προϊόντα τους, για να βοηθήσουν τους αγοραστές κατά την επιλογή τους[75]. Παρόμοια, στις κάβες οι αγοραστές μπορούν να εισάγουν σε μία εφαρμογή τις γευστικές τους επιλογές, με αποτέλεσμα την εμφάνιση σε ψηφιακά ράφια των μπουκαλιών που αποτυπώνουν τις προτιμήσεις τους.

Στον τομέα της ψυχαγωγίας, ερευνητές του πανεπιστημίου MIT των ΗΠΑ δημιούργησαν ένα βιβλίο, το οποίο «φοριέται» στο σώμα του αναγνώστη και του επιτρέπει να «νιώσει» τα συναισθήματα των πρωταγωνιστών της πλοκής. Στον αναγνώστη παρέχεται ένα ειδικό γιλέκο που περιέχει ηλεκτρονικούς αισθητήρες και άλλα ηλεκτρονικά εξαρτήματα και το οποίο συνδέεται με ένα βιβλίο επαυξημένης πραγματικότητας, το οποίο κρατά στα χέρια του. Καθώς εξελίσσεται η πλοκή του βιβλίου, σε συνεργασία με το γιλέκο, δημιουργείται μια σειρά από εμπειρίες (περιοδικές αλλαγές στη θερμοκρασία, δονήσεις πάνω στο σώμα, πρόκληση φωτισμού και ήχων), οι οποίες μεταφέρουν στον αναγνώστη αισθήσεις σχετικές με αυτό που διαβάζει, έτσι ώστε να μπαίνει καλύτερα στο «κλίμα» του βιβλίου. Οι αλλαγές αυτές δεν γίνονται με τυχαίο τρόπο, αλλά ποικίλουν ανάλογα με το περιεχόμενο της σελίδας που διαβάζει ο αναγνώστης. Το βιβλίο αλλάζει με τεχνητό

plans-to-turn-smart-speakers-into-home-phones-1487154781 .

74 Βλ. σχετικά «Ο δείκτης ευφυΐας των έξυπνων συσκευών», (2012), διαθέσιμο σε https://www.kathimerini.gr/economy/international/457788/o-deiktis-eyfy-as-ton-exypnon-syskeyon/

75 Chanel Parks, «3 Reasons Why We're Loving Sephora's Beauty Board», διαθέσιμο σε http://www.huffingtonpost.com/2014/03/13/sephora-beautyboard_n_4956441.html.

τρόπο μέχρι και τον ρυθμό που χτυπά η καρδιά του αναγνώστη, την κατάλληλη στιγμή της συναισθηματικής κορύφωσης. Επιπλέον, το συνδεδεμένο γιλέκο διαθέτει εκατόν πενήντα (150) λαμπτήρες LED που αυξομειώνουν τον φωτισμό γύρω από τον αναγνώστη, καθώς και μικρούς αερόσακους που κατά διαστήματα πιέζουν το σώμα του, ώστε να του δημιουργούν την αναγκαία ψυχοσωματική πίεση, όταν το απαιτεί το σενάριο[76].

Στον τομέα των διασυνδεδεμένων πόλεων και της προστασίας του περιβάλλοντος, υπάρχουν εφαρμογές που πραγματοποιούν ανάλυση των δεδομένων με στόχο τη μείωση των αποβλήτων. Για παράδειγμα, οι «έξυπνοι» κάδοι σκουπιδιών προχωρούν σε συλλογή δεδομένων σε πραγματικό χρόνο και ενεργοποιούν την αποκομιδή των απορριμάτων. Μέσω της ανάλυσης των δεδομένων, οι πόλεις μπορούν τελικά να μειώσουν τον αριθμό των απαιτούμενων αποκομιδών και να ελαχιστοποιήσουν τα καύσιμα και τη σπατάλη των πόρων[77]. Επίσης, δημοφιλείς εφαρμογές χρησιμοποιούνται για τη διευκόλυνση της κυκλοφορίας, ενώ άλλες, σχετικές με την εύρεση θέσεων στάθμευσης σε πραγματικό χρόνο, βοηθούν στην εξοικονόμηση της ενέργειας και των πόρων που απαιτούνται για τη διευθέτηση της κυκλοφορίας[78]. Τέλος, εξελιγμένες τεχνολογικές εφαρμογές επιτρέπουν στις πόλεις να προσαρμόζουν το επίπεδο του εξωτερικού φωτισμού ανάλογα με την ώρα της ημέρας, τον καιρό και

76 Η τεχνική αυτή ονομάζεται «αισθητηριακή φαντασία» (κατά το «επιστημονική φαντασία»). «Η αισθητηριακή φαντασία αφορά νέους τρόπους για να βιώνουμε και να δημιουργούμε ιστορίες», ανέφεραν οι ερευνητές και πρόσθεσαν ότι «παραδοσιακά η λογοτεχνία δημιουργεί και προκαλεί συναισθήματα και ενσυναίσθηση μέσω των λέξεων και των εικόνων. Χρησιμοποιώντας ένα συνδυασμό διασυνδεμένων αισθητήρων και ενεργοποιητών, ο συγγραφέας της αισθητηριακής φαντασίας διαθέτει πλέον νέα μέσα για να μεταφέρει στους αναγνώστες την πλοκή, τη διάθεση και τα συναισθήματα, ενώ παράλληλα αφήνει πάντα χώρο στη φαντασία του αναγνώστη. Τα νέα εργαλεία μπορούν να αξιοποιηθούν κατάλληλα, ώστε να δημιουργήσουν μια εμπειρία αφήγησης που θα απορροφά τελείως τον αναγνώστη και θα είναι προσαρμοσμένη στα μέτρα του». Βλ. σχετικά www.nooz.gr.

77 Βλ. σχετικά «Bigbelly Smart Waste & Recycling Systems Captured over 112 Million Gallons of Public Space Waste Last Year» διαθέσιμο σε http://bigbelly.com/bigbelly-smart-waste-recycling-systems-captured-over-112-million-gallons-of-publicspace-waste-last-year. Βλ. επίσης «Labor and Vehicle Efficiency», διαθέσιμο σε http://bigbelly.com/benefits/optimization.

78 Matthew Shaer, «Google Scoops up Waze in a Deal Reportedly Worth $1.1 Billion», διαθέσιμο σε http://www.csmonitor.com/Technology/, σε Hillary Brill και Scott Jones, «Little Things And Big Challenges: Information Privacy And The Internet Of Things», *American University Law Review*, Vol. 66 (2017): 1183 – 1184 .

την εποχή, δίνοντας την ευκαιρία στις πόλεις να μειώσουν το κόστος της ενέργειας φωτισμού των οδών κατά 30%[79].

Σχετικά με την προστασία της χλωρίδας και της πανίδας, στη Βραζιλία, για να παύσουν την παράνομη αποψίλωση των δασών έχουν ενσωματώσει ειδικές συσκευές στα δένδρα, οι οποίες ειδοποιούν τις αρχές στην περίπτωση που αυτές ενεργοποιηθούν από οποιαδήποτε δραστηριότητα, παράνομη ή μη[80]. Επίσης, στην Κένυα, για την προστασία των βοοειδών, τοποθετούνται στα λιοντάρια «έξυπνα» περιλαίμια, τα οποία εντοπίζουν και κοινοποιούν την τοποθεσία τους σε κτηνοτρόφους και κτηνιάτρους - φροντιστές[81].

3.1 Μη επανδρωμένα αεροσκάφη (Drones)

Τα «μη επανδρωμένα αεροσκάφη», όπως και κάθε άλλη ρομποτική τεχνολογία εντάσσονται στην κατηγορία του διαδικτύου των Πραγμάτων (IoT)[82]. Όπως ίσχυσε για την καινοτομία της φωτογραφικής μηχανής και των υπολογιστών, έτσι και η καινοτομία των μη επανδρωμένων αεροσκαφών[83] εμπίπτει στο γενικό νομικό και

79 Βλ. σχετικά Moor Insights & Strategy, «Echelon's Efficient Connected Lighting Solutions», διαθέσιμο σε http://www.moorinsightsstrategy.com/wp-content/uploads/2015/06/Echelons-Efficient-Connected-Lighting-Solutions-by-Moor-Insights-Strategy.pdf. Βλ. επίσης Echelon, «Shining A Light On Energy Savings», διαθέσιμο σε http://www.echelon.com/assets/blt1f1c055db1151a7c/Outdoor-Lighting-WiredSolution-Brochure.pdf.

80 Zafar Anjum, «How Internet Devices Are Working to Save the Rainforest», διαθέσιμο σε http://www.pcworld.com/article/2042086/how-internet-devices-are-working-to-save-the-rainforest.html.

81 Βλ. σχετικά «Protecting, Monitoring & Researching the Wildlife of Kuku», διαθέσιμο σε http://maasaiwilderness.org/programs/species-research.

82 Βλ. σχετικά «Internet of Things: Privacy & Security in a Connected World», Federal Trade Commission, (2015), διαθέσιμο σε https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf .

83 Μη επανδρωμένα αεροσκάφη (Unmanned Aerial Vehicle – UAV, Unmanned Aerial System – UAS ή Remotely Piloted Aircraft System - RPAS) ή drones ονομάζονται τα κάθε είδους ιπτάμενα οχήματα που δεν έχουν χειριστή στην άτρακτό τους, αλλά πραγματοποιούν πτήσεις είτε αυτόνομα είτε μέσω τηλεκατεύθυνσης. Ο όρος UAV περιγράφει μόνο το χωρίς χειριστή αεροσκάφος. Ο όρος UAS περιλαμβάνει όλες τις συσκευές, το προσωπικό και τις διαδικασίες οι οποίες χρησιμοποιούνται προκειμένου το μη επανδρωμένο αεροσκάφος να θεωρείται ως ολοκληρωμένο σύστημα. Τέλος, ο όρος RPAS καθιερώθηκε σύμφωνα με την ισχύουσα νομοθεσία και με την ανάγκη όλες οι πτήσεις μη επανδρωμένων αεροσκαφών να έχουν τουλάχιστον έναν επιβλέποντα πιλότο στο έδαφος. Τα μη επανδρωμένα ιπτάμενα οχήματα συνήθως έχουν τη μορφή μικρού αεροπλάνου ή ελικοπτέρου με έναν ή

τεχνολογικό πλαίσιο[84]. Τα πρώτα μη επανδρωμένα τηλεκατευθυνόμενα αεροσκάφη εμφανίστηκαν λίγο μετά τον Α΄ Παγκόσμιο Πόλεμο το 1915. Το Radioplane OQ-2 ήταν το πρώτο τηλεκατευθυνόμενο αεροσκάφος κατά την έναρξη του Β΄ Παγκοσμίου πολέμου, το 1940[85]. Η ερασιτεχνική τεχνολογία των UAV (unmanned aerial vehicles) βασίστηκε σε κάποιες στρατιωτικές καινοτομίες, αλλά τα τηλεκατευθυνόμενα αεροσκάφη προϋπήρχαν των δύο παγκοσμίων πολέμων[86]. Τα συστήματα όμως που είναι ευκολότερα στην πτήση μέσω λιγότερο εκπαιδευμένων χειριστών, πιο ανθεκτικά σε διάφορες συνθήκες και με καλύτερους αισθητήρες που συμβάλουν τόσο στην άντληση πληροφοριών, όσο και στην ασφάλεια, εμφανίστηκαν πολύ πιο πρόσφατα και ακολούθησε η εμπορική τους χρήση και τα αυξημένα επίπεδα αυτονομίας[87].

3.1.1 Χρήσεις

Τα μη επανδρωμένα αεροσκάφη (drones) έχει προβλεφθεί ότι θα συμβάλουν αποτελεσματικά στην επιβολή του νόμου, θα προκαλέσουν επανάσταση στις γεωργικές εργασίες, θα μεταβάλουν τον τρόπο και τους κανόνες του πολέμου και θα βελτιώσουν τις υπηρεσίες μεταφορών[88]. Στην Ευρωπαϊκή Ένωση εκδόθηκαν

περισσότερους κινητήρες και έλικες συντονισμένους για πλήρως ελεγχόμενη πτήση από ειδικό πρόγραμμα ή χειριστήριο εδάφους. Βλ. σχετικά «Introduction to Remotely Piloted Aircraft Systems» (RPAS), (2020), διαθέσιμο σε https://www.skybrary.aero/index.php/Introduction_to_Remotely_Piloted_Aircraft_Systems_(RPAS) .

84 Meg Leta Jones, «Does Technology Drive Law? The Dilemma of Technological Exceptionalism In Cyberlaw», *Journal Of Law*, Technology & Policy, No. 2, Technological Exceptionalism in Cyberlaw (2018).

85 Rudolph Herzog, «Rise of the Drones», Lapham's Q, διαθέσιμο σε https://www.laphamsquarterly.org/spies/rise-drones.

86 David Boddington, «Radio-controlled Model Aircraft», The Crowood Press Ltd, (2004).

87 IWM Staff, «A Brief History of Drones», Imperial War Museum. Βλ. σχετικά https://www.iwm.org.uk/history/a-brief-history-of-drones και Technology Quarterly, «Taking Flight», Economist, διαθέσιμο σε https://www.economist.com/technology-quarterly/2017-06-08/civilian-drones.

88 IWM Staff. Βλ. επίσης Shane Crotty, «The Aerial Dragnet: A Drone-ing Need for Fourth Amendment Change», *Valparaiso University Law Review*, Vol. 49/ 1 (2014): 219-265, Michal Mazur, «Six Ways Drones are Revolutionizing Agriculture», *MIT Tech. Rev*, διαθέσιμο σε https://www.technologyreview.com/s/601935/six-ways-drones-are-revolutionizing-agriculture.

διαδοχικά τρεις Κανονισμοί σχετικά με τους κανόνες και τις διαδικασίες που διέπουν τη λειτουργία των μη επανδρωμένων αεροσκαφών[89], ενώ οι χώρες της Ευρωπαϊκής Ένωσης προέβαλαν περιορισμούς ως προς το μέγεθος των μη επανδρωμένων αεροσκαφών και την τοποθεσία πτήσης τους, αλλά και έθεσαν σε εφαρμογή διαδικασίες αδειοδότησης και ασφάλειας[90]. Σχετικά με την περισυλλογή δεδομένων και τις οπτικές τεχνολογίες, η Υπηρεσία Ερευνών του Κογκρέσου των ΗΠΑ προχώρησε το 2015 στη συγγραφή της οδηγίας Domestic Drones and Privacy: A Primer[91]. Η οδηγία αυτή υπογραμμίζει δύο ζητήματα: την ανάγκη προστασίας της ιδιωτικής ζωής στο πλαίσιο της εναέριας παρακολούθησης και τη θεσμική ευθύνη. Τα μη επανδρωμένα αεροσκάφη συγκαταλέγονται στις εφαρμογές της ρομποτικής, όσον αφορά στη νομική και πολιτική θεωρία των ΗΠΑ[92]. Η τεχνολογία τους υπήρξε εξαιρετικά προκλητική για τους Αμερικανούς νομοθέτες, σε σημείο που τέθηκαν περιορισμοί στη χρήση τους από κάποιες Πολιτείες (όπως η Βιρτζίνια, η Πενσυλβάνια και η Β. Καρολίνα) μέχρι την έκδοση των κατάλληλων νομοθετικών πράξεων[93]. Το παράδειγμα αυτών ακολούθησε και η Υπηρεσία Πολιτικής Αεροπορίας των ΗΠΑ, η οποία απαγόρευσε την πτήση εμπορικών μη επανδρωμένων αεροσκαφών, μέχρι την εφαρμογή των κατάλληλων νομοθετικών ρυθμίσεων[94]. Η

89 Βλ. σχετικά Καν (ΕΕ) 2018/1139 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 4ης Ιουλίου 2018, για τη θέσπιση κοινών κανόνων στον τομέα της πολιτικής αεροπορίας («Κανονισμός EASA»), Καν (ΕΕ) 2019/945 της Επιτροπής για συστήματα μη επανδρωμένων αεροσκαφών και φορείς εκμετάλλευσης συστημάτων μη επανδρωμένων αεροσκαφών τρίτων χωρών και Καν (ΕΕ) 2019/947 της Επιτροπής για τους κανόνες και τις διαδικασίες που διέπουν τη λειτουργία μη επανδρωμένων αεροσκαφών.

90 Ενημέρωση της Υπηρεσίας Έρευνας του Ευρωπαϊκού Κοινοβουλίου σχετικά με τα μη εμπορικά Drones στην Ευρωπαϊκή Ένωση, Eur. Parl., 5–7 Οκτώβριος 2015, διαθέσιμο σε http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/571305/EPRS_BRI282015%29571305_EN.pdf .

91 Richard M. Thompson II, «Domestic Drones and Privacy: A Primer», Cong. Res. Serv., R43965, 1, (2015), διαθέσιμο σε https://fas.org/sgp/crs/misc/R43965.pdf.

92 G., Miller, «The Moral Hazards and Legal Conundrums of our Robot-Filled Future», διαθέσιμο σε https://www.wired.com/2014/07/moral-legal-hazards-robot-future, [https://perma.cc/262T-FHB4].

93 Michael L. Smith, «Regulating Law Enforcement's Use of Drones: The Need for State Legislation», Harvard Journal on Legislation, Vol. 52, (2015): 423- 454. Βλ. επίσης John Latimer, «Pennsylvania Senator Launches Drone Moratorium Law», Gov't Tech, (2015), διαθέσιμο σε http://www.govtech.com/state/Pennsylvania-Senator-Launches-Drone-Moratorium-Law.html [https://perma.cc/GU6G-6U5K]

94 Ό.π. υποσημείωση 83.

χρήση των μη επανδρωμένων αεροσκαφών καθυστέρησε σημαντικά εν αναμονή των ρυθμίσεων αυτών, προκαλώντας τη δυσαρέσκεια των κατασκευαστών, οι οποίοι κατηγόρησαν το κράτος ότι ολιγωρεί, παραδίδοντας τα τεχνολογικά πρωτεία σε άλλες αγορές[95]. Αυτού του είδους η αντιμετώπιση, δημιούργησε την ανάγκη μίας νομικής αναμόρφωσης για τις νέες ικανότητες των ολιγοβαρών ημιαυτόνομων ιπτάμενων αντικειμένων, παρότι άλλες χώρες δεν αντιμετώπισαν τα ίδια εμπόδια ή το ίδιο χρονοδιάγραμμα. Ιδιαίτερα κατά την περίοδο της πανδημίας του COVID-19, όπου εισήχθη στα εθνικά λεξικά ο όρος της «κοινωνικής αποστασιοποίησης» (social distancing), η τεχνολογία των μη επανδρωμένων πτητικών μέσων, με τη μεταφορά φαρμάκων και δεμάτων, προσέφερε κοινωνικές υπηρεσίες και μείωσε την επαφή μεταξύ των ατόμων. Για παράδειγμα, η κυβέρνηση της Κίνας προχώρησε σε εθνικά προγράμματα πτήσεων και σε συνεργασία με ιδιωτικές εταιρίες πραγματοποίησε εκατοντάδες πτήσεις προς παράδοση ιατροφαρμακευτικού υλικού και δεμάτων προς τις περιοχές που είχαν πληγεί από τον ιό. Με τον τρόπο αυτό μειώθηκε ο χρόνος παράδοσης στο μισό, σε σχέση με τα παραδοσιακά οδικά μέσα, ενώ αφαιρέθηκε ο ανθρώπινος παράγοντας από τη διαδικασία, βοηθώντας στη μείωση του ρυθμού εξάπλωσης του ιού[96]. Επίσης, τα μη επανδρωμένα αεροσκάφη βοήθησαν στη μεταφορά των ληφθέντων δειγμάτων στα εργαστήρια, οδηγώντας στην ταχύτατη διάγνωση της νόσου και την απομόνωση των μολυσμένων ατόμων, αλλά και χρησιμοποιήθηκαν για την ασφαλή μεταφορά των ιατρικών προμηθειών στα νοσοκομεία, όπου αντιμετωπίζονταν ασθενείς με COVID-19[97].

Στις χρήσεις των μη επανδρωμένων αεροσκαφών, με την ευρεία έννοια, θα μπορούσε να συμπεριληφθεί και ο τομέας των στοχευμένων ανθρωποκτονιών, ως τρόπος

95 S. O' Kane, «The FAA's Drone Regulations Won't Be Ready Until at Least 2017», Verge, (2014) διαθέσιμο σε https://www.theverge.com/2014/12/10/7370955/the-faas-drone-regulations-wont-be-ready-until-at-least-2017 [https://perma.cc/33AN-C86Q].

96 Junwei Yang και Timothy Reuter, «3 ways China is using drones to fight coronavirus» (2020), διαθέσιμο σε https://www.weforum.org/agenda/2020/03/three-ways-china-is-using-drones-to-fight-coronavirus/ .

97 Για παράδειγμα, η εταιρία Zipline, πραγματοποίησε τα τελευταία χρόνια πλέον των 60.000 μεταφορών ιατροφαρμακευτικών υλικών προς τη Ρουάντα και τη Γκάνα. Brent Skorup και Connor Haaland, «How Drones Can Help Fight the Coronavirus», Mercatus Center Research Paper Series, Special Edition Policy Brief (2020).

αντιμετώπισης της διεθνούς τρομοκρατίας. Πέρα από το μοντέλο της παραδοσιακής επιβολής του εσωτερικού νόμου των κρατών[98] σε μία ποινικά κολάσιμη πράξη, όπως είναι η τρομοκρατία, η στοχευμένη ανθρωποκτονία αποτελεί τη μοναδική λύση όταν δεν υπάρχει διαφορετικός τρόπος να αποτραπεί ή να σταματήσει μία τρομοκρατική επίθεση, ώστε, με τη θανάτωση του δράστη, να διασωθούν πλείστες όσες ανθρώπινες ζωές[99]. Σε αντίθεση με την εφαρμογή του εσωτερικού δικαίου των κρατών στο μοντέλο της επιβολής του νόμου, η χρήση αυτού του είδους της δύναμης διέπεται αποκλειστικά από τις διατάξεις του διεθνούς δικαίου για τα ανθρώπινα δικαιώματα[100].

3.1.2 Προστασία της ιδιωτικής ζωής

Στο ερώτημα εάν τα μη επανδρωμένα αεροσκάφη αποτελούν ένα νέο μοναδικό εργαλείο παρακολούθησης, η απάντηση είναι ότι οι ευρωπαϊκές χώρες έχουν ολοκληρωμένα συστήματα προστασίας δεδομένων και οπτικές τεχνολογίες παρακολούθησης των πολιτών ήδη από τα τέλη του 1970 (η Ευρωπαϊκή Ένωση από το 1990 κι έπειτα), κατά συνέπεια η τεχνολογία των μη επανδρωμένων αεροσκαφών είναι πολύ νεώτερη στις ΗΠΑ απ΄ ό,τι οπουδήποτε αλλού[101].

Στο Ηνωμένο Βασίλειο η χρήση μη επανδρωμένων αεροσκαφών με σκοπό τη λήψη εικόνας κάποιου ατόμου χωρίς τη συναίνεσή του, αποτελεί παραβίαση του νόμου

98 David Kretzmer, «Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Self-Defence», *European Journal of International Law (*2005):174.

99 Nils Melzer, «Human Rights Implications of the Usage of Drone and Unmanned Robots in Warfare», European Parliament, Directorate-General for External Policies of the Union, Directorate B, Policy Department, Study (2013): 36.

100 Bence Kis Kelemen, «Targeted Killings and Human Rights Law», *Hungarian Yearbook of International Law and European Law* (2018): 245-259. Βλ. επίσης την Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων, διαθέσιμη σε https://gr.humanrights.com/what-are-human-rights/universal-declaration-of-human-rights/preamble.html .

101 «A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe», Directorate Gen. Internal Policies Union, (2009), διαθέσιμο σε http://www.statewatch.org/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf. Βλ. επίσης Peter Squires, «Evaluating CCTV: Lessons from a Surveillance Culture, Citizens, Cities, and Video Surveillance», EUR. F. URB. SEC. 2, 37 (2010), διαθέσιμο σε http://efus.eu/files/2013/05/CCTV_ANGLAIS.pdf

περί Προστασίας Προσωπικών Δεδομένων (DPA)[102] ή του Κώδικα Πρακτικής του Κλειστού Κυκλώματος Τηλεόρασης (CCTV Code of Practice)[103].

Η Γερμανία από την άλλη πλευρά, έχει πρωτοπορήσει στην προστασία προσωπικών δεδομένων, έπειτα από την εμπειρία της από τον ολοκληρωτισμό του Β΄ Παγκοσμίου Πολέμου. Το Ομοσπονδιακό Συνταγματικό Γερμανικό Δικαστήριο το 1983 εξέδωσε μία απόφαση για την προστασία της ιδιωτικής ζωής[104] κατ' ερμηνεία και στην έκταση της προστασίας που προσφέρεται από το νόμο περί προστασίας προσωπικών δεδομένων, ανάγοντας την προστασία της ιδιωτικής ζωής από τα μη επανδρωμένα αεροσκάφη στους ήδη υπάρχοντες, από το 1970, νόμους προστασίας των δεδομένων: «όπως και στις περιπτώσεις των απλών φωτογραφιών, οι λήψεις που λαμβάνονται από μη εμπορικά μη επανδρωμένα αεροσκάφη δεν επιτρέπεται να παραβιάζουν το δικαίωμα του προσώπου στη φωτογραφία. Σύμφωνα με το άρθρο 22 το Γερμανικού Νόμου για τα δικαιώματα πνευματικής ιδιοκτησίας σε έργα τέχνης και φωτογραφίας (KUG), οι φωτογραφίες ενός προσώπου μπορούν να διαδοθούν ή να παρουσιαστούν στο κοινό μόνο με τη συναίνεση του προσώπου αυτού»[105]. Περαιτέρω, οι ικανότητες, η λειτουργία ή οι προοπτικές των μη επανδρωμένων αεροσκαφών δεν υπήρξαν κάτι το εξαιρετικό για τη Γερμανία, η οποία δεν θεώρησε απαραίτητο να προχωρήσει σε κάποια σημαντική νομική αναμόρφωση σχετικά με αυτά.

Στη Γαλλία, το Συμβούλιο της Επικρατείας, έπειτα από προσφυγή της Ένωσης Ανθρωπίνων Δικαιωμάτων και της οργάνωσης για την προάσπιση των δικαιωμάτων και των ελευθεριών που σχετίζονται με το διαδίκτυο La Quadrature du Net, ζήτησε

102 Εάν ένα drone έχει κάμερα, η χρήση της καλύπτεται από τις διατάξεις του νόμου περί προστασίας προσωπικών δεδομένων. Βλ. σχετικά «Drones», διαθέσιμο σε https://ico.org.uk/for-the-public/drones .

103 «In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information», Info. Comm'r Off., 5 (2017), διαθέσιμο σε https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

104 Πρόκειται για το δικαίωμα του πληροφοριακού αυτοκαθορισμού, δηλαδή τη δυνατότητα του ατόμου να αποφασίζει και να συμπροσδιορίζει πότε και υπό ποιες προϋποθέσεις είναι δυνατή η επεξεργασία των πληροφοριών που το αφορούν. Βλ. σχετικά απόφαση της 15.12.1983 του γερμανικού Ομοσπονδιακού Συνταγματικού Δικαστηρίου στην υπόθεση Volkszählungsgesetz.

105 Wilde Beuger Solmecke, «Civilian Drones and the Legal Issues Surrounding Their Use», (2014), διαθέσιμο σε https://www.wbs-law.de/internetrecht/civilian-drones-legal-issues-surrounding-use-50459 .

από τη γαλλική κυβέρνηση «να σταματήσει χωρίς καθυστέρηση τη χρήση μη επανδρωμένων αεροσκαφών στο Παρίσι, με τα οποία παρακολουθεί τη συμμόρφωση των πολιτών στα πρωτόκολλα ασφαλείας κατά την άρση της απαγόρευσης κυκλοφορίας, λόγω της απουσίας νομικού πλαισίου για τη χρήση αυτών των τεχνολογικών συσκευών». Παρόλο που με τη βιντεοσκόπηση αυτή ο στόχος δεν ήταν η ταυτοποίηση των προσώπων, αλλά η αποτροπή του κινδύνου συναθροίσεων, από μόνη της η ικανότητα των πτητικών αυτών μέσων να ταυτοποιούν τους πολίτες, σε συνδυασμό με τους κινδύνους που εγκυμονεί η δυνατότητα της ταυτοποίησης αυτής, συνιστούν παραβίαση του δικαιώματος στην ιδιωτική ζωή και αντιβαίνουν στους κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα. Το ανώτατο δικαστήριο έκρινε ότι η χρήση των μη επανδρωμένων πτητικών μέσων από τη γαλλική αστυνομία θα μπορούσε αφενός μεν να νομιμοποιηθεί μέσω ειδικού διατάγματος, αφετέρου δε τα μέσα αυτά θα μπορούσαν να διαθέτουν εξοπλισμό που να καθιστά αδύνατο τον εντοπισμό των βιντεοσκοπούμενων πολιτών[106].

Στην Ελλάδα, τον Ιούνιο του 2020 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εξέδωσε την υπ' αριθμό 3/2020[107] Γνωμοδότησή της για το Σχέδιο

106 «Το γαλλικό ΣτΕ απαγόρευσε τη χρήση drones για την επιτήρηση των πολιτών», διαθέσιμο σε https://www.kathimerini.gr/1078711/article/epikairothta/kosmos/to-galliko-ste-apagoreyse-th-xrhsh-drones-gia-thn-epithrhsh-twn-politwn, (18-05-2020). Στο ίδιο πλαίσιο, η Εθνική Επιτροπή Πληροφορικής κι Ελευθεριών της Γαλλίας (CNIL) επέβαλε πρόστιμο στο Γάλλο Υπουργό Εσωτερικών για τη βιντεοσκόπηση των πολιτών μέσω μη επανδρωμένων αεροσκαφών σχετικά με την εφαρμογή των περιοριστικών μέτρων. Βλ. σχετικά https://www.cnil.fr/en/node/120820 .

107 Ως δεδομένο προσωπικού χαρακτήρα νοείται κατ' άρθ. 4 παρ. 1 ΓΚΠΔ και 3 περ. 1 Οδηγίας 2016/680 κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική. Για την ταυτοποίηση του φυσικού προσώπου, η οποία μπορεί να είναι και έμμεση, χωρίς δηλαδή ευθεία αναφορά στο φυσικό πρόσωπο, πρέπει να λαμβάνεται υπόψη το σύνολο των μέσων που μπορούν ευλόγως να χρησιμοποιηθούν, είτε από τον υπεύθυνο επεξεργασίας, είτε από τρίτο . Σύμφωνα με την ΑΠΔΠΧ 41/2017 η έμμεση ταυτοποίηση μπορεί να είναι συνάρτηση πολλών διαφορετικών παραγόντων. Τα ίδια στοιχεία, ο συνδυασμός των οποίων δεν επιτρέπει την ταυτοποίηση ενός προσώπου σε ένα ευρύ κοινωνικό περιβάλλον, μπορεί να οδηγούν σε πλήρη ταυτοποίηση στο πλαίσιο μιας μικρής κοινωνικής ομάδας, όπου όλα τα μέλη της γνωρίζονται μεταξύ τους. Για τον λόγο αυτό, προκειμένου να εξετασθεί εάν έχει λάβει χώρα επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει να λαμβάνεται υπόψη το σύνολο αυτών των παραμέτρων που αφορούν την υπό κρίση επεξεργασία, διότι και η πιθανότητα έμμεσης ταυτοποίησης, όταν δεν είναι αμελητέα, καθιστά, καταρχήν, την πληροφορία, προσωπικό δεδομένο. Έτσι, η λήψη ή και καταγραφή της εικόνας ενός ατόμου από μεγάλο ύψος ή μακρινή απόσταση ή με καλυμμένα χαρακτηριστικά (π.χ. κρανιοφόρος

Προεδρικού Διατάγματος, κατ' εφαρμογή των άρθρων 13 παρ. 1 περ. γ' και 67 παρ. 2 του νόμου 4624/2019[108], δίνοντας κατευθύνσεις σχετικά με τη χρήση συστημάτων βιντεοεπιτήρησης από δημόσιες αρχές σε δημόσιους χώρους.

4 Διαδίκτυο των πραγμάτων και ιδιωτικότητα

Αυτός ο διασυνδεδεμένος κόσμος και οι υποσχέσεις που τον ακολουθούν συνοδεύεται από προκλήσεις για τις ρυθμιστικές αρχές, καθώς οι συσκευές του λειτουργούν μόνο όταν συλλέγεται η πληροφορία. Ο νομικός κόσμος και η νομοθετική εξουσία, επιδιώκοντας την τήρηση ορθών πρακτικών αντιμετώπισης των νέων δεδομένων, πρέπει πλέον να θέσουν τις κατευθυντήριες γραμμές πολιτικής και τις προτεραιότητες εφαρμογής στο πλαίσιο ενός γρήγορα κινούμενου, ταχέως αναπτυσσόμενου διαδικτυακά συνδεδεμένου κόσμου, διαχειριζόμενες νέα κι ευαίσθητα σύνολα δεδομένων, από τον παλμό της καρδιάς και τη θερμοκρασία του σώματος, έως την αναπαραγωγή του περιεχομένου των συσκευών ή τον τρόπο με τον οποίο ο κόσμος διαχειρίζεται τη περιβαλλοντική μόλυνση. Πρέπει ταυτόχρονα να βρεθεί ένα σημείο εξισορρόπησης των καινοτομιών του διαδικτύου των πραγμάτων και της προστασίας της ασφάλειας και της ιδιωτικότητας των πληροφοριών που αυτό

ή μασκοφόρος) που καθιστά αδύνατη την αναγνώριση των φυσικών χαρακτηριστικών του προσώπου ενός υποκειμένου των δεδομένων δεν συνεπάγεται άνευ ετέρου την αδυναμία ταυτοποίησής του, καθώς δύναται εν τέλει να επιτευχθεί από λοιπές πληροφορίες, όπως π.χ. τα εμφανισιακά χαρακτηριστικά (ύψος, σωματοδομή, χρώμα και είδος ενδυμάτων και υποδημάτων) σε συνδυασμό με επιπλέον πληροφορίες (π.χ. επιβίβασή του σε μηχανοκίνητο όχημα, επισήμανση ή καταγραφή της πορείας και του τελικού προορισμού του, επεξεργασία δεδομένων θέσης των κινητών τερματικών συσκευών κινητής τηλεφωνίας για ένα χρονικό διάστημα σε έναν συγκεκριμένο γεωγραφικό χώρο). Από την επεξεργασία και τον συνδυασμό επεξεργασιών δεδομένων προσωπικού χαρακτήρα είναι δυνατή η εξαγωγή συμπερασμάτων που οδηγεί στην δημιουργία προφίλ του φυσικού προσώπου, το οποίο θα αφορά είτε περιστασιακά, είτε σε μόνιμη βάση τις συνήθειες, τους τόπους μόνιμης ή προσωρινής διαμονής, τις καθημερινές και άλλες μετακινήσεις, τις ασκούμενες δραστηριότητες, τις κοινωνικές σχέσεις και τα κοινωνικά περιβάλλοντα στα οποία συχνάζει. Βλ. σχετικά https://www.dpa.gr/portal/page?_pageid=33,120923&_dad=portal&_schema=PORTAL .

108 Νόμος 4624/2019 περί Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 (753009).

συλλέγει[109]. Το κόστος, λοιπόν, για όσα παρέχει το διαδίκτυο των πραγμάτων είναι οι προσωπικές πληροφορίες που μοιράζονται οι χρήστες, από τις αγοραστικές τους συνήθειες, έως ζητήματα σχετικά με την ιδιοκτησία τους. Όταν αυτές οι πληροφορίες συλλέγονται, οι ρυθμιστικές αρχές έρχονται αντιμέτωπες με σύνθετα ερωτήματα, όπως το εάν έχουν γνώση οι καταναλωτές των όσων συλλέγονται και πώς αυτά διαμορφώνονται ή τι θα συμβεί στην περίπτωση που τα δεδομένα αυτά περιέλθουν σε μη εξουσιοδοτημένα άτομα, για παράδειγμα μέσω παραπλανητικών πρακτικών ή κακόβουλων επιθέσεων. Πέραν των ανωτέρω, αξιοσημείωτο για την εξέλιξη του διαδικτύου των πραγμάτων είναι η ικανότητα των συσκευών να επικοινωνούν μεταξύ τους, ακόμα και αυτόνομα, με την συλλογή πληροφοριών, όχι μόνο για άμεση δική τους χρήση, αλλά και για τη χρήση από άλλες συσκευές[110]. Η συσσωμάτωση των δεδομένων από πολλαπλές πηγές του δικτύου των πραγμάτων δημιουργεί σημαντικές ευκαιρίες για τους καταναλωτές, αλλά και τεράστιες ανησυχίες σχετικά με την ιδιωτικότητά τους[111]. Όσο το διαδίκτυο των πραγμάτων γίνεται πιο ολοκληρωμένο, μπορεί να καταστεί ευκολότερο για τα μη εξουσιοδοτημένα μέρη να αποκτήσουν ένα πιο περιεκτικό και ολοκληρωμένο σύνολο δεδομένων ενός ατόμου. Για παράδειγμα, σήμερα εάν κάποιος ήθελε να διαμορφώσει το ψηφιακό προφίλ[112] ενός προσώπου, θα έπρεπε να ανακτήσει πληροφορίες από διάφορες πηγές. Όσοι συγκεντρώνουν

109 Hillary Brill και Scott Jones, «Little Things And Big Challenges: Information Privacy And The Internet o f Things», *American University Law Review*, Vol. 66 (2017): 1183 – 1184.

110 Για παράδειγμα, ο θερμοστάτης της Nest συνδέεται με τη συσκευή Amazon Echo (ένα hands-free ηχείο που ο χρήστης ελέγχει με τη φωνή του) και η πλατφόρμα SmartPlate (έξυπνη πλατφόρμα ευεξίας) συνδέεται με την εφαρμογή Fitbit. Βλ. σχετικά https://www.fitbit.com/global/eu/home και Steven John, «Does Nest work with Alexa?: How to connect Nest devices to Alexa for various at-home commands», (2020), διαθέσιμο σε https://www.businessinsider.com/does-nest-work-with-alexa .

111 Βλ. σχετικά Fed. Trade Comm'n, «Cross-Device Tracking: An Ftc Staff Report 5–7», (2017), διαθέσιμο σε https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-reportjanuary-2017/ftc_cross-device_tracking_report_1-23-17.pdf.

112 Σύμφωνα με το Γενικό Κανονισμό για την Προστασία Δεδομένων η «κατάρτιση προφίλ» αποτελεί οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου. Βλ. επίσης Jeff Kraakevik, «Crafting a positive professional digital profile to augment your practice», (2016), διαθέσιμο σε https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5765898/#:~:text=A%20digital%20profile%20is%20the,profile%20is%20through%20social%20media .

δεδομένα συνεχίζουν πλέον να τα ανακτούν από περισσότερες συσκευές και κατ' επέκταση, αφενός μεν ο προσωπικός έλεγχος στις πληροφορίες του καθενός μειώνεται, αφετέρου δε αυξάνουν οι κίνδυνοι στην ασφάλεια και την ιδιωτικότητα του[113].

Η ανεξάρτητη συλλογή δεδομένων δημιουργεί μία μεγάλη πρόκληση για τις κυβερνήσεις και τα νομοθετικά τους όργανα, οι οποίες μπορεί να μην έχουν τα κατάλληλα εργαλεία για να διαχειριστούν τέτοια ζητήματα. Η βιομηχανία εξαλείφει την ανθρώπινη κρίση πάνω στην πληροφορία και δημιουργεί καινοτόμους τομείς στην επεξεργασία και τη συλλογή δεδομένων από διασυνδεδεμένες συσκευές του διαδικτύου των πραγμάτων[114], όπως τη μηχανική μάθηση[115], την τεχνητή νοημοσύνη[116] και τους εξελιγμένους αλγορίθμους[117]. Οι συσκευές συγκεντρώνουν δεδομένα από τον καθένα μας, αλλά επίσης κάνουν τους ανθρώπους να σιωπούν. Ιδιαίτερα κατά τη διάρκεια της πανδημίας του κορωνοϊού προέκυψαν σημαντικά ζητήματα παραβίασης της ιδιωτικότητας των πολιτών, κυρίως σε τρίτες χώρες, κατά τη διαδικασία ιχνηλάτησης των επαφών όσων ασθένησαν από τον ιό[118]. Στην

113 Hillary Brill και Scott Jones, «Little Things And Big Challenges: Information Privacy and the Internet of Things», *American University Law Review*, Vol. 66 (2017): 1183 – 1184.

114 Brandon Rohrer, «An Adaptive Learning Algorithm for the Internet of Things», διαθέσιμο σε https://brohrer.github.io/adaptive_reinforcement_learning_iot.html. Βλ. επίσης Mika Tanskanen, «Applying Machine Learning to IoT Data», διαθέσιμο σε https://www.sas.com/en_us/insights/articles/big-data/machine-learning-bringsconcrete-aspect-to-iot.html.

115 Το φαινόμενο κατά το οποίο ένα σύστημα βελτιώνει την απόδοσή του κατά την εκτέλεση μιας συγκεκριμένης εργασίας, χωρίς να υπάρχει ανάγκη να προγραμματιστεί εκ νέου ή η ικανότητα ενός υπολογιστικού συστήματος να δημιουργεί μοντέλα ή πρότυπα από ένα σύνολο δεδομένων. Βλ. σχετικά «Μηχανική Μάθηση», διαθέσιμο σε https://repository.kallipos.gr/bitstream/11419/3382/1/02_chapter_04.pdf.

116 Ό.π. υποσημ. 52.

117 Οι αλγόριθμοι επιτρέπουν στο μηχάνημα (υπολογιστή, ρομπότ κ.ά.) να μαθαίνει και να αποφασίζει μόνο του. Βλ, σχετικά «Οι αλγόριθμοι και γιατί χρειάζονται περισσότερο κοινωνικό έλεγχο», (2020), διαθέσιμο σε https://www.tovima.gr/2017/02/12/society/oi-algorithmoi-kai-giati-xreiazontai-perissotero-koinwniko-elegxo/. Βλ. επίσης σχετικά με εξελιγμένους αλγορίθμους Fotios Fitsilis, «Imposing Regulation on Advanced Algorithms», Springer, (2019).

118 Διακρατική περίπτωση παρέμβασης στην ελευθερία και την ιδιωτικότητα των πολιτών αποτέλεσε, με αφορμή την πανδημία του κορωνοϊού COVID-19, η σύσταση από την Αυστραλιανή κυβέρνηση προς τους πολίτες της εγκατάστασης στα κινητά τους τηλέφωνα μίας εφαρμογής που είχε ως στόχο την ιχνηλάτηση των επαφών και των κινήσεών τους. Αν και τα επιδημιολογικά οφέλη αυτής της παραίνεσης υπήρξαν ορατά, εξίσου σημαντικά ήταν και τα ζητήματα που τέθηκαν σχετικά με τις επιπτώσεις στην ιδιωτική ζωή των πολιτών. Προς τούτο, ο αυστραλιανός οργανισμός Liberty Victoria απευθυνόμενος προς την Ομοσπονδιακή και τη Βικτωριανή κυβέρνηση απαίτησε να μην είναι υποχρεωτική η

Ευρωπαϊκή Ένωση το ζήτημα αντιμετωπίστηκε με ανακοίνωση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, στην οποία προτάθηκε η πρόβλεψη ειδικών σχετικών ρυθμίσεων στις εσωτερικές νομοθεσίες των Κρατών – μελών[119]. Στην Ελλάδα ο Ν. 3471/2006 είχε ήδη εντάξει τα δεδομένα θέσης και κίνησης στο απόρρητο των επικοινωνιών και απαγόρευσε την παρακολούθησή τους (άρθρο 4), εκτός αντίθετης ειδικής νομοθετικής πρόβλεψης. Κατ' επέκταση, η χαρτογράφηση των κινήσεων του ασθενούς μόνο με ειδική νομοθετική πρόβλεψη θα μπορούσε να πραγματοποιηθεί και πάντα σε συμφωνία με το δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα και τη συνταγματική αρχή της αναλογικότητας[120].

Τα ζητήματα της ιδιωτικότητας του διαδικτύου των πραγμάτων είναι μεν ιδιαίτερα ευαίσθητα για τους ενήλικες, πολλώ δε μάλλον για τους ανηλίκους. Κυρίως, δε για τους γονείς που έχουν να διαχειριστούν παιδιά που χρησιμοποιούν «έξυπνες» συσκευές και παιχνίδια και δεν είναι ενήμερα για ζητήματα όπως οι πληροφορίες που συγκεντρώνονται από τους κατασκευαστές των παιχνιδιών[121]. Οι γονείς επιλέγουν ολοένα και περισσότερο «διασυνδεδεμένα παιχνίδια», με στόχο να παρέχουν διαδραστική εκπαίδευση και διασκέδαση στα παιδιά τους[122]. Αυτά τα «έξυπνα»

εγκατάσταση αυτής της εφαρμογής, οι πληροφορίες που θα αντληθούν από την εφαρμογή να είναι μόνο κατ' επιλογήν, σε περίπτωση θετικού στον ιό, πολίτη, να υπάρχει απόλυτη διαφάνεια σχετικά με τη συλλογή, αποθήκευση, πρόσβαση και καταστροφή των ευαίσθητων αυτών πληροφοριών, να υπάρξουν εγγυήσεις ότι οι πληροφορίες που θα συγκεντρωθούν δεν θα αξιοποιηθούν για κανέναν άλλο σκοπό, παρά μόνο για τον επιδημιολογικό έλεγχο του κορωνοϊού COVID-19 και τέλος ότι κάθε ίχνος της εφαρμογής και οι δυνατότητες παρακολούθησης θα απενεργοποιηθούν το συντομότερο δυνατό. Από τον ίδιο οργανισμό τονίστηκε ιδιαίτερα ότι η ιδιωτικότητα είναι σημαντική και δεν πρέπει να χρησιμοποιείται ως νόμισμα για την εξαγορά των άλλων ελευθεριών. Βλ. σχετικά «Liberty Victoria calls on the Federal government to make 5 promises about the Tracing App», (2020), διαθέσιμο σε https://libertyvictoria.org.au/content/liberty-victoria-calls-federal-government-make-5-promises-about-tracing-app.

119 Βλ. σχετικά European Data Protection Board, «Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak», διαθέσιμο σε https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en .

120 Φερενίκη Παναγοπούλου-Κουτνατζή, «Η προστασία προσωπικών δεδομένων σε περίοδο πανδημίας», (2020), διαθέσιμο σε https://www.constitutionalism.gr/2020-03-28_panagopoulou-privacy-koronavirus/ .

121 Βλ. σχετικά «Complaint & Request for Investigation, Injunction, & Other Relief», διαθέσιμο σε https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

122 Βλ. σχετικά Future Of Privacy Forum, Family Online Safety Inst., «Kids & The Connected Home: Privacy In The Age Of Connected Dolls, Talking Dinosaurs, And Battling Robots», (2016), διαθέσιμο σε https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-

παιχνίδια δημιουργούν νέες προκλήσεις, τόσο αναφορικά με το πλήθος των πληροφοριών που συγκεντρώνουν οι εταιρίες, όσο και με ποιο τρόπο οι πληροφορίες αυτές μπορούν να τύχουν προστασίας και ασφάλειας. Το 90% των συνδεδεμένων παιχνιδιών συγκεντρώνουν πληροφορίες σχετικές με τα παιδιά και το 70% αυτών των συσκευών μεταφέρουν τις πληροφορίες αυτές μέσω μη κρυπτογραφημένων δικτύων, καθιστώντας τις πληροφορίες αυτές ευάλωτες σε πιθανές κυβερνοεπιθέσεις[123]. Πρόσφατα έγινε γνωστό ότι οι προσωπικές πληροφορίες έξι εκατομμυρίων παιδιών και περισσοτέρων από τεσσάρων εκατομμυρίων γονέων, εκτέθηκαν με μία και μόνο επίθεση[124]. Η παραβίαση αυτή όχι μόνο αφύπνισε τις ρυθμιστικές αρχές σχετικά με τα ζητήματα της ιδιωτικότητας των ανηλίκων και τις συσκευές του διαδικτύου των πραγμάτων[125], αλλά επίσης οδήγησε σε επίσημη έρευνα του Κογκρέσου, η οποία κατέδειξε σοβαρές διαρροές ασφαλείας και σε άλλα δύο συνδεδεμένα παιχνίδια[126]. Σύμφωνα με την εταιρία Rapid7 που υπέδειξε τη διαρροή ασφαλείας, «οι περισσότερες εταιρίες που κατασκευάζουν διασυνδεδεμένες συσκευές γενικά και όχι μόνο παιχνίδια, δεν δίνουν μεγάλη προσοχή στην

Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf.

123 Bill Nelson, «Children's Connected Toys: Data Security & Privacy Concerns», Committee On Commerce, Science & Transportation, Office of Oversight and Investigations, Minority Staff Report, (2016).

124 Η εταιρία Vtech συγκέντρωσε προσωπικές πληροφορίες μέσω από τις συνδεδεμένες ταμπλέτες (tablets) της για παιδιά, οι οποίες περιελάμβαναν ονόματα, φύλα, ημερομηνίες γεννήσεως και φωτογραφίες. Τα δεδομένα που είχαν συλλεχθεί από την εταιρία Vtech παραβιάστηκαν, καθιστώντας προσβάσιμες τις πληροφορίες στους εισβολείς - hackers. Βλ. σχετικά «Data Breach on VTech Learning Lodge», διαθέσιμο σε https://www.vtech.com/en/press_release/2015/data-breach-on-vtech-learning-lodge-update/. Βλ. επίσης Daniel Victor, «Security Breach at Toy Maker VTech Includes Data on Children», διαθέσιμο σε https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html.

125 Βλ. σχετικά «FAQ About Cyber Attack on VTech Learning Lodge», διαθέσιμο σε https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/.

126 Για παράδειγμα, το έξυπνο παιχνίδι της εταιρίας Fisher-Price, ένα ασύρματα συνδεδεμένο λούτρινο ζωάκι με τη μορφή αρκούδου, το οποίο ακούει και θυμάται αυτά που λέει το παιδί, ήταν συνδεδεμένο με έναν επισφαλή διακομιστή, ευάλωτο σε πιθανές επιθέσεις. Οι πληροφορίες που συνέλεγε το παιχνίδι αυτό περιελάμβαναν ηλεκτρονικές διευθύνσεις των γονέων και κωδικούς εισόδου, βαφτιστικά ονόματα παιδιών, ημερομηνίες γεννήσεως και φύλα, κωδικούς ασύρματης σύνδεσης και πληροφορίες σχετικές με κινητά τηλέφωνα, πλέον των φωτογραφιών των παιδιών και ακουστικών δεδομένων που ήταν αποθηκευμένα τοπικά στο παιχνίδι. Βλ. σχετικά «Researchers Discover a Not-so-Smart Flaw in Smart Toy Bear», διαθέσιμο σε https://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/researchers-discover-flaw-in-smart-toy-bear.

ασφάλεια»[127]. Όπως περαιτέρω κατέστη σαφές, η διαρροή των προσωπικών πληροφοριών υπονομεύει τα πιθανά οφέλη των παιχνιδιών αυτών για τα παιδιά, δεδομένου ότι δεν είναι όλα τα διασυνδεδεμένα παιχνίδια βελούδινα αρκουδάκια. Η τεχνολογία η οποία είναι συνυφασμένη με το διαδίκτυο των πραγμάτων μπορεί πράγματι να χρησιμοποιηθεί για διαδραστική γνώση και να φέρει επανάσταση στον τομέα της εκπαίδευσης, καθιστώντας την προστασία της ασφάλειας και της ιδιωτικότητας κομβικό σημείο.

5 Διαδίκτυο των σκέψεων

Αν και διανύουμε την εποχή του διαδικτύου των πραγμάτων, μέσω της τεχνητής νοημοσύνης και της ανάπτυξης των δικτύων πέμπτης γενιάς (5G)[128], κάποιοι επιστήμονες οραματίζονται και εργάζονται προς υλοποίηση του «διαδικτύου των Σκέψεων». Πρόκειται για τις διεπαφές του ανθρώπινου εγκεφάλου με κάποιο υπολογιστικό νέφος (human brain/cloud interfaces). Μέσω της σκέψης θα αποκτήσουμε πρόσβαση τόσο στις σκέψεις των άλλων, όσο και στα δεδομένων των μηχανών. Αν και φαντάζει ταινία επιστημονικής φαντασίας, οι επιστήμονες ευαγγελίζονται ένα μέλλον όπου θα μπορούμε νοερά να ερχόμαστε σε προσωπική επαφή με όλη τη γνώση που βρίσκεται αποθηκευμένη σε ψηφιακή μορφή. Αρκεί να θέσουμε νοερά ένα ερώτημα και η απάντηση θα έρχεται και πάλι νοερά και όχι σε κάποια οθόνη, όπως σήμερα[129].

127 Laura Hautala, «Playtime Is Over: Can Smart Toys Ever Be Safe?», διαθέσιμο σε https://www.cnet.com/news/internet-of-things-connected-smart-toys-rsa-security-conference/ και Dan Goodin, «Internet-Connected Hello Barbie Doll Gets Bitten by Nasty Poodle Crypto Bug», διαθέσιμο σε https://arstechnica.com/security/2015/12/internet-connected-hello-barbie-doll-gets-bitten-by-nasty-poodle-crypto-bug.

128 Τα δίκτυα 5G αποτελούν την επόμενη γενιά σύνδεσης κινητών συσκευών στο διαδίκτυο, προσφέροντας ταχύτητες πιο γρήγορες από ποτέ, αλλά και πιο αξιόπιστες συνδέσεις σε smartphones και άλλες συσκευές. Σύμφωνα με τις τελευταίες έρευνες, το δίκτυο 5G θα μπορεί να προσφέρει συνδέσεις πολύ πιο γρήγορες από τις τρέχουσες συνδέσεις, με τις μέσες ταχύτητες λήψης (περίπου 1GBps) να θεωρούνται ο κανόνας. Βλ. σχετικά «Με απλά λόγια: Τι είναι το 5G και πώς πρόκειται να αλλάξει τη ζωή μας;», (2018), διαθέσιμο σε https://www.epixeiro.gr/article/83575 .

Μια διεθνής ομάδα ερευνητών, με επικεφαλής επιστήμονες του Πανεπιστημίου Μπέρκλεϊ της Καλιφόρνια παρουσίασε το εγχείρημα αυτό στο περιοδικό «Frontiers in Neuroscience», θεωρώντας ότι είναι εφικτό να πραγματοποιηθεί μέσα στον 21ο αιώνα, χάρη στην επιστημονική πρόοδο πεδίων, όπως η νανοτεχνολογία[130], η νανοϊατρική[131], η τεχνητή νοημοσύνη και η επιστήμη των υπολογιστών. Στην ίδια παρουσίαση γνωστοποιούν ότι είναι πλέον θέμα χρόνου να συνδεθούν σε πραγματικό χρόνο τα ανθρώπινα εγκεφαλικά κύτταρα με τα δίκτυα του υπολογιστικού νέφους[132]. Το όραμα μιας τέτοιας διεπαφής εγκεφάλου-νέφους προέρχεται από τον Raymond Kurzweil[133], σύμφωνα με τον οποίο «νευρωνικά νανορομπότ θα μπορούσαν να χρησιμοποιηθούν για να συνδέσουν το βιολογικό νεοφλοιό του ανθρωπίνου εγκεφάλου με το συνθετικό «νεοφλοιό» του υπολογιστικού νέφους και με τον τρόπο αυτό θα είναι δυνατός ο άμεσος έλεγχος των σημάτων από και προς τα εγκεφαλικά κύτταρα. Οι ερευνητές πιστεύουν ότι τέτοιες συσκευές νανορομπότ θα κυκλοφορούν μέσα στα ανθρώπινα αιμοφόρα αγγεία, θα διασχίζουν τον αιματοεγκεφαλικό φραγμό και θα αυτοεγκαθίστανται ανάμεσα ή μέσα στα εγκεφαλικά κύτταρα[134]. Στη συνέχεια θα μεταδίδουν ασύρματα κωδικοποιημένες πληροφορίες προς και από ένα δίκτυο υπερυπολογιστών[135] συνδεδεμένων στο «νέφος», επιτυγχάνοντας έτσι σε πραγματικό

129 Βλ. σχετικά Nuno R. B. Martins, Amara Angelica, Krishnan Chakravarthy, Yuriy Svidinenko, Frank J. Boehm, Ioan Opris, Mikhail A. Lebedev, Melanie Swan, Steven A. Garan, Jeffrey V. Rosenfeld, Tad Hogg και Robert A. Freitas Jr, «Human Brain/Cloud Interface», (2019), διαθέσιμο σε https://www.frontiersin.org/articles/10.3389/fnins.2019.00112/full.

130 Ως Νανοτεχνολογία ορίζεται η επιστήμη, η μηχανική και η τεχνολογία στην νανοκλίμακα, δηλαδή στην κλίμακα διαστάσεων από 1 έως 100nm. Κατ' επέκταση, οι λεγόμενες Νανοεπιστήμες και η Νανοτεχνολογία είναι η μελέτη και η χρήση εφαρμογών εξαιρετικά μικρών διαστάσεων σε πολλά επιστημονικά πεδία, όπως η φυσική, η χημεία, η επιστήμη των υλικών και η μηχανικές επιστήμες. Βλ, σχετικά http://nn.physics.auth.gr/index.php?option=com_content&view=article&id=303%3 .

131 Η Νανοϊατρική αφορά στη χρήση νανοδομημένων υλικών ή υλικών στη νανοκλίμακα, κατασκευασμένα με τέτοιο τρόπο ώστε να έχουν αποτελέσματα στο τομέα της Ιατρικής. Βάση των δομών τους είναι να περιλαμβάνουν μία τουλάχιστον χαρακτηριστική διάσταση έως 300 nm. Βλ. σχετικά http://nn.physics.auth.gr/index.php?option=com_content&view=article&id=693%3A2013-11-05-14-35-39&catid=68%3A2010-09-03-21-09-19&Itemid=158&lang=el .

132 Βλ. σχετικά «Από το Διαδίκτυο των Πραγμάτων στο Διαδίκτυο των Σκέψεων», (2019), διαθέσιμο σε https://www.kathimerini.gr/1036966/article/epikairothta/episthmh/apo-to-diadiktyo-twn-pragmatwn-sto-diadiktyo-twn-skeyewn.

133 Αμερικανός φουτουριστής μηχανικός και συγγραφέας.

134 Robert A. Freitas Jr, Ερευνητής του Ινστιτούτου Μοριακής Παραγωγής στην Καλιφόρνια, ό.π. υποσημ. 119.

135 Πρόκειται για υπολογιστικά συστήματα που αξιοποιούνται σε επιστημονικές εφαρμογές, οι οποίες απαιτούν την εκτέλεση πολλών εκατομμυρίων μαθηματικών πράξεων ή την επεξεργασία μεγάλου όγκου δεδομένων. Λόγω αυτών των απαιτήσεων τέτοιου είδους προβλήματα είτε θα χρειάζονταν απαγορευτικά

χρόνο την παρακολούθηση του εγκεφάλου και την άντληση δεδομένων»[136]. Αν και δεν είναι ιδιαίτερα εξελιγμένο, ένα πειραματικό σύστημα ανθρώπινου εγκεφαλικού δικτύου (BrainNet[137]) έχει ήδη δοκιμασθεί, επιτρέποντας την ανταλλαγή πληροφοριών μέσω της σκέψης και του «νέφους» ανάμεσα σε ατομικούς εγκεφάλους.

Οι επιστήμονες θεωρούν ότι το επόμενο βήμα θα είναι η δημιουργία ενός ενιαίου παγκόσμιου υπερ-εγκεφάλου που θα διασυνδέει τα επιμέρους δίκτυα των εγκεφάλων και των «έξυπνων» μηχανών. Με τον τρόπο αυτό, η ατομική ανθρώπινη σκέψη θα έχει μετατραπεί σε συλλογική.[138]. Σύμφωνα με τις εκτιμήσεις της διεθνούς αυτής επιστημονικής ομάδας, ήδη οι σημερινοί υπερυπολογιστές διαθέτουν ταχύτητες επεξεργασίας ικανές να διαχειριστούν τους αναγκαίους τεράστιους όγκους νευρωνικών και ψηφιακών δεδομένων. Η μεταφορά νευρωνικών[139] (εγκεφαλικών) δεδομένων από και προς τους υπερυπολογιστές στο «νέφος» πιθανότατα θα επιφέρει δυσκολίες ως προς τη συσσώρευση αυτών. «Η πρόκληση αφορά όχι μόνο την εύρεση του εύρους ζώνης για μια τέτοια παγκόσμια μεταφορά δεδομένων, αλλά επίσης και το να καταστεί εφικτή η ανταλλαγή δεδομένων με τους νευρώνες μέσω μικροσκοπικών συσκευών ενσωματωμένων βαθιά μέσα στον εγκέφαλο. Μια λύση που προτείνεται από τους ερευνητές είναι η χρήση μαγνητοηλεκτρικών σωματιδίων

μεγάλο χρόνο για να ολοκληρωθούν από έναν απλό υπολογιστή γραφείου είτε λόγω περιορισμένων πόρων (π.χ. κεντρική μνήμη, αποθηκευτικός χώρος) δεν είναι εφικτό να πραγματοποιηθούν καθόλου. Ένας υπερυπολογιστής σήμερα είναι στην πραγματικότητα ένα σύστημα από εκατοντάδες ή και χιλιάδες υπολογιστές (στους οποίους αναφερόμαστε συνήθως ως κόμβους) που επικοινωνούν μεταξύ τους χρησιμοποιώντας ένα πολύ γρήγορο δίκτυο και οι οποίοι συνεργατικά μπορούν να επιλύουν προβλήματα με μεγάλη ταχύτητα. Βλ. σχετικά https://hpc.grnet.gr/supercomputer/ .

136 Σύμφωνα με τον ερευνητή Nuno R. B. Martins του Εθνικού Εργαστηρίου Λόρενς Μπέρκλεϊ «ένα ανθρώπινο σύστημα διεπαφής εγκεφάλου-νέφους μέσω νευρωνανορομποτικής θα επιτρέψει στους ανθρώπους να έχουν άμεση πρόσβαση σε όλη τη συσσωρευμένη ανθρώπινη γνώση που βρίσκεται στο νέφος, πράγμα που θα αναβαθμίσει σημαντικά τις ανθρώπινες ικανότητες μάθησης και νοημοσύνης». βλ. σχετικά ό.π. υποσημ. 119.

137 Βλ. σχετικά https://www.nature.com/articles/s41598-019-41895-7 .

138 Βλ. σχετικά «Διαδίκτυο των Σκέψεων: Η νέα τάση στο Internet;», (2019) διαθέσιμο σε https://www.efsyn.gr/epistimi/epistimonika-nea/206150_diadiktyo-ton-skepseon-i-nea-tasi-sto-internet .

139 Νευρώνας: ένα νευρικό κύτταρο, η δομική και λειτουργική μονάδα του νευρικού συστήματος. Ένας νευρώνας αποτελείται από ένα κυτταρικό σώμα (περικάρυο) και τις αποφύσεις του, έναν άξονα και έναν ή περισσότερους δενδρίτες. Οι νευρώνες λειτουργούν για την εισαγωγή και μετάδοση ώσεων. Μεταδίδουν ώσεις σε άλλους νευρώνες ή άλλα κύτταρα απελευθερώνοντας νευροδιαβιβαστές στις συνάψεις. Εναλλακτικά ένας νευρώνας μπορεί να απελευθερώσει νευροορμόνες στην κυκλοφορία. βλ. σχετικά https://www.iatronet.gr/iatriko-lexiko/nevrwnas.html .

που θα ενισχύουν αποτελεσματικά την επικοινωνία ανάμεσα στα εγκεφαλικά κύτταρα (τους νευρώνες) και το υπολογιστικό «νέφος». Αυτά τα νανοσωματίδια[140] έχουν ήδη χρησιμοποιηθεί σε ζωντανά ποντίκια για να «ζευγαρώσουν» εξωτερικά μαγνητικά πεδία με νευρωνικά ηλεκτρικά πεδία, έτσι ώστε η ενίσχυση των μαγνητικών σημάτων να οδηγεί σε τροποποίηση της ηλεκτρικής δραστηριότητας των νευρώνων. Οι ερευνητές πιστεύουν ότι αυτό μπορεί να δουλέψει και αντίστροφα: τα ηλεκτρικά σήματα που παράγονται από τους νευρώνες και τα νανορομπότ[141] θα μπορούν να ενισχυθούν μέσω των μαγνητοηλεκτρικών σωματιδίων, πράγμα που θα επιτρέψει την ανίχνευση των σημάτων έξω από το κρανίο. Μια από τις μεγαλύτερες προκλήσεις για τη δημιουργία διεπαφών ανθρωπίνου εγκεφάλου-υπολογιστικού νέφους θα είναι με ποιο τρόπο αυτά τα νανοσωματίδια και τα νανορομπότ θα εισαχθούν με ασφάλεια στον εγκέφαλο μέσω της κυκλοφορίας του αίματος. Οι ερευνητές δήλωσαν πάντως αισιόδοξοι ότι, παρά τις τεχνικές δυσκολίες, «ένα διαδίκτυο των Σκέψεων θα έχει γίνει πραγματικότητα έως το τέλος του αιώνα μας»[142].

140 Πρόκειται για σωματίδια διαφορετικών υλικών, φτιαγμένα σε επίπεδο νανοκλίμακας προκειμένου να διαθέτουν βελτιωμένες ιδιότητες σε σύγκριση με τα συμβατικά (όπως αντιμικροβιακή δράση, μεγαλύτερη διάρκεια ζωής κ.ά.). Βλ. σχετικά https://www.chemist.gr .

141 Ως νανορομπότ ορίζεται κάθε τεχνητή μηχανική δομή με κλίμακα μικρότερη του ενός νανόμετρου, δηλαδή 10-9 μέτρα (το πάχος μιας ανθρώπινης τρίχας είναι περίπου 80.000 nm, ενώ το πάχος ενός φύλλου χαρτιού είναι περίπου 100.000 nm). Βλ. σχετικά «Το 2019 φεύγει, τα νανορομπότ έρχονται», (2019), διαθέσιμο σε https://www.liberal.gr/technology/to-2019-feugei-ta-nanorompot-erchontai/279784 .

142 Nuno R. B. Martins, Amara Angelica, Krishnan Chakravarthy, Yuriy Svidinenko, Frank J. Boehm, Ioan Opris, Mikhail A. Lebedev, Melanie Swan, Steven A. Garan, Jeffrey V. Rosenfeld, Tad Hogg και Robert A. Freitas Jr, «Human Brain/Cloud Interface», (2019), διαθέσιμο σε https://www.frontiersin.org/articles/10.3389/fnins.2019.00112/full.

ΔΕΥΤΕΡΟ ΚΕΦΑΛΑΙΟ: Κρυπτονομίσματα

1 Εισαγωγικά

Κατά τη διάρκεια της ιστορίας, το νόμισμα έχει λάβει δύο μορφές: τη φυσική, όπως ο χρυσός και οι πολύτιμοι λίθοι και τη μορφή των νομισμάτων – χαρτονομισμάτων[1]. Το Bitcoin και τα άλλα κρυπτονομίσματα αποτελούν μια τρίτη κατηγορία, τα ψηφιακά νομίσματα ή κρυπτονομίσματα[2], τα οποία λειτουργούν ως συνδυασμός της θεωρίας των παιγνίων[3], της οικονομίας και της κρυπτογραφίας[4].

1 Γεώργιος Καλλιμόπουλος, «Το δίκαιο του χρήματος», εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα, (1993). Βλ. επίσης Glyn Davies και Duncan Connors, «A History of Money», University of Wales Press; 4th Edition, (2016), όπου περιγράφεται ο τρόπος με τον οποίο η μορφή του χρήματος διαμορφώθηκε με την πάροδο του χρόνου και το πώς η βασική λειτουργία της ανταλλαγής αγαθών εξελίχθηκε σε ένα νομισματικό σύστημα βασισμένο σε νομίσματα από πολύτιμα μέταλλα. Από τον 15ο αι. κι εφεξής καθιερώθηκαν τα οικονομικά συστήματα και το νόμισμα έγινε πλέον αλληλένδετο με το εμπόριο, ενώ στη συνέχεια και κυρίως στα μέσα του 18ου αι. εξελίχθηκε σε ένα σταθερό σύστημα βασιζόμενο στο χρυσό.«»

2 Το ηλεκτρονικό χρήμα είναι ένας ευρέως αποδεκτός όρος για κάθε μορφή χρήματος, νομίσματος ή περιουσιακού στοιχείου, το οποίο δεν έχει φυσική μορφή. Τα ψηφιακά νομίσματα είναι μία υποκατηγορία του ηλεκτρονικού χρήματος, τα οποία επίσης δεν έχουν κάποιο φυσικό αντίγραφο. Τα εικονικά νομίσματα είναι υποκατηγορία των ψηφιακών νομισμάτων, τα οποία έχουν δημιουργηθεί διεθνώς ή κυρίως χρησιμοποιούνται για την αγορά τόσο ψηφιακών, όσο και μη ψηφιακών αγαθών (απτών ή του πραγματικού κόσμου). Τα ψηφιακά και τα εικονικά νομίσματα μπορούν να είναι τόσο κεντρικοποιημένα όσο και αποκεντρωμένα. Ένα κεντρικοποιημένο νόμισμα είναι οποιοδήποτε νόμισμα το οποίο έχει δημιουργηθεί και συντηρείται από κάποια κεντρική ομάδα ή οργανισμό, ενώ το αντίθετο ισχύει για τα αποκεντρωμένα νομίσματα. Τα προσομοιούμενα νομίσματα (ή αλλιώς νομίσματα παιχνιδιών) αποτελούν παραδείγματα κεντρικοποιημένων ψηφιακών νομισμάτων. Αυτού του είδους τα νομίσματα δημιουργήθηκαν για την αγορά αντικειμένων μέσα σε ένα σύστημα προσομοίωσης, κυρίως βιντεοπαιχνιδιών, το οποίο σύστημα ανήκει σε μη κυβερνητική εταιρία ή ομάδα. Τα κρυπτονομίσματα αναφέρονται σε οποιασδήποτε μορφής ηλεκτρονικό χρήμα, το οποίο δημιουργήθηκε με τη χρήση τεχνολογιών κρυπτογραφίας για τη ρύθμιση της δημιουργίας τους και τη διασφάλιση της νομιμότητας των συναλλαγών με αυτά. Επίσημα, το Bitcoin μπορεί να περιγραφεί ως αποκεντρωμένο εικονικό κρυπτονόμισμα. Σε κάθε περίπτωση και δεδομένου ότι όλα τα κρυπτονομίσματα αποτελούν αποκεντρωμένα εικονικά νομίσματα, οι δύο όροι μπορούν να χρησιμοποιηθούν εναλλακτικά. Gina C. Pieters, «The Potential Impact of Decentralized Virtual Currency on Monetary Policy», Federal Reserve Bank of Dallas, Globalization and Monetary Policy Institute Annual Report (2016).

3 John von Neumann και Oskar Morgenstern, «Theory of Games and Economic Behaviour», Princeton University (1953). Η «θεωρία παιγνίων» (game theory) ξεκίνησε ως κλάδος των οικονομικών, πάνω σε παιχνίδια μηδενικού αθροίσματος (zero-sum games). Το κύριο αντικείμενό της είναι η ανάλυση των αποφάσεων σε καταστάσεις στρατηγικής αλληλεξάρτησης. Πρόκειται για μία επιστημονική διαδικασία κατά την οποία μπορεί να μελετηθεί - και πιθανότατα προβλεφθεί, με τη χρήση απλών υπολογισμών και λογικής, ο τρόπος με τον οποίο άτομα ή ομάδες ατόμων λαμβάνουν αποφάσεις, σε ένα ανταγωνιστικό μεταξύ τους, περιβάλλον, είναι δηλαδή η μελέτη των διαδικασιών λήψης στρατηγικών αποφάσεων.

4 R. Grinberg, «Bitcoin: An Innovative Alternative Digital Currency», (2011), *Hastings Science & Technology Law Journal,* Vol. 4.

Κάποιοι θεώρησαν ότι το μέλλον των ψηφιακών νομισμάτων γενικά και του Bitcoin ειδικά, θα εξαρτιόταν από την καθημερινή χρήση τους, με την αγορά καταναλωτικών αγαθών ή την αποπληρωμή υποχρεώσεων. Για το λόγο αυτό και για να τα θέσουν σε κυκλοφορία, προχώρησαν στη δημιουργία και τοποθέτηση Αυτόματων Ταμειολογιστικών Μηχανών (ATM) για Bitcoin[5], με στόχο να διευκολύνουν τις μεταφορές νομισμάτων και να ενθαρρύνουν τις τοπικές επιχειρήσεις να δέχονται τέτοιου είδους νομίσματα για τις πληρωμές των πελατών τους. Σήμερα ελάχιστοι είναι αυτοί που χρησιμοποιούν τα Bitcoin για την αγορά αγαθών και υπηρεσιών - και είναι λογικό, από τη στιγμή που η αξία του μεταβάλλεται από εβδομάδα σε εβδομάδα - άλλοτε εκτινάσσεται στα ύψη[6] και άλλοτε ελαχιστοποιείται. Όπως αποδεικνύεται, λίγοι θέλουν να χρησιμοποιήσουν το Bitcoin ως νόμισμα. Οι περισσότεροι του συμπεριφέρονται ως επενδυτική σταθερά, όπως το ασήμι και ο χρυσός[7], κυρίως για όσο χρονικό διάστημα η τιμή του εξακολουθεί και ανεβαίνει.

Τον πρώτο καιρό της εμφάνισης των κρυπτονομισμάτων, κάθε νέα ιστορία αφορούσε σε άτομα με παραβατικές συμπεριφορές που χρησιμοποιούσαν Bitcoin για την αγορά και την πώληση παράνομων αγαθών και υπηρεσιών. Εκείνη την εποχή αποκαλύφθηκε κι ένα τεράστιο δίκτυο διακίνησης ναρκωτικών ουσιών στο σκοτεινό διαδίκτυο (Darknet[8]), μέσω της εταιρίας Silk Road[9]. Πολλοί μεγάλοι ιστότοποι

5 Βλ. σχετικά https://coinatmradar.com .

6 Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto και Kenji Saito, «Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money», *Hitotsubashi Journal of Economics*, 60(1), (2019): 41-60.

7 Michael Maloney, «Guide To Investing in Gold & Silver: Protect Your Financial Future», WealthCycle Press (2015).

8 Dakota Rudesill, James Caverlee και Daniel Sui, «The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box», Woodrow Wilson International Center for Scholars, STIP 03, (2015), Ohio State Public Law Working Paper No. 314. Το «darknet» (ή σκοτεινό δίκτυο) είναι ένα δίκτυο επικάλυψης, που προσεγγίζεται μόνο με συγκεκριμένο λογισμικό ή άδειες, χρησιμοποιώντας συχνά πρωτόκολλα και θύρες μη τυποποιημένων επικοινωνιών. Δύο χαρακτηριστικοί τύποι darknet είναι τα δίκτυα F2F (φίλος προς φίλο) - συνήθως χρησιμοποιούνται για την ανταλλαγή αρχείων με σύνδεση peer-to-peer και τα δίκτυα ανωνυμίας όπως το Tor, τα οποία προκύπτουν μέσω μιας σειράς ανώνυμων συνδέσεων.

9 Judith Aldridge και David Décary-Hétu, «Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation» (2014). Το FBI έκλεισε τον ιστότοπο τον Οκτώβριο του 2013 και οι ιδρυτές του, οι οποίες μεταγενέστερα προσπάθησαν να τον επαναφέρουν με άλλη μορφή, καταδικάστηκαν εντέλει σε ισόβια κάθειρξη.

κρυπτονομισμάτων επλήγησαν από εισβολείς - hackers και κλοπές. Ήταν εύκολο να υποθέσει κάποιος ότι όλα αυτά τα θέματα θα οδηγούσαν τους νομοθέτες να λάβουν μέτρα σε βάρος του Bitcoin. Μολαταύτα, οι ρυθμιστικές Αρχές καθυστέρησαν να λάβουν θέση. Οι οικονομικές υπηρεσίες των ΗΠΑ δεν προχώρησαν σε επίσημες οδηγίες ως προς τη φορολογική αντιμετώπιση του Bitcoin και των άλλων κρυπτονομισμάτων, παρά μόνο το 2014 και στη συνέχεια άρχισε να διερευνάται κατά πόσο η αρχική προσφορά νομισμάτων (ICO[10]), ένα είδος δημόσιας δημοπρασίας νέων κρυπτονομισμάτων, θα έπρεπε να ρυθμιστεί πιο προσεκτικά.

2 Κρυπτονομίσματα και τρίτοι: χρηματιστήριο, χρηματοπιστωτικά ιδρύματα κι επενδυτές.

Όταν το 2013 κάποιος απευθυνόταν σε επενδυτές της Wall Street σχετικά με το Bitcoin και τα άλλα κρυπτονομίσματα, οι αντιδράσεις τους ποίκιλαν. Ελάχιστοι πίστευαν στην επιτυχία των ψηφιακών νομισμάτων και πολλοί συμμερίζονταν την άποψη του διευθύνοντος συμβούλου της εταιρίας JPMorgan Chase, Jamie Dimon, ο οποίος αποκάλεσε το Bitcoin «απάτη[11], κατάλληλη για εγκληματίες κι εμπόρους ναρκωτικών». Εντέλει και η ίδια η Wall Street χρειάστηκε να προσαρμοστεί όταν τελικά ήρθε αντιμέτωπη με ένα προϊόν στο οποίο οι πελάτες της ήθελαν να επενδύσουν[12]. Με τον ίδιο τρόπο που τη δεκαετία του 1980 η άνοδος των

10 Christian Catalini και Joshua S. Gans, «Initial Coin Offerings and the Value of Crypto Tokens», MIT Sloan Research Paper No. 5347-18, Rotman School of Management Working Paper No. 3137213. (2018). Το ICO (Initial Coin Offering) είναι ο τρόπος με τον οποίο μία εταιρία συγκεντρώνει κεφάλαια χωρίς να πωλήσει μετοχές, εκδίδοντας το δικό της κρυπτονόμισμα.

11 Ο Jamie Dimon στο βάρος των πιέσεων που δέχθηκαν τα χρηματοπιστωτικά ιδρύματα υπέρ των κρυπτονομισμάτων, αναγκάστηκε να δηλώσει μεταμέλεια και να αναιρέσει τις δηλώσεις του σε βάρος του Bitcoin – τον Οκτωβριο του 2017 είχε προσθέσει στα όσα ανωτέρω αναφέρονται ότι «εάν είναι κάποιος αρκετά ανόητος για να αγοράσει Bircoin, μία ημέρα θα πληρώσει το τίμημα». Στις επανορθωτικές δηλώσεις του προσέθεσε ότι «η τεχνολογία blockchain, η οποία αποτελεί το θεμέλιο των Bitcoin, είναι πραγματική και ότι είναι σημαντικό να δει κάποιος ξεχωριστά τα οφέλη των κρυπτονομισμάτων». Kottasová, I., «Jamie Dimon regrets calling bitcoin a 'fraud'», (2018). http://money.cnn.com.

12 Charlotte Davis, «»Bitcoin price: Analyst reveals what Wall Street investment WILL mean for the price of BTC», (2018) διαθέσιμο σε https://www.express.co.uk/finance.

χρεωστικών ομολόγων δημιούργησε μία εντελώς νέα επικερδή χρηματοδότηση[13], κατ' αντιστοιχία η γοργή άνοδος του Bitcoin ώθησε και τα πιο παραδοσιακά χρηματοπιστωτικά ιδρύματα στο παιχνίδι. Προέκυψαν δεκάδες αμοιβαία κεφάλαια βασισμένα στα κρυπτονομίσματα και ακόμα και η Goldman Sachs προχώρησε σε εκκαθαρίσεις μελλοντικών συναλλαγών πελατών της σε Bitcoin. Η άφιξη των θεσμικών επενδυτών στην αγορά των κρυπτονομισμάτων άρχισε να κάνει το Bitcoin να δείχνει λιγότερο ως ένα αβέβαιο τεχνολογικό σχέδιο και περισσότερο ως μία αγορά παρόμοια με όλων των άλλων χρεογράφων[14].

Αυτό που θεωρούν οι επενδυτές ως το σημαντικότερο παράγοντα στο πεδίο των κρυπτονομισμάτων είναι η είσοδος των αμοιβαίων κεφαλαίων και άλλων θεσμικών επενδυτών. Το μονοπάτι για τους μεγάλους επενδυτές άνοιξε, μεταξύ άλλων, το Χρηματιστήριο του Σικάγο[15], το οποίο αποφάσισε να καθιερώσει στο μέλλον συμφωνίες σε Bitcoin[16]. Πολλές τράπεζες άρχισαν να συμβαδίζουν με την απόφαση

13 Πριν από λίγα χρόνια η αγορά ομολόγων είχε να επιδείξει μόνο απλές εκδόσεις ομολόγων (plain vanilla), η αποτίμηση των οποίων δεν παρουσίαζε δυσκολίες. Η άνοδος των επιτοκίων και της διακύμανσής τους στο τέλος της δεκαετίας του 1970 και αρχές της δεκαετίας του 1980 είχε σαν αποτέλεσμα την εμφάνιση νέων τύπων ομολόγων όπως τα ομόλογα μηδενικού επιτοκίου (zero-coupon bonds), τα ομόλογα κυμαινομένου επιτοκίου (floating rate notes-FRNs) ή ομόλογα με ενσωματωμένα δικαιώματα αγοράς ή πώλησης (call ή put options). Νικόλαος Βεργής, «Μέτρηση της αποτελεσματικότητας και του κινδύνου των ομολόγων και των ομολογιακών δανείων ως μεθόδου κρατικής κι εταιρικής χρηματοδότησης. Η σύγχρονη διεθνής κι ελληνική πραγματικότητα», Πανεπιστήμιο Μακεδονίας, Τμήμα Λογιστικής και Χρηματοοικονομικής (2010).

14 Jim Kyung, Soo Liew, Richard Ziyuan Li, Tamás Budavári και Avinash Sharma, «Cryptocurrency Investing Examined», (2019), διαθέσιμο σε https://jbba.scholasticahq.com/article/8720-cryptocurrency-investing-examined . Βλ. επίσης Nathaniel Popper, «Bitcoin Sees Wall Street Warm to Trading Virtual Currency», διαθέσιμο σε https://www.nytimes.com και Nathaniel Popper, «One Firm Is Way Ahead of Wall Street on Bitcoin», διαθέσιμο σε https://www.nytimes.com.

15 Το Χρηματιστήριο του Σικάγο (Chicago Stock Exchange - CHX) ιδρύθηκε το Μάρτιο του 1882 και λειτουργεί υπό την επίβλεψη της Επιτροπής Κεφαλαιαγοράς των ΗΠΑ. Βλ. σχετικά https://www.nyse.com/markets/nyse-chicago .

16 Αναλυτές που μίλησαν στο Bloomberg επισημαίνουν ότι η ιλιγγιώδης άνοδος του πρώτου και ισχυρότερου ψηφιακού νομίσματος στην αγορά spot (αγορά όψεως) αποθαρρύνει τους επενδυτές από το να δεσμεύσουν χρήματα σε προθεσμιακά συμβόλαια. Δεν υπάρχει λόγος να επενδύσει κάποιος χιλιάδες δολάρια σε ένα bitcoin για να το εξαργυρώσει στις 17 Ιανουαρίου 2018, αν μπορεί να έχεις τα ίδια κέρδη μέσα σε μία μέρα. Ένας επενδυτής που θέλει μόνον να συμμετέχει σε αυτό ίσως ενθουσιαζεται από τις μεγάλες διακυμάνσεις του νομίσματος στην αγορά spot. Ο επενδυτής, όμως, που θέλει να «κλειδώσει» τα κέρδος του, θα επιλέξει το Χρηματιστήριο του Σικάγο. Συν τοις άλλοις, η διαπραγμάτευση του bitcoin στην προθεσμιακή αγορά του Σικάγο επιτρέπει σε περισσότερους επενδυτές να πειραματιστούν με την ιδέα του ψηφιακού νομίσματος. Επιφυλακτικές είναι, όμως, οι εταιρείες εκκαθάρισης συναλλαγών εξαιτίας των μεγάλων διακυμάνσεων του bitcoin. Φοβούνται ότι θα αναγκαστούν να καλύψουν συμβόλαια που δεν θα μπορούν να πληρώσουν οι πελάτες τους. Σπανίως θα συναντήσει

αυτή και να διαπραγματεύονται σχετικά τις συμφωνίες. Μολαταύτα είναι ακόμη ασαφές το πόσο θα επηρεάσει η αύξηση των συμβάσεων σε Bitcoin τη ζήτηση σε ψηφιακά νομίσματα.

Εκτός από τους μεγάλους επενδυτές και οι μικροί υπήρξαν εξίσου ενεργοί στην αγορά των Bitcoin. Κινήσεις καθημερινών ανθρώπων σε Bitcoin παρατηρήθηκαν στη Νότια Κορέα και την Κίνα, καθώς και στις ΗΠΑ, όπου συγκεντρώθηκαν στην εταιρία με την επωνυμία Coinbase[17], με έδρα το Σαν Φρανσίσκο και δραστηριότητα την παροχή χρηματιστηριακών υπηρεσιών σε Bitcoin. Ενώ η Κίνα υπήρξε η πιο ενεργή αγορά σε Bitcoin, αυτό άλλαξε στην πορεία, καθώς υπήρξε αυστηρότερη μεταχείριση του θέματος από τις Αρχές της[18].

Συνεπεία των ανωτέρω τέθηκε το καίριος προβληματισμός σχετικά με το εάν είναι ασφαλές να εισέλθει κάποιος στην αγορά αυτή. Τα περισσότερα και μεγαλύτερα ανταλλακτήρια Bitcoin δεν διέπονται από νομοθετικές ρυθμίσεις. Η απουσία επιτήρησης σημαίνει ότι ουδείς ελέγχει το εάν αυτά εξασφαλίζουν τα χρήματα των πελατών τους ή εάν οι μεγάλοι επενδυτές είναι σε θέση να χειραγωγήσουν την αξία των νομισμάτων. Ένα από τα μεγαλύτερα ανταλλακτήρια του κόσμου, το Bitfinex[19], έπεσε πολλές φορές θύμα εισβολής - hacking και παρέχει ελάχιστη διαφάνεια ως προς το χώρο διαφύλαξης των χρημάτων του. Ακόμη και τα ανταλλακτήρια που υπόκεινται σε ρυθμίσεις, όπως το Coinbase[20] στις ΗΠΑ, δεν έχουν ελεγχθεί, όπως άλλα μεγάλα χρηματοπιστωτικά ιδρύματα και οι υπηρεσίες του έχουν τεθεί εκτός λειτουργίας σε κρίσιμες στιγμές.

κανείς κάτι τόσο ευμετάβλητο όσο το bitcoin», σχολιάζει ο σύμβουλος επενδύσεων Ζένον Κάπρον στο Bloomberg. «Το bitcoin έκανε πρεμιέρα στο Χρηματιστήριο του Σικάγου», (2017), διαθέσιμο σε https://www.kathimerini.gr/economy/international/938841/to-bitcoin-ekane-premiera-sto-chrimatistirio-toy-sikagoy/ .

17 Ιδρύθηκε τον Ιούνιο του 2012 και αποτελεί, αφενός μεν ένα πορτοφόλι ψηφιακών νομισμάτων, αφετέρου δε μία πλατφόρμα όπου έμποροι και καταναλωτές μπορούν να κάνουν συναλλαγές με τα νέα ψηφιακά νομίσματα, όπως το Bitcoin, το Ethereum και το Litecoin. Η έδρα του βρίσκεται στο Σαν Φρανσίσκο της Καλιφόρνια. Διαθέσιμο σε https://www.coinbase.com.

18 Lerong Lu, «Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response», *Butterworths Journal of International Banking and Financial Law* (2018), Vol. 33(3), (2018) 178-182.

19 Evelyn Cheng, «Cyberattack temporarily hits bitcoin exchange Bitfinex», διαθέσιμο σε https://www.cnbc.com.

20 Ό.π. σχετικά με το Coinbase.

3 Προβλήματα από τη χρήση των κρυπτονομισμάτων

Τον Ιούλιο του 2017 συνελήφθη στην Ελλάδα ένας Ρώσος πολίτης με την κατηγορία ότι διαχειριζόταν ένα ανταλλακτήριο Bitcoin στη μαύρη αγορά, το οποίο συνέβαλε στο ξέπλυμα δισεκατομμυρίων δολαρίων και υπήρξε ο σύνδεσμος για διάφορες εγκληματικές επιχειρήσεις, σύμφωνα πάντα με το ομοσπονδιακό κατηγορητήριο[21]. Το κατηγορητήριο αυτό που δόθηκε στη δημοσιότητα, περιείχε μία σειρά από παράνομες δραστηριότητες, τις οποίες διευκόλυνε το ανταλλακτήριο Bitcoin (γνωστό ως BTC-E[22]) και οι οποίες συμπεριελάμβαναν απάτες με απαίτηση λύτρων, κλοπές ταυτοτήτων, διακίνηση ναρκωτικών ουσιών και δημόσια διαφθορά. Οι εμπλεκόμενοι που αφαίρεσαν ή απέσπασαν Bitcoin από τα θύματά τους μετέφεραν τα ψηφιακά νομίσματα στο BTC-E, το οποίο στη συνέχεια τα μετέτρεπε σε φυσικά νομίσματα, με τη χρήση ενός πλήθους τραπεζικών λογαριασμών που ανήκαν σε εταιρίες – βιτρίνες. Το BTC-E ιδρύθηκε το 2011, την εποχή που το Bitcoin άρχιζε να κερδίζει για πρώτη φορά σε αξία. Η ταυτότητα των χειριστών του ανταλλακτηρίου παρέμεινε μυστική, ακόμα και όταν άλλα μεγάλα ανταλλακτήρια Bitcoin προσπάθησαν να παρουσιάσουν τις εργασίες τους πιο διαφανείς και φιλικές προς τις Αρχές [23].

Είναι προφανές ότι δεν χρειάζεται να έχει κάποιος ανασφάλειες απέναντι στην τεχνολογία για να ανησυχήσει από τα προβλήματα που προκάλεσε η απότομη άνοδος των κρυπτονομισμάτων στα τέλη του έτους 2017[24]. διαδικτυακές απάτες έκαναν την

21 *ΣτΕ Ολομ. 49/2021*: με την απόφαση 49/2021 της Ολομέλειας του Συμβουλίου της Επικρατείας απερρίφθη η αίτηση ακυρώσεως που άσκησαν η σύζυγος και τα ανήλικα τέκνα του, κατά της απόφασης του Υπουργού Δικαιοσύνης με την οποία διετάχθη η έκδοση και παράδοσή του στις δικαστικές Αρχές της Γαλλίας, των Ηνωμένων Πολιτειών της Αμερικής και της Ρωσικής Ομοσπονδίας. Βλ. επίσης Γιάννης Παπαδόπουλος, «Το «ξέπλυμα» ψηφιακών λύτρων και η σύλληψη Ρώσου στη Χαλκιδική», διαθέσιμο σε https://www.kathimerini.gr/920181/article/epikairothta/ellada/to-3eplyma-yhfiakwn-lytrwn-kai-h-syllhyh-rwsoy-sth-xalkidikh.

22 Η πλατφόρμα BTC-E, η οποία ιδρύθηκε το 2011, έκλεισε έπειτα από παρέμβαση του FBI τον Ιούλιο του 2017 και ξαναάνοιξε το Σεπτέμβριο του ίδιου έτους, με νέο domain name, το WEX.nz. Jon Buck, «Former Bitcoin Exchange BTC-e Reopens as WEX.nz», διαθέσιμο σε https://cointelegraph.com/news/former-bitcoin-exchange-btc-e-reopens-as-wexnz.

23 Nathaniel Popper, «Bitcoin exchange was a nexus of crime, indictment says», διαθέσιμο σε https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html.

24 Στις αρχές του έτους, οι πλατφόρμες των διαφόρων παρόχων χρηματιστηριακής πληροφόρησης, όπως το Bloomberg και το Reuters, παρακολουθούσαν και ανέφεραν τα στατιστικά δεδομένα άνω των 100

εμφάνισή τους, ενώ εισβολείς - hackers αποστράγγιξαν κεφάλαια από διαδικτυακές συναλλαγές. Το εύρος των προβλημάτων αυτών αρχίζει να γίνεται πιο ξεκάθαρο από τη στιγμή που τα ψηφιακά νομίσματα έχασαν περισσότερο από το μισό της αξίας τους στις αρχές του Ιανουαρίου 2018, με την αξία του Bitcoin ειδικά να πέφτει κάτω από τα 7.000$[25]. Οι ρυθμιστικές Αρχές των κρατών φάνηκαν ανίκανες να συμβαδίσουν με την άνοδο των κρυπτονομισμάτων[26] και σημάδια προβληματισμού εμφανίστηκαν σχεδόν σε κάθε επίπεδο αναφοράς - από τις μεγαλύτερες συναλλαγές μέχρι τους νέους ιστότοπους και τα κανάλια συνομιλίας (chat rooms), όπου γινόταν συζήτηση για τη νέα επενδυτική φρενίτιδα.

Οι δύο βασικές ρυθμιστικές Αρχές για θέματα τεχνολογίας στις ΗΠΑ, η Επιτροπή Κεφαλαιαγοράς (Securities and Exchange Commission)[27] και η Επιτροπή Εμπορικών Προθεσμιακών Συμβάσεων (Commodity Futures Trading Commission)[28] κατέληξαν να έχουν ελάχιστες εξουσίες άσκησης εποπτείας στην εκκολαπτόμενη Αγορά των κρυπτονομισμάτων. Η απάντηση στο πρόβλημα θα ήταν είτε να δοθούν νέες

κρυπτονομισμάτων, πέραν των πλέον γνωστών Bitcoin, Etherium και Ripple. Είναι χαρακτηριστικό ότι 9 κρυπτονομίσματα εμφάνιζαν κεφαλαιοποίηση άνω των 10 δισεκατομμυρίων δολαρίων έκαστο, ενώ η κεφαλαιοποίηση των τριών δημοφιλέστερων κρυπτονομισμάτων ξεπερνούσε τα 400 δισεκατομμύρια δολάρια. Οι αποδόσεις έτους κατά το 2017, της τάξεως του 1,318% για το πολυσυζητημένο Bitcoin, αλλά και 36.000% για το λιγότερο γνωστό Ripple, σε καμία περίπτωση δεν θα μπορούσαν να αφήσουν ασυγκίνητο το μέσο προφίλ επενδυτή. Την ίδια στιγμή ωστόσο, οι ετήσιες μεταβλητότητες ύψους, για παράδειγμα, 127% για το Etherium και 183% για το Ripple, προσδιορίζουν επενδύσεις εξαιρετικά υψηλού κινδύνου. Αναφέρεται χαρακτηριστικά ότι μια αρκετά δημοφιλής μετρική κινδύνου στο πεδίο των χρηματοοικονομικών, η λεγόμενη υπό συνθήκη αξία κινδύνου (Conditional Value at Risk, CVAR), υπολογίζεται για το Etherium στο 25%, σε επίπεδο εμπιστοσύνης 99%. Αυτό σημαίνει ότι ένας επενδυτής θα μπορούσε θεωρητικά μόνο σε μια ημέρα να απωλέσει μεσοσταθμικά το 1/4 του κεφαλαίου του, με πιθανότητα 1%. Χ. Δούκας, Π. Ξυδώνας, «Άποψη: Κρυπτονομίσματα και ενεργειακή παραδοξότητα», διαθέσιμο σε https://www.kathimerini.gr/943122/article/oikonomia/ellhnikh-oikonomia/apoyh-kryptonomismata-kai-energeiakh-parado3othta.

25 Βλ. σχετικά https://www.coindesk.com/price

26 Asress Adimi Gikay, «Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union Law», *9 Case W. Res. J.L. Tech. & Internet 1* (2018).

27 Σε μία εποχή διαφορετικών πολιτικών σχεδιασμών σχετικά με το μέλλον, η Επιτροπή Κεφαλαιαγοράς των ΗΠΑ θα χρειαστεί να αντιμετωπίσει προκλήσεις, οι οποίες προκύπτουν από ένα ολοένα αυξανόμενο και αυτοματοποιημένο περιβάλλον διεθνών αξιογράφων, όπως επίσης και από το παραδοσιακό καθήκον της εξισορρόπησης των αναγκών, τόσο των επενδυτών του λιανικού εμπορίου, όσο και των θεσμικών επενδυτών. Βλ. σχετικά «The Future of the Securities and Exchange Commission in a Changing World», Κέντρο Στρατηγικής και Διεθνών Σπουδών, Ουάσιγκτον (2015).

28 Πρόκειται για μία ανεξάρτητη κυβερνητική αρχή των ΗΠΑ, η οποία ιδρύθηκε το 1974 με σκοπό να ρυθμίζει τις αγορές συμβολαίων μελλοντικής εκπλήρωσης και δικαιωμάτων προαίρεσης. Βλ. σχετικά https://www.cftc.gov.

αρμοδιότητες στις δύο Αρχές ή να δημιουργηθεί μία νέα υπηρεσία αρμόδια για τα θέματα αυτά. Οι Διοικητές των Αρχών αυτών έχουν επανειλημμένα υπογραμμίσει τους κινδύνους που προκύπτουν από τις πλατφόρμες ανταλλαγής κρυπτονομισμάτων, οι οποίες αυτοαποκαλούνται ανταλλακτήρια και οι οποίες δίνουν εσφαλμένα την εντύπωση ότι είναι νομικά οριοθετημένες. Οι επενδυτές, οι οποίοι κάνουν χρήση αυτών των μέσων, δεν απολαμβάνουν της προστασίας που θα απολάμβαναν, εάν συναλλάσσονταν μέσω χρηματιστών σε καταχωρημένα ανταλλακτήρια – χρηματιστήρια. Κι ενώ οποιαδήποτε πράξη κλοπής θα μπορούσε να αντιμετωπιστεί μέσω των κοινών διατάξεων του Δικαίου (διότι και τα κρυπτονομίσματα αποτελούν μία μορφή ιδιοκτησίας, παρότι άυλα), μολαταύτα, αφενός μεν η ποινική δίωξη δεν αποτελεί ένα ιδιαίτερα αποτελεσματικό όπλο κατά των εισβολέων – hackers, οι οποίοι λεηλατούν τα ηλεκτρονικά πορτοφόλια, αφετέρου τα ανταλλακτήρια βρίσκονται διασκορπισμένα ανά τον κόσμο, οπότε η εύρεση των υπευθύνων είναι μία μεγάλη πρόκληση[29].

Η επιβολή νομικών ρυθμίσεων στα ανταλλακτήρια θα αποτελούσε ένα σημαντικό βήμα για την εξασφάλιση των συναλλαγών που πραγματοποιούνται σε αυτά. Αυτό, όμως, θα είχε σημαντικό κόστος, διότι οι απαιτήσεις συμμόρφωσης και η υποχρέωση υποβολής εκθέσεων για ένα ανταλλακτήριο είναι κομβικές. Η λειτουργία τους με την ελάχιστη δυνατή κυβερνητική επίβλεψη υπήρξε σημείο αναφοράς για τους υποστηρικτές των κρυπτονομισμάτων, αλλά η άνοδος της αγοράς, η οποία έδωσε πάτημα σε μεγάλης κλίμακας παράνομες δραστηριότητες, τροφοδοτεί την ανάγκη για λογοδοσία.

Η απότομη απώλεια της αξίας των κρυπτονομισμάτων στο μισό, από τον Ιανουάριο του 2018 κι εφεξής, υπήρξε αναπάντεχη. Οι επικεφαλής των βασικών ρυθμιστικών αρχών δήλωσαν ότι η κατάσταση παρουσίασε μία απρόσμενη πρόκληση[30]. Μία από

29 Peter J. Henning, «Should Congress Create a Crypto-Cop?», διαθέσιμο σε https://nyti.ms.

30 Αυτές οι αγορές είναι νέες, εξελισσόμενες και διεθνείς, ανέφεραν σε άρθρο τους στην εφημερίδα The Wall Street Journal οι Jay Clayton και Christopher Giancarlo, Πρόεδροι της Αμερικανικής Επιτροπής Κεφαλαιαγοράς και της Επιτροπής Εμπορικών Προθεσμιακών Συμβάσεων, αντίστοιχα. Και ως τέτοιες, απαιτούν από εμάς να είμαστε ευέλικτοι και να κοιτάμε μπροστά. Jay Clayton και J. Christopher Giancarlo, «Regulators Are Looking at Cryptocurrency», διαθέσιμο σε https://www.wsj.com.

αυτές τις προκλήσεις που αντιμετωπίζουν είναι το ποσοστό της παραπλανητικής δραστηριότητας που εμφανίζεται στις αγορές των κρυπτονομισμάτων και σε τι επίπεδο μπορούν να το ελέγξουν νόμιμα. Κάποιες διαδικτυακές ομάδες προσπαθούν να χειραγωγήσουν τις αξίες των ψηφιακών νομισμάτων, κάτι που είναι γνωστό ως σύστημα «pump-and-dump»[31]. Παραπλήσιες τακτικές με μετοχές είναι παράνομες, αλλά τα άτομα που διαχειρίζονται τις ομάδες αυτές δήλωσαν ότι δεν θεώρησαν ότι θα εφαρμόζονταν και στα ψηφιακά νομίσματα οι ίδιοι κανόνες με τις μετοχές.

Με το δεδομένο ότι οι ρυθμιστικές Αρχές άργησαν να αντιδράσουν στα θέματα αυτά, ανέλαβε σημαντικό ρόλο ο ιδιωτικός τομέας. Το Facebook[32] και το Twitter[33] ανακοίνωσαν στις αρχές Φεβρουαρίου και Μαρτίου 2018 αντίστοιχα ότι δεν θα επέτρεπαν εφεξής τις διαφημίσεις που σχετίζονται με ψηφιακά νομίσματα. Επίσης, η JPMorgan Chase και η Bank of America δήλωσαν ότι θα αποθάρρυναν τους πελάτες τους από τη χρήση καρτών για την αγορά κρυπτονομισμάτων. Το παράδειγμά τους ακολούθησε και η Citigroup[34]. Επίσης, οι επενδυτές έχουν εκφράσει ιδιαίτερες ανησυχίες σχετικά με το μεγαλύτερο ανταλλακτήριο Bitcoin του κόσμου, το Bitfinex[35], το οποίο παρέχει ελάχιστες πληροφορίες σχετικά με τις μεθόδους του και έχει εγείρει ανησυχίες ως προς τη φερεγγυότητά του ή την εμπλοκή του στη χειραγώγηση της αξίας του Bitcoin[36].

31 Η δόλια πρακτική του να ενθαρρύνονται επενδυτές στην αγορά μεριδίων μίας εταιρίας με στόχο την τεχνητή άνοδο της αξίας της μετοχής και στη συνέχεια την πώληση των μετοχών όσο η αξία τους είναι υψηλή. Christian Leuz, Steffen Meyer, Maximilian Muhn, Eugene Soltes και Andreas Hackethal, «Who Falls Prey to the Wolf of Wall Street? Investor Participation in Market Manipulation» διαθέσιμο σε https://ideas.repec.org/p/nbr/nberwo/24083.html (2017).

32 Brian Fung, «Facebook is banning ads for bitcoin and other cryptocurrencies», (2018), διαθέσιμο σε https://www.washingtonpost.com/news/the-switch/wp/2018/01/30/facebook-bans-misleading-advertisements-for-cryptocurrencies-including-bitcoin.

33 Thomas Wilson, «Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind», (2018), διαθέσιμο σε https://www.independent.co.uk/news/business/analysis-and-features/twitter-ban-cryptocurrency-adverts-regulators-bitcoin-facebook-social-media-a8277176.html.

34 Andrew Liptak, «Three major banks confirm that they won't allow cryptocurrency transactions with their credit cards», (2018), διαθέσιμο σε https://www.theverge.com/2018/2/4/16971666/cryptocurrency-bitcoin-jpmorgan-chase-bank-of-america-citigroup-credit-card.

35 Πρόκειται για μία πλατφόρμα ανταλλαγής ψηφιακών περιουσιακών στοιχείων, η οποία προσφέρει υπηρεσίες σύγχρονων τεχνολογιών και παρόχους παγκόσμιας ρευστότητας σε όσους ενδιαφέρονται για ανταλλαγή ψηφιακών νομισμάτων. Ιδρύθηκε το 2012. Βλ. σχετικά https://www.bitfinex.com.

36 Nathaniel Popper, «As Bitcoin bubble loses air, frauds and flaws rise to surface», διαθέσιμο σε https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html.

Περαιτέρω, η Ν. Κορέα, μία από τις χώρες που υιοθέτησαν σε εξαιρετικά μεγάλο βαθμό την τεχνολογία των κρυπτονομισμάτων[37] εισήγαγε το Μάρτιο του 2020 ειδικές διατάξεις για τη ρύθμιση και νομιμοποίηση των κρυπτονομισμάτων και των συναλλαγών με αυτά. Συγκεκριμένα, εγκρίθηκε η τροποποίηση των διατάξεων περί χρηματοπιστωτικών υπηρεσιών της χώρας, μέσω των οποίων (διατάξεων) θα εξουσιοδοτούνται οι χρηματοοικονομικοί ρυθμιστικοί φορείς της Κορέας να εποπτεύουν αποτελεσματικά τη δημιουργούμενη βιομηχανία και να αναπτύξουν κανόνες για την καταπολέμηση, μεταξύ άλλων διαδικασιών, της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Πρόκειται για μία μεθοδευμένη κίνηση που αποδεικνύει την αυξανόμενη αποδοχή της τεχνολογίας blockchain και ιδιαίτερα των κρυπτονομισμάτων στο πλαίσιο των χρηματοπιστωτικών υπηρεσιών σε τοπικό και παγκόσμιο επίπεδο.

4 Ειδικότερα θέματα κατά τη χρήση των κρυπτονομισμάτων

Η παραγωγή ενός Bitcoin απαιτεί μεγάλη ποσότητα ηλεκτρικής ενέργειας. Στον κόσμο των κρυπτονομισμάτων η διαδικασία αυτή ονομάζεται «εξόρυξη» (mining)[38]. Η ενέργεια που απαιτείται για την παραγωγή κάθε ψηφιακού νομίσματος ισοδυναμεί

37 Η Ν. Κορέα υπήρξε στο προσκήνιο κατά την έκρηξη των κρυπτονομισμάτων και αποτελεί μία από τις λίγες χώρες με τόσο ευρεία αποδοχή της τεχνολογίας. Έρευνες κατά το 2017 έδειξαν ότι περισσότερο από το ένα τρίτο των εργαζομένων στη χώρα υπήρξαν ενεργοί επενδυτές σε κρυπτονομίσματα, όπως τα Bitcoin και Ethereum. Η μεγαλύτερη πόλη της χώρας, η Σεούλ προχώρησε στη δημιουργία του δικού της κρυπτονομίσματος, το S-coin, το οποίο σχεδιάστηκε με στόχο να περιορίσει τη φρενίτιδα. Danny Crichton, «South Korea passes one of the world's first comprehensive cryptocurrency laws», διαθέσιμο σε https://techcrunch.com/2020/03/05/south-korea-passes-one-of-the-worlds-first-comprehensive-cryptocurrency-laws.

38 Τα νέα Bitcoin δημιουργούνται μέσω μίας αποκεντρωμένης διαδικασίας που καλείται εξόρυξη – mining και μέσω της οποίας τα άτομα επιβραβεύονται από το δίκτυο για τις υπηρεσίες τους. Η εξορύκτες (miners) Bitcoin επεξεργάζονται συναλλαγές και ασφαλίζουν το δίκτυο χρησιμοποιώντας εξειδικευμένο λογισμικό (hardware) και σε αντάλλαγμα συλλέγουν νέα bitcoins. Καμία κεντρική εξουσία ή προγραμματιστής δεν έχει τη δύναμη να ελέγξει ή να κατευθύνει το σύστημα για να αυξήσει τα παραγόμενα κέρδη. Τα Bitcoin δημιουργούνται με προβλέψιμο ρυθμό που ολοένα μειώνεται. Ο αριθμός των νέων Bitcoin που δημιουργείται κάθε χρόνο αυτόματα μειώνεται στο μισό, προοδευτικά, μέχρι η έκδοσή τους να σταματήσει εντελώς όταν εξορυχθούν στο σύνολο 21 εκατομμύρια Bitcoin. Marc Bresett, «Bitcoin: What You Need To Know About The Cryptocurrency», independently published (2017).

με την ενέργεια που καταναλώνει ένα μέσο αμερικανικό νοικοκυριό σε δύο χρόνια. Το σύνολο του δικτύου των υπολογιστών που είναι συνδεδεμένο με το δίκτυο Bitcoin καταναλώνει τόση ενέργεια καθημερινά, όση μία χώρα[39]. Το ίδιο ισχύει και με το δίκτυο που υποστηρίζει το Ethereum, το δεύτερο σε αξία ψηφιακό νόμισμα. Και όπως ήταν αναμενόμενο, η κατανάλωση ενέργειας αυτών των συστημάτων αυξήθηκε με την εκτίναξη της αξίας των νομισμάτων, οδηγώντας σε μία σθεναρή αντιπαράθεση ανάμεσα στους υποστηρικτές των δύο νομισμάτων. Εντούτοις, οι λάτρεις της τεχνολογίας των κρυπτονομισμάτων θεωρούν ότι η κατανάλωση ενέργειας αξίζει τον κόπο μπροστά στο σημαντικότερο σκοπό της εξασφάλισης των δικτύων του Bitcoin και του Ethereum και τη δημιουργία μίας νέου είδους χρηματοπιστωτικής υποδομής, ελεύθερης από παρεμβάσεις τραπεζών και κυβερνήσεων[40].

Ειδικότερα, όλοι οι υπολογιστές που εμπλέκονται στην εξόρυξη των νομισμάτων βρίσκονται σε ένα διαρκή αγώνα δρόμου, στην προσπάθειά τους να βρουν μία συγκεκριμένη, σχετικά τυχαία απάντηση σε ένα μαθηματικό αλγόριθμο. Ο αλγόριθμος αυτός είναι τόσο σύνθετος που ο μόνος τρόπος να εξευρεθεί η επιθυμητή λύση είναι η εκτέλεση όσο το δυνατόν περισσότερων περιπτώσεων[41]. Αλλά κάθε περίπτωση συνεπάγεται περισσότερη ενέργεια και ηλεκτρισμό. Έχει υπολογιστεί ότι κάθε συναλλαγή σε Bitcoin απαιτεί 80.000 φορές περισσότερη ενέργεια από κάθε συναλλαγή σε κάρτα Visa. Άλλοι υποστηρίζουν ότι και η παραγωγή και η διατήρηση του φυσικού χρήματος και του χρυσού επίσης απαιτεί μεγάλες ποσότητες ενέργειας, σε κάποιες περιπτώσεις όσο και η χρήση του Bitcoin ή και περισσότερη[42].

---

39 Mishra, S., P., Jacob, V., Radhakrishnan, S. «Bitcoin Mining and Its Cost» (2017).

40 Nathaniel Popper, «There is nothing virtual about Bitcoin's energy appetite», διαθέσιμο σε https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

41 Kelvin Wang, «Bitcoin: Everything You Need To Know: (blockchain and Cryptocurrency technologies, Internet Money Guide on Trading, Making and Mining, Digital Gold Rush)», CreateSpace Independent Publishing Platform (2017).

42 Reuben Jackson «Bitcoin mining uses as much energy as mining for gold, according to new research» (2018), διαθέσιμο σε https://www.weforum.org/agenda/2018/11/study-reveals-that-bitcoin-mining-uses-as-much-energy-as-mining-for-gold/ .

Οι θιασώτες των κρυπτονομισμάτων υποστηρίζουν ότι όσοι ασχολούνται με την εξόρυξη Bitcoin έχουν την τάση να τοποθετούν τα συστήματά τους κοντά σε φθηνές και συχνά πράσινες πηγές ενέργειας. Πολλές εταιρίες εξόρυξης τοποθέτησαν τους διακομιστές τους κοντά σε γεωθερμικά πεδία ενέργειας στην Ισλανδία και υδροηλεκτρικά πεδία ενέργειας στην Πολιτεία της Ουάσινγκτον. Από την άλλη, τα ψηφιακά νομίσματα Ripple[43] και Stellar[44], τα οποία δημιουργήθηκαν μετά από το Bitcoin, έχουν σχεδιαστεί να μην απαιτούν ηλεκτρική ενέργεια κατά την εξόρυξή τους[45]. Πιθανόν η μεγαλύτερη αλλαγή να προέλθει από νέες τεχνικές εξόρυξης, τις οποίες χρησιμοποιούν ήδη ψηφιακά νομίσματα μικρότερης εμβέλειας. Η νέα τεχνική, γνωστή ως «proof of stake» (απόδειξη συμμετοχής[46]), μοιράζει νέα νομίσματα σε άτομα που μπορούν να αποδείξουν ότι έχουν ήδη νομίσματα στην κατοχή τους, ενώ η υπάρχουσα μέθοδος, η οποία βασίζεται αποκλειστικά στην ενέργεια του υπολογιστή ονομάζεται «proof of work» (απόδειξη εργασίας)[47]. Με αυτή τη μέθοδο, οι λογαριασμοί και οι άνθρωποι που αποκτούν νέα νομίσματα δεν χρειάζεται να έχουν ήδη άλλα στην κατοχή τους, αλλά απλά απαιτείται πλήθος υπολογιστών να λάβουν μέρος στον αγώνα δρόμου εξόρυξης. Η νέα αυτή μέθοδος ενισχύεται τόσο λόγω της ανησυχίας για την κατανάλωση ενέργειας, όσο και λόγω της πεποιθήσεως ότι θα οδηγήσει σε λιγότερους κεντρικούς υπολογιστές που επιβλέπουν το σύστημα. Δεν είναι καθόλου ξεκάθαρο, όμως, εάν η μέθοδος αυτή θα είναι εξίσου ασφαλής όσο αυτή που χρησιμοποιείται από τα Bitcoin. Και οι νομικοί που υποστηρίζουν το

43 Βλ. για ορισμό κατωτέρω σχετικό υποκεφάλαιο.

44 Βλ. για ορισμό κατωτέρω σχετικό υποκεφάλαιο.

45 Helena Bedwell, Vanessa Dezem, Stephen Stapczynski και Jonathan Tirone, «The Cost of Crypto Is Turning Miners Towards Green Power», διαθέσιμο σε.https://www.bloomberg.com/news/articles/2018-02-04/power-hungry-crypto-mines-clean-up-as-cost-of-electricity-grows.

46 «Proof of Stake» (PoS): πρόκειται για εναλλακτική μορφή επαλήθευσης κι επιβεβαίωσης των συναλλαγών. Ο «επαληθευτής» – Validator επιλέγεται ανάλογα με τον αριθμό των συμμετοχών - νομισμάτων που έχει στο πορτοφόλι του και τη χρονική προτεραιότητα κάθε συμμετοχής. Αυτό επιτρέπει τη δημιουργία ενός έμπιστου και διανεμόμενου δικτύου με πιστούς επαληθευτές, οι οποίοι κερδίζουν μέρος ή το σύνολο των εξόδων της συναλλαγής. Nicolas Houy, «It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency» (2014).

47 «Proof of Work» (PoW): η επιβεβαίωση της εργασίας που έχει πραγματοποιηθεί και αποδεικνύεται ότι είναι σωστή. Το Bitcoin και άλλα εναλλακτικά κρυπτονομίσματα ακολουθούν αυτή την πρακτική για να εξασφαλίσουν ότι η γνησιότητα της αλυσίδας είναι σωστή. Yogesh Malhotra, «Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System» (2013).

Bitcoin, θεωρούν ότι με τη νέα πρόταση θα χαθούν όλες οι ιδιότητες που καθιστούν πολύτιμα τα κρυπτονομίσματα[48].

Τα κρυπτονομίσματα υποστηρίζεται ότι έχουν ιδιαίτερη απήχηση στους millennials[49] στις ΗΠΑ, οι οποίοι ενηλικιώθηκαν μέσα στην οικονομική κρίση και τώρα βλέπουν να απειλείται η σταθερότητα της παγκόσμιας οικονομίας[50]. Σε αντίθεση με τις προηγούμενες γενιές, πολλοί από αυτούς δεν έχουν συντάξεις, είναι δύσπιστοι στην επένδυση χρημάτων σε αμοιβαία κεφάλαια και είναι απόλυτα εξοικειωμένοι με την απόκτηση ψηφιακών περιουσιακών στοιχείων που έχουν ασαφή αξία. Καθώς ο δρόμος προς τη σταθερότητα που άλλοτε προσέφεραν η ανώτερη και μεσαία τάξη παρεμποδίζεται από τα δάνεια, τα τεράστια κόστη για τη συντήρηση των ιδιοκτησιών και την επισφαλή αγορά εργασίας, αυτοί οι επενδυτές βλέπουν τα κρυπτονομίσματα ως το πιο ρηξικέλευθο, αν όχι ουτοπικό, μέσο επένδυσης χρημάτων. Το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης βρίθουν από κερδοσκόπους, οι οποίοι θεωρούν τα ψηφιακά νομίσματα ως λαχνούς λαχείου. Για τους υποαπασχολούμενους, έστω και η

48 Nathaniel Popper, «There is nothing virtual about Bitcoin's energy appetite», διαθέσιμο σε https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

49 Οι Millennials ή αλλιώς Generation Y, είναι η γενιά στην οποία ανήκουν όσοι γεννήθηκαν μεταξύ του 1980 και του 2000. Είναι νέοι, εθισμένοι στην τεχνολογία, άθεοι (σε μεγαλύτερο ποσοστό από την προηγούμενη γενιά) και σε σημαντικό ποσοστό άνεργοι (συγκριτικά με τους γονείς τους στην ίδια ηλικία), ως εκ τούτου με χαμηλότερη αγοραστική δύναμη - ο μέσος όρος των εισοδημάτων τους έχει μειωθεί σε διπλάσιο ποσοστό από αυτό του γενικού πληθυσμού των ενηλίκων. Σύμφωνα με τους ερευνητές, πρόκειται για άτομα που παραμένουν περισσότερο χρόνο κάτω από την οικογενειακή στέγη, που αποταμιεύουν ελάχιστα και επιδιώκουν την εμπειρία, όχι την ιδιοκτησία - το 78% των Millennials θα προτιμούσε να ξοδέψει χρήματα για μια εμπειρία, παρά για κάποιο υλικό αγαθό. Ήδη, η οικονομία και οι αγορές έχουν αρχίσει να προσαρμόζονται στις ανάγκες και επιθυμίες της γενιάς αυτής. Οι δαπάνες τους προσανατολίζονται σε τομείς όπως ταξίδια, ψυχαγωγία, τεχνολογία, διαδικτυακό στοιχηματισμό, social media, συνδρομητική τηλεόραση, αλυσίδες εστιατορίων και πλατφόρμες ψηφιακής διανομής ή αναπαραγωγής βίντεο και μουσικής. Κάνουν αγορές μέσω διαδικτύου, αναζητούν κουπόνια, βλέπουν ελάχιστα τηλεόραση κι επιλέγουν το διαδίκτυο για την ενημέρωση και τη διασκέδασή τους. Ιδιαίτερα στις χώρες της ΝΑ Ευρώπης, οι Millennials είναι μορφωμένοι, με αβέβαιο όμως μέλλον. Πολλοί εξ αυτών βρίσκονται εκτός της αγοράς εργασίας ή υποαπασχολούνται, ενώ αρκετοί έχουν μεταναστεύσει σε άλλες χώρες, πιο ανεπτυγμένες, για να αναζητήσουν καλύτερη τύχη – στην Ελλάδα 300.000 νέοι επιστήμονες εγκατέλειψαν τη χώρα εν καιρώ κρίσης. Ιωάννης Πρωτοπαπαδάκης, «Ποιοι είναι οι Millennials; Πώς μπορείτε να τους προσεγγίσετε;», διαθέσιμο σε https://www.epixeiro.gr/article/2641.

50 Rob Bogosian και Charlene Rousseau, «How and Why Millennials are Shaking Up Organizational Cultures», *Rutgers Business Review*, Vol. 2/ 3 (2017): 386-394. Βλ. επίσης και «3 reasons why millennials need to diversify investments in cryptocurrencies», (2021), διαθέσιμο σε https://economictimes.indiatimes.com/markets/stocks/news/3-reasons-why-millennials-need-to-diversify-investments-in-cryptocurrencies/articleshow/80840141.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst .

ελάχιστη πιθανότητα μία επένδυση της αξίας των 100$ να φτάσει στα 100εκ δολάρια, όπως θα είχε συμβεί με επένδυση σε Bitcoin το 2010, είναι πολύ δελεαστικό για να περάσει απαρατήρητο. Σε κάθε περίπτωση πάντως, δεν είναι μόνο οι εικοσάρηδες οι οποίοι έχουν χάσει την εμπιστοσύνη τους στα παραδοσιακά επενδυτικά εργαλεία. Σε αντίθεση με την παραδοσιακή συντηρητική οικονομία, τα ψηφιακά νομίσματα (όπως κάποιοι προτιμούν να τα αποκαλούν, αντί για κρυπτονομίσματα, όρος που φέρει το στίγμα του ξεπλύματος μαύρου χρήματος στη μαύρη αγορά[51]) έχουν επιφέρει επανάσταση στο διαδίκτυο κι έχουν δημιουργήσει τεράστιες ευκαιρίες για όσους είναι διατεθειμένοι να επενδύσουν . Στην αρχή ήταν το διαδίκτυο της πληροφορίας, στη συνέχεια εξελίχθηκε σε διαδίκτυο των πραγμάτων και των μέσων κοινωνικής δικτύωσης και σήμερα αποτελεί το διαδίκτυο της νομισματικής αξίας. Κάποιοι πιστεύουν ότι τα κρυπτονομίσματα έχουν αφήσει πίσω τους τα σκοτεινά χρόνια, όταν ήταν ακόμη ο τομέας αυτών που πιστεύουν στην αναρχία και σε λίγα χρόνια θα αποτελούν την καθημερινότητά μας.

Μολαταύτα, υπάρχουν ακόμα εμπόδια στη μαζική δημοτικότητα των νομισμάτων αυτών: οι επενδυτές πρέπει να είναι πολύ εξοικειωμένοι με το διαδίκτυο και να εμπιστεύονται για τις χρηματικές τους συναλλαγές τα ανταλλακτήρια κρυπτονομισμάτων, όπως το Coinbase ή το Poloniex. Επίσης, κάποιες συναλλαγές παρουσιάζουν περίπλοκες και αργές διαδικασίες αναγνώρισης ταυτότητας και ορισμένα κράτη δεν επιτρέπουν τους χρήστες να επενδύσουν ακόμη σε αυτά. Εντούτοις, η χρήση τους γίνεται ολοένα και ευκολότερη και σε κάποιες περιπτώσεις οι ανταλλαγές γίνονται και με τη χρήση πιστωτικής κάρτας για ταχύτερες αγορές[52].

Από τη στιγμή που κάποιος αγοράσει ψηφιακά νομίσματα, υφίσταται κίνδυνος εισβολής (hacking[53]). Ακόμη και χρήστες που έχουν τις γνώσεις να χρησιμοποιήσουν

51 Teddy Waynne, «Grandpa had a pension. This generation has cryptocurrency», διαθέσιμο σε https://www.nytimes.com/2017/08/03/style/what-is-cryptocurrency.html.

52 Kailey Leinz, «People Desperate to Buy Bitcoin Are Paying With Credit Cards», διαθέσιμο σε https://www.bloomberg.com/news/articles/2018-01-11/bitcoin-buyers-turn-to-credit-cards-as-fomo-breeds-risk-taking.

53 Το «hacking» συνήθως αναφέρεται ως μία εισβολή χωρίς άδεια σε έναν ηλεκτρονικό υπολογιστή ή ένα δίκτυο. Το πρόσωπο που ασχολείται με τέτοιου είδους δραστηριότητες – hacker, έχει τη δυνατότητα να

την πιστοποίηση δύο παραγόντων στα τηλέφωνά τους (two factor authentication[54]), μπορεί να μην έχουν την τεχνογνωσία να εγκαταστήσουν την τεχνολογία «cold storage»[55] ή το σύστημα της αποθήκευσης νομισμάτων εκτός διαδικτύου. Δεν υπάρχει κάποια σχετική επιτροπή Ασφάλειας που διασφαλίζει τα απολεσθέντα χρήματα και η απώλεια είναι μη αναστρέψιμη. Μολαταύτα, ακόμη κι εάν ξεπεραστεί ο κίνδυνος και τα νομίσματα είναι πλέον προστατευμένα, υπάρχει πάντα το ρίσκο της επένδυσης, μεγεθυμένο από τη μεταβλητότητα των κρυπτονομισμάτων. Για το λόγο αυτό οι λίγοι επενδυτές, ενώ συμμετέχουν σε βραχυπρόσθεσμες συναλλαγές, η πλειονότητά τους επιλέγει να τα κρατήσει για μία ζωή (hodl[56]), από το να τα εκποιήσει για προσωρινά κέρδη. Πέρα από τα πιθανά μακροπρόθεσμα κέρδη, πολλοί κάτοχοι κρυπτονομισμάτων τα βλέπουν ως ένα όχημα για κοινωνική αλλαγή. Κάποια κρυπτονομίσματα χρησιμεύουν αποκλειστικά ως εναλλακτική μορφή χρήματος ή απέκτησαν δημοφιλία μέσω κερδοσκόπων, όπως το Dogecoin[57], ενώ άλλα, όπως το

μεταβάλλει το ίδιο το σύστημα ή τα χαρακτηριστικά ασφαλείας για να πετύχει το στόχο του, ο οποίος συνήθως είναι διαφορετικός από τον αρχικό σκοπό του συστήματος. Το hacking μπορεί επίσης να αναφέρεται σε μη κακόβουλες δραστηριότητες, οι οποίες συνήθως περιλαμβάνουν ασυνήθιστες ή αυτοσχέδιες αλλαγές στον εξοπλισμό ή στις διαδικασίες. Οι διάφορες τεχνικές οι οποίες χρησιμοποιούνται για το hacking περιλαμβάνουν ενδεικτικά: έλεγχο τρωτότητας (Vulnerability scanner), σπάσιμο κωδικών (Password cracking), Δούρειο Ίππο (Trojan horse), ιούς (Viruses) κλπ. Βλ. σχετικά https://www.techopedia.com.

54 «Two-factor authentication» (2FA): πρόκειται για την πιστοποίηση σε δύο βήματα, μία διαδικασία ασφαλείας με την οποία ο χρήστης παρέχει δύο παράγοντες πιστοποίησης για να επιβεβαιώσει την ταυτότητά του, σε αντίθεση με την πιστοποίηση ενός παράγοντα (single-factor authentication -SFA), με την οποία ο χρήστης παρέχει μόνο έναν παράγοντα ταυτοποίησης, συνήθως έναν κωδικό πρόσβασης – password. Jay P. Kesan και Carol M. Hayes, «Self Defense in Cyberspace: Law and Policy», TPRC 2011, *Illinois Public Law Research Paper No. 11-16*, Illinois Program in Law, Behavior and Social Science Paper No. LBSS12-08 (2011).

55 Στην τεχνολογία των Bitcoin η διαδικασία «cold storage» αποτελεί την τεχνική με την οποία κρατούνται εφεδρικά νομίσματα εκτός διαδικτύου. Αυτή η παράμετρος ασφαλείας είναι απαραίτητη όταν διακινούνται μεγάλα ποσά ψηφιακών νομισμάτων. Βλ. σχετικά https://en.bitcoin.it/wiki.

56 Αναγραμματισμός της λέξης hold, ο οποίος προέκυψε ως ορολογία των οπαδών των κρυπτονομισμάτων και σημαίνει hold on for dear life. Jake Frankenfield, «HODL», (2020), διαθέσιμο σε https://www.investopedia.com/terms/h/hodl.asp .

57 Το Dogecoin αποτελεί τόσο ένα εναλλακτικό αντιπληθωριστικό νομισματικό όργανο, όσο και μία πληθωριστική εξερεύνηση της οικοδόμησης κοινότητας γύρω από ένα κρυπτο – περιουσιακό στοιχείο. Usman W. Chohan, «A History of Dogecoin», Discussion Series: Notes on the 21st Century, (2017).

Ripple και το Ethereum χρησιμοποιούνται και στο φυσικό κόσμο, τόσο από τα άτομα, όσο και από τράπεζες και χρηματοπιστωτικά ιδρύματα.[58][59]

5 Είδη κρυπτονομισμάτων

5.1 Bitcoin[60]

Πριν αρκετά χρόνια, οι ενθουσιώδεις οπαδοί της τεχνολογίας άρχισαν να συζητούν για ένα νέο και μυστηριώδες επίτευγμα, το Bitcoin. Υπήρχαν φήμες, ότι το ψηφιακό αυτό νόμισμά θα έφερνε επανάσταση στη σύγχρονη οικονομία και θα καθιστούσε το στηριζόμενο από τις κυβερνήσεις νομισματικό σύστημα, απαρχαιωμένο. Ή απλά θα αποτελούσε μία μανία που θα έφθινε. Το Bitcoin έκανε την εμφάνισή του στο κοινό το έτος 2008, από έναν σκιώδη δημιουργό, ο οποίος απαντούσε στο όνομα Satoshi Nakamoto[61] και ο οποίος επικοινωνούσε αποκλειστικά μέσω ηλεκτρονικού ταχυδρομείου και μέσων κοινωνικής δικτύωσης. Παρόλο που κατά καιρούς απέδωσαν την ταυτότητά του σε πολλούς, κανένας δεν επιβεβαιώθηκε με ασφάλεια μέχρι σήμερα[62]. Ο Satoshi (όπως είναι γνωστός στον κόσμο των Bitcoin) δημιούργησε τους κανόνες του δικτύου των Bitcoin και στη συνέχεια, το έτος 2009, άφησε ελεύθερο το λογισμικό στον κόσμο. Ο ίδιος εξαφανίστηκε τρία έτη αργότερα. Πλέον οποιοσδήποτε μπορεί να κατεβάσει και να χρησιμοποιήσει το λογισμικό και ο

58 Teddy Waynne, «Grandpa had a pension. This generation has cryptocurrency», διαθέσιμο σε https://www.nytimes.com/2017/08/03/style/what-is-cryptocurrency.html.

59 Steven Johnson, «Beyond the Bitcoin bubble», διαθέσιμο σε https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html.

60 Reuben Grinberg, «Bitcoin: An Innovative Alternative Digital Currency», *Hastings Science & Technology Law Journal*, Vol. 4 (2011): 160.

61 Bill Stonehem, «Satoshi Nakamoto: The Bitcoin Founder», First Rank Publishing (2016).

62 Το Μάιο του 2016 ένας Αυστραλός επιχειρηματίας, ο Κρεγκ Ράιτ, σε συνέντευξη που παραχώρησε στο BBC δήλωσε ότι είναι ο δημιουργός του εικονικού νομίσματος Bitcoin. Η αποκάλυψη αυτή αμφισβητείται έως και σήμερα. «Ο επιχειρηματίας Κ. Ράιτ είναι ο δημιουργός του Bitcoin», διαθέσιμο σε https://www.naftemporiki.gr/finance/story/1099156/o-epixeirimatias-k-rait-einai-o-dimiourgos-tou-bitcoin .

ίδιος ο δημιουργός του δεν ασκεί περισσότερο έλεγχο πάνω στο δίκτυο από ό,τι οποιοσδήποτε άλλος χρήστης του[63].

Κάποιοι θεωρούν το Bitcoin τίποτε άλλο παρά μία κερδοσκοπική «φούσκα» που ενεργοποίησε τις διαδικτυακές πωλήσεις ναρκωτικών ουσιών[64] και τις πληρωμές λύτρων[65] ή αποτέλεσε μία νέα «συνεισφορά» στο φαινόμενο της υπερθέρμανσης του πλανήτη, χαρακτηρισμούς που το νόμισμα αυτό δεν τους αξίζει. Αντιθέτως, οι υποστηρικτές του Bitcoin πιστεύουν ότι συνέβαλε στη δημιουργία του πρώτου χρηματοπιστωτικού δικτύου, χωρίς την ανάμειξη οποιασδήποτε κυβέρνησης ή εταιρίας[66]. Σε χώρες όπως η Ζιμπάμπουε ή η Αργεντινή[67], το Bitcoin συχνά παρείχε ένα πιο σταθερό περιβάλλον για την τοποθέτηση χρημάτων από ό,τι το εγχώριο χρηματοπιστωτικό σύστημα. Και στις χώρες με πιο σταθερές οικονομίες, το Bitcoin οδήγησε σε μία αναταραχή νέων επενδύσεων, εργασιών και εταιριών. Με το να χαρακτηρίσει κάποιος το Bitcoin ως κάτι ανώφελο έχει αποτύχει στο να δει ολόκληρη την εικόνα. Μόνο οι θέσεις εργασίας που δημιουργήθηκαν είναι ένα ευθύ, μετρήσιμο και θετικό αντίκτυπο που το Bitcoin προσέφερε στην οικονομία.

Τι είναι το Bitcoin και πώς λειτουργεί

63 Nathaniel Popper, «What is Bitcoin? All about the mysterious digital currency», διαθέσιμο σε https://www.nytimes.com/2017/05/15/business/all-about-bitcoin-the-mysterious-digital-currency.html.

64 Sean Foley, Jonathan R. Karlsen και Tālis J. Putniņš, «Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?», *Review of Financial Studies* (2018).

65 You just have 10 days to send us the Bitcoin. After 10 days we will remove your private key and it's impossible to recover your files. Πρόκειται για ένα μήνυμα που στάλθηκε στους εργαζομένους του Νοσοκομείου Medstar. Κατά τη διάρκεια λίγων μηνών, την άνοιξη του 2016, δεκατέσσερα νοσοκομεία σε τέσσερα νοσοκομειακά συστήματα, αντιμετώπισαν επιθέσεις. Οι δράστες που γνώριζαν την κρισιμότητα της πρόσβασης των ιατρών στα ηλεκτρονικά τους δεδομένα και κυρίως στα δεδομένα των ασθενών, προκειμένου να τους παράσχουν την κατάλληλη περίθαλψη, εμπόδισαν την πρόσβαση αυτή απαιτώντας λύτρα σε Bitcoin Τουλάχιστον ένα από αυτά τα νοσοκομειακά κέντρα, το Hollywood Presbyterian Medical Center στο Λος Άντζελες, παραδέχθηκε δημόσια ότι ικανοποίησε την απαίτηση της πληρωμής των 40 Bitcoin, ποσού που ισοδυναμούσε τότε σε 17.000 δολάρια περίπου. Deborah R. Farringer, «Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals», *Seattle University Law Review*, Vol. 40, Belmont University College of Law Research Paper No. 2017-35 (2017): p. 937.

66 Reuben Grinberg, «Bitcoin: An Innovative Alternative Digital Currency», *Hastings Science & Technology Law Journal*, Vol. 4 (2011): 160.

67 Jill Carlson, «Cryptocurrency and Capital Controls», (2016), διαθέσιμο σε https://ssrn.com/abstract=3046954 .

Το Bitcoin αποτελεί ένα ψηφιακό αντικείμενο, το οποίο μπορεί να σταλεί ηλεκτρονικά από τον ένα χρήστη στον άλλο, σε οποιοδήποτε σημείο του κόσμου. Επίσης είναι η ονομασία ενός δικτύου πληρωμών, μέσα στο οποίο κινούνται τα νομίσματα Bitcoin[68]. Σε αντίθεση με κάθε παραδοσιακό δίκτυο πληρωμών, όπως η Visa ή η American Express, κανένας ιδιώτης ή εταιρία δεν διαχειρίζονται το δίκτυο αυτό. Αντιθέτως, αποτελεί ένα αποκεντρωμένο δίκτυο υπολογιστών σε όλον τον κόσμο, το οποίο παρακολουθεί όλες τις συναλλαγές σε Bitcoin και το οποίο σχεδιάστηκε με τέτοιον τρόπο, ώστε να δημιουργήσει ένα νομισματικό και χρηματοπιστωτικό δίκτυο, πέρα από τον έλεγχο οποιασδήποτε κυβερνήσεως ή εταιρίας[69]. Οι υπολογιστές οι οποίοι συμμετέχουν σε αυτό και ανιχνεύουν τις συναλλαγές σε Bitcoin, ενεργοποιούνται από τα νομίσματα που εξορύσσονται κάθε δέκα λεπτά και με τον τρόπο αυτό παραμένουν στο δίκτυο.

Ο τρόπος αγοράς Bitcoin είναι πολύ απλός: υπάρχουν εταιρίες – ανταλλακτήρια στις περισσότερες χώρες, τα οποία πωλούν Bitcoin, ανταλλάσσοντάς τα με το τοπικό νόμισμα. Για παράδειγμα, στις ΗΠΑ, η εταιρία με την επωνυμία Coinbase[70] συνδέεται με τον τραπεζικό λογαριασμό ή την πιστωτική κάρτα του καταναλωτή στον οποίο πωλεί νομίσματα με αντάλλαγμα αμερικανικά δολάρια. Το να αποκτήσει κάποιος λογαριασμό στην Coinbase είναι παρόμοιο με το να αποκτήσει έναν παραδοσιακό τραπεζικό λογαριασμό ή ένα λογαριασμό χρηματιστηριακών συναλλαγών, με προαπαιτούμενο, όμως, συνεχείς επιβεβαιώσεις της ταυτότητας του χρήστη. Για αυτούς που δεν επιθυμούν να αποκαλύψουν την ταυτότητά τους, υπάρχουν υπηρεσίες όπως η LocalBitcoins[71], η οποία συνδέει μεταξύ τους άτομα που

68 J. Baldwin, «In Digital We Trust: Bitcoin Discourse», *Digital Currencies, and Decentralized Network Fetishism,* Palgrave Communications, Vol. 4, Issue 1 (2018): 14-14.

69 Ying-Ying Hsieh και Jean-Philippe Vergne, «Bitcoin and the Rise of Decentralized Autonomous Organizations», *Journal of Organization Design*, (2017).

70 Ό.π. σχετικά με Coinbase.

71 Στο συγκεκριμένο ανταλλακτήριο παρατηρούνται μεγάλες διαφοροποιήσεις στις αξίες των νομισμάτων σε σχέση με τις τιμές της αγοράς. Τα ευρήματα υποδεικνύουν ότι το βαρόμετρο για τη διαμόρφωση των αξιών δεν είναι η αντίδραση στις συνθήκες της αγοράς, αλλά οι συνέπειες από την αποδοχή υψηλού ρίσκου των τρόπων πληρωμών από το ίδιο το ανταλλακτήριο. Με το να επιτρέπεται στους πωλητές, για παράδειγμα, να προσφέρουν Bitcoin ως αντάλλαγμα για κωδικούς δωροκαρτών, το ίδιο το Bitcoin αποκτά αξία τέσσερις, με πέντε φορές μεγαλύτερη από αυτή της αγοράς. Αυτές οι συναλλαγές είναι

θέλουν να αγοράσουν ή να πωλήσουν Bitcoin ανταλλάσσοντάς τα με μετρητά, χωρίς να απαιτείται κάποια επιβεβαίωση της ταυτότητάς τους. Για να αρχίσει να δέχεται κάποιος Bitcoin είναι ακόμα πιο απλό: το μόνο που χρειάζεται είναι να δημιουργήσει μία διεύθυνση Bitcoin, κάτι που γίνεται ανώνυμα, από οποιονδήποτε έχει πρόσβαση στο διαδίκτυο.

Όλες οι συναλλαγές σε Bitcoin καταχωρούνται στο κοινό καθολικό[72] του δικτύου, γνωστό ως blockchain[73]. Οι Αρχές επιβολής του νόμου και οι οικονομικές Αρχές μπορούν σε κάποιες περιπτώσεις να κάνουν χρήση της τεχνολογίας αυτής με στόχο να ανακαλύψουν συναλλαγές μεταξύ παραβατών. Ωστόσο, από τη στιγμή που οι χρήστες δεν έχουν συνδέσει την πραγματική τους ταυτότητα με τη διεύθυνση Bitcoin, είναι σε γενικές γραμμές ασφαλείς. Οι αυξανόμενες υπηρεσίες ξεπλύματος Bitcoin, γνωστές ως tumblers[74] – σκουπίδια, αναμιγνύουν πολλές συναλλαγές μεταξύ τους, ώστε να καταστήσουν ακόμα πιο σύνθετο τον εντοπισμό των συναλλαγών για τις Αρχές. Η προσπάθεια μετατροπής των αποκτηθέντων Bitcoin σε εγχώριο νόμισμα ενδέχεται να φρενάρει τις παραβατικές συμπεριφορές. Οι περισσότερες εταιρίες εντός των ΗΠΑ που μετατρέπουν Bitcoin σε δολάρια, απαιτούν από τους πελάτες τους να παρέχουν πιστοποιητικά ταυτοποίησής τους, κάτι που καθιστά εύκολα

συνήθως μικρές σε αξία και η δημιουργία μίας ημερήσιας σταθμισμένης αξίας σειράς τιμών του Bitcoin εμφανίζει με μεγαλύτερη ακρίβεια τις καθημερινές κινήσεις τιμών του ανταλλακτηρίου LocalBitcoins. Marc Holub και Jackie Johnson, «Bitcoin Price Anomalies on Localbitcoins: The AU$/BTC Market» (2018).

72 Γενικό καθολικό είναι μία συλλογή όλων των λογαριασμών μιας εταιρίας,η οποία περιέχει περιληπτικά όλες τις οικονομικές συναλλαγές κατά τη διάρκεια μιας λογιστικής περιόδου και χρησιμοποιεί το διπλογραφικό λογιστικό σύστημα. Σταμάτης Δρίτσας, Γεώργιος Σωτηρόπουλος, Ευάγγελος Περάκης και Χριστίνα Λειβαδά, «Το Δίκαιο της Λογιστικής», Νομική Βιβλιοθήκη, (2017).

73 Η τεχνολογία με την οποία καταγράφονται οι συναλλαγές σε ένα παγκόσμιο καθολικό, το οποίο στηρίζεται σε ένα δίκτυο υπολογιστών, χωρίς τη μεσολάβηση κυβερνήσεων ή εταιριών. F. Xavier Olleros και Majlinda Zhegu, «Blockchain Technology: Principles and Applications», Research Handbook on Digital Transformations, Edward Elgar, (2016). Βλ. επίσης Christian Catalini και Joshua S. Gans, «Some Simple Economics of the blockchain», Rotman School of Management Working Paper No. 2874598 MIT Sloan Research Paper No. 5191-16 (2017).

74 «Cryptocurrency tumbler» ή «cryptocurrency mixing service»: πρόκειται για υπηρεσίες οι οποίες προσφέρονται για να αναμείξουν μεταξύ τους πιθανόν αναγνωρίσιμα κεφάλαια κρυπτονομισμάτων, με στόχο να παρεμποδίσουν την ανίχνευση της αρχικής πηγής εσόδου. Έχουν αναπτυχθεί για να βελτιώσουν την ανωνυμία των κρυπτονομισμάτων, συνήθως των bitcoin, από τη στιγμή που υπάρχει το δημόσιο καθολικό που καταγράφει όλες τις συναλλαγές. Usman W. Chohan, «The Cryptocurrency Tumblers: Risks, Legality and Oversight», Discussion Paper Series: Notes on the 21st Century(2017).

εντοπίσιμη για τις Αρχές την εγκληματική δραστηριότητα - αντίθετα, εκτός των ΗΠΑ υπάρχουν πολλά ανταλλακτήρια Bitcoin που δεν απαιτούν από τους πελάτες τους να κάνουν εγγραφή χρησιμοποιώντας τα πραγματικά τους στοιχεία[75], ενώ είναι ακόμη πιο απλό να αγοράσει κάποιος αγαθά διαδικτυακά με Bitcoin, χωρίς να μετατρέψει τα ψηφιακά νομίσματα σε δολάρια ή ευρώ.

Το δέλεαρ των νέων Bitcoin ενθαρρύνει περισσότερο κόσμο στη χρήση πολλών και ταχύτατων υπολογιστών και στην κατανάλωση πολλής ενέργειας με στόχο το ξεκλείδωμα περισσοτέρων νέων νομισμάτων, τα οποία διανέμονται κάθε δέκα λεπτά περίπου[76]. Προκύπτει λοιπόν ένας τεράστιος όγκος διακομιστών ανά τον κόσμο αφιερωμένων στην εξόρυξη Bitcoin[77]. Η διαδικασία της εξόρυξης είναι θεμελιώδης για την ύπαρξη του κρυπτονομίσματος, καθώς με αυτή όλοι οι υπολογιστές λειτουργούν ως λογιστές για το δίκτυο των Bitcoin[78]. Και ο αλγόριθμος που χρησιμοποιείται από τους υπολογιστές απαιτεί την καταγραφή όλων των νέων συναλλαγών που γίνονται στο δίκτυο. Η διαδικασία εξόρυξης ήταν εξ αρχής δύσκολη, ώστε κανένας να μην μπορεί να διαμοιράσει τα αρχεία[79]. Το 2008, η πρώτη εφημερίδα που αναφέρθηκε στο Bitcoin, έκανε λόγο για ένα σύστημα που είχε σχεδιαστεί για να εμποδίσει τον «άπληστο εισβολέα», ο οποίος ίσως επιχειρήσει να τροποποιήσει τα αρχεία και να εξαπατήσει κόσμο με την κλοπή των πληρωμών τους. Χάρη στην εξόρυξη και τους λογιστικούς κανόνες, ο εισβολέας θα ωφελούνταν τελικά μόνο εάν εφήρμοζε τους κανόνες. Οι κανόνες αυτοί κράτησαν τους εισβολείς μακριά για όσα έτη το δίκτυο είναι σε λειτουργία. Και χωρίς αυτή τη διαδικασία, οι επιστήμονες συμφωνούν ότι το Bitcoin δεν θα λειτουργούσε.

75 Για παράδειγμα, Binance, Bitpanda κλπ.

76 Engin Iyidogan, «Incentive Mechanism and Economic Model of Blockchain Based Cryptocurrencies», (2018), διαθέσιμο σε https://www.competitionpolicyinternational.com/incentive-mechanism-and-economic-model-of-blockchain-based-cryptocurrencies/ .

77 Campbell R. Harvey, «Cryptofinance», Duke University - Fuqua School of Business, National Bureau of Economic Research (NBER) (2016).

78 Dr Garrick Hileman και Michel Rauchs, «2017 Global Cryptocurrency Benchmarking Study» (2017), διαθέσιμο σε https://cointelegraph.com/storage/uploads/view/2017-global-cryptocurrency-benchmarking-study.pdf .

79 Campbell R. Harvey, «Bitcoin Myths and Facts», (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479670 .

Η αξία του Bitcoin και οι διακυμάνσεις της

Η θεαματική άνοδος του Bitcoin, ειδικά την εποχή των μέσων κοινωνικής δικτύωσης, ενθάρρυνε τους κερδοσκόπους στην αγορά κρυπτονομισμάτων, με την ελπίδα του εύκολου και γρήγορου κέρδους[80]. Οι επενδυτές αυτοί δεν χρησιμοποιούσαν τα κρυπτονομίσματα για την αγορά αγαθών, αλλά ως επένδυση - σαν να ήταν εικονικός χρυσός, ουσιαστικά ένας τρόπος αποταμίευσης μακριά από οποιονδήποτε έλεγχο[81]. Η αξία του Bitcoin, το οποίο είναι γνωστό για τη μεταβλητότητά του, κατέρρευσε αρκετές φορές στο παρελθόν, για διαφορετικούς λόγους κι αιτίες (όπως εισβολές (hacking), επεμβάσεις ρυθμιστικών αρχών, τεχνολογικές αναβαθμίσεις ή εξ αιτίας του ανταγωνισμού με άλλα κρυπτονομίσματα). Μολονότι η αξιοπιστία του Bitcoin επλήγη από εξωτερικούς παράγοντες, η ολοένα αυξανόμενη αποδοχή των κρυπτονομισμάτων οδήγησε τις τιμές του σε υψηλότερα επίπεδα[82].

Πολλοί θεωρούν ότι τα ψηφιακά νομίσματα θα γίνουν δελεαστικά μόνο εάν είναι εύκολα και φτηνά στην κυκλοφορία τους[83]. Οι διαφωνίες που έχουν προκύψει δημιούργησαν πλήθος ανταγωνιστών του Bitcoin. Όμως η κοινότητα που έχει δημιουργηθεί γύρω από το Bitcoin έχει περιχαρακωθεί γύρω από τα προτερήματα που προκύπτουν από την ομοιότητά του με το χρυσό και δεν εστιάζει στην αδυναμία

80 Guglielmo Maria Caporale και Alex Plastun, «Price Overreactions in the Cryptocurrency Market», CESifo Working Paper Series No. 6861 (2018).

81 C. M. Christopher, «Why on Earth Do People Use Bitcoin?», *Business & Bankruptcy L.J.*, Forthcoming (2014).

82 Spencer Wheatley, Didier Sornette, Tobias Huber, Max Reppen, και Robert N. Gantner, «Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model», Swiss Finance Institute Research Paper No. 18-22 (2018).

83 J-C Gerlach, Guilherme Demos και Didier Sornette «Dissection of Bitcoin's Multiscale Bubble History», Swiss Finance Institute Research Paper No. 18-30 (2018). Βλ. επίσης Lerong Lu, «Bitcoin: Speculative Bubble», Financial Risk and Regulatory Response, *Butterworths Journal of International Banking and Financial Law*, Vol. 33(3), (2018): 178-182 και Jérôme Kreuser και Didier Sornette, «Bitcoin Bubble Trouble», *Forthcoming in Wilmott Magazine,* Swiss Finance Institute Research Paper No. 18-24, (2018).

του να συναγωνιστεί το σύστημα πληρωμών Pay Pal[84] ή την υπηρεσία μεταφοράς χρημάτων Western Union[85].

Η αξία του Bitcoin, η οποία κυμαίνεται συνεχώς, καθορίζεται από την ελεύθερη αγορά, η οποία δεσμεύεται από τις συναλλαγές, με τρόπο παραπλήσιο με την προσφορά και ζήτηση σε επίπεδο χρηματιστηρίου και χρυσού[86]. Οι επενδυτές της τεχνολογίας αγόρασαν νομίσματα κι εκτίναξαν την αξία τους, ελπίζοντας σε ένα παγκόσμιο ψηφιακό χρηματοπιστωτικό δίκτυο. Στις αρχές του 2017 η αξία του Bitcoin ανέρχετο σε λιγότερο από 1.000 δολάρια. Τον Οκτώβριο του 2017 ανήλθε σε 5.000 δολάρια, το Νοέμβριο του ίδιου έτους διπλασιάστηκε και το Δεκέμβριο του 2017 η αξία ενός και μόνου Bitcoin ανήλθε, σε μερικά ανταλλακτήρια, στα 20.000 δολάρια[87]. Με την τιμή αυτή, η συνολική αξία των Bitcoin που ήταν σε κυκλοφορία εκείνη τη δεδομένη στιγμή ανέρχετο σε 300 δισεκατομμύρια δολάρια[88].

Τον Ιούνιο του 2018 σε επιστημονικό άρθρο[89] επισημάνθηκε η ανάγκη δημιουργίας μίας οργανωμένης εκστρατείας σε βάρος της χειραγώγησης της τιμής του Bitcoin και άλλων κρυπτονομισμάτων. Το άρθρο αυτό προκάλεσε συζητήσεις σχετικά με το

84 Η PayPal δίνει τη δυνατότητα σε οποιοδήποτε φυσικό ή νομικό πρόσωπο που διαθέτει ηλεκτρονική διεύθυνση να πραγματοποιεί με ασφάλεια και χωρίς κόστος πληρωμές, είτε ως δέκτης είτε ως αποστολέας, μέσω του διαδικτύου, σε πραγματικό χρόνο. Η PayPal (Europe) S.à r.l. et Cie, S.C.A. είναι νομίμως εξουσιοδοτημένη ως πιστωτικός οργανισμός στο Λουξεμβούργο (Άρ. 2 του Νόμου της 5ης Απριλίου 1993 για τον οικονομικό τομέα, όπως τροποποιήθηκε και τελεί υπό την προληπτική επίβλεψη της ρυθμιστικής αρχής του Λουξεμβούργου, του Commission de Surveillance du Secteur Financier, με καταστατική έδρα στο Λουξεμβούργο L-1150). Η PayPal Inc., μητρική εταιρεία της PayPal (Europe) S.à r.l. et Cie, S.C.A. έχει την έδρα της στην Καλιφόρνια, ΗΠΑ. Βλ. σχετικά https://www.paypal.com.

85 Πρόκειται για μία διεθνή εταιρία μεταφοράς χρημάτων, η οποία πραγματοποιείται είτε μέσω κάποιου τοπικού αντιπροσώπου είτε μέσω του ιστότοπου που διαθέτουν είτε μέσω κάποιας εφαρμογής ενός έξυπνου κινητού. Βλ. σχετικά https://www.westernunion.com.

86 Lawrence J. Trautman, «Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox?» *Richmond Journal of Law and Technology*, Vol. 20/ 4 (2014).

87 Η αξία του Bitcoin το Δεκέμβριο του 2020 ανέρχετο στα 18.714,84 δολάρια. Βλ. σχετικά https://coinmarketcap.com.

88 Για να αντιληφθεί κάποιος τα μεγέθη, αρκεί να αναλογιστεί ότι η αξία όλων των μετοχών της εταιρίας Goldman Sachs ανέρχεται περίπου στα 90 δισεκατομμύρια δολάρια. Βλ. σχετικά http://www.goldmansachs.com.

89 John M. Griffin και Amin Shams, «Is Bitcoin Really Un-Tethered?» (2018), διαθέσιμο σε https://whartonliquidity.files.wordpress.com/2018/09/is_bitcoin_really_untethered.pdf .

βαθμό που τα κέρδη του Bitcoin τα περασμένα έτη ήταν περισσότερο αποτέλεσμα χειραγώγησης από μεγάλους επενδυτές, παρά της πραγματικής ζήτησης[90].

Περαιτέρω, έχει παρατηρηθεί ότι μέχρι σήμερα, ο αριθμός των ατόμων που χρησιμοποίησαν Bitcoin για την αγορά αγαθών υπήρξε πολύ μικρότερος σε σύγκριση με όσους τα αγόραζαν λόγω της σπανιότητάς τους, ενώ λόγω της αυξανόμενης αξίας του, όσοι είχαν στην κατοχή τους νομίσματα δίσταζαν να τα χρησιμοποιήσουν ως μέσο πληρωμής αγαθών[91]. Η παραδοχή αυτή επηρέασε και το λογισμικό του Bitcoin και οδήγησε στο να τεθεί ως όριο των νομισμάτων που θα εξορύσσονταν, τα 21 εκατομμύρια[92]. Λόγω λοιπόν της σπανιότητάς του, η αξία του είχε αυξανόμενη πορεία και το κατέστησε ελκυστικό αντικείμενο επένδυσης. Κάποιοι προσπάθησαν να κάνουν εκτίμηση της τιμής του βασιζόμενοι στη δημοτικότητά του. Το 2019, προτάθηκε μια πιο αξιόπιστη μέθοδος πρόβλεψης της τάσης της τιμής ενός κρυπτονομίσματος, μέσω της τεχνητής νοημοσύνης. Ερευνητές του Πολυτεχνείου Κρήτης δημιούργησαν ένα σύστημα πρόβλεψης τεχνητής νοημοσύνης, με την ονομασία «PATSOS», βασισμένο σε κανόνες, που αναπαριστούν τη λειτουργία της σκέψης του ανθρώπινου εγκεφάλου[93]. Το σύστημα αυτό προβλέπει την ανοδική ή

90 Πολλοί εξέφρασαν την ανησυχία ότι οι τιμές υπέστησαν πιέσεις από το Bitfinex, ένα από τα μεγαλύτερα και υπό ελάχιστο έλεγχο ανταλλακτήρια. Οι ιδιοκτήτες του ανταλλακτηρίου αυτού κλητεύθηκαν από τις Αμερικανικές Αρχές έπειτα από ανησυχητικά άρθρα που δημοσιεύθηκαν στον Τύπο. Βλ. σχετικά Matthew Leising, «U.S. Regulators Subpoena Crypto Exchange Bitfinex, Tether», (2018), διαθέσιμο σε https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc .

91 Οι περισσότεροι κάτοχοι Bitcoin δεν θα ήθελαν να καταναλώσουν ένα νόμισμα που την επόμενη εβδομάδα πιθανόν να είχε διπλάσια αξία. Lerong Lu, «Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response», *Butterworths Journal of International Banking and Financial Law* Vol. 33(3) (2018): 178-182.

92 Το Bitcoin και άλλα κρυπτονομίσματα έχουν ανώτατα όρια κυκλοφορίας στα πρωτόκολλά τους, με το Bitcoin να έχει ως ανώτατο αριθμό εξόρυξης τα 21εκ νομίσματα. Θα εξαχθούν ακόμα 4,3 εκατομμύρια Bitcoin μέχρι το έτος 2140 για να συμπληρωθεί το όριο αυτό. Στα πρωτόκολλα αυτά έχουν συμμορφωθεί οι συναινούντες χειριστές τους. Τίθεται, όμως, το ερώτημα από τους ειδικούς εάν αυτά τα ανώτατα όρια αποτελούν τρόπο παράνομου καθορισμού της ποσότητας των νομισμάτων, κατά παράβαση των αντιμονοπωλιακών διατάξεων. Έχει αποδειχθεί ότι υφίσταται ένα αντιμονοπωλιακό ρίσκο που λαμβάνουν οι χειριστές των κρυπτονομισμάτων, το οποίο μπορεί να τους οδηγήσει στην απόδοση ποινικών και αστικών ευθυνών. Peder Ostbye, «The Case for a 21 Million Bitcoin Conspiracy», *Journal of Financial Transformation*, Capco Institute, Vol. 48, (2018): 88-97 .

93 Το νεύρο - ασαφές σύστημα, που ονομάστηκε «PATSOS», αποκτά νοημοσύνη από την επαναλαμβανόμενη εκπαίδευση, με σκοπό την δημιουργία βέλτιστων κανόνων που προβλέπουν την τάση της τιμής του κρυπτονομίσματος. Το μοντέλο βασίζεται στον ανθρώπινο τρόπο σκέψης, δηλαδή σε ένα σύστημα κανόνων. Βλ. σχετικά George Atsalakis, Ioanna Atsalaki, Fotis Pasiouras και Konstantinos

καθοδική πορεία της τιμής σε ποσοστό επιτυχούς πρόβλεψης 63,22%[94]. Περαιτέρω, οι ερευνητές σύγκριναν την αποτελεσματικότητα του συστήματος πρόβλεψης εκτελώντας αγοραπωλησίες και με άλλα δημοφιλή κρυπτονομίσματα όπως το Ethereum, Litcoin και Ripple. Τα κερδοφόρα ποσοστά και στις τρεις περιπτώσεις επιβεβαίωσαν την αποτελεσματικότητα του μοντέλου[95].

Μειονεκτήματα του Bitcoin

Παρότι οι συναλλαγές με Bitcoin έχουν πολλαπλασιαστεί εκθετικά, παραμένει ένα νόμισμα δυσκίνητο και δύσκολο στη χρήση[96] – μία συναλλαγή μπορεί να διαρκέσει έως και δέκα λεπτά και η τιμή του είναι εξαιρετικά ασταθής. Τίθεται λοιπόν το ερώτημα πώς πέτυχε ως επενδυτικό εργαλείο, αφού απέτυχε ως νόμισμα[97].

Υπάρχουν τέσσερις διαφορετικές προσεγγίσεις ως προς αυτό:

I. Η ώθηση που έλαβε από τα επιχειρηματικά κεφάλαια[98] και από την έγκριση της αμερικανικής κυβέρνησης, αν και τα πρώτα χρόνια το ενδιαφέρον των επενδυτών ήταν πολύ περιορισμένο, γιατί η ιδέα της κρυπτογράφησης είχε συνδεθεί με τις διαδικτυακές μαύρες αγορές, όπου εγκληματικές οργανώσεις χρησιμοποιούν ψηφιακά νομίσματα για να διακινήσουν ναρκωτικά ή

D. Zopounidis, «Bitcoin prices forecasting with neuro-fuzzy techniques», *European Journal of Operational Research*, 276/2 (2019): 770–780.

94 Στις χρηματαγορές, οποιοδήποτε σύστημα πρόβλεψης επιτυγχάνει πάνω από 52% ακρίβεια, θεωρείται κερδοφόρο. «Πώς μπορούμε να προβλέψουμε την κίνηση του bitcoin», (2019), https://www.brief.com.cy/blockchaincrypto/pos-mporoyme-na-problepsoyme-tin-kinisi-toy-bitcoin .

95 Ιωάννα Ατσαλάκη, Γιώργος Σ. Ατσαλάκης, Κωνσταντίνος Ζοπουνίδης και Φώτης Πασιούρας, «Bitcoin και Τεχνητή Νοημοσύνη», διαθέσιμο σε https://m.naftemporiki.gr/story/1526339/bitcoin-kai-texniti-noimosuni.

96 C. Beer και B. Weber, «Bitcoin – The Promise and Limits of Private Innovation in Monetary and Payment Systems», Monetary Policy and the Economy. Q4/2014, (2015):53-66 .

97 Wee Seng Wong, Dennis Saerbeck, και Dante Delgado Silva, «Cryptocurrency: A New Investment Opportunity? An Investigation of the Hedging Capability of Cryptocurrencies and Their Influence on Stock, Bond and Gold Portfolios» (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125737 .

98 Jonathan Rohr and Aaron Wright, «Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets», Cardozo Legal Studies Research Paper No. 527, University of Tennessee Legal Studies Research Paper No. 338 (2017).

παράνομα και λαθραία προϊόντα.[99] Θα μπορούσε να υποστηριχθεί ότι το ψηφιακό αυτό νόμισμα είχε συνδεθεί με τη φοροαποφυγή και το ξέπλυμα μαύρου χρήματος. Από τη στιγμή, όμως, που το FBI έκλεισε τον ιστότοπο Silk Road[100], το Bitcoin, όπως και άλλα κρυπτονομίσματα επαινέθηκαν από γερουσιαστές ως «νόμιμες χρηματοοικονομικές υπηρεσίες».

II. Πολλοί αναφέρονται στο Bitcoin ως ψηφιακό χρυσό[101]. Στις αρχές του Νοεμβρίου του 2017 το Bloomberg ανέφερε ότι η φράση «buy Bitcoin» ξεπέρασε σε αναζητήσεις στο διαδίκτυο τη φράση «buy gold», υποδηλώνοντας ότι η άνοδός του οφείλεται σε επενδυτές οι οποίοι το θεωρούν ως σύγχρονο ισοδύναμο ενός πολύτιμου μετάλλου.

III. Πρόκειται για αποθεματικό νόμισμα της αγοράς ICO[102]. Το 2017 η πρακτική αυτή εκτοξεύτηκε, συγκεντρώνοντας περισσότερα από 2 δισεκατομμύρια δολάρια για τις νέες εταιρίες. Αναλυτές εκτιμούν ότι το γεγονός ότι αυτό συμβαίνει εν κρυπτώ, είναι καθοριστικής σημασίας και ότι όσοι επιλέγουν τη μέθοδο αυτή το κάνουν για να μην καταβάλουν φόρους.

IV. Αποτελεί μία επενδυτική απάτη - «φούσκα»[103]. Ακόμα και αν κάποιος ισχυριστεί ότι η τεχνολογία blockchain[104] είναι ένα ευφυές σύστημα ή ότι τα κρυπτονομίσματα είναι ο νέος χρυσός και το Bitcoin το αποθεματικό νόμισμα της αγοράς ICO, είναι παράξενο να παρατηρεί κανείς την αξία ενός προϊόντος

99 Robert Augustus Hardy και Julia R Norgaard, «Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web», (2016), διαθέσιμο σε https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/reputation-in-the-internet-black-market-an-empirical-and-theoretical-analysis-of-the-deep-web/560A8645D47BBDDC4E71101EC1C100CA .

100Ό.π. υποσημείωση 9.

101 John O. McGinnis και Kyle Roche, «Bitcoin: Order without Law in the Digital Age», *Northwestern Public Law Research Paper* No. 17-06 (2017). Βλ. επίσης Adam Hayes, «The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets» (2015) και «Buy Bitcoin Overtakes Buy Gold as Private Gold Trading Declines in October» διαθέσιμο σε https://www.ccn.com.

102 Ό.π. υποσημείωση 10 σχετικά με ICO.

103 Jim Kyung-Soo Liew και Levar Hewlett, «The Case for Bitcoin for Institutional Investors: Bubble Investing or Fundamentally Sound?» (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082808 .

104 Ό.π. υποσημείωση 69 σχετικά με blockchain.

να διπλασιάζεται μέσα σε έξι εβδομάδες, χωρίς καμία συναλλαγή[105]. Αντιθέτως, παρατηρείται μία απόκλιση μεταξύ του όγκου συναλλαγών σε Bitcoin, ο οποίος έχει αυξηθεί περισσότερο από 32 φορές από το 2012 και της τιμής αγοράς του, η οποία έχει αυξηθεί περισσότερο από 1.000 φορές[106]. Οι έρευνες δείχνουν ότι η περισσότεροι κάτοχοι Bitcoin τα αγοράζουν με σκοπό την ανταλλαγή σε δολάρια. Για τους περισσότερους, το Bitcoin δεν είναι νόμισμα, αλλά κάτι συλλεκτικό[107].

Περαιτέρω, όσοι αγοράζουν Bitcoin ή άλλα ψηφιακά νομίσματα γίνονται συχνά στόχος εισβολέων - hackers, οι οποίοι έχουν γίνει ειδικοί στο να διεισδύουν στους λογαριασμούς Bitcoin[108]. Τα «πορτοφόλια» Bitcoin (Bitcoin wallets[109]) είναι ευάλωτα σε νέου είδους επιθέσεις, οι οποίες δεν υφίστανται στους συνήθεις τραπεζικούς λογαριασμούς. Και το πιο σημαντικό, σε αντίθεση με τα χρήματα σε έναν τραπεζικό

105 Mitsuru Iwamura, Yukinobu Kitamura, Tsutomu Matsumoto και Kenji Saito «Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money», *Hitotsubashi Journal of Economics,* vol 60/1 (2019): 41-60.

106 Neil Gandal, JT Hamrick, Tyler Moore και Tali Oberman, «Price Manipulation in the Bitcoin Ecosystem», CEPR Discussion Paper No. DP12061 (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977479 .

107 «Bitcoin: η αυταπάτη που θα μπορούσε να κατακτήσει τον κόσμο», διαθέσιμο σε https://tvxs.gr/news/kosmos/bitcoin-i-aytapati-poy-tha-mporoyse-na-kataktisei-ton-kosmo.

108 Kelvin F.K. Low και Ernie G. S. Teo, «Legal Risks of Owning Cryptocurrencies», *Reed Elsevier*, Handbook of blockchain, Digital Finance, and Inclusion, Vol. 1, 1st Edition, (2018): 225-247.

109 Τα εικονικά νομίσματα μπορούν να αγοραστούν σε πλατφόρμα ανταλλαγής με τη χρήση συμβατικού χρήματος. Στη συνέχεια, εμβάζονται σε εξατομικευμένο λογαριασμό σε Bitcoin, ο οποίος καλείται «ψηφιακό πορτοφόλι». Χρησιμοποιώντας το πορτοφόλι αυτό, οι καταναλωτές μπορούν να αποστέλλουν Bitcoins διαδικτυακά οπουδήποτε ή να τα μετατρέπουν σε συμβατικό νόμισμα. Όλα τα «πορτοφόλια» διαλειτουργούν μεταξύ τους, όπως συμβαίνει με το ηλεκτρονικό ταχυδρομείο. Υπάρχουν τρία είδη πορτοφολιών νομισμάτων Bitcoin: α) το ψηφιακό, το οποίο είναι εγκατεστημένο σε υπολογιστή, β) το φορητό ή χάρτινο, το οποίο επιτρέπει στους χρήστες να μεταφέρουν τα ψηφιακά νομίσματα επάνω τους, να τα ανταλλάσουν με ευκολία και να πληρώνουν σε καταστήματα με τη σάρωση του κωδικού και γ) το διαδικτυακό πορτοφόλι. Ωστόσο, τα ψηφιακά πορτοφόλια δεν είναι απαραβίαστα έναντι των ηλεκτρονικών εισβολέων (hackers) και επίσης μπορεί να κλαπούν, όπως συμβαίνει και με τα συμβατικά πορτοφόλια. Έχουν αναφερθεί περιπτώσεις καταναλωτών, οι οποίοι έχασαν εικονικά νομίσματα αξίας άνω του 1 εκατομμυρίου δολαρίων, οι δε προοπτικές ανάκτησής τους είναι ελάχιστες. Επιπλέον, εάν ο χρήστης χάσει το κλειδί ή το συνθηματικό κωδικό πρόσβασης στο ψηφιακό του πορτοφόλι, μπορεί να χάσει για πάντα και τα εικονικά νομίσματά του. Δεν υπάρχουν κεντρικές υπηρεσίες καταχώρισης συνθηματικών κωδικών ή έκδοσης συνθηματικών κωδικών αντικατάστασης. Adam J. Levitin, «Pandora's Digital Box: The Promise and Perils of Digital Wallets», *University of Pennsylvania Law Review,* Vol. 166, (2017).

λογαριασμό, όταν ένα Bitcoin χαθεί, δεν υπάρχει τρόπος να επιστραφεί και καμία ασφάλεια δεν μπορεί να καλύψει την απώλειά του[110].

Από την άλλη πλευρά, υπάρχουν επίσης όρια και στις ικανότητες του συστήματος των Bitcoin. Ένας όρος που έχει καταχωρηθεί στο λογισμικό του Bitcoin είναι ότι το δίκτυο θα επεξεργάζεται μόνο περίπου πέντε συναλλαγές το δευτερόλεπτο – εξαιρετικά περιορισμένη δυνατότητα σε σύγκριση με τις 25.000 συναλλαγές που διαχειρίζεται η Visa κάθε δευτερόλεπτο[111]. Πολλοί αρχικοί οπαδοί του νομίσματος θεώρησαν ότι το σύστημα θα επεκτεινόταν ώστε να δέχεται περισσότερες συναλλαγές, χωρίς να απωλέσει την υπόστασή του ως ψηφιακό προϊόν και πρότειναν την τροποποίηση των όρων που θα οδηγούσε στο διπλασιασμό της ικανότητας του συστήματος. Αλλά άλλοι επενδυτές εξέφρασαν την ανησυχία τους ότι η γρήγορη επέκταση του συστήματος θα απειλήσει την ανεξαρτησία του Bitcoin, με το επιχείρημα ότι για να υπάρχει ένα παγκόσμιο νόμισμα, δεν πρέπει αυτό να ελέγχεται από μία τράπεζα ή μία χώρα ή από πολλές μαζί. Εάν κινδυνεύσει η αποκέντρωση που έχει καθιερωθεί από το ίδιο το νόμισμα, το Bitcoin θα καταρρεύσει[112]. Επιπλέον, η σχεδίαση του Bitcoin δεν θα μπορούσε να ανταγωνιστεί το Pay Pal[113] ή τη Visa[114], καθώς κάθε συναλλαγή καταχωρείται σε χιλιάδες υπολογιστές ανά τον κόσμο. Τα επιχειρήματα αυτά υπερίσχυσαν και έκτοτε, όσοι ενδιαφέρονταν να

110 Nathaniel Popper, «Bitcoin's price has soared. What comes next?», διαθέσιμο σε https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html.

111 Matthew Chen και Anton Badev, «Bitcoin: Technical Background and Data Analysis», FEDS Working Paper No. 2014-104 (2014).

112 Αυτή η αποκέντρωση είναι αποτέλεσμα της ασυνήθιστης σχεδίασης του Bitcoin, η οποία επιτρέπει στους ακολούθους του να συγκρατούν και να καταγράφουν τις εγγραφές από καθεμία συναλλαγή σε Bitcoin, χωρίς την παρέμβαση κάποιας κεντρικής αρχής. Εάν αυξηθούν οι συναλλαγές, μόνο οι μεγάλες εταιρίες θα είναι σε θέση να καταχωρήσουν τις εγγραφές. Βλ. σχετικά Christian Catalini και Joshua S. Gans, «Some Simple Economics of the blockchain», Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16 (2017).

113 Ό.π. υποσημείωση 86 σχετικά με Pay Pal.

114 Πρόκειται για μία πολυεθνική εταιρία αμερικανικών συμφερόντων που προσφέρει χρηματοπιστωτικές υπηρεσίες, με έδρα το Foster City της Καλιφόρνια. Παρέχει τη δυνατότητα ηλεκτρονικής μεταφοράς κεφαλαίων, μέσω των πιο γνωστών, παγκοσμίως προϊόντων, με την επωνυμία Visa, όπως πιστωτικών καρτών, δωροκαρτών και καρτών αναλήψεων. Βλ. σχετικά σε https://usa.visa.com.

πραγματοποιήσουν πληρωμές με ψηφιακά νομίσματα, άρχισαν να ερευνούν εναλλακτικούς τρόπους, μέσω των ανταγωνιστών του Bitcoin[115].

Τέλος και με το δεδομένο ότι δεν υπάρχει κάποια κεντρική αρχή που να διευθύνει το Bitcoin, κανείς δεν έχει την εξουσία να επιβάλει στους νέους χρήστες να αποκαλύψουν τις ταυτότητές τους. Κατά συνέπεια, από τη στιγμή που κάποιος μπορεί να δέχεται Bitcoin σε οποιοδήποτε μέρος του κόσμου, χωρίς να αποκαλύπτει την ταυτότητά του, το νέο αυτό κρυπτονόμισμα αποτέλεσε ένα αγαπημένο εργαλείο για τους εισβολείς - hackers ως προς την αναζήτηση λύτρων. Για τους παραβάτες το Bitcoin έγινε πολύ πιο ελκυστικό από ό,τι το σύστημα της εταιρίας Western Union[116], το οποίο σε γενικές γραμμές απαιτεί από τους πελάτες του να παρέχουν στοιχεία της ταυτότητάς τους, προτού ανοίξουν κάποιον λογαριασμό και δεχθούν χρήματα.

Ανταγωνιστές Bitcoin

Όταν εμφανίστηκε το Bitcoin, το έτος 2009, περιγραφόταν ως ένας ακόμη τρόπος ηλεκτρονικών πληρωμών[117]. Προσφάτως, πολλοί προγραμματιστές που εργάζονται στο πεδίο του λογισμικού Bitcoin δήλωσαν ότι το σύστημα στην παρούσα του μορφή πάσχει ως προς την αγορά αγαθών. Θεωρούν ότι σχεδιάστηκε περισσότερο για να χρησιμοποιηθεί ως ένα είδος σπάνιου εμπορεύματος, όπως ο ψηφιακός χρυσός, το οποίο επιτρέπει στους καταναλωτές να διατηρήσουν τα χρήματά τους εκτός κυβερνητικών και εταιρικών ελέγχων. Κατά συνέπεια, πολλοί από αυτούς που επιθυμούν να χρησιμοποιήσουν ψηφιακά νομίσματα για διαδικτυακές αγορές, στρέφονται στους ανταγωνιστές των Bitcoin[118].

115 Nathaniel Popper, «Bitcoin hasn't replaced cash, but investors don' t care», διαθέσιμο σε https://www.nytimes.com/2017/12/06/technology/bitcoin-payments-gold.html.

116 Ό.π. υποσημείωση 87 σχετικά με Western Union.

117 Beat Weber, «Can Bitcoin Compete with Money?», *Journal of Peer Production 4* (2014).

118 Lawrence H. White, «The Market for Cryptocurrencies», GMU Working Paper in Economics No. 14-45 (2014).

Το Δεκέμβριο του 2020 ο αριθμός των κρυπτονομισμάτων ανερχόταν σε 4.253[119], ενώ το Μάιο του 2018 υπήρχαν 1823 διαφορετικά είδη κρυπτονομισμάτων[120], τα οποία χρησιμοποιούν διαφορετικά δίκτυα τεχνολογίας blockchain ως δομή τους. Πέρα από τα Bitcoin, αρκετά δημοφιλή είναι και τα Ethereum, Bitcoin Cash, Ripple, Litecoin κλπ. Τα κρυπτονομίσματα αυτά προσπάθησαν να διαφοροποιηθούν από τα Bitcoin, μέσω άλλων τεχνολογιών και πράξεων εμπορικής προώθησης (marketing)[121]. Επίσης, πολλοί επενδυτές επενδύουν τα χρήματά τους σε κατά παραγγελίαν ψηφιακά νομίσματα τα οποία έχουν εμφανίσει επιχειρηματίες. Αυτά έχουν σχεδιαστεί για να χρησιμεύσουν ως εσωτερικοί μηχανισμοί πληρωμών, σε σχέση με νέα λογισμικά που δημιουργούν οι επιχειρηματίες αυτοί [122].

Δεδομένου ότι όλα τα κρυπτονομίσματα είχαν μηδαμινή αξία στην αρχή, παρουσιάζεται πλέον το φαινόμενο της δημιουργίας νέων δισεκατομμυριούχων[123], με συνεχώς μεταβαλλόμενες περιουσίες. Η ταχέως αυξανόμενη αξία του Ripple[124], ενός ανταγωνιστικού του Bitcoin, κρυπτονομίσματος, αποκάλυψε το το παράλογο των αγορών των κρυπτονομισμάτων, οι οποίες καθοδηγούνται κυρίως από το φόβο της απώλειας αξίας (FOMO – Fear Of Missing Out[125]). Το Ripple δεν είναι το μοναδικό ψηφιακό νόμισμα που τρέφεται από αυτό το φόβο. Το έτος 2017 υπήρξαν 29 νομίσματα, συμπεριλαμβανομένων των Einsteinium και Byteball, τα οποία εκτινάχθηκαν, σύμφωνα με τον πάροχο δεδομένων OnChainFx[126], περισσότερο από

119 Βλ. σχετικά σε https://gr.investing.com/crypto/currencies

120 Dr Garrick Hileman και Michel Rauchs, «2017 Global Cryptocurrency Benchmarking Study» (2017), διαθέσιμο σε https://cointelegraph.com/storage/uploads/view/2017-global-cryptocurrency-benchmarking-study.pdf .

121 Ahmed J.D. Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School, (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

122 Nathaniel Popper, «Bitcoin's price has soared. What comes next?», διαθέσιμο σε https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html.

123 Aaron Stanley, «The rise — and fall — of the cryptocurrency millionaires», διαθέσιμο σε https://www.ft.com/content/d0df4322-1559-11e8-9c33-02f893d608c2.

124 Βλ. κατωτέρω σχετικό υποκεφάλαιο.

125 Shana Clor-Proell, Ryan Guggenmos, και Kristina M. Rennekamp, «Mobile Devices and Investment Apps: The Effects of Push Notification, Information Release, and the Fear of Missing Out», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2991262 .

126 Βλ. σχετικά σε https://onchainfx.com

το 1600% του Bitcoin. Περίπου 40 ψηφιακά νομίσματα αξίζουν περισσότερο από 1 δισεκατομμύρια δολάρια, παρόλο που πολλά από αυτά ουδέποτε χρησιμοποιήθηκαν σε κάποιου είδους αγοραπωλησία, εκτός από κερδοσκοπικές συναλλαγές.

5.2 **Ethereum - Ether**

Το δίκτυο Ethereum[127], ένα δίκτυο ψηφιακών νομισμάτων πιο προσαρμόσιμο από τα Bitcoin, σχεδιάστηκε παρέχοντας περισσότερες δυνατότητες από το να αποτελεί μόνο ένα ψηφιακό νόμισμα. Οι υπολογιστές στους οποίους στηρίζεται μπορούν να αξιοποιηθούν και για άλλες εργασίες, όπως για προγράμματα στο δίκτυο, κάτι που καλείται Decentrilized Applications ή DApps[128] (αποκεντρωμένες εφαρμογές) ή για την υποστήριξη «έξυπνων» συμβάσεων (smart contracts)[129]. Αυτό οδήγησε στη δημιουργία μίας τεράστιας κοινότητας προγραμματιστών, οι οποίοι εργάζονται πάνω σε αυτό το λογισμικό[130]. Η αξία του Ether, του ψηφιακού νομίσματος του δικτύου, αυξάνει, όχι όμως με τους ρυθμούς των Bitcoin.

127 Το δίκτυο Ethereum που παράγει το ψηφιακό νόμισμα Ether, δημιουργήθηκε το 2015 από τον Vitalik Buterin, 21 ετών, ο οποίος γεννήθηκε στη Ρωσία και μεγάλωσε στον Καναδά. Ο Buterin εμπνεύστηκε το λογισμικό από το Bitcoin και για το λόγο αυτό παρουσιάζουν κάποια κοινά στοιχεία, όπως το ότι και τα δύο φιλοξενούνται και συντηρούνται από υπολογιστές εθελοντών ανά τον κόσμο, οι οποίοι επιβραβεύονται για την συμμετοχή τους με ψηφιακά νομίσματα που κυκλοφορούν στο δίκτυο κάθε ημέρα. Stavros Stavroyiannis, «Expected Shortfall via Filtered Historical Simulation for Bitcoin and Ethereum» (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162537 .

128 Πρόκειται για εφαρμογές που λειτουργούν αέναα και οι οποίες, αντίθετα με ό,τι συμβαίνει με τις υπόλοιπες που υπάρχουν σήμερα, δεν απαιτούν κάποιον ενδιάμεσο για να λειτουργήσουν ή για να χειριστούν τις πληροφορίες του χρήστη, αλλά συνδέουν απευθείας τους παρόχους με τους χρήστες. Shaen Corbet, Charles James Larkin, Brian M Lucey, Andrew Meegan και Larisa Yarovaya, «Cryptocurrency Reaction to FOMC Announcements: Evidence of Heterogeneity Based on blockchain Stack Position», (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3073727 .

129 Andreas M. Antonopoulos και Gavin Wood, «Mastering Ethereum: Buildin Smart Contracts and Dapps», O' Reilly Media, Sebastopol, (2019): 127. Βλ. επίσης Νικόλαος Θεοδωράκης και Γεώργιος Καλογεράκης, «Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. Ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου», *ΔiΜΕΕ,* τ.1, έτος 16ο (2019): 6.

130 Nathaniel Popper, «Move over Bitvoin. Ether is the digital currency of the moment», (2017), διαθέσιμο σε https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html.

5.3 **Ripple**

Το Ripple δημιουργήθηκε το 2012 από τον Jed McCaleb, τον προγραμματιστή που στο παρελθόν είχε δημιουργήσει το ανταλλακτήριο των Bitcoin Mt. Gox, το οποίο στη συνέχεια κατέρρευσε[131]. Ο McCaleb σχεδίασε το Ripple ως μία ταχύτερη και πιο αποτελεσματική εκδοχή του Bitcoin, χωρίς να υπάρχει η διαδικασία εξόρυξης που τα Bitcoin χρησιμοποιούν για τη διανομή νέων νομισμάτων και για την ασφάλεια του δικτύου τους. Σε συνεργασία με τον Chris Larsen προχώρησαν στη σύσταση μίας εταιρίας με την επωνυμία Ripple και τη δημιουργία ενός λογισμικού ανοιχτού κώδικα, το οποίο παρέχει τη δυνατότητα μετακίνησης χρημάτων μεταξύ ψηφιακών πορτοφολιών[132]. Το νόμισμα Ripple είναι ένα από τα ψηφιακά νομίσματα που μπορούν να μεταφερθούν με αυτό το λογισμικό. Στη συνέχεια, ο McCaleb αποχώρησε από την εταιρία, έχοντας στην κυριότητά του ένα μεγάλο αριθμό νομισμάτων Ripple και προχώρησε στη δημιουργία ενός ανταγωνιστικού λογισμικού, γνωστού ως Stellar[133]. Το λογισμικό αυτό εξελίχθηκε γρηγορότερα από το Ripple με την αξία των νομισμάτων του – τα Lumens[134], να ανέρχεται περίπου στα 14 δισεκατομμύρια δολάρια, καθιστώντας το το 7ο σε σειρά μεγαλύτερο κρυπτονόμισμα[135]. Οι περισσότερες αγορές και πωλήσεις Ripple πραγματοποιούνται στη Νότιο Κορέα, όπου η χρήση των κρυπτονομισμάτων πραγματοποιείται από μικρούς επενδυτές, σύμφωνα με τους παρόχους δεδομένων που καταγράφουν τις συναλλαγές σε ψηφιακά νομίσματα[136].

Σήμερα η εταιρία Ripple έχει επικεντρωθεί στο να διαθέτει το λογισμικό της σε χρηματοπιστωτικά ιδρύματα κατά τη διαδικασία ανταλλαγής ξένων νομισμάτων,

131 «What is Ripple? A step-by-step guide to XRP», διαθέσιμο σε https://www.finder.com.

132 Ό.π. υποσημείωση 111 σχετικά με τα ψηφιακά πορτοφόλια.

133 Πρόκειται για μία πλατφόρμα που συνδέει τράπεζες, συστήματα πληρωμών και ανθρώπους, μετά την ενοποίηση των οποίων τα χρήματα κινούνται με ταχύτητα, αξιοπιστία και ελάχιστο κόστος. Βλ. σχετικά https://www.stellar.org .

134 Βλ. σχετικά https://www.stellar.org/lumens .

135 Βλ. σχετικά https://coinmarketcap.com/currencies/stellar .

136 J. Young, «South Korea More Than Doubled Ripple's Price in Single Week», διαθέσιμο σε https://cointelegraph.com.

κάτι που οι τράπεζες μέχρι τώρα το πραγματοποιούσαν μέσω μίας δυσκίνητης διαδικασίας που περιελάμβανε διαφορετικούς λογαριασμούς σε κάθε εμπλεκόμενη χώρα. Πάνω από 100 τράπεζες χρησιμοποιούν την τεχνολογία Ripple, συμπεριλαμβανομένων των American Express και Banco Santander[137]. Το παράδοξο είναι ότι οι τράπεζες που χρησιμοποιούν το λογισμικό Ripple δεν είναι απαραίτητο να χρησιμοποιούν και νομίσματα Ripple για την μετατροπή δολαρίων, ευρώ ή γιεν[138].

5.4 **KodakCoin**

Ένα άλλο ψηφιακό νόμισμα που τέθηκε σε κυκλοφορία τον Ιανουάριο του 2018 είναι το KodakCoin[139], το οποίο θεωρείται ως ένα «φωτογραφοκεντρικό ψηφιακό νόμισμα που θα ωθήσει τους φωτογράφους και τα πρακτορεία να αποκτήσουν μεγαλύτερο έλεγχο στη διαχείριση των δικαιωμάτων των φωτογραφιών». Η βασική ιδέα πίσω από το KodakCoin είναι να χρησιμοποιηθεί η τεχνολογία blockchain προς βοήθεια των φωτογράφων στη διαχείριση των συλλογών τους, με τη δημιουργία μόνιμων και αμετάβλητων αρχείων - αποδεικτικών δικαιωμάτων πνευματικής ιδιοκτησίας[140]. Η

137 Stan Higgins, «Saudi Central Bank to Test Ripple Payments Tech», διαθέσιμο σε https://www.coindesk.com/saudi-central-bank-test-ripple-payments-tech. Βλ. επίσης Sean Williams, «5 Big Banks Currently Testing Ripple's blockchain Technology», διαθέσιμο σε https://www.fool.com/investing/2017/12/17/5-big-banks-currently-testing-ripples-blockchain-t.aspx και «Cryptocurrency News: Ripple jubilant as major international bank adopts their platform», διαθέσιμο σε https://www.express.co.uk/finance/city/914301/cryptocurrency-news-national-bank-abu-dhabi-ripple-transactions.

138 Nathaniel Popper, «Rise of Bitcoin competitor Ripple creates wealth to rival Zuckerberg», (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/04/technology/bitcoin-ripple.html.

139 Παρά την ονομασία του, το νόμισμα αυτό δεν είναι δημιούργημα της εταιρίας Kodak. Η εταιρία πίσω από αυτό, η WENN Digital, έχει έδρα την Καλιφόρνια και σχετίζεται με ένα Βρετανικό πρακτορείο φωτογραφιών, το οποίο εξειδικεύεται στις άδειες φωτογραφιών παπαράτσι. Σύμφωνα με το συμφωνητικό άδειας ανάμεσα στις δύο εταιρίες, η Kodak δεν θα λάβει καμία ευθεία αμοιβή από τη δημόσια προσφορά των νομισμάτων, αλλά μόνο ένα μειοψηφικό μερίδιο από τη WENN Digital της τάξεως του 3% του συνόλου των νομισμάτων KodakCoin που θα τεθούν σε κυκλοφορία και δικαιώματα επί των μελλοντικών εσόδων. Shaen Corbet, Charles James Larkin, Brian M. Lucey και Larisa Yarovaya, Kodakcoin: A blockchain Revolution or Exploiting a Potential Cryptocurrency Bubble? (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3140551 .

140 Οι φωτογράφοι θα μπορούν να ανεβάζουν τις φωτογραφίες τους σε μία πλατφόρμα που ονομάζεται KodakOne, θα δημιουργούν για κάθε φωτογραφία μία άδεια βασισμένη στην τεχνολογία blockchain και θα χρησιμοποιούν λογισμικό που θα διαπερνά όλο διαδίκτυο (web-crawling software), αναζητώντας παραβιάσεις πνευματικών δικαιωμάτων. Αντί για συμβατικά χρήματα, οι φωτογράφοι θα μπορούν να αμείβονται από τους πελάτες τους σε KodakCoin. Chris Berg, Jason Potts και Sinclair Davidson,

εταιρία επίσης κατοχύρωσε με συμφωνία αδειοδότησης, την απόκτηση ενός υπολογιστή εξόρυξης Bitcoin, τον οποίο ονόμασε Kodak KashMiner και ο οποίος επιτρέπει στους χρήστες να δημιουργούν τα δικά τους κρυπτονομίσματα.

Θα μπορούσε να σκεφτεί κάποιος ότι ένα ψηφιακό νόμισμα που επιχειρεί να φέρει ένα σύστημα δίκαιης απόκτησης αδειών για τους καλλιτέχνες, θα ήταν εύκολα προσβάσιμο. Αντιθέτως, λόγω ρυθμιστικών απαιτήσεων, τα ψηφιακά νομίσματα KodakCoin θα είναι διαθέσιμα μόνο στους επονομαζόμενους «διαπιστευμένους επενδυτές»[141] στις ΗΠΑ. Ακόμα κι εάν υπάρξουν φωτογράφοι με τις απαιτούμενες προϋποθέσεις των διαπιστευμένων επενδυτών, θα ήταν εξαιρετικά δύσκολο να αναλώσουν τα KodakCoin ή να τα ανταλλάξουν με μετρητά. Η Επιτροπή Κεφαλαιαγοράς των ΗΠΑ έχει προειδοποιήσει ότι τίτλοι, όπως τα KodakCoin που μεταβιβάζονται ιδιωτικά, θα είναι δύσκολο να επαναμεταβιβαστούν – όσοι επενδύσουν σε αυτά ίσως χρειαστεί να τα κρατήσουν επ' αόριστον[142].

5.5 **Petro**

Δεν πρόκειται στην πράξη για ανταγωνιστή του Bitcoin, αλλά ουσιαστικά για την ύστατη προσπάθεια της κυβέρνησης της Βενεζουέλας να αντιμετωπίσει την κρίση που πλήττει τη χώρα τα τελευταία χρόνια και έχει επιφέρει τεράστιες ελλείψεις σε είδη πρώτης ανάγκης, όπως τρόφιμα και φάρμακα, αύξηση της εγκληματικότητας και κατάρρευση των δημόσιων υπηρεσιών και του συστήματος υγείας[143]. Η αξία αυτού του ψηφιακού νομίσματος προέκυψε από τα αποθέματα πετρελαίου της χώρας, της

«KodakOne could be the start of a new kind of intellectual property», διαθέσιμο σε https://theconversation.com/kodakone-could-be-the-start-of-a-new-kind-of-intellectual-property-89966.

141 Διαπιστευμένος επενδυτής θεωρείται το πρόσωπο του οποίου η περιουσία αποτιμάται σε πάνω από 1εκ δολάρια αξία ή το ετήσιο εισόδημά του ανέρχεται τουλάχιστον στα 200.000 δολάρια. Meredith R. Conway, «Money, Money, Money; It's a Rich Man's World: Making the Corporate Tax Fair», *17 J. Bus. L.* (2015): 1181.

142 Kevin Roose, «Kodak's dubious cryptocurrency gamble», διαθέσιμο σε https://www.nytimes.com/2018/01/30/technology/kodak-blockchain-bitcoin.html .

143 Kirk Semple και Nathaniel Popper, «Venezuela Launches Virtual Currency,Hoping to Resuscitate Economy», διαθέσιμο σε https://www.nytimes.com/2018/02/20/world/americas/venezuela-petro-currency.html. Βλ. επίσης Usman W. Chohan, «Cryptocurrencies as Asset-Backed Instruments: The Venezuelan Petro», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3119606 .

οποίας η κυβέρνηση έτρεφε την ελπίδα ότι θα συνέβαλλε στην εξόφληση των δανείων και την έναρξη εισαγωγών των ειδών πρώτης ανάγκης. Είναι χαρακτηριστικό, δε, ότι το Petro αποτελεί το πρώτο κρυπτονόμισμα που τέθηκε σε κυκλοφορία από μία χώρα.

Πολλοί αναλυτές και επικριτές της κυβέρνησης Μαδούρο υπήρξαν απαισιόδοξοι για το συγκεκριμένο εγχείρημα. Θεώρησαν ότι πρόκειται για μία κίνηση απελπισίας από ένα καθεστώς απομονωμένο από τα υπόλοιπα κράτη, του οποίου η οικονομία βρίσκεται εκτός ελέγχου και οι επενδυτές δεν πίστεψαν ότι η κυβέρνηση θα διατηρήσει πιστά τη σύνδεση ανάμεσα στο νόμισμα και την αξία του πετρελαίου. Η ιστορία θα δείξει τελικά εάν αυτό το εγχείρημα θα στεφθεί με επιτυχία και θα δώσει μία ανάσα ζωής στους κατοίκους της Βενεζουέλα – όσους έχουν απομείνει στη χώρα και δεν έχουν μεταναστεύσει στα γειτονικά κράτη αναζητώντας μία καλύτερη τύχη ή θα υποφέρει τα ίδια δεινά με το χρέος της χώρας[144].

6 Τεχνολογία blockchain

Στη σημερινή εποχή έχουμε εξοικειωθεί ιδιαίτερα με την αποκαλούμενη οικονομία της διαδικτυακής πληροφορίας. Η οικονομία αυτή έχει εκτοπίσει την οικονομία της βιομηχανικής πληροφορίας που χαρακτήριζε την παραγωγή της πληροφορίας από το δεύτερο μισό του 19ου αιώνα έως και τον 20ό αιώνα Αυτό που χαρακτηρίζει την οικονομία της διαδικτυακής πληροφορίας είναι ότι η αποκεντρωμένη ατομική δράση παίζει ένα πολύ σημαντικότερο ρόλο από αυτό που έπαιζε ή θα μπορούσε να παίζει στην οικονομία της βιομηχανικής πληροφορίας[145]. Ένα από τα πολλά υποσχόμενα

144 «Maduro bids to revive Venezuela's 'petro' cryptocurrency», (2020), διαθέσιμο σε https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency . Βλ. επίσης Leon Markovitz, «Venezuela’s Petro Cryptocurrency Is a Gift to Future Generations», (2018), διαθέσιμο σε https://www.coindesk.com/venezuelas-petro-cryptocurrency-is-a-gift-to-future-generations .

145 F. Xavier Olleros και Majlinda Zhegu, «Blockchain Technology: Principles and Applications», Research Handbook on Digital Transformations, Edward Elgar, (2016). Βλ. επίσης Christian Catalini και Joshua S. Gans, «Some Simple Economics of the blockchain», Rotman School of Management Working Paper No.

επιτεύγματα της νέας οικονομίας είναι η τεχνολογία του διαμοιρασμένου καθολικού – λογιστικού βιβλίου, γνωστή ως «blockchain»[146]. Το δίκτυο αυτό συντηρείται από μία ομάδα αποκεντρωμένων ατόμων, τα οποία εξορύσσουν Bitcoin, εγκρίνουν συναλλαγές και επιβραβεύονται για την εργασία τους με νέα Bitcoin[147]. Το Παγκόσμιο Οικονομικό Φόρουμ (World Economic Forum[148]) εκτιμά ότι περισσότερες από 25 χώρες επενδύουν σε τεχνολογία blockchain, υποβάλλοντας περισσότερα από 2.500 διπλώματα ευρεσιτεχνίας και επενδύοντας περί τα 1,3 δισεκατομμύρια δολάρια. Ο ιδρυτής και Πρόεδρος του Παγκόσμιου Οικονομικού Φόρουμ Klaus Schwab[149] δίδει την εξής ερμηνεία για την τεχνολογία αυτή: πρόκειται για ένα διαμοιρασμένο, προγραμματιζόμενο, κρυπτογραφικά ασφαλές και έμπιστο λογιστικό βιβλίο (καθολικό[150]), το οποίο δεν ελέγχεται από κάποιον συγκεκριμένο χρήστη και μπορεί να επιθεωρηθεί από τον οποιονδήποτε. Η τεχνολογία αυτή συγκρίνεται συχνά με το πρωτόκολλο TCP/IP[151], πάνω στο οποίο στηρίζεται το

2874598. MIT Sloan Research Paper No. 5191-16 (2017), Lawrence J. Trautman, «Is Disruptive blockchain Technology the Future of Financial Services?» 69 The Consumer Finance Law Quarterly Report 232 (2016), Marcella Atzori, «Blockchain Technology and Decentralized Governance: Is the State Still Necessary?» (2015), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 , Sinclair Davidson, Primavera De Filippi και Jason Potts, Economics of blockchain, (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751, Ryan Amsden και Denis Schweizer, «Are blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3163849 .

146 Στα ελληνικά έχει προταθεί η μετάφραση του όρου ως «αλυσίδα κοινοποιήσεων» ή «αλυσίδα συστοιχιών» ή «αλυσίδα κατανεμημένης εγγραφής». Καμία όμως απόδοση δεν μπορεί να περιγράψει επακριβώς τη λειτουργία της τεχνολογίας αυτής. Για το λόγο αυτό στην παρούσα διατηρείται ο αγγλικός όρος blockchain.

147 «Bitcoin: η αυταπάτη που θα μπορούσε να κατακτήσει τον κόσμο», διαθέσιμο σε http://tvxs.gr.

148 Το Παγκόσμιο Οικονομικό Φόρουμ, το οποίο έχει αφιερωθεί στη βελτίωση της παγκόσμιας οικονομικής κατάστασης, είναι ένας οργανισμός με στόχο τη δημόσια και ιδιωτική συνεργασία. Το Φόρουμ απασχολεί τους καλύτερους επιστήμονες στους τομείς της πολιτικής, των επιχειρήσεων και άλλων τομέων της κοινωνίας, με στόχο τη διαμόρφωση παγκόσμιων, τοπικών και βιομηχανικών σχεδίων. Ιδρύθηκε το έτος 1971 ως μη κερδοσκοπικός οργανισμός και τα κεντρικά του βρίσκονται στη Γενεύη της Ελβετίας. Το Φόρουμ καταβάλει κάθε προσπάθεια να αναδείξει την επιχειρηματικότητα σε παγκοσμίου ενδιαφέροντος θεματική, διατηρώντας παράλληλα τα υψηλότερα πρότυπα διακυβέρνησης. Βλ. σχετικά https://www.weforum.org

149 Klaus Schwab, «The Fourth Industrial Revolution», (2017), διαθέσιμο σε https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab .

150 Ό.π. υποσημ. 69.

151 «TCP/IP» (Transmission Control Protocol/Internet Protocol): πρόκειται για μία ακολουθία πρωτοκόλλων επικοινωνίας, τα οποία χρησιμοποιούνται για την διασύνδεση του συσκευών δικτύου στο διαδίκτυο. Το TCP/IP μπορεί επίσης να χρησιμοποιηθεί ως πρωτόκολλο επικοινωνίας σε ένα ιδιωτικό δίκτυο (intranet ή extranet). Βλ. σχετικά https://searchnetworking.techtarget.com/definition/TCP-IP .

διαδίκτυο. Και οι δύο τεχνολογίες επιτρέπουν την εφαρμογή ενός νέου επιπέδου υπηρεσιών. Με τον ίδιο τρόπο που επέφερε το διαδίκτυο ουσιώδεις μεταβολές στον τρόπο με τον οποίο ανταλλάσσουμε πληροφορίες, η τεχνολογία blockchain, ως καινοτομία ανοιχτού κώδικα, υπόσχεται να φέρει την επανάσταση στον τρόπο με τον οποίο πραγματοποιούνται οι συναλλαγές ανάμεσα στους ιδιώτες, τις επιχειρήσεις, ακόμη και τα μηχανήματα.

Στην τεχνολογία blockchain οι συναλλαγές κατηγοριοποιούνται διαδοχικά σε ομάδες. Κάθε ομάδα είναι αλυσιδωτά συνδεδεμένη με την προηγούμενη και καταγράφεται αμετάβλητα σε ένα peer-to-peer[152] δίκτυο, με τη χρήση μηχανισμών έμπιστης κρυπτογράφησης και ασφάλειας. Η τήρησή του πραγματοποιείται από όλους τους συμμετέχοντες, όπως έχει συμφωνηθεί, χωρίς να απαιτείται κάποια κεντρική Αρχή.

Τα βασικά χαρακτηριστικά της τεχνολογίας αυτής είναι[153]:

I. Διαφάνεια: όλα τα δεδομένα είναι δημόσια, δεν μπορούν να μεταβληθούν αυθαίρετα κι ελέγχονται εύκολα.

II. Πλεόνασμα: κάθε χρήστης διατηρεί ένα αντίγραφο των δεδομένων και με αυτόν τον τρόπο τα δεδομένα δεν μπορούν να τεθούν εκτός λειτουργίας λόγω κάποιας δυσλειτουργίας του συστήματος ή από επιβλαβείς ενέργειες τρίτων.

III. Σταθερότητα: η μεταβολή των αρχείων είναι απαγορευτική και απαιτεί συγκατάθεση που να παρέχεται σύμφωνα με το πρωτόκολλο, για παράδειγμα από την πλειοψηφία των χρηστών. Με τον τρόπο αυτό εξασφαλίζεται η ακεραιότητα.

IV. Απουσία διαμεσολάβησης: η απουσία των μεσαζόντων, όπως οι τράπεζες ή οι συλλογικές κοινωνίες από τις συναλλαγές μειώνει τα έξοδά τους και τους

152 Σύνδεση με ένα δίκτυο υπολογιστών στο οποίο κάθε υπολογιστής μπορεί να λειτουργήσει ως εξυπηρετητής (server) για τους υπόλοιπους, επιτρέποντας τη διαμοιρασμένη πρόσβαση στα αρχεία και τα περιφερειακά, χωρίς την ανάγκη ύπαρξης ενός κεντρικού εξυπηρετητή (server). Βλ. σχετικά https://searchnetworking.techtarget.com/definition/peer-to-peer .

153 F. Xavier Olleros και Majlinda Zhegu, Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, Edward Elgar, (2016).

κινδύνους που συνδέονται με τους μεσάζοντες. Αυτό δεν σημαίνει, βέβαια, ότι δεν προκύπτουν νέα είδη μεσαζόντων, ως αποτέλεσμα της βαθύτερης εφαρμογής των τεχνολογιών blockchain στον κοινωνικό ιστό.

Σήμερα, το πιο γνωστό παράδειγμα επιτυχούς εφαρμογής της βασισμένης στο blockchain τεχνολογίας είναι το Bitcoin[154]. Άλλα κρυπτονομίσματα, όπως το Ether ή το Litecoin προσπαθούν να αντιγράψουν την επιτυχία αυτή. Παραδοσιακά μέχρι σήμερα οι περισσότερες απόπειρες για ψηφιακά νομίσματα παρουσίασαν το ίδιο ελάττωμα: σχεδόν όλα όσα είναι διαθέσιμα online, μπορούν με μεγάλη ευκολία να αντιγραφούν. Το γεγονός αυτό θα σήμαινε το τέλος του ψηφιακού νομίσματος. Το πρόβλημα αυτό λύθηκε με την τεχνολογία blockchain[155], της οποίας οι δυνατότητες δεν αφορούν μόνο τον τομέα των πληρωμών. Η δημοσιότητα που απέκτησαν τα προϊόντα που σχετίζονται με την τεχνολογία αυτή αποδεικνύεται και από το εξής παράδειγμα: μία βρετανική εταιρία προσέθεσε τη λέξη «blockchain» στην επωνυμία της και είδε τις μετοχές της να αυξάνουν κατά 394%[156]. Αλλά η φρενίτιδα αυτή δεν μείωσε τον επενδυτικό ενθουσιασμό για το ίδιο το Bitcoin, αντιθέτως τον απλοποίησε. Και η πιθανή εφαρμογή της τεχνολογίας blockchain σε όλα τα είδη των βιομηχανιών, από τις αυτοκινητοβιομηχανίες έως τις ασφαλιστικές εταιρίες, ενέπνευσε ακόμα και τους μη σχετικούς με την τεχνολογία, να μάθουν για τα κρυπτονομίσματα και αυτό χρησίμευσε ως πνευματικό εφαλτήριο για τους επενδυτές σε Bitcoin[157]. Ο επιχειρηματικός κόσμος επέδειξε μεγάλο ενδιαφέρον σχετικά με την τεχνολογία αυτή, ως αποκεντρωμένο χρηματοπιστωτικό δίκτυο[158]. Πολλά πιστωτικά ιδρύματα στοιχηματίζουν ότι οι χρηματικές συναλλαγές κάποια μέρα θα γίνονται και

154 Renato dos Santos, «On the Philosophy of Bitcoin/blockchain Technology: Is It a Chaotic, Complex System?», (2017), διαθέσιμο σε https://onlinelibrary.wiley.com/doi/abs/10.1111/meta.12266 .

155 «Can you duplicate Bitcoins and Cryptocurrency?», διαθέσιμο σε https://blockogy.com .

156 Lisa Pham, «This Company Added the Word 'Blockchain' to Its Name and Saw Its Shares Surge 394%», (2017), διαθέσιμο σε https://www.bloomberg.com/news/articles/2017-10-27/what-s-in-a-name-u-k-stock-surges-394-on-blockchain-rebrand .

157 Ludovic Phalippou, «The Future of Private Markets» (2018), Βλ. επίσης «19 Corporations Working On blockchain And Distributed Ledgers», διαθέσιμο σε https://www.cbinsights.com.

158 Katya Malinova και Andreas Park, «Market Design with blockchain Technology», (2017), διαθέσιμο σε https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/19_slides_park.pdf?la=en .

στον πραγματικό κόσμο σε δίκτυα όπως των Bitcoin[159], τα οποία λειτουργούν ταχύτερα, πιο αποτελεσματικά και με μεγαλύτερη ασφάλεια από ό,τι τα παραδοσιακά χρηματοπιστωτικά συστήματα.

Η σημασιολογική συζήτηση[160] σχετικά με το τι είναι σωστό ή όχι τεχνικά στο Bitcoin, αφορά στους ειδικούς των Η/Υ και λίγο απασχολεί τον έξω κόσμο[161]. Όμως οι διαφωνίες μέσα στην κοινότητα των Bitcoin παρακολουθούνται στενά από τους υπευθύνους των κεντρικών τραπεζών και τα στελέχη της χρηματοοικονομικής βιομηχανίας. Οι ειδήμονες των χρηματοοικονομικών παρακολουθούν στενά τις επιτυχίες και τις αποτυχίες του Bitcoin, καθώς πειραματίζονται με την τεχνολογία blockchain. Πολλά μεγάλα ινστιτούτα ελπίζουν ότι θα ενσωματώσουν την τεχνολογία αυτή στα σχέδιά τους τα σχετικά με τις υποδομές της παγκόσμιας μελλοντικής οικονομίας. Η υπεύθυνη του Digital Currency Initiative του MIT[162] θεωρεί ότι ο κόσμος παρατηρεί την τεχνολογία αυτή, διότι βλέπει την αρχή ενός νέου χρηματοοικονομικού συστήματος, το οποίο έχει πολύ διαφορετική δομή από το σημερινό[163].

159 «Four blockchain Use Cases for Banks. FinTech Network», διαθέσιμο σε https://blockchainapac.fintecnet.com.

160 Η σημασιολογία αναφέρεται στην κατανόηση και κατάλληλη χρήση του νοήματος σε μεμονωμένες λέξεις, φράσεις, προτάσεις και ακόμη μεγαλύτερων μονάδων. Αλίκη Κασσωτάκη, «Στρατηγικές Ανάπτυξης Σημασιολογικών Δομών του Λόγου», διαθέσιμο σε https://upbility.gr/blogs/blog/79662083 .

161 Christian Cachin, Angelo De Caro, Pedro Moreno-Sanchez, Björn Tackmann και Marko Vukolic, «The Transaction Graph for Modeling blockchain Semantics», (2017), διαθέσιμο σε https://assets.pubpub.org/oh4wbdb0/71581340107043.pdf .

162 Στόχος του Ινστιτούτου DCI είναι να φέρει κοντά τους πιο σημαντικούς επιστήμονες του Πανεπιστημίου MIT και άλλων Ακαδημαϊκών Ιδρυμάτων για να διευθύνουν την έρευνα που απαιτείται για την υποστήριξη της εξέλιξης των ψηφιακών νομισμάτων και της τεχνολογίας blockchain. Όλοι μαζί οι πανεπιστημιακοί φορείς και τα ερευνητικά ινστιτούτα συνεργάζονται με ανεξάρτητες ομάδες της πανεπιστημιακής κοινότητας, φοιτητές και ερευνητές για τη συγγραφή επιστημονικών εργασιών, τη διαχείριση πρωτότυπων τεχνολογιών και τη δημιουργία σχετικών λογισμικών ανοιχτού κώδικα. Βλ. σχετικά https://dci.mit.edu

163 Neha Narula, «Digital Currency Initiative and Federal Reserve Bank of Boston Announce CBDC Design Collaboration», (2020), διαθέσιμο σε https://medium.com/mit-media-lab-digital-currency-initiative/digital-currency-initiative-and-federal-reserve-bank-of-boston-announce-cbdc-design-collaboration-39041d8fe2 .

6.1 Εφαρμογές της τεχνολογίας blockchain

I. Χρηματοπιστωτικές/Ασφαλιστικές υπηρεσίες: η τεχνολογία blockchain έρχεται να απλοποιήσει σημαντικά τον παραδοσιακό δαπανηρό, περίπλοκο και αργό τρόπο επεξεργασίας κι εκκαθάρισης των συναλλαγών, όπου εμπλέκονται περισσότερα μέρη για την ολοκλήρωση μίας συναλλαγής (πράκτορες, θεματοφύλακες, διαχειριστές εκκαθάρισης κλπ), κάτι που καθίσταται περιττό με τη χρήση της νέας τεχνολογίας. Προσφέρεται ταχύτητα κατά την επιβεβαίωση κι εκκαθάριση των συναλλαγών, ανεξάρτητα από τη γεωγραφική θέση των συναλλασσόμενων. Επίσης, ως μέσο διεκπεραίωσης πληρωμών, η νέα τεχνολογία θα απλοποιήσει και θα επιταχύνει τη διαδικασία επιβεβαίωσης - αυτή θα είναι άμεση και χωρίς τη μεσολάβηση τρίτων (τράπεζας)[164].

II. Τήρηση μητρώων: η νέα τεχνολογία παρέχει ένα νέο τρόπο καταχώρισης και αποθήκευσης πληροφοριών σε μία αλυσίδα δεδομένων, χωρίς διπλές εγγραφές ή εσφαλμένες καταχωρήσεις σε μητρώα όπως το κτηματολόγιο, το ληξιαρχείο, το μητρώο εταιρειών, το φορολογικό μητρώο, το μητρώο δικαιωμάτων ή της βιομηχανικής ιδιοκτησίας. Περαιτέρω, η καταχώριση δεδομένων δύναται να συνδυαστεί με επιπλέον λειτουργικές δυνατότητες, οι οποίες ενσωματώνονται στην εκάστοτε πλατφόρμα[165].

164 Στη διεθνή μεταφορά εμπορευμάτων, στην περίπτωση του «Cash Against Documents» (CAD), ο παραλήπτης των εμπορευμάτων πρέπει να περιμένει από αρκετές ώρες έως και μερικές ημέρες για να παραλάβει τα εμπορεύματα, μέχρι ο μεταφορέας να λάβει την επιβεβαίωση για λογαριασμό του αποστολέα ότι το τίμημα έχει καταβληθεί. Κων/νος Λογαράς, «Η Τεχνολογία blockchain, οι εφαρμογές και οι νομικές πτυχές της. Τι είναι η τεχνολογία blockchain, ποιες είναι οι κυριότερες εφαρμογές της και οι κυριότερες νομικές πτυχές της», (2018), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/h-tehnologia-blockchain-oi-efarmoges-kai-oi-nomikes-ptyhes-tis.

165 Σε μία πειραματική εφαρμογή της τεχνολογίας από το χρηματιστήριο του NASDAQ το 2016, καταχωρήθηκε η κυριότητα κινητών αξιών των χρηστών, όπως τηρείται από την κεντρική αρχή (CSD), και στη συνέχεια αποδόθηκαν δικαιώματα ψήφου μέσω tokens, ώστε οι χρήστες να μπορούν να τα «ξοδεύουν» και να ψηφίζουν στις συνελεύσεις, εφόσον ήταν και φορείς του αντίστοιχου δικαιώματος ψήφου. Ό.π. υποσημείωση 164.

III. «Έξυπνα» συμβόλαια (smart contracts[166]): αν και υφίστανται εδώ και χρόνια, η τεχνολογία blockchain τους παρέχει νέες δυνατότητες[167]. Καταργείται η ανάγκη για την ύπαρξη τρίτων μερών και εξασφαλίζεται ότι όλοι οι συμμετέχοντες γνωρίζουν τις λεπτομέρειες του συμβολαίου και ότι οι συμβατικοί όροι θα εκπληρώνονται αυτόματα όταν πληρωθούν ορισμένες προϋποθέσεις.

IV. Ψηφιακή διακυβέρνηση: Η ψηφιακή διακυβέρνηση και ηλεκτρονική ψηφοφορία καθίσταται πλέον πολύ πιο ασφαλείς και υπό διαφανείς διαδικασίες μέσω της κρυπτογράφησης των δεδομένων, έτσι ώστε να καθίσταται εξαιρετικά δύσκολη η παραποίησή τους.

V. Διαχείριση ψηφιακής ταυτότητας: Η δημιουργία ψηφιακής ταυτότητας με την τεχνολογία blockchain θα παρέχει την ασφάλεια των προσωπικών δεδομένων μέσω της κρυπτογράφησης και τη διαχείρισή τους από τους ίδιους τους χρήστες. Περαιτέρω, θα είναι δυνατή η συγχώνευση περισσότερων δεδομένων ταυτοποίησης (ταυτότητα, διαβατήριο, άδεια οδήγησης, κωδικοί πρόσβασης, μητρώα κοινωνικής ασφάλισης) σε μία ψηφιακή ταυτότητα η οποία θα εγγράφεται σε οποιοδήποτε μητρώο.

166 Ψηφιοποιημένα συμβόλαια στα οποία έχει ενσωματωθεί κώδικας υπό τη μορφή Αν – [συμβεί] αυτό – τότε [θα συμβεί] – εκείνο (if –this – then – that, εν συντομία IFTTT), τα οποία εκτελούνται αυτόματα αν πληρωθούν οι προϋποθέσεις που έχουν τεθεί. Ό.π. υποσημείωση 164.

167 Χαρακτηριστική περίπτωση αποτελεί ο λεγόμενος διακόπτης εκκίνησης σε ένα όχημα (starter interrupter), δηλαδή, η συσκευή η οποία έχει ενσωματωμένο ένα τέτοιο συμβόλαιο, το οποίο εκτελείται αυτόματα σε περίπτωση που παραβιαστούν οι όροι χρηματοδότησης για την απόκτηση του οχήματος, οπότε και δεν επιτρέπει την εκκίνηση του κινητήρα. Christian Cachin, Angelo De Caro, Pedro Moreno-Sanchez, Björn Tackmann και Marko Vukolic, «The Transaction Graph for Modeling blockchain Semantics», (2017), διαθέσιμο σε https://assets.pubpub.org/oh4wbdb0/71581340107043.pdf .

6.2 Νομικά ζητήματα της τεχνολογίας blockchain Δίκαιο πνευματικής ιδιοκτησίας

Η τεχνολογία blockchain παρέχει τη δυνατότητα της γνώσης και της διάθεσης της πληροφορίας σύμφωνα με τις διατάξεις προστασίας των πνευματικών δικαιωμάτων[168], μέσω αυτού που καλείται «αξιόπιστη χρονοσήμανση» (Trusted Timestamping[169]). Η αξιόπιστη χρονοσήμανση[170], η αλληλουχία χαρακτήρων ή στοιχείων που δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια και κατ' επέκταση παρέχουν ασφαλή παρακολούθηση του χρόνου δημιουργίας και τροποποίησης ενός εγγράφου, είναι ένα απαραίτητο εργαλείο στον επιχειρηματικό κόσμο, καθώς επιτρέπει στα ενδιαφερόμενα μέρη να γνωρίζουν με βεβαιότητα την ημεροχρονολογία σύνταξης του αμφισβητούμενου εγγράφου. Σύμφωνα με τον Ευρωπαϊκό Κανονισμό eIDAS[171] (Κανονισμός 2014/ 910), η χρονοσήμανση είναι μία από τις ηλεκτρονικές υπηρεσίες που θεωρούνται κλειδιά για τις ασφαλείς διασυνοριακές ηλεκτρονικές συναλλαγές και το κεντρικό δομικό στοιχείο για την Ενιαία Ψηφιακή Αγορά (Digital Single Market[172]). Έως ένα βαθμό η τεχνολογία blockchain μπορεί να θεωρηθεί ως μία βάση δεδομένων από επιβεβαιωμένες δημόσιες χρονοσημάνσεις. Παρέχει τη δυνατότητα στον καθένα να δηλώσει δημόσια και αμετάκλητα ότι κάποιο συγκεκριμένο γεγονός έχει συμβεί μια συγκεκριμένη στιγμή. Επιπλέον, η τεχνολογία αυτή μπορεί να καταστεί πολύ

168 Alexander Ivanovitch Savelyev, «Copyright in the blockchain era: promises and challenges», *Computer Law & Security Review, Vol.* 34/3 (2018): 550-561.

169 Η χρονοσήμανση είναι μία αλληλουχία χαρακτήρων ή κωδικοποιημένης πληροφορίας που ταυτοποιεί το πότε συμβαίνει ένα συγκεκριμένο συμβάν, παρέχοντας συνήθως ημερομηνία και ώρα της ημέρας, μερικές φορές με ακρίβεια κλάσματος δευτερολέπτου. Bela Gipp, Norman Meuschke και André Gernandt. «Decentralized Trusted Timestamping using the Crypto Currency Bitcoin», (2015).

170 Ν. 4727/2020 περί Ψηφιακής Διακυβέρνησης.

171 «eIDAS» (electronic IDentification, Authentication and trust Services): πρόκειται για έναν ευρωπαϊκό Κανονισμό που περιέχει προϋποθέσεις σχετικές με την ηλεκτρονική αναγνώριση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές της εσωτερικής αγοράς. Εκδόθηκε τον Ιούλιο του 2014, τέθηκε σε εφαρμογή το Σεπτέμβριο του ίδιου έτους και είναι σε ισχύ από τον Ιούλιο του 2016. Βλ. σχετικά https://ec.europa.eu

172 Πρόκειται για την πολιτική που συμπεριλαμβάνεται στην Ευρωπαϊκή Ενιαία Αγορά (European Single Market) και καλύπτει τις περιπτώσεις του ψηφιακού μάρκετινγκ, του ηλεκτρονικού εμπορίου και των τηλεπικοινωνιών. Τέθηκε σε ισχύ για πρώτη φορά το Μάιο του 2015. Βλ. σχετικά https://ec.europa.eu

χρήσιμη στον καθορισμό του τεκμηρίου των συγγραφικών δικαιωμάτων και της επίλυσης διαφωνιών ως προς τη χρονική προτεραιότητα στον τομέα αυτό[173].

Η συνάρτηση κατακερματισμού (hash function) διαμορφώνει τη βάση της ασφάλειας και του αμετάβλητου της τεχνολογίας blockchain[174]. Με τη συνάρτηση αυτή, η οποία είναι ένας μαθηματικός τύπος ο οποίος μετατρέπει τα πρωτότυπα δεδομένα σε αποτυπώματα δεδομένων που ονομάζονται τιμές (hashes), ο δικαιούχος των πνευματικών δικαιωμάτων μπορεί να αποκτήσει μία μοναδική σύνοψη του προστατευομένου έργου του[175]. Δύο τέτοιες συνόψεις μπορούν να είναι ίδιες μόνο εάν τα αρχικά δεδομένα είναι ίδια: μικρές διαφορές θα οδηγήσουν σε διαφορετικό αριθμό τιμών. Αυτές οι τιμές θα διαχωρίσουν το ένα προστατευμένο έργο από το άλλα. Στην περίπτωση που υπάρξει κάποια συναλλαγή προστατευμένου από πνευματικά δικαιώματα έργου (για παράδειγμα εκχώρηση ή άδεια), η τιμή - hash αυτού του έργου που συμπεριλαμβάνεται στη συναλλαγή και επιβεβαιώνεται σύμφωνα με το πρωτόκολλο blockchain, προσδίδει πλέον στη συναλλαγή το πλεονέκτημα της χρονοσήμανσης και το περιεχόμενό της κωδικοποιείται. Συνεπεία αυτού, η πληροφορία σχετικά με το δικαιούχο των πνευματικών δικαιωμάτων και οι μεταγενέστερες μεταβολές αυτού, με τα αντίστοιχα χρονικά σημεία είναι ενσωματωμένα στη blockchain και δεν μπορούν να πλαστογραφηθούν. Κατ' επέκταση, αρχεία σχετικά με το δικαιούχο ενός προστατευόμενου με πνευματικά δικαιώματα έργου αντανακλώνται αναπόφευκτα στη βάση δεδομένων blockchain και μπορούν εύκολα να επιβεβαιωθούν από κάθε ενδιαφερόμενο πρόσωπο.

---

173 Dan Hunter και Jake Goldenfein, «Blockchains, Orphan Works, and the Public Domain», *Columbia Journal of Law & the Arts*, Vol. 41, No. 1 (2017).

174 Η συνάρτηση κατατεμαχισμού, γνωστή και ως συνάρτηση κατακερματισμού, είναι μια μαθηματική συνάρτηση όπου εισάγεται κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο δεδομένο σταθερού μεγέθους αναπαράστασης. Το μέγεθος αυτό μπορεί να είναι από 32bit μέχρι 256bit ή περισσότερα, ανάλογα με το λόγο χρήσης της συνάρτησης. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται «τιμές κατατεμαχισμού» (hash values), «κώδικες κατατεμαχισμού» (hash codes), «αθροίσματα κατατεμαχισμού» (hash sums) ή απλά «τιμές» (hashes). Ameer Rosic, «What is Hashing? Under the hood of blockchain», διαθέσιμο σε https://blockgeeks.com/guides/what-is-hashing/.

175 Kazuhiro Kondo, «Multimedia Information Hiding Technologies and Methodologies for Controlling data», IGI Global (2012).

Η εφαρμογή της τεχνολογίας αυτής μπορεί να αντικαταστήσει δυσκίνητους μηχανισμούς απόδειξης της πνευματικής ιδιοκτησίας επί των προστατευομένων έργων[176], όπως είναι η καταχώριση σε κρατικούς φορείς ή σε συλλογικά όργανα προστασίας των πνευματικών δικαιωμάτων (για παράδειγμα καταχώριση ενός λογισμικού σε γραφεία ευρεσιτεχνιών) ή ακόμα περισσότερο να αντικαταστήσει την απαρχαιωμένη και περιττή μέθοδο αποστολής από το δικαιούχο ενός γράμματος που να περιέχει το έργο, προς τον ίδιο, με στόχο την απόκτηση βεβαίας χρονολογίας μέσω της σφραγίδας του ταχυδρομείου[177].

Η διαφορά που εισάγει η τεχνολογία blockchain σε σχέση με τις συμβατικές τεχνολογίες είναι στο επίπεδο εμπιστοσύνης. Ο κύριος στόχος ενός ψηφιακού αποτυπώματος είναι να χρησιμεύσει ως ένα εργαλείο που να απαλλάσσει από τους διαδικτυακούς μεσάζοντες και κατά συνέπεια, να μην εξαρτάται από την πολιτική κάθε ξεχωριστής διαδικτυακής πλατφόρμας και των υποδομών της[178]. Οι όροι χρήσης (terms of use[179]) των παραδοσιακών τεχνολογιών είναι δυνατόν να μεταβάλλονται μονομερώς οποιαδήποτε χρονική στιγμή, αναπόφευκτη συνέπεια της «συγκέντρωσης» (centralization[180]). Η τεχνολογία blockchain από την άλλη, προσφέρει μία λύση βασιζόμενη στις αρχές της αποκέντρωσης (decentralization[181]). Απουσιάζει η εξάρτηση από κάποιον εξειδικευμένο πάροχο και οι όροι χρήσης (terms

176 JP. Danko, «Blockchain Copyright Protection – A Viable Solution To Prove Ownership of Creative Works?», (2018), διαθέσιμο σε https://www.diyphotography.net/blockchain-copyright-protection-a-viable-solution-to-prove-ownership-of-creative-works/ .

177 Bill Rosenblatt, «Dot blockchain Media Makes blockchain Plus Watermarking a Reality», διαθέσιμο σε https://copyrightandtechnology.com.

178 Bill Rosenblatt, «New White Paper: Watermarking Technology and blockchains in the Music Industry» (2017) διαθέσιμο σε https://copyrightandtechnology.com.

179 Ό.π. υποσημείωση 122.

180 Η διαδικασία κατά την οποία οι αποφάσεις λαμβάνονται από λίγους. Όλες οι σημαντικές αποφάσεις και ενέργειες στα κατώτατα επίπεδα και όλα τα θέματα και οι ενέργειες στα ανώτατα επίπεδα υπόκεινται στην έγκριση αυτού που τα διαχειρίζεται. Σύμφωνα με τον Allen, συγκέντρωση είναι η συστηματική και συνεχής συγκέντρωση της εξουσίας σε κεντρικά σημεία του οργανισμού. https://www.managementstudyguide.com .

181 Η συστηματική εξουσιοδότηση σε όλα τα επίπεδα της διαχείρισης στον οργανισμό. Στην περίπτωση της αποκέντρωσης η εξουσία διατηρείται στους υπεύθυνους διαχείρισης για την ανάληψη ύψιστης σημασίας αποφάσεων και για τη χάραξη της πολιτικής που αφορά όλο το σύστημα. Οι υπόλοιπες εξουσίες μπορούν να παραχωρηθούν στα μεσαία και κατώτερα επίπεδα διαχείρισης. https://www.managementstudyguide.com .

of use) μπορούν να ενσωματωθούν στον κώδικα, οι αλλαγές του οποίου απαιτούν τη συγκατάθεση της πλειονότητας των χρηστών. Ένα τέτοιο σύστημα μπορεί να είναι πιο έμπιστο και βιώσιμο μακροπρόθεσμα. Εξάλλου, εάν το μητρώο στηρίζεται στην τεχνολογία blockchain, τα αντίγραφά του θα είναι διαθέσιμα σε όλους τους χρήστες. Ως εκ τούτου, οι εγγραφές που σχετίζονται με τα πνευματικά δικαιώματα δεν θα εξαφανιστούν ξαφνικά από την εταιρία που διατηρεί τη βάση δεδομένων, ούτε θα αλλοιωθούν ή παραβιαστούν. Αυξάνει ενδεχομένως και η βαρύτητά τους ως αποδεικτικά στοιχεία σε περίπτωση δικαστικής διαμάχης σχετικά με τα πνευματικά δικαιώματα, παρόλο που οι εκπρόσωποι των δικαστικών αρχών θα χρειαστεί να εγκλιματιστούν σε σχέση με τη χρήση των αποδεικτικών στοιχείων που βασίζονται σε τεχνολογικές καινοτομίες[182].

Με την ανάπτυξη κρυπτογραφικών μηχανισμών για τη λήψη της συναίνεσης, ελαχιστοποιείται η ανάγκη ενός ενδιάμεσου φορέα και δημιουργείται ένα ταχύ κι έμπιστο σύστημα μεταφοράς αξιών, με χαμηλότερα κόστη μεταβιβάσεων και με ασφαλή και δίκαιη απόδοση των δικαιωμάτων στους δικαιούχους τους. Κάποιοι θεωρούν ότι μέσω αυτής της τεχνολογίας, οι χρήστες θα μπορούν να καταβάλουν τα δικαιώματα απευθείας στους δικαιούχους τους, όπως και να αποκτήσουν γενικά και άλλα οφέλη[183]. Στον αντίποδα των ανωτέρω και ως αντίλογος αυτών, αναπτύσσεται ο φόβος ότι η Τέχνη θα ελέγχεται από συστήματα υπερ - υπολογιστών και θα

182 Βλ. για παράδειγμα απόφαση *Disney v. Redbox* περί διαχωρισμού των ορίων ανάμεσα στη μεταβίβαση και την άδεια. Bill Rosenblatt, «Judge's Ruling in Redbox Case Raises Concerns for Physical/Digital Content Bundles», (2018), διαθέσιμο σε https://copyrightandtechnology.com .

183 Για παράδειγμα, με τα έξυπνα συμβόλαια (smart contracts) οι κάτοχοι των δικαιωμάτων θα μπορούν να διαχειρίζονται τα δικαιώματά τους και να κατανέμουν τα έσοδά τους. Οι συναλλαγές θα είναι διαφανείς και ασφαλείς και η αποτύπωση με ακρίβεια της προσφοράς και της ζήτησης θα μπορούσε να οδηγήσει σε πιο δυναμική τιμολόγηση. Επιπλέον, θα μπορούσε να προκύψει ένα σύστημα αναγνώρισης, όπου οι παραγωγοί και οι χρήστες θα μπορούσαν να επαληθεύσουν ο ένας την ιδιότητα του άλλου. Από τα ανωτέρω συνάγεται ότι μεταβάλλονται οι κλασικοί τρόποι παραγωγής του έργου. Τα αποκλειστικά συμβόλαια ανάμεσα στους κατόχους των δικαιωμάτων και των φορέων σχετικά με την εκχώρηση των δικαιωμάτων δύνανται να αντικατασταθούν από τα έξυπνα συμβόλαια. Το νέο περιβάλλον θα μπορούσε να συμπεριλαμβάνει μία ή περισσότερες βάσεις δεδομένων με πληροφορίες σχετικές με τα πνευματικά δικαιώματα, νέες μορφές εγγράφων, ταχύτερους τρόπους πληρωμών και διαφάνεια. Βλ. George Bouchagiar, «Collective Management Organizations as Fiduciaries and Blockchains's Potential for Copyright Management», *Journal of the Copyright Society of the USA,* Vol. 66, No 2, (2019): 201-225.

αναπτύσσεται από αυτούς, όχι για λόγους αισθητικούς, αλλά για αγοραστικούς και οικονομικούς[184].

Καταλήγοντας, η τεχνολογία blockchain έχει τη δυνατότητα να αλλάξει τον τρόπο με τον οποίο το προστατευόμενο με πνευματικά δικαιώματα έργο διανέμεται στον ψηφιακό κόσμο. Ειδικότερα, μπορεί να παρέχει ευρεία πρόσβαση στην πληροφορία που σχετίζεται με την πνευματική ιδιοκτησία, διαφάνεια και δυνατότητα ανίχνευσης των μεταγενέστερων αλλαγών της[185].

Συμβάσεις

Οι συμβάσεις – ενοχικές ή υποσχετικές[186] - συνάπτονται από τα συμβαλλόμενα μέρη χωρίς τη συμβολή της τεχνολογίας blockchain. Μόνο για την εκπλήρωση των υποχρεώσεων που απορρέουν από τη σύμβαση τα μέρη έχουν τη δυνατότητα να κάνουν χρήση της τεχνολογίας αυτής, με την εγγραφή της σύμβασης σε κάποιο μπλοκ[187], κάτι που προσφέρει διαφάνεια και δημοσιότητα στις έννομες σχέσεις[188]. Επιπλέον επιτυγχάνεται η «βέλτιστη εκτέλεση και ερμηνεία της συγκεκριμένης σύμβασης», καθώς αυτή μετατρέπεται σε «έξυπνη» σύμβαση και αυτοματοποιείται η εκτέλεσή της. Η αρχική δικαιοπραξία εξακολουθεί να καλύπτεται από τις ειδικές διατάξεις των σχετικών συμβάσεων και τους γενικούς κανόνες του Αστικού Κώδικα. Επομένως, η μεταχείρισή της από την πλευρά του δικαίου δεν επηρεάζεται από την

184 Weihong Huang, Renfa Li, Jianbo Xu, Yin Huang και Osama Hosam, «Intellectual property protection for FPGA designs using the public key cryptography», (2019), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/1687814019836838 .

185 Bill Rosenblatt, «Get Ready for the blockchain Tsunami» (2018), διαθέσιμο σε https://copyrightandtechnology.com .

186 Καλλιρρόη Δ. Παντελίδου, «Γενικό Ενοχικό Δίκαιο», 2019, Νομική Βιβλιοθήκη, Αθήνα.

187 Τα μπλοκς (Blocks) είναι αρχεία όπου καταγράφονται μόνιμα τα δεδομένα που σχετίζονται με το δίκτυο των Bitcoin, κυρίως σε ό,τι αφορά τις πρόσφατες συναλλαγές. Jake Frankenfield, «Block (Bitcoin Block)», διαθέσιμο σε https://www.investopedia.com/terms/b/block-bitcoin-block.asp#:~:text=What%20Is%20a%20Block%20(Bitcoin,a%20ledger%20or%20record%20book.

188 Η ενσωμάτωση της εγγραφής τελεί υπό την αναβλητική αίρεση της επιβεβαίωσής της από τους κόμβους του οικείου δικτύου (ΑΚ 201επ). Με τον τρόπο αυτό, η τεχνολογία αυτή αποτελεί έναν οιονεί ιδιωτικό αποδεικτικό ή συστατικό τύπο οριζόμενο από τα μέρη. Θεοδωράκης Νικόλαος και Καλογεράκης Γεώργιος, «Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. Ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου», *ΔiMEE,* τ.1, έτος 16ο (2019): 18.

ένταξή της στη σχετική πλατφόρμα με την τεχνολογία blockchain και κρίνεται με βάση το σχετικό νομοθετικό πλαίσιο και την αρχή της αυτοτέλειας. Σε περίπτωση ανατροπής της σύμβασης, αυτή επηρεάζει και τη σχετική εγγραφή, κάτι που επιτυγχάνεται με τη διόρθωση της παλαιότερης χρονικά με νέα αντιλογιστική εγγραφή (reverse transaction)[189]. Παρότι η διόρθωση της εγγραφής πραγματοποιείται ανάμεσα στα μέρη, επιβάλλεται η προστασία των καλόπιστων τρίτων που εμπιστεύτηκαν την εγγραφή[190]. Περαιτέρω ζητήματα που ανακύπτουν είναι το κατά πόσο μπορεί να εφαρμοστεί στις συμβάσεις που αναρτώνται στις πλατφόρμες της τεχνολογίας blockchain η προστατευτική νομοθεσία για τον καταναλωτή ή για το χρήστη υπηρεσιών διαδικτύου[191]. Η απάντηση είναι κατ' αρχάς αρνητική, με εξαίρεση μόνο τις περιπτώσεις όπου οι αντισυμβαλλόμενοι μπορούν να θεωρηθούν προμηθευτές, δηλαδή προχωρούν στη δικαιοπραξία, της οποίας η εγγραφή αποτυπώνεται στην πλατφόρμα, στο πλαίσιο της επαγγελματικής τους δραστηριότητας και σε αυτό το πλαίσιο μπορεί να τύχει εφαρμογής η 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[192]

189 Ν. Ρόκας, Χ. Γκόρτσος, Α. Μικρουλέα και Χ. Λιβαδά, «Στοιχεία Τραπεζικού Δικαίου», έκδ. 3η Νομική Βιβλιοθήκη, Αθήνα(2016), 512.

190 De facto δημόσια πίστη προς τις πλατφόρμες blockchain ως προς την τυπικότητα των εγγραφών τους, με στόχο την ακριβή αποτύπωση κάθε φορά της έννομης κατάστασης – αρχή της εμπιστοσύνης. Ό.π. υποσημείωση 191.

191 Δεδομένης της ανάπτυξης της οικονομίας του διαμοιρασμού, μεταβάλλεται το οικονομικό μοντέλο των συμβάσεων «Business to Consumer» (B2C) σε συμβάσεις «Consumer to Consumer» (C2C), προκαλώντας εύλογες απορίες ως προς το εφαρμοστέο δίκαιο στο νέο αυτό είδος συμβάσεων. Συγκεκριμένα, ο Ν 2251/1994 περί προστασίας των καταναλωτών που εφαρμόζεται στο ελληνικό δίκαιο, εφαρμόζεται αποκλειστικά σε συμβάσεις που έχουν το μοντέλο του προμηθευτή-καταναλωτή (B2C) ή το ΠΔ 131/2003 (Οδηγία 2000/31) που αφορά στην Κοινωνία της Πληροφορίας ελέγχεται κατά πόσο είναι εφαρμόσιμο στο νέο μοντέλο συμβάσεων, καθώς επιβάλλει συγκεκριμένες προϋποθέσεις ως προς τη σύναψη συμβάσεων με τη χρήση τεχνολογιών του διαδικτύου. Ανθ. Παπαδοπούλου, Επισκ.ΕΔ (2018): 237, σε Θεοδωράκης Νικόλαος και Καλογεράκης Γεώργιος, «Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. Ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου», *ΔiΜΕΕ,* τ.1, έτος 16ο (2019): 19.

192 «Η παρούσα οδηγία θα πρέπει να εφαρμόζεται σε κάθε σύμβαση με την οποία ο έμπορος προμηθεύει ή αναλαμβάνει να προμηθεύσει ψηφιακό περιεχόμενο ή ψηφιακή υπηρεσία στον καταναλωτή. Οι πάροχοι πλατφόρμας μπορούν να θεωρηθούν έμποροι στο πλαίσιο της παρούσας οδηγίας εάν ενεργούν για σκοπούς που αφορούν τη δική τους επιχειρηματική δραστηριότητα ως οι άμεσοι αντισυμβαλλόμενοι του καταναλωτή για την προμήθεια ψηφιακού περιεχομένου ή ψηφιακής υπηρεσίας. Τα κράτη μέλη θα

Δίκαιο της Απόδειξης

Οι εγγραφές που πραγματοποιούνται σε πλατφόρμες όπως αυτή της τεχνολογίας blockchain, φέρουν τον τύπο της ηλεκτρονικής απόδειξης[193]. Οι εγγραφές αποτελούν ιδιωτικά ηλεκτρονικά έγγραφα, τα οποία διαθέτουν βεβαία χρονολογία, μέσω της εγκεκριμένης ηλεκτρονικής χρονοσφραγίδας[194] που ενσωματώνεται σε κάθε μπλοκ. Εξομοιώνονται με τα ιδιωτικά έγγραφα[195], με την ταυτοποίηση του συντάκτη τους μέσω της ηλεκτρονικής του υπογραφής, η οποία έχει την ίδια ισχύ με την ιδιόχειρη[196]. Δεδομένου ότι η πλατφόρμα υφίσταται μόνο ηλεκτρονικά, τα έγγραφα που εξάγονται από αυτή φέρουν την ισχύ πρωτοτύπου, εφόσον φέρουν α) την εγκεκριμένη ηλεκτρονική χρονοσφραγίδα, β) είτε την εγκεκριμένη ηλεκτρονική σφραγίδα του φορέα είτε την εγκεκριμένη ηλεκτρονική υπογραφή του αρμόδιου για την έκδοση του αντιγράφου οργάνου.

πρέπει να παραμένουν ελεύθερα να επεκτείνουν την εφαρμογή της παρούσας οδηγίας σε παρόχους πλατφόρμας που δεν πληρούν τις απαιτήσεις για να θεωρηθούν έμποροι σύμφωνα με τον ορισμό της παρούσας οδηγίας»

193 Το δεδομένο που δημιουργείται, παραποιείται, αποθηκεύεται ή επικοινωνείται από κάθε διάταξη, υπολογιστή ή υπολογιστικό σύστημα ή διαβιβάζεται μέσω ενός συστήματος επικοινωνίας που σχετίζεται με τη δικαιοδοτική διαδικασία. Χρυσούλα Μιχαηλίδου, «Κυβερνοέγκλημα και ηλεκτρονική απόδειξη - ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά», *The art of Crime,* Νοέμβριος 2018, διαθέσιμο σε https://theartofcrime.gr.

194 Βλ. σχετικά Ν 4727/2020 περί Ψηφιακής Διακυβέρνησης.

195 Δεν θεωρούνται αποσπάσματα από ηλεκτρονικώς τηρούμενα εμπορικά βιβλία, κατά τον ΚπολΔ (άρθρο 444), αφού το βιβλίο του καθολικού είναι προαιρετικό εμπορικό βιβλίο. Εξάλλου, οι εγγραφές σε μία πλατφόρμα blockchain δεν μπορούν να θεωρηθούν ότι σχηματίζουν και συναπαρτίζουν το βιβλίο του καθολικού, λόγω της αποσπασματικότητάς τους. *Β*λ. Κων/νος Χριστοδούλου, «Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία. Μετά τις νέες κοινοτικές ρυθμίσεις», εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, (2001): 63.

196 Γιώργος Γιαννόπουλος, «Εισαγωγή στη Νομική Πληροφορική. Μια πρώτη προσέγγιση της σχέσης δικαίου & νέων τεχνολογιών», Νομική Βιβλιοθήκη (2018) σε Θεοδωράκης Νικόλαος και Καλογεράκης Γεώργιος, «blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. Ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου», *ΔiΜΕΕ,* τ. 1, έτος 16ο (2019): 20

Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Μετά και την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (2016/679)[197] έχει επικρατήσει η άποψη ότι όποιος συμμετέχει σε μία πλατφόρμα τεχνολογίας blockchain πρέπει να αντιμετωπίζεται ως υπεύθυνος επεξεργασίας δεδομένων[198]. Επιπλέον, δεδομένου του αμετάβλητου χαρακτήρα της αλυσίδας και της αδυναμίας αλλοίωσής της, δημιουργείται ένα μόνιμο ιστορικό, το οποίο έρχεται σε αντίθεση με το προβλεπόμενο στο άρθρο 17 ΓΚΠΔ δικαίωμα του υποκειμένου των δεδομένων στη λήθη, το οποίο τείνει να αντιμετωπιστεί ενωσιακά από τα αρμόδια όργανα και το ΔΕΕ[199]. Προβληματισμό επίσης δημιουργεί το γεγονός ότι ο ΓΚΠΔ βασίζεται κυρίως σε κεντρικά συστήματα – δίκτυα διαχείρισης προσωπικών δεδομένων, σε αντίθεση με την τεχνολογία blockchain και τον αποκεντρωτικό χαρακτήρα της.

«Έξυπνα» συμβόλαια

Σε ένα «έξυπνο» συμβόλαιο[200] η ερμηνεία των συμβατικών όρων δεν επιδέχεται παρανοήσεις κατά την εκτέλεσή του. Η γλώσσα προγραμματισμού με την οποία έχει συνταχθεί το συμβόλαιο, σε αντίθεση με την ανθρώπινη γλώσσα, δεν χωράει

197 Βλ. σχετικά Ιωάννης Ιγγλεζάκης, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019)», Interactive Books, 2020. Βλ. επίσης Λίλιαν Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα», Σάκκουλας, Αθήνα, 2017 και Φερενίκη Παναγοπούλου – Κουτνατζή, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων», Σάκκουλας, Αθήνα, 2018.

198 Γίνεται δεκτό κυρίως από τη γερμανική θεωρία.

199 Βλ. σχετικά το από 3 Οκτωβρίου 2018 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου σχετικά με τις τεχνολογίες κατανεμημένου καθολικού (DLT) και το σύστημα blockchain: οικοδόμηση εμπιστοσύνης με αποδιαμεσολάβηση (2017/2772(RSP)), όπου υπογραμμίζεται ότι παρόλο που η τεχνολογία DLT προωθεί την αυτοκυρίαρχη ταυτότητα, το «δικαίωμα στη λήθη»δεν έχει εύκολη εφαρμογή στην τεχνολογία αυτή και τονίζεται ότι είναι υψίστης σημασίας να τηρείται κατά τη χρήση των τεχνολογιών DLT η ενωσιακή νομοθεσία περί προστασίας των δεδομένων και ιδιαίτερα ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ/GDPR)·καλεί την Επιτροπή και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) να προσφέρουν περαιτέρω καθοδήγηση στο θέμα αυτό. Διαθέσιμο σε https://op.europa.eu/el/publication-detail/-/publication/d94752df-35ee-11ea-ba6e-01aa75ed71a1

200 Βλ. σχετικά ανωτέρω υποσημείωση 169 σχετικά με τα έξυπνα συμβόλαια.

αμφισημίες. Περισσότεροι άνθρωποι μπορεί να αποδώσουν διαφορετικό νόημα στις ίδιες λέξεις, όχι όμως και περισσότεροι υπολογιστές στον κώδικα ενός «έξυπνου» συμβολαίου. Επιπλέον, όταν ένα «έξυπνο» συμβόλαιο έχει ενσωματωθεί σε πλατφόρμα blockchain, είναι εξαιρετικά δύσκολο να τροποποιηθούν οι όροι του, όπως θα συνέβαινε σε μία παραδοσιακή σύμβαση μετά τη σύναψή της, στην περίπτωση αλλαγών στο νομοθετικό πλαίσιο. Αυτό θα μπορούσε να αντιμετωπισθεί με τη διασύνδεση των «έξυπνων» συμβολαίων με βάσεις δεδομένων, με στόχο την αυτόματη ενημέρωσή τους σχετικά με το ισχύον νομοθετικό πλαίσιο και με το διαχωρισμό των όρων τους σε επιδεχόμενους τροποποιήσεων ή μη. Περαιτέρω, στις περιπτώσεις που άπτονται του ιδιωτικού διεθνούς δικαίου, είναι δυσχερής ο εντοπισμός των κριτηρίων (όπως παράδειγμα του τόπου κατοικίας των μερών, του τόπου κατάρτισης μίας σύμβασης ή του τόπου εκπλήρωσης) για τον προσδιορισμό του εφαρμοστέου δικαίου, όταν αυτό δεν είναι με σαφήνεια προσδιορισμένο μεταξύ των συμβαλλομένων μερών, λόγω της διασυνοριακής φύσης των συναλλαγών σε μία πλατφόρμα blockchain. Σοβαρές ενστάσεις τίθενται επίσης και κατά τη διαδικασία της εκτέλεσης. Κατά την πτωχευτική διαδικασία, τίθενται τα ερωτήματα εάν στην περίπτωση του διακόπτη εκκίνησης[201] θα προστατεύεται ο οφειλέτης ή εάν θα μπορεί να κάνει χρήση των περιουσιακών του στοιχείων, όταν τεθεί σε καθεστώς πτώχευσης ή κατά την προπτωχευτική διαδικασία, κατά την οποία αναστέλλονται οποιεσδήποτε πράξεις εκτέλεσης σε βάρος του[202].

Αποκεντρωμένοι αυτόνομοι οργανισμοί (DAO)

Πρόκειται για νομικά μορφώματα, η λειτουργία των οποίων έχει προβλεφθεί σε «έξυπνα» συμβόλαια, μέσω μίας πλατφόρμας blockchain. Δραστηριοποιούνται και διοικούνται αποκεντρωμένα και οι κανόνες τους είναι εγκατεστημένοι στο λογισμικό

201 Βλ. σχετικά ανωτέρω υποσημείωση 171 σχετικά με το διακόπτη εκκίνησης.

202 Κωνσταντίνος Λογαράς, «Η Τεχνολογία Blockchain, οι εφαρμογές και οι νομικές πτυχές της», (2018), διαθέσιμο σε https://www.naftemporiki.gr/story/1363055/i-texnologia-blockchain-oi-efarmoges-tis-kai-oi-nomikes-ptuxes-tis .

υπολογιστών που βρίσκονται σε διαφορετικά μέρη του κόσμου. Όπως είναι αναμενόμενο, τα νομικά ζητήματα που προκύπτουν, άπτονται πολλών θεμάτων, όπως για παράδειγμα του εφαρμοστέου δικαίου, της κτήσης νομικής προσωπικότητας, της δημοσιότητας, του τρόπου διοίκησής του κ.ο.κ.[203]

7 Θέματα φορολόγησης

Όπως θα ήταν αναμενόμενο, οι τεχνολογικές αλλαγές της σημερινής εποχής επηρεάζουν και τη δυνατότητα υπολογισμού, είσπραξης κι επιστροφής των φόρων. Οι υπολογιστές έχουν καταστεί ταχύτεροι και τα συστήματα παρακολούθησης είναι ανθεκτικότερα από ποτέ. Η ψηφιακή αποθήκευση έχει γίνει εξαιρετικά φθηνή και εύκολα προσβάσιμη. Επιπλέον, η τεχνητή νοημοσύνη έχει θέσει ενδιαφέροντα ερωτήματα σχετικά με τα χαρακτηριστικά μιας οντότητας που μπορεί να φορολογηθεί και τροποποιώντας βασικές σταθερές του φορολογικού οικοδομήματος[204]. Η τεχνολογία έχει απομακρύνει τη δραστηριότητα από τα παραδοσιακά συστατικά της οικονομίας και την έχει στρέψει σε νέες, παλαιότερα αφορολόγητες, δραστηριότητες. Χαρακτηριστικό παράδειγμα αυτών αποτελούν τα κρυπτονομίσματα[205]. Αυτή η αλλαγή απειλεί τη δυνατότητα των κυβερνήσεων να διατηρήσουν μία σταθερή ροή εισοδημάτων, καθώς διάφορες μορφές εισοδήματος έχουν μετατραπεί σε κατηγορίες που είναι αφορολόγητες. Από την άλλη πλευρά, η τεχνολογία έχει δημιουργήσει τρόπους απόδοσης φόρων και πιστώσεων με τρόπους που στο παρελθόν ήταν ανέφικτοι. Το μεγάλο ερώτημα που τίθεται πλέον είναι εάν και με ποιον τρόπο θα μπορούσαν να φορολογηθούν τα κρυπτονομίσματα[206].

203 Usman W. Chohan, «The Decentralized Autonomous Organization and Governance Issues», (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055 .

204 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

205 Marian Y. Omri, «Are Cryptocurrencies 'Super' Tax Havens?», *112 Michigan Law Review First Impressions 38* (2013), διαθέσιμο σε https://repository.law.umich.edu/mlr_fi/vol112/iss1/2 .

206 Lee David Kuo Chuen, Guo Li Και Wang Yu, «Cryptocurrency: A new investment opportunity?», *Journal of Alternative Investments,* 20/3, (2018): 16-40.

Η απρόσμενη άνοδος της αξίας του Bitcoin και των υπολοίπων κρυπτονομισμάτων προκάλεσε ανησυχία ως προς τη ζημία που θα μπορούσαν αυτά να προκαλέσουν μακροπρόθεσμα στη δημόσια οικονομική, μέσω της απώλειας των φορολογικών εσόδων. Ο πυρήνας της τεχνολογίας υπογραμμίζει ότι τα κρυπτονομίσματα και η τεχνολογία blockchain στηρίζονται στην ανωνυμία[207]: οι συναλλαγές είναι δημόσιες, αλλά συνδέονται μόνο με μία ηλεκτρονική διεύθυνση, κάτι που καθιστά την τεχνολογία αυτή ελκυστική[208]. Αλλά η ανωνυμία κινεί την παραοικονομία, η οποία αυτή τη στιγμή διεξάγεται μέσω μετρητών και κατά συνέπεια καθίσταται ως μία σημαντική πηγή απωλεσθέντων φορολογικών εσόδων. Η Υπηρεσία Εσωτερικού Εισοδήματος (IRS[209]) των ΗΠΑ, εκτιμά ότι σε ετήσια βάση χάνονται περίπου 500 δισεκατομμύρια δολάρια μόνο από αδήλωτα εισοδήματα. Και η παραοικονομία πλήττει τις ΗΠΑ σε μικρότερο ποσοστό σε σχέση με παραοικονομίες άλλων κρατών. Εάν τα κρυπτονομίσματα επρόκειτο να αντικαταστήσουν τα μετρητά ως το επιθυμητό ανώνυμο μέσο συναλλαγής, θα επέκτειναν σημαντικά την παραοικονομία καθώς είναι πολύ πιο βολικά από τα μετρητά[210] - δεν χρειάζονται Αυτόματες Ταμειολογιστικές Μηχανές (ATM) και μπορούν να μεταφερθούν χρήματα από το ένα άτομο σε άλλο με ασφάλεια, ανεξάρτητα από τον τόπο κατοικίας αποστολέα και παραλήπτη[211]. Έντονες ανησυχίες εκφράστηκαν από τους ειδικούς σχετικά με την εξέλιξη του Bitcoin σε «ένα νέο Ελβετικό τραπεζικό λογαριασμό»[212]. Δεδομένου ότι

207 Rebecca M. Bratspies, «Cryptocurrency and the Myth of the Trustless Transaction», *25 Mich. Telecomm. & Tech. L. Rev.* 1 (2018).

208 David J. Shakow, «The Tax Treatment of Tokens: What Does it Betoken?», *Tax Notes*, Vol. 156, U of Penn, Inst for Law & Econ Research Paper No. 17-45, (2017): 1387.

209 «Internal Revenue Service»: πρόκειται για την κρατική αμερικανική υπηρεσία είσπραξης φόρων, η οποία εφαρμόζει στην πράξη τον Κώδικα Εσωτερικού Εισοδήματος που έχει ψηφιστεί από το Κογκρέσο. Βλ. σχετικά https://www.irs.gov .

210 Ammous Saifedean, «Can Cryptocurrencies Fulfil the Functions of Money?», Columbia University, Center on Capitalism and Society, Working Paper No. 92 (2016).

211 Chris Berg, Sinclair Davidson και Jason Potts, «Beyond Money: Cryptocurrencies, Machine-Mediated Transactions and High Frequency Bartering» (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3158047 .

212 Δεν πρέπει να επιτρέψουμε στο ισχυρό ψηφιακό νόμισμα Bitcoin να μετατραπεί σε ελβετικό τραπεζικό λογαριασμό της μοντέρνας εποχής, χρησιμοποιούμενο για απόκρυψη αθέμιτων συμπεριφορών, δήλωσε ο Υπουργός Οικονομικών των ΗΠΑ Steven Mnuchin. «Bitcoin shouldn't become the new 'Swiss bank account': Mnuchin», διαθέσιμο σε https://www.thelocal.ch/20180113/bitcoin-shouldnt-become-the-new-swiss-bank-account-mnuchin.

ο κίνδυνος αυτός είναι πλέον αντιληπτός, δημιουργείται η τάση προς την άρση της ανωνυμίας των κρυπτονομισμάτων. Το Νοέμβριο του 2017 ένας ομοσπονδιακός δικαστής των ΗΠΑ διέταξε το Coinbase να αποκαλύψει την ταυτότητα των πελατών του που διατηρούν περισσότερους από 14.000 λογαριασμούς[213]. Περαιτέρω η τεχνολογία blockchain καθιστά δύσκολη τη φορολόγηση και των εμπορικών κερδών από τα κρυπτονομίσματα.

Μία πρώτη προσέγγιση επίλυσης των θεμάτων φορολόγησης θα ήταν για τις κυβερνήσεις να αποδεχθούν τη δυσκολία της απευθείας φορολόγησης των συναλλαγών σε κρυπτονομίσματα και να αντισταθμίσουν τις απώλειες εσόδων με την αύξηση φορολογικών δεικτών[214]. Ο αντίλογος, βέβαια είναι ότι, αν και τα κρυπτονομίσματα παρέχουν ευκαιρίες φοροδιαφυγής και παράνομων συναλλαγών, επίσης μειώνουν δραστικά το κόστος των χρηματοπιστωτικών συναλλαγών. Μία άλλη προσέγγιση, υποστηριζόμενη από πολλούς οικονομολόγους, θα αποτελούσε η τροποποίηση του φορολογικού συστήματος με τη φορολόγηση του εισοδήματος κατά την ανάλωση, αντί κατά τη λήψη του και η μετατροπή του, ουσιαστικά, σε νέο είδος φόρου κατανάλωσης[215].

Η προοπτική των σημαντικών απωλειών φορολογικών εσόδων γα τις κυβερνήσεις δεν αποτελεί μόνο πρόβλημα για τις ίδιες, αλλά και για τα ίδια τα κρυπτονομίσματα[216]. Για να μπορέσουν να επιβιώσουν μακροπρόθεσμα ως αποτελεσματικά μέσα καθημερινών συναλλαγών, η ίδια η κοινότητα των κρυπτονομισμάτων πρέπει να αποτρέψει τη φοροδιαφυγή. Αυτό θα συμπεριλαμβάνει εξισορροπιστικές πράξεις, με την προστασία της ανωνυμίας των συναλλαγών, αλλά και ταυτόχρονα με την παροχή επαρκών πληροφοριών για την πρόληψη της

213 Κάτι που μεταφράζεται σε περίπου 9 εκατομμύρια συναλλαγές. «A Federal Judge Just Ordered Coinbase to Report More Than 10,000 Users to the IRS», διαθέσιμο σε https://futurism.com.

214 Kartik Hegadekatti και S. G. Yatish, «Examining Taxation of Fiat Money and Bitcoins vis-a-vis Regulated Cryptocurrencies», *International Finance eJournal,* Vol. 8/ 117 (2016).

215 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

216 Richard Holden και Anup Malani, «Why the I.R.S. Fears Bitcoin», διαθέσιμο σε https://www.nytimes.com/2018/01/22/opinion/irs-bitcoin-fear.html

φοροδιαφυγής. Γενικά, η πάταξη της φοροδιαφυγής απαιτεί από την κοινότητα των κρυπτονομισμάτων την ενίσχυση της εμπιστοσύνης της προς τις κυβερνήσεις. Από τη στιγμή που αυτό έρχεται σε αντίθεση με την ίδια τη φιλοσοφία του κινήματος των κρυπτονομισμάτων, θα αποτελέσει μία εξαιρετικά δύσκολη, αλλά απαραίτητη πρόκληση[217].

7.1 **Η φορολόγηση σε σχέση με την τεχνολογία blockchain και το διαμοιρασμένο δημόσιο καθολικό (shared public ledger).**

Το μεγαλύτερο, ίσως, τεχνολογικό επίτευγμα, το οποίο δεν έχει συμπεριληφθεί ακόμη στο Φορολογικό Δίκαιο, είναι η τεχνολογία blockchain και το δημόσιο καθολικό[218]. Η επαναστατική φύση της τεχνολογίας αυτής δικαίως έχει κερδίσει τον τίτλο «το νέο Google»[219]. Όλες οι επιβεβαιωμένες συναλλαγές συμπεριλαμβάνονται σε αυτό και μέσω αυτού τα ψηφιακά «πορτοφόλια» μπορούν να υπολογίσουν το εναπομείναν υπόλοιπο, ενώ οι νέες συναλλαγές μπορούν να επαληθεύσουν την κυριότητα των δαπανηθέντων ψηφιακών νομισμάτων. Η ακεραιότητα και η χρονολογική σειρά του καθολικού blockchain προκύπτουν μέσω της κρυπτογραφίας[220].

Το κλειδί της τεχνολογίας αυτής αποτελεί ο δημόσιος χαρακτήρας των δεδομένων[221]. Οποιοσδήποτε ανά τον κόσμο μπορεί να αναγνωρίσει μία αντεγραμμένη ή απατηλή συναλλαγή σε ένα τεράστιο δημόσιο υπολογιστικό φύλλο προκειμένου να αποτρέψει κάθε αντιγραφή των Bitcoin χωρίς εξουσιοδότηση και αυτό επιτυγχάνεται μέσω των

217 Richard Holden και Anup Malani, «Why the I.R.S. fears Bitcoin», διαθέσιμο σε https://www.nytimes.com/2018/01/22/opinion/irs-bitcoin-fear.html

218 F. Xavier Olleros και Majlinda Zhegu, «Blockchain Technology: Principles and Applications», Research Handbook on Digital Transformations, Edward Elgar, (2016).

219 «The blockchain is the new Google», διαθέσιμο σε https://techcrunch.com.

220 Larissa Lee, «New Kids on the blockchain: How Bitcoin's Technology Could Reinvent the Stock Market», *Hastings Business Law Journal,* Vol. 12/ 2, University of Utah College of Law Research Paper No. 138 (2016).

221 Κωνσταντίνος Λογαράς, «Η τεχνολογία Blockchain, οι εφαρμογές της και οι νομικές πτυχές της», (2018), διαθέσιμο σε https://www.naftemporiki.gr/story/1363055/i-texnologia-blockchain-oi-efarmoges-tis-kai-oi-nomikes-ptuxes-tis .

δημόσιων και ιδιωτικών κλειδιών κρυπτογράφησης[222]. Το δημόσιο καθολικό είναι προσβάσιμο στον καθένα και μπορεί να αντλήσει πληροφορίες για προηγούμενες συναλλαγές ενός συγκεκριμένου νομίσματος, για να διασφαλίσει ότι αυτό έγινε αποδεκτό από τον πραγματικό του ιδιοκτήτη και όχι από κάποιον προγενέστερο. Οι πράκτορες της Εσωτερικής Υπηρεσίας Εσόδων (IRS) των ΗΠΑ καταβάλλουν προσπάθειες να ανακαλύψουν υπόπτους φοροδιαφυγής μέσω των δημοσίων καθολικών, αντιστοιχίζοντας δημόσιες διευθύνσεις με άτομα[223]. Παρόλα αυτά, τα υπάρχοντα συστήματα παρακολούθησης δεν έχουν τη δυνατότητα να αποκαλύπτουν πάντα τους παραβάτες – η πιθανότητα βελτίωσης των συστημάτων αυτών παραμένει πάντα ανοιχτή.

Η ευρύτητα της απήχησης της νέας τεχνολογίας υποδηλώνει ότι πολλές συναλλαγές, οι οποίες αρχικά ήταν δύσκολο να εντοπιστούν, τώρα μπορούν τόσο να εντοπιστούν, όσο και να φορολογηθούν. Άλλες εφαρμογές, μέσω της τεχνολογίας αυτής παρέχουν τη δυνατότητα ελέγχου των αρχείων σε πραγματικό χρόνο. Σε θέματα μισθοδοσίας, οι φορολογικές Αρχές των κρατών θα μπορούν να έχουν πρόσβαση ελέγχου σε όλα τα αρχεία των υπαλλήλων και να προχωρούν στην αντιστοίχισή τους με τις πληρωμές όλων των εργοδοτών[224]. Το όριο για τη βάση των νέων φόρων εξαρτάται από το τι ακριβώς θέλουν να ανιχνεύσουν με την τεχνολογία blockchain οι ιδιωτικές αγορές και οι κυβερνήσεις. Εάν αρχίσουν να ανιχνεύουν αγαθά, όπως έργα τέχνης, εισιτήρια συναυλιών ή αθλητικά αναμνηστικά, αυτά θα μπορούσαν εύκολα να αποτελέσουν αντικείμενο φορολόγησης. Τα ιδιαίτερα χαρακτηριστικά αυτών των αντικειμένων

222 Κάθε συναλλασσόμενος έχει δύο κρυπτογραφικά σχετιζόμενα κλειδιά: το ένα είναι δημόσιο, το οποίο ο καθένας στον κόσμο μπορεί να το δει και να το χρησιμοποιήσει και το δεύτερο είναι ιδιωτικό, το οποίο συνδέεται με μαθηματικό τρόπο με το πρώτο, αλλά αδύνατον να αποκρυπτογραφηθεί μέσω αυτού. Κάθε συναλλασσόμενος έχει τη δυνατότητα να αποστείλει Bitcoin σε κάποιον άλλο χρησιμοποιώντας το δημόσιο κλειδί. Με τη χρήση του ιδιωτικού μόνο ο αποδέκτης έχει πρόσβαση στο περιεχόμενο. Βλ. σχετικά Michèle Finck, «Blockchains and Data Protection in the European Union», Max Planck Institute for Innovation & Competition Research Paper No. 18-01 (2017).

223 Manoj Viswanathan, «Tax Compliance in a Decentralizing Economy», (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002213 .

224 Shaun Sutner, «Blockchain payroll systems coming to HR tech», διαθέσιμο σε https://searchhrsoftware.techtarget.com/feature/Blockchain-payroll-systems-coming-to-HR-tech.

είναι το ότι είναι επιρρεπή στην παραποίηση[225] και την υπερτίμηση. Για να καταπολεμηθεί η παραχάραξη, η τεχνολογία blockchain μπορεί να επιβεβαιώσει τη δημόσια αναγνώριση της αυθεντικότητάς τους μέσω του δημόσιου καθολικού[226]. Ως αποτέλεσμά αυτού, οι αρμόδιες Αρχές θα μπορούσαν να αποκτήσουν πρόσβαση για να εξακριβώσουν το χρονικό σημείο κατά το οποίο τα αντικείμενα αυτά επαναμεταβιβάζονται με στόχο το κέρδος και να εισπράξουν τους αναλογούντες φόρους. Οι αρμόδιες Αρχές μπορούν επίσης να επιβάλουν συγκεκριμένες προϋποθέσεις για την εγγραφή στο καθολικό blockchain για ορισμένα πολυτελή αγαθά, με στόχο την καταπολέμηση της παραποίησης. Μολαταύτα, οποιαδήποτε προϋπόθεση εγγραφής πρέπει να συμβαδίζει με τις προσωπικές ελευθερίες των συναλλασσομένων, δεδομένου ότι θα παρέχονται σε τρίτους δεδομένα που αφορούν στις συναλλαγές, τα οποία προστατεύονται είτε από υπό τη σφαίρα της ιδιωτικής ζωής στις ΗΠΑ είτε σύμφωνα με τις διατάξεις του ΓΚΠΔ στην Ευρωπαϊκή Ένωση και των εφαρμοστικών νόμων των κρατών – μελών της.

7.2 Η φορολόγηση σε σχέση με την ICO (Initial Coin Offering)

Οι «αρχικές προσφορές νομισμάτων» (ICOs - Initial Coin Offerings[227]) αφορούν στην πρώτη κυκλοφορία ενός νέου κρυπτονομίσματος, το οποίο συγκεντρώνει χρήματα μέσω διαδικτυακής χρηματοδότησης ή χρηματοδότησης από το πλήθος

225 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

226 Henry M. Kim και Marek Laskowski, «Towards an Ontology-Driven blockchain Design for Supply Chain Provenance», (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828369 .

227 Οι «Αρχικές Προσφορές Νομισμάτων» (Initial Coin Offerings) επιτρέπουν σε νεοφυείς επιχειρήσεις να αντλήσουν κεφάλαια χωρίς την εμπλοκή τραπεζών και εταιρειών. Σε μια ICO η άντληση των κεφαλαίων γίνεται με την πώληση ψηφιακών στοιχείων ενεργητικού, των λεγόμενων tokens, σε ενδιαφερόμενους χρήστες και επενδυτές έναντι ψηφιακών νομισμάτων όπως το Bitcoin ή το Ether. Τα tokens μπορούν να χρησιμοποιηθούν για την αγορά αγαθών και υπηρεσιών στην πλατφόρμα της εταιρείας ή να διατηρηθούν ως επένδυση. Ο αγοραστής μπορεί να ανταλλάξει ανά πάσα στιγμή τα tokens στο διαδίκτυο, αλλά δεν γίνεται μέτοχος της εταιρείας. Saman Adhami, Giancarlo Giudici και Stefano Martinazzi, «Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings», *Journal of Economics and Business* (2018): 64-75.

(crowdfunding)[228]. Σε αντίθεση με την «αρχική δημόσια προσφορά» (IPO – Initial Public Offering), η οποία παρέχει στους αγοραστές των μετοχών ποσοστό ιδιοκτησίας στην εταιρία, η αρχική προσφορά νομισμάτων προσφέρει στους αγοραστές μερίδιο στα δικαιώματα ενός έργου (project). Οι καταναλωτές αγοράζουν νομίσματα με την ελπίδα ότι τόσο η κοινότητα, όσο και η νομισματική πολιτική θα ευημερήσουν. Με τη μέθοδο αυτή διακυβεύονται μεγάλα χρηματικά ποσά: από τον Ιανουάριο έως τον Αύγουστο του 2017 είχαν προκύψει ήδη 1,1 δισεκατομμύρια δολάρια από έσοδα ICO[229], ποσό δεκαπλάσιο σε σχέση με τα έσοδα του έτους 2016, δεδομένο που αποδεικνύει την ταχύτατη εξέλιξη του φαινομένου. Όπως ήταν αναμενόμενο, προέκυψαν ερωτηματικά σε σχέση με τη φορολόγηση των ICO[230], ιδιαίτερα ως προς τα εάν πρέπει να αντιμετωπιστούν ως καθαρό εισόδημα ή εάν πρέπει να τύχουν μεταχείρισης αντίστοιχης με τη συμβατική χρηματοδότηση με επιχειρηματικά κεφάλαια. Τυπικά, το συναλλασσόμενο μέρος, το οποίο εισάγει ICO, θα κατέχει ένα ποσοστό των νομισμάτων και στη συνέχεια θα προστατεύει τα κεφάλαιά του από την πώληση όλων των άλλων νομισμάτων. Η αξία των νομισμάτων αυτών μπορεί να αυξηθεί σημαντικά από τη μία εβδομάδα στην άλλη, πολλές φορές και στο 100% ή περισσότερο.

228 Πρόκειται για την διαδικασία άντλησης (μικρών) κεφαλαίων μέσω ενός μεγάλου αριθμού επενδυτών. Η ιδέα του crowdfunding ξεκίνησε από τον χώρο της μουσικής στις αρχές της προηγούμενης δεκαετίας και σταδιακά επεκτάθηκε και σε άλλους τομείς οικονομικής δραστηριότητας –κυρίως από το 2008 και μετά. Σ' αυτό συνέβαλλε σημαντικά και η διεθνής οικονομική κρίση, μιας και οι τράπεζες άρχισαν έκτοτε να θεωρούν την έναρξη μικρών επιχειρήσεων ιδιαίτερα επισφαλείς για τα χρήματά τους. Οι επίδοξοι επιχειρηματίες λοιπόν (και όχι μόνο) άρχισαν να αναζητούν εναλλακτικούς τρόπους χρηματοδότησης – και τους βρήκαν στις πλατφόρμες crowdfunding. «Crowdfunding σε απλά ελληνικά», (2018), διαθέσιμο σε http://www.itech4u.gr.

229 Navroop K. Sahdev, «The Tokenization of the Economy: ICOs and the Implications for Entrepreneurship», (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3057083 .

230 Jason G Allen, «What's Offered in an ICO? Digital Coins as Things» (2018). Βλ. επίσης Octavian Nica, Karolina Piotrowska καιKlaus Reiner Schenk-Hoppé, «Cryptocurrencies: Economic Benefits and Risks», University of Manchester, FinTech working paper no. 2 (2017).

7.3 Η φορολόγηση των κρυπτονομισμάτων

Τα κρυπτονομίσματα θα έχουν εξαιρετικά ανοδική πορεία με τις κατάλληλες νομοθετικές και φορολογικές ρυθμίσεις[231]. Αντιθέτως, η χρήση τους θα μειωθεί στην περίπτωση που είναι απαγορευτικά δυσκίνητη η συμμόρφωσή τους με τις κανονιστικές και φορολογικές απαιτήσεις. Εάν σε κάποιες χώρες η συμμόρφωση αυτή είναι απλούστερη και διαμορφώνονται οι κατάλληλες υποδομές που θα εμπνεύσουν εμπιστοσύνη στη χρήση των κρυπτονομισμάτων, οι χώρες αυτές θα καταστούν «κρυπτονομισματικοί παράδεισοι»[232]. Πολλοί πλέον θα χρησιμοποιούν αυτές τις δομές και τα νομικά πλαίσια έκαστης χώρας και πιθανότατα μεγάλα ποσοστά οικονομικής δραστηριότητας θα δρομολογούνται μέσω αυτής. Η συνολική κεφαλαιοποίηση της αγοράς των κρυπτονομισμάτων ανέρχεται σε εκατοντάδες δισεκατομμύρια και συνεχώς αυξάνεται. Κατ' επέκταση, υπάρχει μεγάλη πιθανότητα μία χώρα ή μία ομάδα χωρών να επωφεληθούν από τη χρήση τους. Επιπρόσθετα, η αποδοχή των κρυπτονομισμάτων από τις αγορές έχει αρχίσει να έχει μία συνεχή ροή[233]. Εταιρίες όπως οι Target, Expedia, Victoria Secret, Dell, Zappos υπήρξαν μερικές από τις μικρότερης εμβέλειας επιχειρήσεις που αποδέχτηκαν το Bitcoin ως μέσο πληρωμών.

Δεδομένου λοιπόν ότι πλέον πολλές συναλλαγές πραγματοποιούνται μέσω της τεχνολογίας των κρυπτονομισμάτων, οι φορολογικές Αρχές των ΗΠΑ υποχρεώθηκαν να ορίσουν μία σειρά από φορολογικές κατευθυντήριες γραμμές, ώστε να μη

231 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf . Βλ. επίσης Joseph Walton, «Cryptocurrency Public Policy Analysis» (2014).

232 Marian Y. Omri, «Are Cryptocurrencies super tax heavens?», *Michigan Law Review First Impressions,* volume 112 (2013), διαθέσιμο σε https://repository.law.umich.edu/mlr_fi/vol112/iss1/2 . Τέτοιοι κρυπτονομισματικοί παράδεισοι είναι σήμερα οι Γερμανία, Δανία, Σιγκαπούρη, Λευκορωσία και Σλοβενία στην Ευρώπη, Πουέρτο Ρίκο, Νησιά Μάρσαλ κοκ στον υπόλοιπο κόσμο. Sudhir Khatwani, «Countries With 0% Tax On Bitcoin/Cryptos: Tax Free Life», διαθέσιμο σε https://coinsutra.com

233 Elise Moreau, «13 major retailers and services that accept Bitcoin», (2018), διαθέσιμο σε https://www.lifewire.com.

χρειαστεί να μετατοπιστούν οι συναλλαγές αυτές στο εξωτερικό[234]. Από τη στιγμή που διακυβεύονται συναλλαγές δισεκατομμυρίων δολαρίων, οι αρμόδιες Αρχές έπρεπε να προσπαθήσουν να διατηρήσουν το μεγαλύτερο ποσοστό της αξίας των συναλλαγών στο εσωτερικό του κράτους.

Σχετικά με το θέμα της φορολόγησης των κρυπτονομισμάτων, διαφορετικές ανά τον κόσμο κυβερνήσεις έχουν υιοθετήσει εξαιρετικά αποκλίνουσες προσεγγίσεις[235]. Μέρος της απόκλισης προκύπτει από τη μορφή την οποία προσδίδει μία κυβέρνηση στα ψηφιακά νομίσματα - και κατ' επέκταση τα φορολογεί αντίστοιχα. Άλλες αιτίες διαφορετικότητας στις μεθόδους είναι οι κυριαρχικές και οικονομικές επιπτώσεις της φορολόγησης των κρυπτονομισμάτων κατά περίπτωση. Σήμερα υπάρχουν διάφορα νομικά πρότυπα σε σχέση με τα κρυπτονομίσματα.

Η φορολόγηση των κρυπτονομισμάτων ως ιδιοκτησία

Η Υπηρεσία Εσωτερικού Εισοδήματος (IRS) των ΗΠΑ εξέδωσε το 2014 οδηγία σύμφωνα με την οποία τα κρυπτονομίσματα πρέπει να αντιμετωπίζονται φορολογικά ως ιδιοκτησία[236]. Από αυτό συνάγεται ότι τα ψηφιακά νομίσματα δεν τυγχάνουν αντιμετώπισης πραγματικών νομισμάτων, παρόλο που χρησιμοποιούνται ως μέσο για κάποιες συναλλαγές. Την ίδια αντιμετώπιση είχαν τα κρυπτονομίσματα και από τις κυβερνήσεις του Ισραήλ[237] και της Σιγκαπούρης[238]. Πράγματι, σε κάποιες περιπτώσεις, τα κρυπτονομίσματα λαμβάνουν ρόλο ιδιοκτησίας και όχι νομισμάτων,

234 Vincenzo Villamena, «Cryptocurrency and taxes: What you need to know», (2018), διαθέσιμο σε https://www.cnbc.com/2018/01/30/cryptocurrency-and-taxes-what-you-need-to-know.html .

235 Adam Bergman, «What you should know about taxation of cryptocurrencies», (2018), διαθέσιμο σε https://www.forbes.com/sites/greatspeculations/2018/01/03/what-you-should-know-about-taxation-of-cryptocurrencies/ .Βλ. επίσης «Legal Status of Cryptocurrency», (2018), διαθέσιμο σε https://lawstrust.com/en/ico/pravovoj-status-kriptovalyut .

236 Adam Bergman, «What you should know about taxation of cryptocurrencies», (2018), διαθέσιμο σε https://www.forbes.com/sites/greatspeculations/2018/01/03/what-you-should-know-about-taxation-of-cryptocurrencies/ .

237 Samburaj Das, «Israel Tax Authority Deems Bitcoin a Taxable Asset», (2017), διαθέσιμο σε https://fintechranking.com/2017/01/16/israel-tax-authority-deems-bitcoin-a-taxable-asset/ .

238 Maria Santos, «Singapore revenue authority recognizes and taxes Bitcoin», (2018), διαθέσιμο σε https://99bitcoins.com/singapore-revenue-authority-recognizes-and-taxes-bitcoin/ .

όπως για παράδειγμα όταν παρέχουν ορισμένα προνόμια αντί να χρησιμεύουν ως μέσα συναλλαγής. Τέτοια περίπτωση αποτελεί το νόμισμα Legends (LGD[239]). Επίσης, καθώς ο αριθμός των αρχικών προσφορών νομισμάτων (ICO) πληθαίνει, πολλά κρυπτονομίσματα θα έχουν πολύ περιορισμένη χρήση και για μία μόνο συγκεκριμένη λειτουργία. Πολλά νομίσματα, για παράδειγμα, έχουν την έννοια της αξίωσης για τη διανομή μεριδίων από συγκεκριμένα έργα - projects[240]. Αυτά εμφανίζονται περισσότερο ως ιδιοκτησία, παρά ως πραγματικά νομίσματα, παρότι έχουν ρευστοποιήσιμη αξία στην ελεύθερη αγορά – δεν χρησιμοποιούνται πρωτίστως ως νομίσματα ανταλλαγής, αλλά ως μερίδια κερδών από ένα έργο και τα οποία ενδεχομένως να χρησιμεύσουν ως ανταλλακτικό μέσο για άλλα αντικείμενα ή νομίσματα. Παρόλα αυτά, το μεγαλύτερο ποσοστό των κρυπτονομισμάτων πράγματι επιδιώκουν να είναι πρωτίστως εναλλακτικές μορφές των παραδοσιακών νομισμάτων και να ανταλλάσσονται με αυτά κοινά αγαθά, χωρίς συχνά να έχουν κάποια δική τους εγγενή αξία – αρκεί το γεγονός ότι είναι ευρέως αποδεκτά από τους άλλους[241].

Όπως είναι επόμενο, οι συνέπειες της φορολόγησης των κρυπτονομισμάτων ως ιδιοκτησία είναι δυσμενέστερη για τους χρήστες τους, οι οποίοι πρέπει να αποδείξουν κέρδη ή ζημίες σε κάθε συναλλαγή τους με αυτά[242], απαίτηση που αφενός μεν γίνεται αρκετά επαχθής για τους καθημερινούς χρήστες, αφετέρου δε γίνεται πιο περίπλοκη με τις διακυμάνσεις της αξίας των κρυπτονομισμάτων μέσα σε μία ημέρα.

---

239 Το συγκεκριμένο νόμισμα εξαργυρώνεται σε προνόμια VIP σε κλαμπ του Λας Βέγκας, σε όσους το κατέχουν σε μεγάλες ποσότητες. Λειτουργικά συμπεριφέρεται ως ιδιοκτησία, από τη στιγμή που η κυκλοφορία του περιορίζεται στο συγκεκριμένο μέρος – δεν έχει το εύρος της χρήσης των υπολοίπων κρυπτονομισμάτων, τα οποία μπορεί να είναι ευρέως αποδεκτά από την εμπορική κοινότητα. «LGD Coin - Legends Room - Voted #1 PICK for 2018», διαθέσιμο σε https://steemit.com. Βλ. επίσης Jamie Redman, «Las Vegas Strip Club Aims to Use Cryptocurrency for Daily Operations», (2017), διαθέσιμο σε https://news.bitcoin.com/las-vegas-strip-club-cryptocurrency-daily-operations/ .

240 Όπως για παράδειγμα το Solar DA, το οποίο σχετίζεται με την οικοδόμηση φωτοβολταϊκών εγκαταστάσεων ανά τον κόσμο και διανέμει τα κέρδη στους ιδιοκτήτες των νομισμάτων, Βλ. σχετικά https://solarcoin.org .

241 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

242 Bruce Blythe, «How Are Gains or Losses on Cryptocurrencies Taxed?», (2018), διαθέσιμο σε https://tickertape.tdameritrade.com.

Διαφορετικές προσεγγίσεις κρατών

Σε αντίθεση με το αμερικανικό σύστημα φορολόγησης των κρυπτονομισμάτων ως ιδιοκτησία, άλλες χώρες έχουν προσεγγίσει τα κρυπτονομίσματα γενικά και το Bitcoin ειδικά, με λιγότερο επαχθείς φορολογικές ρυθμίσεις. Στην Ευρωπαϊκή Ένωση και με βάση την απόφαση του Ευρωπαϊκού Δικαστηρίου C-264/14[243], κρίθηκε ότι τα κρυπτονομίσματα αποτελούν συνάλλαγμα, ως μέσο πληρωμής και οι συναλλαγές με αυτά θεωρούνται παροχή υπηρεσιών. Η αγορά και η πώλησή τους δεν υπόκεινται σε ΦΠΑ, αλλά μπορεί να υπόκεινται σε άλλου είδους φόρους, οι οποίοι διαφέρουν εντός των χωρών – μελών της Ευρωπαϊκής Ένωσης.

Στη Βρετανία οι περισσότερες συναλλαγές σε κρυπτονομίσματα, τα οποία θεωρούνται περιουσιακό στοιχείο και όχι νόμισμα, εξαιρούνται από τον Φόρο Προστιθέμενης Αξίας και υπόκεινται είτε σε φόρο εισοδήματος είτε σε φόρο κεφαλαιουχικών κερδών. Η παραγωγή νομίσματος ως επιχειρηματική δραστηριότητα υπάγεται σε φόρο, ενώ στην περίπτωση που κάποιος επενδύει ατομικά σε κρυπτονομίσματα, υπόκειται σε φόρο κερδών από κεφάλαιο στα κέρδη που προέρχονται από τις επενδύσεις αυτές[244].

243 Το άρθρο 2, παράγραφος 1, στοιχείο γ', της οδηγίας 2006/112/ΕΚ του Συμβουλίου, της 28ης Νοεμβρίου 2006, σχετικά με το κοινό σύστημα φόρου προστιθέμενης αξίας, έχει την έννοια ότι αποτελούν παροχή υπηρεσιών εξ επαχθούς αιτίας κατά τη διάταξη αυτή συναλλαγές όπως οι επίμαχες στην κύρια δίκη, οι οποίες συνίστανται σε αγοραπωλησίες συμβατικών νομισμάτων έναντι του εικονικού νομίσματος «bitcoin» και αντιστρόφως, έναντι καταβολής χρηματικού ποσού που αντιστοιχεί στο περιθώριο κέρδους που προκύπτει από τη διαφορά μεταξύ, αφενός, της τιμής στην οποία ο οικείος επιχειρηματίας αγόρασε το συνάλλαγμα και, αφετέρου, της τιμής στην οποία πώλησε το συνάλλαγμα αυτό στους πελάτες του. 2) Το άρθρο 135, παράγραφος 1, στοιχείο ε', της οδηγίας 2006/112 έχει την έννοια ότι στις πράξεις που απαλλάσσονται από τον ΦΠΑ κατά την εν λόγω διάταξη εμπίπτει η παροχή υπηρεσιών όπως οι επίμαχες στην κύρια δίκη, οι οποίες συνίστανται σε ανταλλαγές συναλλάγματος μεταξύ συμβατικών νομισμάτων και μονάδων του εικονικού νομίσματος «bitcoin», έναντι καταβολής χρηματικού ποσού που αντιστοιχεί στο περιθώριο κέρδους που προκύπτει από τη διαφορά μεταξύ, αφενός, της τιμής στην οποία ο οικείος επιχειρηματίας αγόρασε το συνάλλαγμα και, αφετέρου, της τιμής στην οποία πώλησε το συνάλλαγμα αυτό στους πελάτες του. Βλ. σχετικά Απόφαση του Δικαστηρίου (πέμπτο τμήμα) της 22ας Οκτωβρίου 2015 [αίτηση του Högsta förvaltningsdomstolen (Σουηδία) για την έκδοση προδικαστικής αποφάσεως] — Skatteverket κατά David Hedqvist (Υπόθεση C-264/14) , διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CA0264&from=IT.

244 «Φορολογία κρυπτονομισμάτων στο εξωτερικό και την Ελλάδα», (2020), διαθέσιμο σε https://horizonlawfirm.gr/forologia-kryptonomismaton-sto-exoteriko-ke-stin-ellada/.

Η Σλοβενία[245] δεν αποδέχεται τα κρυπτονομίσματα ούτε ως νομίσματα ούτε ως ιδιοκτησία. Το κράτος φορολογεί τις πληρωμές που πραγματοποιούνται με τα κρυπτονομίσματα ως εισόδημα για τους ιδιώτες και δεν υπάρχει φόρος από κεφαλαιουχικά κέρδη σε οποιαδήποτε αύξηση της αξίας τους.

Η Γερμανία[246] έχει αντίστοιχη προσέγγιση, χαρακτηρίζοντάς τα όχι ως νομίσματα, αλλά ως οικονομικό μέσο. Παρά το γεγονός ότι το Bitcoin υπόκειται σε φόρο κεφαλαιουχικών κερδών στη Γερμανία, ο φόρος αυτός επιβάλλεται μόνο αν τα κέρδη από κρυπτονομίσματα αποκτήθηκαν εντός ενός έτους από την απόκτηση τους[247].

Η Ελβετία[248] έχει την καλύτερη αντιμετώπιση απέναντι στα κρυπτονομίσματα, μη θεωρώντας τα ούτε αγαθό, ούτε υπηρεσία, αλλά αντιμετωπίζοντάς τα ως νομίσματα. Αυτό έχει ως αποτέλεσμα να μην επιβάλλονται στις συναλλαγές ΦΠΑ ή άλλοι σχετιζόμενοι φόροι. Ένα από τα πιο δημοφιλή μέρη για την τεχνολογία blockchain και για τις νεοσύστατες εταιρίες κρυπτονομισμάτων είναι η πόλη Zug[249]. Κάποιοι εκτιμούν ότι το ένα τέταρτο (1/4) των παγκόσμιων κεφαλαίων σε κρυπτονομίσματα βρίσκεται σε ελβετικά ιδρύματα. Ο βασικός λόγος για αυτή την τάση, πέρα από την ίδια τη φορολογική προσέγγιση της χώρας απέναντι στα κρυπτονομίσματα, είναι το κανονιστικό πλαίσιο που διέπει τα ιδρύματα αυτά[250]. Οι ελβετικοί νόμοι επιτρέπουν σε αυτά να λειτουργούν με ευρύ σκοπό, ο οποίος τους παρέχει τη δυνατότητα να δικαιολογήσουν επενδύσεις με αρχικές προσφορές νομισμάτων (ICO)[251]. Παρόλα αυτά, το μοντέλο αυτό είναι αμφιλεγόμενο. Κατ' αρχάς, τα νομίσματα που εκδίδουν

245 «Tax Treatment of Cryptocurrencies in Slovenia», (2018), διαθέσιμο σε http://www.nomoretax.eu.

246 «Germany: A Surprising Bitcoin Tax Haven», (2018), διαθέσιμο σε http://www.nomoretax.eu.

247 «Φορολογία κρυπτονομισμάτων στο εξωτερικό και την Ελλάδα», (2020), διαθέσιμο σε https://horizonlawfirm.gr/forologia-kryptonomismaton-sto-exoteriko-ke-stin-ellada/.

248 «Switzerland now a Cryptocurrency Tax Haven», (2018), διαθέσιμο σε https://bit-media.org.

249 Darius Mcquaid, «It's a revolution' Cryptocurrency investors flock to Swiss town Crypto Valley», (2018), διαθέσιμο σε https://www.express.co.uk.

250 Το ίδιο το ίδρυμα είναι ανεξάρτητο και έχει διορισμένο Διοικητικό Συμβούλιο, το οποίο επιβλέπει τη διαχείριση και τη λειτουργία του. Επίσης, εκδίδει νομίσματα σε ανταλλαγή χρήματος, τα οποία στη συνέχεια τα χρησιμοποιεί για την εξέλιξη των προγραμμάτων και των τεχνολογιών υπέρ των κρυπτονομισμάτων. Matthew Allen, «Swiss financial centre opens up to bitcoin», (2018), διαθέσιμο σε https://www.swissinfo.ch.

251 Brenna Hughes Neghaiwi, «Top Swiss cryptocurrency lawyer questions 'stupid' ICO structure», (2018), διαθέσιμο σε https://uk.reuters.com.

τα ιδρύματα αυτά θεωρούνται τεχνικά περισσότερο ως «αναμνηστικά» μίας δωρεάς και όχι τόσο ως αντικείμενα διαθέσιμα προς αγορά. Μολαταύτα, επειδή πολλές, εάν όχι οι περισσότερες από τις «δωρεές» των ιδρυμάτων πραγματοποιούνται με δεδομένη την προσδοκία της φοροαπαλλαγής, τα ιδρύματα αποκτούν φορολογικά πλεονεκτήματα έχοντας περισσότερο χαρακτήρα κοινωνικών επενδύσεις υψηλού κινδύνου, παρά πραγματικά φιλανθρωπικό, χωρίς προσδοκίες επιστροφής[252]. Αν και τα ελβετικά ιδρύματα δεν εξαιρούνται αυτομάτως από το φόρο, αλλά πρέπει να έχουν φιλανθρωπικό σκοπό για να υπαχθούν σε καθεστώς απαλλαγής, ο ολοένα αυξανόμενος αριθμός τους καθιστούν πιο πιθανό το γεγονός της εξαίρεσης από το φόρο και της μη πληρωμής των υπερβολικών ελβετικών εταιρικών φορολογικών συντελεστών[253].

Στην Ιαπωνία, τα κρυπτονομίσματα αναγνωρίζονται επίσημα ως μέσο πληρωμής. Η πώλησή τους ήδη από την 1η Ιουλίου 2017, απαλλάσσεται από τον φόρο κατανάλωσης (8%). Τα κέρδη που αποκτήθηκαν από τη διαπραγμάτευση κρυπτονομισμάτων θεωρούνται έσοδα και υπόκεινται σε όλα τα παραδοσιακά είδη φορολογίας, όπως το φόρο εισοδήματος, το φόρο κεφαλαιουχικών κερδών και τον εταιρικό φόρο[254].

Στην Αυστραλία, οι φορολογικές Αρχές θεωρούν πως τα κρυπτονομίσματα δεν είναι χρήματα ή ξένο νόμισμα, αλλά ένα περιουσιακό στοιχείο με σκοπό το κεφαλαιουχικό κέρδος. Οι συναλλαγές σε κρυπτονομίσματα για προσωπικούς σκοπούς απαλλάσσονται από τη φορολογία σε δύο περιπτώσεις: α) αν το κρυπτονόμισμα χρησιμοποιήθηκε ως πληρωμή για αγαθά και υπηρεσίες για προσωπική χρήση και β) αν η αξία της συναλλαγής είναι χαμηλότερη από 10.000 δολάρια Αυστραλίας. Η παραγωγή και η ανταλλαγή κρυπτονομισμάτων για επαγγελματικούς σκοπούς

252 Selva Ozelli, «Why Switzerland is Becoming a Crypto Nation with a Flourishing ICO Market: Expert Take», (2018), διαθέσιμο σε https://cointelegraph.com.

253 Peter Hody, «Crypto Currencies: Switzerland's New Banking Secrecy?», (2018), διαθέσιμο σε https://www.finews.com.

254 «Φορολογία κρυπτονομισμάτων στο εξωτερικό και την Ελλάδα», (2020), διαθέσιμο σε https://horizonlawfirm.gr/forologia-kryptonomismaton-sto-exoteriko-ke-stin-ellada/.

θεωρούνται χρηματιστηριακή συναλλαγή και φορολογούνται σύμφωνα με τις σχετικές διατάξεις[255].

Μία άλλη χώρα γνωστή για την πολιτική της απέναντι στα κρυπτονομίσματα είναι ο Μαυρίκιος, ο οποίος είναι γνωστός ως «το νησί του Ethereum»[256], λόγω της φιλικής πολιτικής του απέναντι στις νεοσύστατες εταιρίες κρυπτονομισμάτων[257]. Το κράτος επέτρεψε καινοτομίες και συνεργασίες σε τέτοιο βαθμό που στο Μαυρίκιο υπάρχει η δεύτερη μεγαλύτερη τράπεζα στον κόσμο με δανειακό σύστημα τεχνολογίας blockchain, τη SALT[258]. Η εταιρική σχέση της με την Κρατική Τράπεζα του Μαυρικίου (SBM) επιτρέπει το δανεισμό περιουσιακών στοιχείων με εγγύηση σε κρυπτονομίσματα. Από φορολογική άποψη, το κράτος παρέχει μία εξαιρετικά χρήσιμη φορολογική δομή, γνωστή ως GBC2[259] («Global Business Company» με προσδιορισμό κατηγορίας 2). Εταιρίες με άδεια GBC2 οφείλουν να δρουν εκτός του κράτους του Μαυρικίου - τυπικά δεν συνδέονται με γεωγραφική τοποθεσία και εξαιρούνται των φόρων, κάτι που τις καθιστά στέρεη επιλογή για το ICO.

Τέλος, το Μάρτιο του 2020, ο Γερουσιαστής των Ηνωμένων Πολιτειών Paul Gosar παρουσίασε «το Νομοσχέδιο για τα κρυπτονομίσματα του έτους 2020», ένα νομοσχέδιο που προσπαθεί να χαρτογραφήσει σε ευρεία κλίμακα τα ψηφιακά νομίσματα και να παράσχει όχι μόνο σαφήνεια, αλλά και νομιμότητα σε αυτά. Η

255 Ό.π. υποσημείωση 261.

256 Darryn Pollock, «Ethereum Island Mauritius Craves To Become blockchain Paradise», (2018), διαθέσιμο σε https://cointelegraph.com.

257 Kyle Torpey, «The Republic of Mauritius's Regulatory Sandbox Could Attract blockchain Startups», (2018), διαθέσιμο σε https://bitcoinmagazine.com.

258 Michael Kimani, «SALT Lending and Mauritius State Bank Partner on blockchain Backed Cash Loans», (2018), διαθέσιμο σε https://cryptovest.com.

259 Η κατηγορίας δύο (2) Παγκόσμια Εταιρία Επιχειρήσεων («Global Business Company» - GBC 2) είναι ένα είδος εταιρίας που έχει έδρα το Μαυρίκιο, αλλά δραστηριοποιείται εκτός της χώρας. Απαιτούνται κατά μέσο όρο δύο- τρεις ημέρες για να ιδρυθεί και προτιμάται για την κατοχή και διαχείριση ιδιωτικών περιουσιακών στοιχείων, καθώς παρέχει μεγαλύτερη εχεμύθεια με τη διάρθρωση των συμμετοχών μέσω εξουσιοδοτημένων μετόχων. Φορολογικά θεωρείται μη εγχώρια και επιπλέον απολαμβάνει φοροαπαλλαγές. Εταιρίες που ασχολούνται με δραστηριότητες τιμολόγησης, προώθησης αγαθών και διεθνών συναλλαγών συχνά χρησιμοποιούν τη δομή της GBC2. Βλ. σχετικά https://www.offshorecompanycorp.com, https://bbcincorp.com.

πρόταση του Gosar διαχωρίζει τα νομίσματα αυτά σε τρεις κατηγορίες: κρυπτοπροϊόντα, κρυπτονομίσματα και κρυπτοχρεόγραφα[260].

Κλείνοντας και παρά τις ιδιόμορφες φορολογικές ρυθμίσεις των κρατών που παρουσιάστηκαν ανωτέρω, η επικρατέστερη διεθνής τάση είναι να ρυθμίζει τα κρυπτονομίσματα ως «ιδιοκτησία» ή «περιουσιακό στοιχείο». Οι περισσότερες χώρες δεν έχουν πλησιάσει ακόμα την ιδέα της μεταχείρισης των κρυπτονομισμάτων ως νομισμάτων, τόσο σε τεχνική, όσο και και νομική βάση.

Η αναγνώριση των κρυπτονομισμάτων ως νομισμάτων– πολιτικοοικονομικές προεκτάσεις.

Τα νομίσματα αποτελούν ένα μοναδικό αγαθό που κυκλοφορεί ως μέσο συναλλαγής. Το Bitcoin και τα άλλα είδη κρυπτονομισμάτων φαίνεται ότι συνάδουν με την περιγραφή αυτή, καθώς είναι σε κυκλοφορία, αλλά και είναι ευρέως αποδεκτά ως μέσο συναλλαγής. Ενώ οι αρχαίοι Αιγύπτιοι χρησιμοποιούσαν ως χρήμα μεταλλικούς δακτυλίους, η δυναστεία των Tang στην Κίνα για πρώτη φορά έκανε χρήση χαρτονομισμάτων περί τον 7ο αιώνα μ.Χ και η εταιρία Western Union ολοκλήρωσε την πρώτη ηλεκτρονική μεταφορά χρημάτων το 1871[261]. Η πιο σημαντική κατηγορία χρημάτων σήμερα είναι το παραστατικό χρήμα (fiat money[262]), το οποίο δεν στηρίζεται σε κάποιο άλλο υλικό αποθεματικό, αλλά αποκτά αξία επειδή γίνεται

260 Από τα συμφραζόμενα του νομοσχεδίου, προέκυπτε ότι τα ψηφιακά νομίσματα όπως το Bitcoin κατηγοριοποιούνται περισσότερο ως κρυπτοπροϊόντα, παρά ως κρυπτονομίσματα. Kollen Post, «US Congressman Introduces Crypto-Currency Act of 2020», διαθέσιμο σε https://cointelegraph.com/news/us-congressman-introduces-crypto-currency-act-of-2020.

261 Felix Martin, «Money: The Unauthorized Biography--From Coinage to Cryptocurrencies», Vintage, Reprint Edition, (2015).

262 Παραστατικό χρήμα ή αλλιώς χρήμα αναγκαστικής κυκλοφορίας είναι το μέσον πληρωμής, το οποίο δεν καλύπτεται από αποθεματικό άλλων υλικών (π.χ. χρυσός) και επομένως στερείται κάποιας εσωτερικής αξίας, έστω και έμμεσα. Επιβάλλεται στις συναλλαγές από κάποια αρχή (συνήθως το κράτος), τόσο στις πληρωμές, όσο και στις εισπράξεις. Εκφράζεται με κάποια νομισματική μονάδα και έχει την μορφή συνήθως χαρτονομισμάτων και κερμάτων, τα οποία μπορεί να έχουν ονομαστική αξία ίση, πολλαπλάσια ή υποπολλαπλάσια της νομισματικής μονάδας. Benton E. Gup, «What Is Money? From Commodities to Virtual Currencies/Bitcoin» (2014).

αποδεκτό από όλα τα συναλλασσόμενα μέρη. Αντίστοιχα, το Bitcoin και τα άλλα κρυπτονομίσματα είναι παρόμοια με το παραστατικό χρήμα, διότι δεν έχουν εσωτερική αξία.

Σε απάντηση του ερωτήματος εάν το Bitcoin αποτελεί χρήμα, αμερικανικό δικαστήριο στην υπόθεση *United States v. Faiella*[263] εξέτασε τον ορισμό του «χρήματος» (ο οποίος είναι συναφής με τον ορισμό του νομίσματος) και διευκρίνισε ότι το Bitcoin πράγματι εμπίπτει στην έννοια του χρήματος, καθώς χρησιμοποιείται ευρέως ως μέσο συναλλαγής και εμπίπτει στην εφαρμογή του νόμου περί ξεπλύματος μαύρου χρήματος.

Στην περίπτωση που τελικά τα κρυπτονομίσματα ετύγχαναν νομικής αντιμετώπισης νομισμάτων και όχι ιδιοκτησίας, θα προέκυπταν σημαντικές οικονομικές συνέπειες[264]. Πέρα από το ότι η αξία τους θα αυξανόταν, καθώς θα υπήρχε πλέον ένα μέσο συναλλαγών χωρίς τον αρνητικό φορολογικό παράγοντα της αναγνώρισης κέρδους ή ζημίας σε κάθε συναλλαγή, θα ενισχυόταν η προσπάθεια κυρίως του Bitcoin να αποτελέσει ένα παγκόσμιο νομισματικό αποθεματικό. Το Διεθνές Νομισματικό Ταμείο[265], το οποίο επιλέγει τα νομίσματα αναφοράς, βάσει της παγκόσμιας οικονομικής σημασίας τους, δημιουργεί ένα αποθεματικό από «Ειδικά Τραβηκτικά Δικαιώματα» (Special Drawing Rights)[266]. Δεδομένου ότι το δολάριο

263 *US v. Faiella and Shrem* – «Ruling on Bitcoin as Money or Funds», 39F. Supp. 3D344, (2014), διαθέσιμο σε https://internetlawcommentary.com. Πρόκειται για την πρώτη δικαστική απόφαση σχετικά με τα Bitcoin, κάτι που την καθιστά εξαιρετικά σημαντική και παράγει αντίστοιχα το πρώτο δεδικασμένο σχετικά με τη νομοθεσία για τα Bitcoin. Σύμφωνα με την απόφαση αυτή, τα bitcoin υπάγονται στους νόμους περί ξεπλύματος μαύρου χρήματος και τραπεζικών χρεογράφων.

264 Nika Antonikova, «Real Taxes on Virtual Currencies: What Does the IRS Say?», *Virginia Tax Review,* Vol. 34/ 3 (2014).

265 Το Διεθνές Νομισματικό Ταμείο (ΔΝΤ) λειτουργεί για την ενίσχυση της διεθνούς νομισματικής συνεργασίας, τη διασφάλιση της οικονομικής σταθερότητας, τη διευκόλυνση του διεθνούς εμπορίου, την προώθηση υψηλών ποσοστών απασχόλησης και σταθερής οικονομικής ανάπτυξης και τη μείωση της φτώχειας σε ολόκληρο τον κόσμο. Το ΔΝΤ ιδρύθηκε το 1945, κυβερνάται και ελέγχεται από τις 186 κυβερνήσεις των κρατών-μελών, τα οποία προέρχονται σχεδόν από κάθε άκρη της γης. Βλ. σχετικά https://www.imf.org/external/lang/Greek/np/exr/facts/glanceg.htm.

266 Ένα διεθνές αποθεματικό περιουσιακό στοιχείο, το οποίο δημιουργήθηκε από το ΔΝΤ το 1969, ως εναλλακτική μορφή των υφιστάμενων επίσημων συναλλαγματικών διαθεσίμων των χωρών-μελών του. Τα «Ειδικά Τραβηκτικά Δικαιώματα» δεν είναι νόμισμα και δεν έχουν φυσική παρουσία όπως το χρήμα, αλλά αποτελούν λογιστική καταχώριση και αντιπροσωπεύουν απαίτηση για συναλλαγματικά αποθέματα νομισμάτων των χωρών-μελών του ΔΝΤ (ευρώ, ιαπωνικά γιεν, λίρες, δολάρια κτλ), με τα οποία μπορούν

των ΗΠΑ απολαμβάνει στην παρούσα φάση μία εξέχουσα θέση ως κύριο νόμισμα, η Κίνα και άλλες χώρες θα επιθυμούσαν ένα σύστημα όπου ένα ουδέτερο νόμισμα θα ήταν πιο ισχυρό και η επιρροή των ΗΠΑ θα μειωνόταν σχετικά. Επιπρόσθετα, με ένα τέτοιο σύστημα η κεντρική τράπεζα των ΗΠΑ θα απολάμβανε λιγότερης ισχύος ως προς τη χειραγώγηση των οικονομικών κύκλων και της οικονομίας γενικότερα. Περαιτέρω, θα περιοριζόταν η κερδοσκοπία των τραπεζών. Κατά συνέπεια, η μη φορολόγηση των κρυπτονομισμάτων ως ιδιοκτησία θα ενίσχυε τις χρήσεις και τη δημοφιλία τους.

Παρά τις ανωτέρω επιφυλάξεις, το Σεπτέμβριο του 2020 η πολιτεία του Wyoming στις ΗΠΑ ενέκρινε την αίτηση του Kraken, ενός από τα πρώτα ανταλλακτήρια κρυπτονομισμάτων, για τη δημιουργία Ιδρύματος Αποθεμάτων Ειδικού Σκοπού (SPDI), ήτοι δόθηκε η πρώτη επίσημη άδεια τράπεζας στον κόσμο για ψηφιακά περιουσιακά στοιχεία. Η Kraken Financial, όπως ονομάζεται, θα προσφέρει αρχικά τις υπηρεσίες της μόνο στις ΗΠΑ, αλλά σύντομα θα λειτουργήσει σε παγκόσμια κλίμακα. Θα έχει τη δυνατότητα να κάνει ό,τι και μία παραδοσιακή τράπεζα, με τη διαφορά πως θα προσφέρει και υπηρεσίες θεματοφυλακής για κρυπτονομίσματα. Παρότι υπάρχει ήδη η δυνατότητα θεματοφυλακής από πιστωτικά ιδρύματα, η κίνηση αυτή είναι ριζική, διότι για πρώτη φορά θα αφορά ιδιώτες και επιχειρήσεις και όχι μόνο θεσμικούς φορείς[267].

να ανταλλαγούν. Βλ. σχετικά http://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR.

267 Λόγω των ιδιαίτερων συνθηκών ίδρυσής της, η Kraken θα υποχρεούται να διατηρεί το 100% των καταθέσεών της ανά πάσα στιγμή (και όχι ένα κλάσμα μόνο, όπως συμβαίνει στις παραδοσιακές τράπεζες). Εάν οι πελάτες της προβούν σε αναλήψεις, οφείλει να είναι σε θέση να εκπληρώσει την υποχρέωση να τους παρέχει τα χρήματα, ανεξάρτητα από το πόσα δάνεια έχει σε εκκρεμότητα. Κατά το πρώτο έτος λειτουργίας, η Kraken Financial ελπίζει να παρέχει θεματοφυλακή σε ψηφιακά περιουσιακά στοιχεία, λογαριασμούς ταμιευτηρίου, υπηρεσίες εμβασμάτων και χρηματοδότησης. Με την πάροδο του χρόνου υπολογίζει να επεκταθεί και σε άλλες υπηρεσίες, όπως στην έκδοση χρεωστικών καρτών που θα τροφοδοτούνται από τον καταθετικό λογαριασμό των πελατών σε κρυπτονομίσματα. Βλ. σχετικά Βασίλης Παζόπουλος, «Δόθηκε η πρώτη άδεια τράπεζας κρυπτονομισμάτων», (2020), διαθέσιμο σε https://www.euro2day.gr/investments/crypto/article/2042288/dothhke-h-proth-adeia-trapezas-kryptonomismaton-.html .

Προστασία της ιδιωτικότητας και επιβολή του φόρου

Αναφορικά με το εξαιρετικά σημαντικό θέμα της πάταξης του ξεπλύματος βρώμικου χρήματος και της διασφάλισης της σωστής είσπραξης των φόρων, τίθενται σημαντικά ζητήματα σχετικά με την προστασία της ιδιωτικότητας των χρηστών[268]. Η τωρινή αντιμετώπιση του ζητήματος δεν καλύπτει αποτελεσματικά τα θέματα της τεχνολογίας blockchain, σε σχέση με τα περισσότερα κρυπτονομίσματα. Το ερώτημα που προκύπτει σε αυτή τη βάση είναι ο τρόπος με τον οποίο θα εξισορροπήσουν τελικά τα οφέλη που προκύπτουν από η δυνατότητα εντοπισμού της κυριότητας σε κάθε μονάδα κρυπτονομίσματος που περιέχεται στο καθολικό blockchain, με τα ζητήματα προστασίας προσωπικών δεδομένων που προκύπτουν για τους πολίτες. Το Bitcoin με τον τρόπο λειτουργίας του δεν αποτελεί πλέον μία ανώνυμη πηγή συναλλαγών, καθώς οι περισσότερες συναλλαγές μπορούν να συνδεθούν με μία δημόσια ταυτότητα, η οποία μπορεί να οδηγήσει στους ιδιώτες κατά την εγγραφή τους σε έναν ιστότοπο συναλλαγών[269]. Κατά συνέπεια, το ιστορικό ενός μεταβιβασμένου Bitcoin μπορεί ήδη να εντοπιστεί με σχετική ευκολία. Άτομα ιδιαίτερα εξοικειωμένα με την τεχνολογία των κρυπτονομισμάτων έχουν τη δυνατότητα να διαφύγουν τον εντοπισμό, λαμβάνοντας ιδιαίτερα μέτρα διαφύλαξης των συναλλαγών τους, καθιστώντας τις ενέργειες αυτές και την ανωνυμία τους τη βάση για το αδίκημα του ξεπλύματος μαύρου χρήματος μέσω της χρήσης των κρυπτονομισμάτων[270]. Εάν απαιτούνταν οι εγγραφές των χρηστών να γίνονταν με ταυτόχρονη δημόσια ταυτοποίηση συνδεδεμένη με τα περιουσιακά στοιχεία τους, ανεξάρτητα από το η απαίτηση αυτή θα προερχόταν από μία κρατική υπηρεσία ή κάποιο χρηματοπιστωτικό ίδρυμα, αυτό θα αποτελούσε μεν επεξεργασία ευαίσθητων

268 Nika Antonikova, «Real Taxes on Virtual Currencies: What Does the IRS Say?», *Virginia Tax Review,* Vol. 34/ 3 (2014).

269 Benjamin Fabian, Tatiana Ermakova, Jonas Krah, Ephan Lando και Nima Ahrary, «Adoption of Security and Privacy Measures in Bitcoin – Stated and Actual Behavior», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184130 .

270 Saman Jafari, Tien Vo-Huu, Bahruz Jabiyev, Alejandro Mera και Reza Mirzazade Farkhani, «Cryptocurrency: A Challenge to Legal System», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172489 .

προσωπικών δεδομένων, αλλά με το άλλοθι της σημαντικής καταπολέμησης του μαύρου χρήματος, η οποία θα οδηγούσε σε αύξηση των εισπράξεων, σε μείωση της φοροδιαφυγής και σε φορολογική ισότητα[271].

Η λύση στο θέμα της φορολόγησης των κρυπτονομισμάτων πιθανόν να μπορούσε να δοθεί με τη διαφοροποίηση αυτών που χρησιμεύουν για επενδύσεις ή για κερδοσκοπία (speculation) από αυτά που χρησιμοποιούνται ως νομίσματα[272]. Αυτός ο διαχωρισμός στην παρούσα φάση είναι εξαιρετικά δύσκολος, δεδομένων των τύπων που πρέπει να εφαρμοστούν και του εντοπισμού που πρέπει να γίνει για να επιβληθεί ένας τέτοιος κανόνας. Ένας ιδιώτης πρέπει να αποδείξει ότι ο λογαριασμός του δεν είναι επενδυτικός. Πιθανόν στον μέλλον με τις βελτιώσεις της τεχνολογίας, η εφαρμογή του κανόνα αυτού να είναι πιο εύκολη λογιστικά. Και από τη στιγμή που αυτό θα επιτευχθεί, η φορολόγηση των κρυπτονομισμάτων θα γίνει κατά περίπτωση: είτε ως ιδιοκτησία, για τις επενδύσεις και την κερδοσκοπία είτε ως νομίσματα με τη χρήση αυτή.

8 Τα κρυπτονομίσματα στην ελληνική πραγματικότητα και η φορολόγησή τους

Στη χώρα μας κατά το έτος 2018 πραγματοποιούνταν ημερησίως συναλλαγές σε Bitcoin ύψους 21.000 ευρώ, κατά προσέγγιση[273]. Εβδομήντα (70) καταστήματα το δέχονταν ως μέσο πληρωμής, ενώ παράλληλα λειτουργούσαν και τέσσερις Αυτόματες Ταμειολογιστικές Μηχανές (ATM) ψηφιακών νομισμάτων στην Αθήνα

271 Isabelle Ioannides και Simona Guagliardo, «EU-US Trade and Investment Relations: Effects on Tax Evasion, Money Laundering and Tax Transparency In-Depth Analysis», Reference No: PE 598.602. Brussels: European Parliamentary Research Service (2017).

272 Ahmed Sami, «Cryptocurrency & Robots: How To Tax and Pay Tax on Them», Yale Law School (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocuments/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf . Βλ. επίσης Adam Bergman, «What You Should Know About Taxation Of Cryptocurrencies», διαθέσιμο σε https://www.forbes.com.

273 «Τα κρυπτονομίσματα «επελαύνουν» και στην ελληνική πραγματικότητα», διαθέσιμο σε http://www.dealnews.gr/roi/item/219451#.XoTbgIgzZPY.

και τη Θεσσαλονίκη[274]. Σήμερα, οι επιχειρήσεις που δέχονται πληρωμές σε bitcoin έχουν πολλαπλασιαστεί, ενώ τα ATM ανέρχονται πλέον σε 56 ανά την Ελλάδα[275]. Παρότι λόγω της φύσης του νομίσματος είναι αδύνατο να υπάρξουν σαφή και επιβεβαιωμένα στοιχεία, η είσοδος του Bitcoin στη χώρα μας έγινε ιδιαίτερα αισθητή μετά από τη θέσπιση των capital controls, με την ελπίδα ότι κάποιοι θα έβρισκαν διέξοδο στην κίνηση χρηματικών ποσών[276]. Για το λόγο αυτό, διάφορες επιχειρήσεις εξαγωγών προτίμησαν να κάνουν συναλλαγές σε Bitcoin για να παρακάμψουν τους περιορισμούς. Παρόλο που η Τράπεζα της Ελλάδος[277] έχει εκφράσει ρητά τις επιφυλάξεις της και έχει επανειλημμένα προειδοποιήσει για τη χρήση των κρυπτονομισμάτων, οι ελληνικές τράπεζες έτειναν να διευκολύνουν πελάτες τους που ήθελαν να προχωρήσουν σε επενδύσεις σε κρυπτονομίσματα, χωρίς παράλληλα να διαφωνούν με τους ενδεχόμενος κινδύνους.

274 Βλ. σχετικά https://coinatmradar.com/country/83/bitcoin-atm-greece

275 Βλ. σχετικά Αγγελική Βελεσιώτη, «Στον «πυρετό» του Bitcoin: Πόσα ATMs λειτουργούν στην Ελλάδα», (2020), διαθέσιμο σε https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/ston-pireto-tou-bitcoin-posa-atms-litourgoun-stin-ellada/ και https://coinatmradar.com/country/83/bitcoin-atm-greece/

276 Βάσω Αγγελέτου, «Οι Έλληνες αγοράζουν Bitcoin παρά τα capital controls», διαθέσιμο σε https://www.insider.gr/hristika/ependyseis/68904/oi-ellines-agorazoyn-bitcoin-para-ta-capital-controls.

277 Με δεδομένο ότι τα εικονικά νομίσματα, όπως είναι για παράδειγμα το Bitcoin, εξακολουθούν να βρίσκονται στο προσκήνιο της δημοσιότητας και με γνώμονα την ενημέρωση του κοινού για τους κινδύνους που σχετίζονται με τη χρήση τους, συμπεριλαμβανομένου και αυτού της απώλειας χρημάτων, η Τράπεζα της Ελλάδος παραπέμπει στην πρόσφατη σχετική κοινή ανακοίνωση της Ευρωπαϊκής Αρχής Τραπεζών (ΕΒΑ), της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) και της Ευρωπαϊκής Αρχής Κινητών Αξιών και Αγορών (ESMA) με τίτλο: «ESAs warn consumers of risks in buying virtual currencies» (ΑΓΓΛ) (2018). Βλ. σχετικά https://www.bankofgreece.gr.

Το Bitcoin κατά τη νομολογία του Ευρωπαϊκού Δικαστηρίου[278], αποτελεί μέσο πληρωμής, συνεπώς η αγοραπωλησία του από επιτηδευματίες δεν εμπίπτει στο πεδίο του ΦΠΑ. Από την άλλη πλευρά, δεν υπάρχει σχετική πρόβλεψη ως προς τη φορολογία του από πλευράς εισοδήματος. Κατά μία άποψη, δεν εντάσσεται ούτε στις ειδικές περιπτώσεις όπου η υπεραξία απαλλάσσεται του φόρου και υπόκειται μόνο σε εισφορά αλληλεγγύης (άρθρο 43Α του ΚΦΕ)[279]. Επιπρόσθετα, αυτό το ηλεκτρονικό νόμισμα δεν μπορεί να θεωρηθεί τίτλος ο οποίος διέπεται ξεκάθαρα από τις διατάξεις του άρθρου 42 του ΚΦΕ. Ελλείψει σχετικής νομοθεσίας, μία φορολογική και όχι χρηματοοικονομική προσέγγιση, θα μπορούσε να θεωρήσει το Bitcoin ως τίτλο, από τη στιγμή που αποκτήθηκε με σκοπό την κερδοσκοπία[280].

Η Ανεξάρτητη Αρχή Δημοσίων Εσόδων εξέτασε ήδη τη δυνατότητα φορολόγησης των κρυπτονομισμάτων, όπως αυτό προκύπτει από το Επιχειρησιακό της Σχέδιο για το 2019[281]. Από τον εντοπισμό κινήσεων με εμβάσματα χιλιάδων ευρώ, από

278 Με την από 22 Οκτωβρίου 2015 απόφασή του (C 264/14 - 5ο τμήμα) το Ευρωπαϊκό Δικαστήριο έκρινε ότι η αγορά και πώληση Bitcoin έναντι άλλων νομισμάτων δεν υπάγεται σε ΦΠΑ, όπως για παράδειγμα δεν υπάγεται σε ΦΠΑ η αγορά και πώληση Ευρώ έναντι Δολαρίων Αμερικής. Διατακτικό: *1) Το άρθρο 2, παράγραφος 1, στοιχείο γ', της οδηγίας 2006/112/ΕΚ του Συμβουλίου, της 28ης Νοεμβρίου 2006, σχετικά με το κοινό σύστημα φόρου προστιθέμενης αξίας, έχει την έννοια ότι αποτελούν παροχή υπηρεσιών εξ επαχθούς αιτίας κατά τη διάταξη αυτή συναλλαγές όπως οι επίμαχες στην κύρια δίκη, οι οποίες συνίστανται σε αγοραπωλησίες συμβατικών νομισμάτων έναντι του εικονικού νομίσματος «bitcoin» και αντιστρόφως, έναντι καταβολής χρηματικού ποσού που αντιστοιχεί στο περιθώριο κέρδους που προκύπτει από τη διαφορά μεταξύ, αφενός, της τιμής στην οποία ο οικείος επιχειρηματίας αγόρασε το συνάλλαγμα και, αφετέρου, της τιμής στην οποία πώλησε το συνάλλαγμα αυτό στους πελάτες του. 2) Το άρθρο 135, παράγραφος 1, στοιχείο ε', της οδηγίας 2006/112 έχει την έννοια ότι στις πράξεις που απαλλάσσονται από τον ΦΠΑ κατά την εν λόγω διάταξη εμπίπτει η παροχή υπηρεσιών όπως οι επίμαχες στην κύρια δίκη, οι οποίες συνίστανται σε ανταλλαγές συναλλάγματος μεταξύ συμβατικών νομισμάτων και μονάδων του εικονικού νομίσματος «bitcoin», έναντι καταβολής χρηματικού ποσού που αντιστοιχεί στο περιθώριο κέρδους που προκύπτει από τη διαφορά μεταξύ, αφενός, της τιμής στην οποία ο οικείος επιχειρηματίας αγόρασε το συνάλλαγμα και, αφετέρου, της τιμής στην οποία πώλησε το συνάλλαγμα αυτό στους πελάτες του.* C 264/14/EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 14.12.2015.

279 Βλ. Κων/νος Νανόπουλος, «Ποια είναι η φορολογία υπεραξίας από Bitcoins», διαθέσιμο σε https://www.newsbeast.gr/financial/arthro/2718492/pia-ine-i-forologia-iperaxias-apo-bitcoins.

280 Η πραγματοποίηση πάνω από τριών ομοειδών συναλλαγών επί μη διαπραγματεύσιμων τίτλων σε διάστημα ενός εξαμήνου, νοούνται ως 'επιχειρηματικές', καθιστώντας τον υπόχρεο, επιτηδευματία (παρ. 3 του άρθρου 21 του ΚΦΕ). Σε αυτή την περίπτωση, ο φορολογούμενος οφείλει να προβεί σε έναρξη επαγγέλματος, να καταβάλει τις αναλογούσες εισφορές στον ΕΦΚΑ και κατ' επέκταση θα φορολογείται με την κλίμακα των ελευθέρων επαγγελματιών, βάσει του άρθρου 15 του ΚΦΕ.

281 Συγκεκριμένα στην ενότητα Ψηφιακές πλατφόρμες και ηλεκτρονικά συστήματα πληρωμών αναφέρθηκε ότι «Μεγάλες είναι οι προκλήσεις που αντιμετωπίζει η φορολογική αρχή σε νέες, με παγκόσμια εμβέλεια, ψηφιακές πλατφόρμες εμπορίας ή παροχής υπηρεσιών και συστήματα πληρωμών σε επίπεδο ανταγωνισμού και φορολογικών εσόδων. Τέλος, η χρήση κρυπτονομισμάτων (Bitcoin, Ethereum, Ripple,

μετατροπές Bitcoin σε ευρώ ή άλλα ξένα νομίσματα, προκύπτει ότι ελάχιστοι δηλώνουν τα υπερκέρδη από συναλλαγές τέτοιων νομισμάτων. Το εντυπωσιακό είναι ότι τα έσοδα αυτά δηλώνονται κυρίως από ανέργους ή άτομα χωρίς εισοδήματα, αλλά με σημαντική ακίνητη περιουσία, με στόχο την κάλυψη τεκμηρίων. Επίσης, από πολλούς φορολογούμενους τίθεται το ερώτημα κατά πόσο και με ποιον τρόπο οφείλουν να αναγράψουν τα εμβάσματα σε ευρώ από τα διεθνή ανταλλακτήρια Bitcoin (Kraken, Bitstamp, Gemini κλπ), αλλά και πως αυτά θα αιτιολογηθούν[282]

κ.ά.) στο εξωτερικό έχει ξεκινήσει ακόμη και από φορολογούμενους για την αποπληρωμή των φορολογικών τους υποχρεώσεων. Αυτό σημαίνει ότι το προσεχές διάστημα η φορολογική αρχή θα κληθεί να αντιμετωπίσει τη νέα τάση συναλλαγών με ψηφιακό χρήμα που υπάρχει μέσω διαδικτύου, αλλά και να προτείνει τη θεσμοθέτηση της φορολόγησης των κρυπτονομισμάτων και ως επένδυση χαρτοφυλακίου, ήτοι με φόρο 15%, όπως στις μετοχές». Βλ. σχετικά «Επιχειρησιακό Σχέδιο ΑΑΔΕ», (2019), διαθέσιμο σε https://www.aade.gr/epiheirisiaka-shedia/epiheirisiako-shedio-aade-2019. Βλ. επίσης Γιώργος Παλαιτσάκης, «Οι αλλαγές στη φορολογία το 2019», (2019), διαθέσιμο σε https://www.naftemporiki.gr/finance/story/1461604/aade-oi-allages-sti-forologia-to-2019.

282 Η λύση που κάποιοι επιλέγουν ήδη, πριν νομοθετηθεί η φορολογία των κερδών αυτών, είναι η δήλωσή τους στο Ε1 γιατί, εάν δεν προκύπτουν άλλα εισοδήματα, αλλά εισπράχθησαν μεγάλα ποσά από bitcoin μέσω εμβασμάτων, γνωρίζουν πως κάθε προσαύξηση καταθέσεων εντοπίζεται πλέον από την αρμόδια φορολογική αρχή. Οι πιο συνεπείς δηλώνουν αρχικά την αξία κτήσης και μετά την αξία πώλησης στους κωδικούς 743 και 781. Μετά καταχωρούν την «υπεραξία» που αποκόμισαν στον κωδικό 865 του Ε1 και φορολογούνται με ποσοστό 15%, σαν να επρόκειτο για κέρδη από τους τόκους καταθέσεων ή μερίδια αλλοδαπής. Με τον τρόπο αυτό αποφεύγεται η φορολόγηση με τεκμήρια για πλασματικό εισόδημα με 29% σαν κέρδη από επιχειρήσεις (και με προκαταβολή φόρου 100% για την επόμενη χρονιά). Βλ. σχετικά Κωστής Πλάντζος, «Φόρο στα κέρδη από το bitcoin σχεδιάζει η εφορία», (2019), διαθέσιμο σε https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/foro-sta-kerdi-apo-to-bitcoin-sxediazei-i-eforia/.

ΤΡΙΤΟ ΚΕΦΑΛΑΙΟ: Εικονική κι Επαυξημένη Πραγματικότητα

1 Εισαγωγικά

Μπορεί να φανταστεί κάποιος την εξής εικόνα: ενώ οδηγεί εκτός πόλης, ένα μεγάλο αντικείμενο προσκρούει στο αυτοκίνητό του, με αποτέλεσμα την παραμόρφωση του άξονά του. Μετά από ολιγόλεπτη στάση και αναμονή, συνεχίζει κανονικά την πορεία του, καθώς ο άξονας έχει αυτοθεραπευτεί. Μπορεί να φαντάζει ως στιγμιότυπο ταινίας επιστημονικής φαντασίας, αλλά τα υλικά που «αυτοθεραπεύονται» και «θυμούνται» το σχήμα τους (auto-healing and shape-memorizing) έχουν ήδη κάνει την εμφάνισή τους και βρίσκονται στο εμπόριο, με στόχο να καλυτερέψουν την καθημερινότητα των ατόμων[1]. Η δημιουργία ενός εξυπνότερου κόσμου, όπου τα κτίρια θα «αισθάνονται» και θα προβλέπουν τις εξωτερικές θερμοκρασίες, προσαρμόζοντας αντίστοιχα τα συστήματα θέρμανσης ή ψύξης, όπου θα συναντά κανείς αυτοκίνητα που δεν χρειάζονται οδηγούς ή ειδικά γυαλιά θα τους καθοδηγούν κατά τη διάρκεια της οδήγησης, όπου οι ηλεκτρονικές συσκευές θα διαγιγνώσκουν από μόνες τους τα προβλήματά τους, μοιάζουν να έχουν προέλθει από κάποια φουτουριστική ταινία. Στην πραγματικότητα, όμως, όλα αυτά υπάρχουν ήδη. Τα προηγούμενα παραδείγματα βοηθούν στη διαμόρφωση μίας εικόνας σχετικά με τον τρόπο λειτουργίας της τεχνολογίας που βασίζεται στην επαυξημένη πραγματικότητα και το πώς αυτή η τεχνολογία έχει εισέλθει στην καθημερινότητά, προσπαθώντας να την κάνει ευκολότερη και πιο αποτελεσματική.

1 Κατά τη διάρκεια της τελευταίας του επίσκεψης στην Ελλάδα, ο Eric Schmidt, Πρόεδρος του Διοικητικού Συμβουλίου και πρώην Διευθύνων Σύμβουλος της Google, δήλωσε ότι «το καλό με την επιστημονική φαντασία είναι ότι συχνά σε προετοιμάζει για το μέλλον». Βλ. σχετικά «Οι τεχνολογικές προβλέψεις του Eric Schmidt», (2014), διαθέσιμο σε https://www.fortunegreece.com/article/technologikes-provlepsis-tou-eric-schmidt.

Έπειτα από πολλά έτη δημοσιότητας, οι τεχνολογίες εμβύθισης χρήστη[2] (immersive technologies), οι οποίες περιλαμβάνουν τις τεχνολογίες της επαυξημένης, της εικονικής και της μικτής πραγματικότητας, με τη δημοφιλία των προϊόντων τους, κυρίως των συσκευών που στηρίζονται σε αυτές, σύντομα θα εμφανιστούν σε πολλές χρήσεις στην καθημερινότητα, κάτι που εγείρει ανησυχίες κοινωνικής και οικονομικής φύσεως και οδηγεί στην ανάγκη ρύθμισής τους.

Η εικονική κι επαυξημένη πραγματικότητα επικαλύπτονται με πολλούς τρόπους, καθώς παρουσιάζουν κοινά πλεονεκτήματα και κινδύνους. Και στις δύο περιπτώσεις, προκύπτουν ανησυχίες για πρακτικά ζητήματα, καθώς η φύση τους είναι τέτοια που αποσπά την προσοχή του ατόμου. Φυσικοί τραυματισμοί κατά την απόπειρα διάβασης τοίχων, παραπάτημα σε σκάλες και περιδιάβαση σε μη ασφαλείς περιοχές είναι κοινά τόσο στην εικονική, όσο και στην επαυξημένη πραγματικότητα[3]. Κι ενώ θεωρούνται συνδεδεμένες τεχνολογίες, ταυτόχρονα αποκλίνουν σε πολλά σημεία. Η βασική διαφορά τους είναι ότι ενώ η εικονική πραγματικότητα τείνει να ενθαρρύνει το άτομο στην απομάκρυνσή του από το φυσικό του περιβάλλον, η επαυξημένη πραγματικότητα συνήθως ενθαρρύνει την αυξημένη διάδρασή του με αυτό. Για να γίνει αυτό αντιληπτό, αρκεί να έχει κάποιος στο μυαλό του την αντίθεση ανάμεσα στην εικόνα όπου ο χρήστης φορά οπτικοακουστικό σύστημα για να κυνηγήσει δαίμονες στο περιβάλλον του QuiVR[4], με αυτή όπου το άτομο βρίσκεται σε υπόγειο

2 Στις τεχνολογίες εμβύθισης ο χρήστης εμβυθίζεται ολοκληρωτικά σ' ένα τεχνητό, τρισδιάστατο κόσμο ο οποίος δημιουργείται ολοκληρωτικά από έναν υπολογιστή. Η θέαση, με σημείο αναφοράς το κεφάλι, παρέχει μια φυσική διασύνδεση για την πλοήγηση σε τρισδιάτατο χώρο και επιτρέπει να κοιτάς και να περπατάς τριγύρω, ακόμα και να πετάς μέσα από εικονικά περιβάλλοντα. Η στερεοσκοπική θέαση τονίζει την αντίληψη βάθους και την αίσθηση του χώρου. Ο εικονικός κόσμος παρουσιάζεται σε πλήρες μέγεθος και σχετίζεται αρμονικά με το ανθρώπινο μέγεθος. Δημήτριος Συνδουκάς, «Συστήματα Πολυμέσων, Ενότητα 10: Εικονική πραγματικότητα», Τμήμα Διοίκησης Επιχειρήσεων (Γρεβενά).

3 Roya Bagheri, «Virtual Reality: The Real Life Consequences», *UC Davis Business Law Journal,* Vol. 17/1 (2016): 101-120. Βλ. επίσης Samuel Mallick, «Augmenting Property Law: Applying the Right to Exclude in the Augmented Reality Universe», *Vanderbilt Journal of Entertainment and Technology Law,* Vol. 19/ 4, Vanderbilt University, School of Law (2017): 1057- 1065.

4 Πρόκειται για ένα από τα χαρακτηριστικότερα παιχνίδια εικονικής πραγματικότητας, όπου ο χρήστης έχοντας στα χέρια του τόξο και βέλη, προσπαθεί να επιβιώσει από φανταστικούς εχθρούς. Βλ. σχετικά http://outerlimitsvirtualreality.com/quivr.

σιδηρόδρομο προσπαθώντας να αιχμαλωτίσει όλα τα Pokemon, στο περιβάλλον του Pokémon Go[5].

Η εικονική πραγματικότητα βυθίζει τους χρήστες της σε εικονικά περιβάλλοντα μέσα από συγχρονισμένες οθόνες, οι οποίες έχουν ελαφρώς μεταβληθεί. Ο χρήστης βλέπει τις οθόνες μέσω ειδικών φακών και με αυτό τον τρόπο δημιουργεί ένα στερεοσκοπικό αποτέλεσμα, το οποίο προσαρμόζεται στις κινήσεις του κεφαλιού του[6]. Αυτό το αποτέλεσμα βυθίζει το χρήστη σε έναν απόλυτα ψηφιακό κόσμο, ο οποίος εξομοιώνεται με τον τρόπο με τον οποίο λειτουργεί η όραση για να δημιουργήσει βάθος. Γενικότερα, η εικονική πραγματικότητα μπορεί να προσδιοριστεί ως «ένα πραγματικό ή προσομοιωμένο περιβάλλον στο οποίο ο χρήστης απολαμβάνει την εμπειρία της τηλεπαρουσίας»[7]. Αντίστοιχα, οι οθόνες εικονικής πραγματικότητας που τοποθετούνται στο κεφάλι - VR head-mounted displays (HMDs) χρησιμοποιούνται στο να βλέπει κάποιος και διαφορετικό από το εξωτερικό περιβάλλον του.

Η επαυξημένη πραγματικότητα διαφοροποιείται από την εικονική στο ότι προσλαμβάνει την ψηφιακή πληροφορία, ανάμεσα σε άλλα ερεθίσματα και παρουσιάζει την πληροφορία αυτή στο φυσικό περιβάλλον του χρήστη σε πραγματικό χρόνο[8]. Με άλλα λόγια, η επαυξημένη πραγματικότητα συμπληρώνει το φυσικό περιβάλλον των χρηστών και δεν το αντικαθιστά ολοκληρωτικά, όπως η εικονική πραγματικότητα[9]. Στις μέρες μας οι περισσότερες συσκευές επαυξημένης ή

5 John Davison, «WTF Is 'Pokémon Go,' Explained», *Rolling Stone,* (2016), διαθέσιμο σε https://www.rollingstone.com/culture/features/wtf-is-pokemon-go-explained-20160711.

6 «How Virtual Reality Works, The Economist Explains», *(*2015), διαθέσιμο σε https://www.economist.com/the-economist-explains/2015/09/01/how-virtual-reality-works .

7 Τηλεπαρουσία είναι η αίσθηση του να βρίσκεσαι αλλού. Jonathan Steuer, «Defining Virtual Reality: Dimensions Determining Telepresence», Social Responses to Communication Technologies Paper 104, Stanford University Department of Communication, Stanford, CA (1993).

8 Jon Martindale, «What is augmented reality? Augmented reality brings VR to the real world in all sorts of exciting ways», διαθέσιμο σε https://www.digitaltrends.com/virtual-reality/what-is-augmented-reality/.

9 Ryan Calo, Tamara Denning, Batya Friedman, Tadayoshi Kohno, Lassana Magassa, Emily McReynolds, Bryce C. Newell & Jesse Woo, «Augmented Reality: A Technology and Policy Primer», (2016), διαθέσιμο σε https://digitalcommons.law.uw.edu/techlab/1.

εικονικής πραγματικότητας (HMDs) απαιτούν κάποιου είδους σύνδεση με το χρήστη, παρότι οι εφαρμογές της επαυξημένης πραγματικότητας εξακολουθούν να υπάρχουν και χωρίς τη χρήση αυτών[10].

Ο κόσμος στον οποίο ζούμε είναι δομημένος από ανισότητες: ταξικές, φύλων, φυλών, σεξουαλικού προσανατολισμού, ατόμων με αναπηρία. Οι τεχνολογίες της εικονικής[11] κι επαυξημένης πραγματικότητας[12] παρέχουν την υπόσχεση ενός τελειοποιημένου κόσμου, ο οποίος προσφέρει μεγαλύτερη διέγερση και συνδεσιμότητα και δείχνει να είναι απαλλαγμένος από ανισότητες και περιορισμούς που απαντώνται στον «πραγματικό» κόσμο. Μολαταύτα, αυτού του είδους οι τεχνολογίες για να είναι πραγματικά καινοτόμες πρέπει να μεταφέρουν τους χρήστες πέρα από τα όρια και τις προκαταλήψεις τους[13]. Όταν οι υπάρχουσες ανισότητες δεν είναι ούτε αναγνωρίσιμες ούτε απευθυντέες στον «πραγματικό» κόσμο, τείνουν να αναπαραχθούν και να επαυξηθούν στον εικονικό κόσμο. Δημιουργούνται νέοι κόσμοι βασιζόμενοι στην ταυτότητα και τις δράσεις των ατόμων, οι οποίοι, εικονικοί και πραγματικοί, είναι προϊόντα της ανθρώπινης επιλογής και της ανθρώπινης δημιουργίας. Οι δημιουργοί της εικονικής και επαυξημένης πραγματικότητας

10 John Corpuz, «Best Augmented Reality Apps», διαθέσιμο σε https://www.tomsguide.com/us/pictures-story/657-best-augmented-reality-apps.html.

11 Η τεχνολογία της εικονικής πραγματικότητας (VR) καθιστά δυνατό το να βιώνει κάποιος οποιαδήποτε εμπειρία, οπουδήποτε και ανά πάσα στιγμή. Πρόκειται για το πιο επιβλητικό είδος των τεχνολογιών πραγματικότητας και μπορεί να πείσει το ανθρώπινο μυαλό ότι βρίσκεται σε κάποια τοποθεσία, χωρίς αυτό να συμβαίνει. Συσκευές που τοποθετούνται στο κεφάλι και λειτουργούν με τη χρήση ακουστικών και τηλεχειριστηρίων παρέχουν την απόλυτη εμπειρία. Με τις πιο σημαντικές εταιρίες τεχνολογιών (όπως οι Facebook, Google και Microsoft) να επενδύουν δισεκατομμύρια δολαρίων σε αυτού του είδους την τεχνολογία, το μέλλον της εικονικής πραγματικότητας διαφαίνεται καθοριστικό για την καθημερινότητά μας. Βλ. σχετικά http://www.realitytechnologies.com/virtual-reality.

12 Η επαυξημένη πραγματικότητα (AR) μπορεί για πολλούς να μη θεωρείται τόσο συναρπαστική όσο η εικονική, αλλά η τεχνολογία αυτής αποδεικνύεται ένα πολύ χρήσιμο εργαλείο για την καθημερινότητα μας. Από τα φίλτρα των μέσων κοινωνικής δικτύωσης, έως τις χειρουργικές διαδικασίες, η επαυξημένη πραγματικότητα γίνεται ολοένα και πιο δημοφιλής, καθώς μεταφέρει στοιχεία του εικονικού κόσμου στον πραγματικό και με τον τρόπο αυτό επαυξάνει όσα βλέπουμε, ακούμε και αισθανόμαστε. Συγκρινόμενη με τις άλλες τεχνολογίες πραγματικότητας, η επαυξημένη στέκεται ανάμεσα από τον πραγματικό και τον εικονικό κόσμο. Βλ. σχετικά http://www.realitytechnologies.com/virtual-reality.

13 Mary Anne Franks, «The Desert of the Unreal: Inequality in Virtual and Augmented Reality»,*UC Davis Law Review,* Vol. 51, University of Miami Legal Studies Research Paper No. 17-24 (2017).

καλούνται να αποφασίσουν ποιες πτυχές της ιστορίας θα αναπαράγουν, θα ενισχύσουν ή θα τροποποιήσουν.

Εάν κάποιος κοιτάξει γύρω του στο χώρο εργασίας του, θα ανακαλύψει έναν απίστευτα μεγάλο όγκο ψηφιακής πληροφορίας σχετικά με το «έξυπνο» τηλέφωνό του, τον υπολογιστή του, τον εκτυπωτή του ή κάποιο έργο τέχνης, η οποία πληροφορία αφορά στο υλικό, την προέλευση, την τιμή, τις τεχνικές λεπτομέρειες και χαρακτηριστικά, τις αξιολογήσεις από τρίτους. Για τη λήψη της πληροφορίας αυτής, η οποία είναι ορατή και απευθείας αξιοποιήσιμη από το χρήστη, συνδέεται μαζί της στο φυσικό περιβάλλον. Μέχρι σήμερα η επιστήμη έχει καταφέρει η πληροφορία αυτή να είναι προσβάσιμη μέσω του υπολογιστή ή του «έξυπνου» τηλεφώνου, τα οποία έχουν το ρόλο της τρέχουσας διεπαφής ανάμεσα στην πραγματικότητα και τον ψηφιακό κόσμο. Η τεχνολογία της επαυξημένης πραγματικότητας πραγματεύεται αφενός μεν τη δυνατότητα της παρουσίασης όλης της διαθέσιμης πληροφορίας, χωρίς να είναι απαραίτητη η αναζήτησή της μέσω ενός «έξυπνου» τηλεφώνου, αφετέρου δε την όσο πιο φυσική απεικόνισή της, η οποία επιτυγχάνεται μέσω τριών διαστάσεων. Δεδομένου ότι οι υπολογιστές και τα «έξυπνα» τηλέφωνα αποτελούν δισδιάστατες διεπαφές, οι ειδικοί εργάζονται πάνω σε συστήματα με τη μορφή γυαλιών και χρησιμοποιούνται για τη μεταφορά δεδομένων[14]. Όσο πιο φυσικά και φιλικά στο χρήστη παρέχονται τα ψηφιακά δεδομένα μέσω προσαρμοσμένων διεπαφών, τόσο πιο αποτελεσματική και ασφαλής θα μπορεί να είναι η χρήση τους στο μέλλον. Σημειώνεται επίσης ότι δεν υπάρχει

14 Όταν κατασκευάζονται νέες μηχανές ή συσκευές, τα δεδομένα ή τα σχέδια θα μπορούσαν εξ αρχής να είναι τρισδιάστατα. Μέσω της εικονικής περιήγησης, οι χρήστες των έξυπνων τηλεφώνων θα μπορούσαν να πλοηγούνται απερίσπαστοι σε ιστοσελίδες κατασκευαστικών εταιριών κι εργοστασιακών εγκαταστάσεων προς αναζήτηση προϊόντων. Στο πεδίο της εκπαίδευσης, η μάθηση επιτυγχάνεται κατά 30% ταχύτερα όταν πραγματοποιείται εικονικά. Rowena Rodrigues και Anaïs Rességuier, Trilateral Research, «The underdog in the AI ethical and legal debate: human autonomy», (2019), διαθέσιμο σε https://www.ethicsdialogues.eu/2019/06/12/the-underdog-in-the-ai-ethical-and-legal-debate-human-autonomy/ .

μόνο μία νέα τεχνολογία ανά τομέα και περιβάλλον παραγωγής, αλλά πολλές και διαφορετικές τεχνολογίες[15].

Οι αντιδράσεις του κόσμου απέναντι στις νέες τεχνολογίες ποικίλουν κι εξαρτώνται από την εξοικείωση του καθένα με τις νέες εφαρμογές. Ενώ η πρώτη αντίδραση είναι ο ενθουσιασμός, όταν γίνεται προσπάθεια ενσωμάτωσης της επαυξημένης πραγματικότητας στην καθημερινή εργασία, οι χρήστες εστιάζουν κυρίως σε πρακτικά ζητήματα, όπως η χρηστικότητα της εφαρμογής ή οι οπτικές συνθήκες του περιβάλλοντος, ζητήματα τα οποία δεν έχουν ακόμα επιλυθεί αποτελεσματικά. Ο στόχος είναι να αποτυπωθεί όλη η χρήσιμη πληροφορία απευθείας στο οπτικό πεδίο του χρήστη, στο σωστό πλαίσιο. Σε αυτό το επίπεδο, οι ειδικοί της επαυξημένης πραγματικότητας προσπαθούν να δημιουργήσουν «έξυπνες» διεπαφές που να ανταποκρίνονται κατάλληλα, όπως γυαλιά ή ακουστικά μετάδοσης δεδομένων και παράλληλα να ανακαλύψουν τον τρόπο με τον οποίο η ψηφιακή πληροφορία θα παρουσιάζεται με φυσικό τρόπο, ώστε να χρησιμοποιείται στο βέλτιστο βαθμό, χωρίς οι χρήστες να αποσπώνται ή να κατακλύζονται από πρόσθετη και περιττή εικονική πληροφορία[16].

2 Εφαρμογές των τεχνολογιών εικονικής κι επαυξημένης πραγματικότητας

Το εικονικό περιβάλλον και όλων των ειδών τα εικονικά δεδομένα τυγχάνουν πολλών εφαρμογών και κατά τη διαδικασία εξέλιξής τους[17], οι τεχνολογίες της εικονικής κι

15 Στην Ευρώπη υπάρχουν χώρες που είναι πρωτοπόροι στις έρευνες στους τομείς των νέων τεχνολογιών, όπως η Γερμανία, η Αυστρία, η Γαλλία, το Ηνωμένο Βασίλειο, η Ολλανδία, η Πολωνία και η Τσεχία. Επίσης, γίνονται σημαντικές προσπάθειες και σε εταιρίες στις ΗΠΑ. Βλ. σχετικά «World Economic Forum Announces 100 New Technology Pioneers In 2020 Cohort», (2020), διαθέσιμο σε https://www.weforum.org/press/2020/06/world-economic-forum-announces-100-new-technology-pioneers-in-2020-cohort/ .

16 «Mixed reality – how real and virtual worlds are merging», (2020), διαθέσιμο σε https://job-wizards.com/en/mixed-reality-how-real-and-virtual-worlds-are-merging/ .

17 Adam Thierer, Camp, J. «Permissionless Innovation and Immersive Technology: Public Policy for Virtual and Augmented Reality», Mercatus Working Paper, Mercatus Center at George Mason

επαυξημένης πραγματικότητας τείνουν να επιφέρουν την επανάσταση σε πολλούς τομείς κι επαγγέλματα[18]. Ενδεικτικά αναφέρονται:

i. Παιχνίδια: τόσο η εικονική, όσο και η επαυξημένη πραγματικότητα μεταβάλλουν τον τρόπο με τον οποίο βιώνει ο χρήστης την εμπειρία του παιχνιδιού. Εντυπωσιακοί τίτλοι που τοποθετούν τον παίκτη εντός του παιχνιδιού απελευθερώνονται σε πλατφόρμες αποκλειστικής διανομής, όπως η Oculus Store και σε γνωστές πλατφόρμες παιχνιδιών, όπως οι Steam, PlayStation Network, Google Play και το iOS App Store. Η κυκλοφορία του Pokémon GO, τον Ιούλιο του 2016 από την εταιρία Niantic, ενός παιχνιδιού επαυξημένης πραγματικότητας στο οποίο όλοι οι χρήστες συγκέντρωναν φανταστικούς χαρακτήρες Pokémon σε δημόσιους χώρους, δημιούργησε ένα παγκόσμιο φαινόμενο[19]. Δύο εβδομάδες μετά την κυκλοφορία του, το παιχνίδι συγκέντρωσε 21 εκατομμύρια χρήστες μόνο στις ΗΠΑ και αποτέλεσε την πλέον προσοδοφόρα εφαρμογή παιχνιδιού για «έξυπνο» τηλέφωνο[20].

ii. Κινηματογράφοι και εκδηλώσεις: οι μικρού μήκους ταινίες εικονικής πραγματικότητας 360°, οι οποίες παρουσιάστηκαν στο Φεστιβάλ κινηματογράφου Sundance ανάμεσα στους μεγαλύτερους παραγωγούς του Χόλιγουντ, επίσης πειραματίζονται με το μέσο αυτό[21]. Επιπρόσθετα, η εταιρία Oculus παρουσίασε ένα «εικονικό θέατρο», το οποίο στηρίζεται στην εικονική πραγματικότητα κι επιτρέπει στους χρήστες να αγοράζουν ή να ενοικιάζουν ταινίες δύο διαστάσεων (2D) και να τις παρακολουθούν, μαζί και με άλλο

University, Arlington, VA, (2017).

18 Richard Bennett, «The Year of Augmented Reality», διαθέσιμο σε https://hightechforum.org/the-year-of-augmented-reality/. Βλ. επίσης Eric Lancheres, «Virtual Reality Is Coming and It Will Change the World in 2016», διαθέσιμο σε https://www.engadget.com/2015-11-15-virtual-reality-is-coming-and-it-will-change-the-world-in-2016.html.

19 Alex Hern, «Pokémon Go Becomes Global Craze as Game Overtakes Twitter for US Users», διαθέσιμο σε https://www.theguardian.com/technology/2016/jul/12/pokemon-go-becomes-global-phenomenon-as-number-of-us-users-overtakes-twitter.

20 Brett Swanson, «The 5G-Pokémon Moment», διαθέσιμο σε https://www.aei.org/technology-and-innovation/innovation/5g-pokemon-moment/.

21 Ashley Leiva, «How VR Experiments at Sundance Are Bringing Our Bodies into the Picture», (2016), διαθέσιμο σε https://www.wareable.com. Βλ. επίσης Richard Bennett, «Augmented Reality Drama», (2016), διαθέσιμο σε https://hightechforum.org/augmented-reality-content-and-communication.

περιεχόμενο, σε εικονικό κινηματογράφο[22]. Κάποιοι άλλοι πάροχοι επίσης πειραματίζονται με αντίστοιχα συστήματα θέασης[23], παρέχοντας τη δυνατότητα αναμετάδοσης γεγονότων σε πραγματικό χρόνο, όπως τους Ολυμπιακούς Αγώνες[24].

iii. Μουσεία: Μουσεία ανά τον κόσμο, όπως το Μητροπολιτικό Μουσείο Τέχνης στη Νέα Υόρκη (Metropolitan Museum of Art), το Μουσείο Ολοκαυτώματος και Κέντρο Εκπαίδευσης στο Ιλινόις (Holocaust Museum and Education Center) και το Μουσείο Φυσικής Ιστορίας στο Λονδίνο (Natural History Museum) έχουν υιοθετήσει τεχνολογίες εικονικής κι επαυξημένης πραγματικότητας, με στόχο να εμπλουτίσουν την εκπαιδευτική εμπειρία των επισκεπτών τους, στους οποίους παρέχεται η δυνατότητα για παράδειγμα, να θαυμάσουν φημισμένα έργα τέχνης μέσω τρισδιάστατης διαδραστικής τεχνολογίας, να συνομιλήσουν με έναν επιζώντα του ολοκαυτώματος με τη χρήση τεχνολογίας «φυσικής γλώσσας» (natural language)[25] ή ακόμα να εξερευνήσουν απολύτως αληθοφανή εικονικά περιβάλλοντα ωκεανών της

22 Erich Schwartzel, «Virtual-Reality Movies: Get Ready for the VR Revolution», (2016), διαθέσιμο σε https://www.wsj.com/articles/virtual-reality-movies-get-ready-for-the-vr-revolution-1457030357. Βλ. επίσης Michal Addady, «Oculus Teams Up with 20th Century Fox to Bring Virtual Reality to Movies», (2015), διαθέσιμο σε https://fortune.com/2015/09/27/oculus-movies-virtual-reality/.

23 Todd Spangler, «Netflix, Hulu to Launch Virtual-Reality Apps», (2015), διαθέσιμο σε https://variety.com/2015/digital/news/netflix-hulu-virtual-reality-apps-1201601645/. Βλ. επίσης «Chinese Film Director Jia Zhangke to Experiment with Virtual Reality Film—a Romance», (2016), διαθέσιμο σε https://www.scmp.com/culture/film-tv/article/1977929/chinese-film-director-jia-zhangke-experiment-virtual-reality-film.

24 Joan E. Solsman, «Juiced for Olympics in VR? Better Grab a Samsung Headset», (2016), διαθέσιμο σε https://www.cnet.com/news/juiced-about-olympics-in-virtual-reality-better-grab-a-samsung-headset/.

25 «Natural language processing» (NLP): πρόκειται για κλάδο που υπόκειται στις επιστήμες της Γλωσσολογίας, των Υπολογιστών, της Μηχανικής Πληροφοριών και της Τεχνητής Νοημοσύνης και αφορά στη διάδραση μεταξύ των υπολογιστών και των ανθρωπίνων (φυσικών) γλωσσών. Συγκεκριμένα μελετά το πώς τα προγράμματα των υπολογιστών επεξεργάζονται και αναλύουν μεγάλο όγκο δεδομένων φυσικών γλωσσών. Οι προκλήσεις που παρουσιάζονται στις φυσικές γλώσσες συχνά αφορούν την αναγνώριση ομιλίας, την κατανόηση της φυσικής γλώσσας και τη γέννηση αυτής. Βλ, σχετικά https://en.wikipedia.org/wiki/Natural_language_processing.

Καμβριανής[26] περιόδου[27]. Στην Ελλάδα, για παράδειγμα, το Ίδρυμα Μείζονος Ελληνισμού δημιούργησε ένα διαδραστικό ψηφιακό χώρο αφιερωμένο στη Ναυμαχία της Σαλαμίνας, όπου θα ζωντανεύουν τα γεγονότα μέσω της εικονικής πραγματικότητας, σε συνδυασμό με τα εκθέματα και την ιστορική αφήγηση[28].

iv. Εκπαίδευση: η εικονική πραγματικότητα έχει εισέλθει στον τομέα της εκπαίδευσης με πολλές και σημαντικές εφαρμογές. Το πρόγραμμα της Google «Expedition Pioneer» επιτρέπει στους διδάσκοντες να παρουσιάζουν φημισμένα τοπία κι ερείπια μέσω περιηγήσεων 360°, με τη χρήση του Google Cardboard[29]. Επίσης, παραγωγές ντοκιμαντέρ, έχουν φιλμογραφηθεί σε βίντεο 360°, όπως αυτή του Discovery Channel (Discovery Channel's VR app)[30]. Παράλληλα όμως, μία ολοένα αυξανόμενη μερίδα δημιουργών ταινιών, πολιτικών, ερευνητών, εργαζομένων πάνω στα ανθρώπινα δικαιώματα, ακόμα και προσώπων επιβολής του νόμου, διαβλέπουν έναν ευρύτερο κοινωνικό σκοπό στην ικανότητα του αναπτυσσόμενου μέσου να κάνει τους ανθρώπους να αισθάνονται σαν να είχαν ζήσει την εμπειρία από πρώτο χέρι[31]. Με τη χρήση των τεχνολογιών εικονικής πραγματικότητας, τα άτομα αυτά προσπαθούν να αντιληφθούν την ενσυναίσθηση των θεατών για άλλα άτομα ή ομάδες. Επίσης, στα τέλη του έτους 2016, η Κυβέρνηση Ομπάμα παρουσίασε

26 Η περίοδος η οποία ακολούθησε τον Παλαιοζωικό αιώνα και μέσω της καμβριανής έκρηξης, οδήγησε, κατά τους δαρβινιστές, στη δημιουργία πολλών νέων ζωντανών οργανισμών. Douglas Fox, «What sparked the Cambrian explosion?», (2016), διαθέσιμο σε https://www.nature.com/news/what-sparked-the-cambrian-explosion-1.19379 .

27 Ellen Gamerman, «A Look at the Museum of the Future», διαθέσιμο σε https://www.wsj.com/articles/a-look-at-the-museum-of-the-future-1444940447.

28 «Εικονική αναπαράσταση της «Ναυμαχίας της Σαλαμίνας» από το Ίδρυμα Μείζονος Ελληνισμού», διαθέσιμο σε https://www.in.gr/2020/05/21/culture/texni/eikoniki-anaparastasi-tis-naymaxias-tis-salaminas-apo-idryma-meizonos-ellinismou/.

29 Βλ. σχετικά https://www.google.com/edu/expeditions

30 Janco Roettgers, «Sharks, Survival and Surfing: Discovery Goes Virtual Reality with New Apps», (2015), διαθέσιμο σε https://finance.yahoo.com/news/sharks-survival-surfing-discovery-goes-virtual-reality-apps-172530893.html .

31 Elizabeth Dwoskin, Michael Alison Chandler και Brian Fung, «Auschwitz, Sex Assault and Police Shootings: Where Virtual Reality Is Going Next», (2016), διαθέσιμο σε https://www.washingtonpost.com/news/the-switch/wp/2016/11/11/auschwitz-sex-assault-and-police-shootings-where-virtual-reality-is-going-next/.

μία νέα εφαρμογή επαυξημένης πραγματικότητας για «έξυπνα» τηλέφωνα, η οποία επέτρεπε στους χρήστες να εστιάσουν την κάμερα πάνω σε ένα χαρτονόμισμα δολαρίου και να βιώσουν την εμπειρία της ζωής μέσα στο Λευκό Οίκο, μέσω ενός διαδραστικού τρισδιάστατου βίντεο[32].

v. Υγεία: Οι παραδοσιακές δισδιάστατες τεχνικές απεικόνισης, όπως οι αξονικές και οι μαγνητικές τομογραφίες, μετατρέπονται σε τρισδιάστατα μοντέλα. Οι ιατροί βλέπουν τα μοντέλα αυτά μέσω συστημάτων όπως το Google Cardboard, με στόχο τη διευκόλυνση επεμβάσεων σε περιστατικά που άλλοτε ήταν μη εγχειρήσιμα[33]. Στα τέλη του 2016, ένας χειρουργός στο Ηνωμένο Βασίλειο υπήρξε ο πρώτος ιατρός που χρησιμοποίησε την εφαρμογή Snap's Spectacles για να καταγράψει μία επέμβαση κήλης, με στόχο να διδάξει τη διαδικασία σε άλλους[34]. Οι ιατροί επίσης χρησιμοποιούν την εικονική πραγματικότητα για να αντιμετωπίσουν τον πόνο του άκρου – φαντάσματος[35], το σύνδρομο περιφερειακού πόνου των κατώτερων άκρων[36], τις διαταραχές από το μετατραυματικό στρες (PTSD)[37], φοβίες[38], εγκαύματα[39] και παθήσεις

32 Josh Earnest, «How to See the White House on a Dollar Bill», (2016), διαθέσιμο σε https://obamawhitehouse.archives.gov/blog/2016/11/30/how-see-white-house-dollar-bill.

33 Edgar Cervantes, «Google Cardboard Helps Doctor Save Baby's Life», (2016), διαθέσιμο σε https://www.androidauthority.com/google-cardboard-helps-doctor-save-babys-life-664885/.

34 Dalton, «Re-live the First Surgery Recorded via Snapchat Spectacles», διαθέσιμο σε https://www.engadget.com/2016-12-15-first-snapchat-spectacles-surgery.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACYAv-pIsY7UzKdSnLn1VH5U1faEAn4hxmnAQsOCg8mV7-_L2rRFzGAYv5bO8Xz-9qO5FWAs15KX8rHtU9aBHG9i9_LyP6o6vQ4rMr-kqxW7kvsrBpFsGuX3rLZjn8U59VY5UySbjLRrqVH3Q6MAsbsoIuzTrBlBtGaZluBWFSTy.

35 «Μέλος φάντασμα» ονομάζεται το μέλος που έχει ακρωτηριασθεί, μετά από τραυματισμό ή χειρουργείο και ο ασθενής το αισθάνεται, αλλά δεν το βλέπει (σαν φάντασμα). Όταν πονά, τότε ο πόνος χαρακτηρίζεται πόνος από μέλος φάντασμα. Βλ. σχετικά σε https://www.iatronet.gr/ygeia/pathologia/article/19854/o-ponos-toy-meloys-fantasma.html. Βλ. επίσης Tanya Lewis, «Virtual Reality Treatment Relieves Amputee's Phantom Pain», (2014), διαθέσιμο σε https://www.scientificamerican.com/author/tanya-lewis/.

36 Andrea Stevenson, «Two Virtual Reality Pilot Studies for the Treatment of Pediatric CRPS», *Pain Medicine,* Vol. 16/ 8, (2015): 1644–47.

37 Christina Couch, «Healing Minds with Virtual Reality», (2015), διαθέσιμο σε https://www.pbs.org/wgbh/nova/article/vr-therapy/.

38 David Cox, «Virtual Reality Can Help People Conquer Their Phobias», (2014), διαθέσιμο σε https://www.theguardian.com/science/blog/2014/oct/16/virtual-reality-phobias-public-speaking-flying.

39 «Easing Pain for Burns Victims Using Virtual Reality», (2011), διαθέσιμο σε https://www.bbc.com/news/health-12297569 .

των ματιών, όπως η αμβλυωπία ή «τεμπέλικο» μάτι (amblyopia - lazy eye)[40]. Οι ψυχίατροι κάνουν χρήση των τεχνολογιών επαυξημένης πραγματικότητας με στόχο να βοηθήσουν τα παιδιά με σύνδρομο αυτισμού να αναγνωρίσουν τα συναισθήματα και να έχουν κατάλληλες συναισθηματικές αντιδράσεις[41]. Το Νοέμβριο του 2016 εγκαινιάστηκε στο Λονδίνο το πρώτο παγκόσμιο κέντρο εικονικής ιατρικής εκπαίδευσης[42]. Γενικότερα, η αναπτυσσόμενη τεχνολογία θα μπορούσε να χρησιμοποιηθεί για την ενθάρρυνση μεγαλύτερης φυσικής άσκησης, μέσω της «παιχνιδοποίησης» δράσεων ρουτίνας ή παραδοσιακών δραστηριοτήτων. Παιχνίδια όπως το Pokémon GO ή η εφαρμογή των «έξυπνων» τηλεφώνων «Zombies, Run!» ενθαρρύνουν τους παίκτες μέσω της διεκδίκησης βραβείων, να γίνουν πιο δραστήριοι[43].

vi. Εκπαίδευση εργαζομένων και συστήματα παρακολούθησης: εικονικοί βιομηχανικοί προσομοιωτές, όπως ο ForgeFX χρησιμοποιούνται για την εκπαίδευση των εργαζομένων να αντιμετωπίζουν πολλαπλά και πολύπλοκα καθήκοντα, προτού τα αντιμετωπίσουν στην καθημερινότητά τους[44]. Επίσης, οι αγρότες έχουν τη δυνατότητα να χρησιμοποιήσουν συστήματα επαυξημένης πραγματικότητας για τη διαχείριση των καλλιεργειών τους εξ αποστάσεως[45].

vii. Μηχανική και διακόσμηση εσωτερικών χώρων: η τεχνολογία των εικονικών μοντέλων συνδυάζεται με τα αξεσουάρ εικονικής πραγματικότητας (VR

40 Diane Tsai, «This Virtual Reality Game Could Help Treat Lazy Eye», (2016). διαθέσιμο σε https://time.com/4154830/virtual-reality-lazy-eye/. Βλ. επίσης Kent Bye, «Using VR to Treat Lazy Eye with 'Vivid Vision», (2016), διαθέσιμο σε https://www.roadtovr.com/using-vr-treat-lazy-eye-vivid-vision/.

41 Nitish Kulkarni, Stanford Researchers Treat Autism with Google Glass, (2015), διαθέσιμο σε https://techcrunch.com/2015/10/19/stanford-researchers-treat-autism-with-google-glass/.

42 Kris Kolo, «Mativision Launches World's First Virtual Medical Reality Training Facility», (2016), διαθέσιμο σε https://www.thevrara.com/blog2/2016/11/3/mativision-launches-worlds-first-virtual-medical-reality-training-facility.

43 Rachel Bachman και Sarah E. Needleman, «Want to Exercise More? Try Screen Time», (2016), διαθέσιμο σε https://www.wsj.com/articles/want-to-exercise-more-try-screen-time-1481976002.

44 Eric Carson, «How Virtual Reality Gets Industrial Training Simulators Closer to Real Life than Ever Before», (2016), διαθέσιμο σε https://www.techrepublic.com/article/how-virtual-reality-gets-industrial-training-simulators-closer-to-real-life-than-ever-before.

45 Jeff Kavanaugh, «How Mixed Reality and Machine Learning Are Driving Innovation in Farming», (2016), διαθέσιμο σε https://techcrunch.com/2016/11/17/how-mixed-reality-and-machine-learning-are-driving-innovation-in-farming/.

HMDs - head-mounted display) για την κατασκευή τρισδιάστατων σχεδίων οχημάτων[46], κτηρίων[47] και προκατασκευασμένων σπιτιών κι επιχειρήσεων[48], επιτρέποντας παράλληλα στα άτομα να δουν και να περιηγηθούν, ακόμα και να αναρριχηθούν εικονικά σε 360° μέσα σε αυτές τις κατασκευές. Αυτού του είδους η τεχνολογία μπορεί να συνδράμει στη μείωση των εξόδων κατασκευής, παραγωγής και σχεδίασης[49]

viii. Αγορά ακινήτων: τα εικονικά μοντέλα μεταβάλλουν τον τρόπο με τον οποίο μελλοντικοί ιδιοκτήτες ακινήτων βλέπουν την αγορά ακινήτων. Οι αγοραστές μπορούν να επιθεωρήσουν το ακίνητο, σε περιήγηση 360° και να σχεδιάσουν εναλλακτικές, ελαχιστοποιώντας με τον τρόπο αυτό τα έξοδα μετάβασης στις ιδιοκτησίες[50]. Αντίστοιχα, οι παραθεριστές μπορούν να έχουν εικόνα του προορισμού τους σε εικονική[51] ή επαυξημένη μορφή πριν προχωρήσουν στην κράτηση της κατοικίας.

ix. Δημοσιογραφία: η εικονική πραγματικότητα μεταβάλλει τη μορφή με την οποία μπορούν να ειπωθούν οι ιστορίες στα μέσα ενημέρωσης. Οι δημοσιογράφοι εκμεταλλεύονται την τεχνολογία με στόχο τη δημιουργία επιβλητικών ιστοριών και ντοκιμαντέρ[52], με στόχο και την ψυχαγωγία. Το Μάιο του 2016, η εφημερίδα New York Times εισήγαγε το NYTVR, μία

46 Leo King, Ford, «Where Virtual Reality Is Already Manufacturing Reality», (2014), διαθέσιμο σε https://www.forbes.com/sites/leoking/2014/05/03/ford-where-virtual-reality-is-already-manufacturing-reality/#761025986e4d.

47 Sam Lubell, «VR Is Totally Changing How Architects Dream Up Buildings», (2016), διαθέσιμο σε https://www.wired.com/2016/11/vr-totally-changing-architects-dream-buildings/. Βλ. επίσης John Gaudiosi, «This Company Is Redesigning How It Works with Virtual Reality», (2015), διαθέσιμο σε https://fortune.com/2015/09/02/virtual-reality-interior-design/.

48 Sonia Schechter, «Virtual Reality for Retail: Lowe's Holoroom Rolls Out to US Retail Locations», (2015), διαθέσιμο σε https://www.marxentlabs.com.

49 Kate Murphy, «Your New Home: Ready to See Now, via Virtual Reality», (2016), διαθέσιμο σε https://www.nytimes.com/2016/05/12/style/virtual-reality-interior-design.html.

50 John Gaudiosi, «Now You Can Shop for Luxury Homes in Virtual Reality», (2015), διαθέσιμο σε https://fortune.com.

51 Robin Burks, «How Drones and Virtual Reality Will Change Tourism», (2015), διαθέσιμο σε https://www.techtimes.com/articles/57076/20150601/how-drones-and-virtual-reality-will-change-tourism.htm.

52 Angela Watercutter, «This Ebola Documentary Shows VR Film's Radical Potential», (2015), διαθέσιμο σε https://www.wired.com/2015/09/vr-ebola-film/.

εφαρμογή για τα «έξυπνα» τηλέφωνα, η οποία επιτρέπει στους χρήστες να ακούσουν ιστορίες από το στόμα βραβευμένων δημοσιογράφων, με την εμπειρία βίντεο 360°[53].

x. Οδήγηση: οι εφαρμογές επαυξημένης πραγματικότητας πάνω στο παρμπρίζ του αυτοκινήτου έχουν αρχίσει να κυριαρχούν στα αυτοκίνητα της νέας γενιάς[54]. Αυτές οι εφαρμογές παρέχουν στους οδηγούς πρόσθετες πληροφορίες σχετικά με την ταχύτητα, την κατεύθυνση, τις στροφές και τις προειδοποιητικές πινακίδες, όπως επίσης και δίνουν τη δυνατότητα για προσωπική επικοινωνία με τηλεφωνικές κλήσεις ή γραπτά μηνύματα[55].

xi. Διαφήμιση: η εικονική πραγματικότητα έρχεται να ενεργοποιήσει νέες διαφημιστικές πλατφόρμες, όπως η Immersv, οι οποίες στοχεύουν να εμπνεύσουν τους κατασκευαστές παιχνιδιών και τους σχεδιαστές των εφαρμογών, παρέχοντάς τους ευκαιρίες να αυξήσουν το εισόδημά τους. Η κεντρική ιδέα είναι να πείσουν τις διαφημιστικές εταιρίες να εισάγουν διαφημιστικά βίντεο με εικονικές εμπειρίες[56].

xii. NASA: χρησιμοποιεί την τεχνολογία της εικονικής πραγματικότητας από το 1990, αλλά από τότε που εμφανίστηκαν νεώτερα και πιο ισχυρά συστήματα, των οποίων το κόστος είναι απειροελάχιστο σε σχέση με τα ήδη υπάρχοντα, αυξάνεται ολοένα και περισσότερο η πιθανότητα για την παροχή της εκπαίδευσης της διαστημικής αεροναυτικής με τις τεχνολογίες αυτές[57].

---

53 Βλ. σχετικά http://www.nytimes.com/marketing/nytvr. Βλ. επίσης Erin Griffith, «Can Virtual Reality Save Journalism?», (2015), διαθέσιμο σε https://fortune.com/2016/05/02/virtual-reality-nyt-newfronts/.

54 Ronan Glon, «Distracted behind the Wheel? Try One of These Aftermarket Heads-Up Displays», (2017), διαθέσιμο σε https://finance.yahoo.com/news/distracted-behind-wheel-try-one-161533448.html.

55 Cuong Tran, Karlin Bark και Victor Ng-Thow-Hing, «A Left-Turn Driving Aid Using Projected Oncoming Vehicle Paths with Augmented Reality», in *Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications,* New York, Association for Computed Machinery (2015): 300–307.

56 Jeff Grubb, «Immersv Enables Virtual Reality Developers to Advertise Their Games in Other VR Apps», (2016), διαθέσιμο σε https://venturebeat.com/2016/03/10/immersv-enables-virtual-reality-developers-to-advertise-their-games-in-other-vr-apps/.

57 Erin Carson, «NASA Shows the World Its 20-Year Virtual Reality Experiment to Train Astronauts: The Inside Story», (2016), διαθέσιμο σε https://www.techrepublic.com/article/nasa-shows-the-world-its-20-year-vr-experiment-to-train-astronauts/.

xiii. Στρατός: ο αμερικανικός στρατός χρησιμοποιεί ήδη από τη δεκαετία του 1990 έως και σήμερα την τεχνολογία της εικονικής πραγματικότητας, μέσω των προσομοιώσεων μάχης, της ιατρική εκπαίδευσης, των προσομοιωτών πτήσεων και οχημάτων, ακόμα και των εκστρατειών στρατολόγησης[58]. Επιπλέον, το Αμερικανικό Γραφείο Θαλασσίων Ερευνών δημιούργησε ένα νέο πρόγραμμα εικονικής πραγματικότητας με την ονομασία «Bravemind», το οποίο ασχολείται αποκλειστικά με θεραπευτικές τεχνικές που έχουν ως στόχο τη μείωση των συμπτωμάτων του Συνδρόμου Μετατραυματικού Στρες (PTSD)[59].

Παρά τις ανωτέρω εφαρμογές των νέων τεχνολογιών, υπάρχουν κάποιοι σκεπτικιστές, οι οποίοι αμφιβάλλουν σχετικά με την ευρεία διάδοσή τους[60]. Ωστόσο και στο παρελθόν υπήρξαν τέτοιου είδους αμφιβολίες, για παλαιότερες τεχνολογίες. Όπως αναφέρει ο Jason Brush, αντιπρόεδρος της εταιρίας «Possible»[61]: κάθε νέο τεχνολογικό μέσο που διεισδύει στη ζωή μας έχει τουλάχιστον μία φορά χαρακτηριστεί, στην καλύτερη περίπτωση, ανεφάρμοστο. Καθένα από αυτά καθιερώθηκε τελικά με επιτυχία χάρη σε αφοσιωμένους δικηγόρους και οπαδούς, οι οποίοι πάλεψαν για να αποδείξουν την αξία αυτού που οι άλλοι θεωρούσαν ανόητο[62].

3 Κοινωνικός εγκλιματισμός στις νέες τεχνολογίες

Ο αέναος πειραματισμός της κοινωνίας, ο οποίος είναι κατά περίπτωση ανεκτός, θα έχει σημαντικές προεκτάσεις για τις τεχνολογίες της εικονικής και της επαυξημένης πραγματικότητας. Ακόμη και αν χρειαστεί ικανό διάστημα προσαρμογής σε αυτές,

58 «Virtual Reality in the Military», (2016), διαθέσιμο σε https://www.vrs.org.uk/virtual-reality-military/.

59 Οι τεχνικές αυτές εφαρμόστηκαν σε είκοσι άτομα του στρατιωτικού προσωπικού με μέσο όρο υπηρεσίας τα οκτώ έτη. Βλ. σχετικά Tanya Lewis, «Virtual-Reality Tech Helps Treat PTSD in Soldiers», (2014), διαθέσιμο σε https://www.livescience.com/47258-virtual-reality-ptsd-treatment.html

60 «Why VR/AR May NOT Be the Next Big Thing», (2016), διαθέσιμο σε https://www.arovia.com/.

61 Πρόκειται για μία εταιρία με ψηφιακές εφαρμογές που ασχολείται με τα επιστημονικά πεδία της δημιουργίας της τεχνολογίας, της στρατηγικής και των δεδομένων, με στόχο τη δημιουργία εμπειριών διάδρασης. Βλ. σχετικά σε https://www.possible.com

62 Jason Brush, «Why Virtual Reality Matters», (2016), διαθέσιμο σε https://www.vox.com/2016/6/28/12046730/virtual-reality-vr-creative-content-industry-investment.

τόσο για τα άτομα, όσο και για τις ομάδες, οι κοινωνικές νόρμες[63] τελικά προσαρμόζονται με το χρόνο. Κατ' επέκταση, πολλές από τις ανησυχίες σχετικά με την κακή χρήση των τεχνολογιών αυτών μπορεί να μην υλοποιηθούν, καθώς οι συμπεριφορές μεταβάλλονται με την υιοθέτηση και αφομοίωση νέων εργαλείων και υπηρεσιών στην καθημερινότητά μας[64]. Η κοινωνική πίεση και οι προσωπικοί κανόνες αποδεκτής χρήσης και δεοντολογίας συχνά δρουν ως ρυθμιστικές αρχές της ορθής ή της κακής χρήσης των νέων τεχνολογιών, «διότι οι κανόνες αποτρέπουν πολλές πρακτικές, οι οποίες είναι εφικτές, αλλά ανεπιθύμητες»[65]. Όπως έχει δείξει η ιστορία, η θεωρία αυτή αποδεικνύεται σωστή ως προς τις ανησυχίες που προκύπτουν για θέματα προστασίας της ιδιωτικής ζωής. Για παράδειγμα, στα τέλη του 1800, η εμφάνιση της φωτογραφικής μηχανής προκάλεσε ποικιλία αντιδράσεων σχετικά με την προστασία της ιδιωτικής ζωής. Σε γνωστό νομικό περιοδικό της εποχής οι Samuel Warren και Louis Brandeis δημοσίευσαν άρθρο σχετικό με τη φωτογραφική μηχανή και την προστασία της ιδιωτικής ζωής, στο οποίο ισχυρίστηκαν ότι οι στιγμιαίες φωτογραφίες και η επιχειρήσεις των εφημερίδων εισέβαλαν στον ιερό χώρο της ιδιωτικής και οικογενειακής ζωής και ότι ο μεγάλος αριθμός μηχανικών συσκευών απειλεί να υλοποιήσει την πρόβλεψη ότι «ό,τι ψιθυρίζεται στη ντουλάπα θα εμφανιστεί από την καμινάδα»[66]. Η ανταπόκριση του κοινού, όμως, στη φωτογραφική μηχανή, αποδείχθηκε αρκετά διαφορετική. Πολλοί αγόρασαν τις δικές τους συσκευές, οι οποίες μετατράπηκαν στα σύγχρονα εργαλεία που χρησιμοποιούμε σήμερα. Την ίδια στιγμή, οι κοινωνικοί κανόνες και η δεοντολογία αποθάρρυναν την

63 Πρόκειται για τη συμπεριφορά που κρίνεται κατάλληλη στο πλαίσιο μίας κοινωνικής ομάδας. «Η προκατάληψη και οι διακρίσεις μέσα από την κοινωνική ψυχολογία», (2016), διαθέσιμο σε https://socialpolicy.gr/2016

64 Adam Thierer, «Muddling Through: How We Learn to Cope with Technological Change», (2014), διαθέσιμο σε https://techliberation.com.

65 Daniel Castro και Alan McQuinn, «The Privacy Panic Cycle: A Guide to Public Fears about New Technologies», Information Technology and Innovation Foundation, Washington, DC (2015). Βλ. επίσης Cass R. Sunstein, Social Norms and Social Roles *Columbia Law Review* 96 (1996): 903–968 και Cristina Bicchieri, «The Grammar of Society: The Nature and Dynamics of Social Norms», Cambridge, UK, Cambridge University Press (2006).

66 Samuel D. Warren και Louis D. Brandeis, «The Right to Privacy», *Harvard Law Review* 4 (1890): 193–220, 195.

αθέμιτη χρήση της φωτογραφικής μηχανής σε δημόσιους χώρους. Αυτό δεν σημαίνει ότι δεν προέκυψαν κάποια από τα προβλήματα που επεσήμαναν οι Warren και Brandeis – απεναντίας, πολλοί άνθρωποι εξακολουθούν να κάνουν χρήση της φωτογραφικής μηχανής με ανεπίτρεπτο κοινωνικά και νομικά, τρόπο και κρίνεται αναγκαίο να επιβληθούν κυρώσεις για την παραβίαση της ιδιωτικής ζωής με νομοθετικές διατάξεις.

Περαιτέρω, και η ίδια η νομοθεσία εξελίχθηκε, σε απάντηση των ανησυχιών που εξέφρασαν οι Warren and Brandeis. Στο αμερικανικό δίκαιο, οι διατάξεις περί αδικοπραξιών που σχετίζονται με την παραβίαση της ιδιωτικής ζωής, συμπεριλαμβανομένων των σχετικών με τη δημοσιοποίηση ιδιωτικών γεγονότων, μπορούν να εφαρμοστούν και στις περιπτώσεις παράνομης χρήσης της τεχνολογίας της φωτογραφίας, ενώ στο ευρωπαϊκό δίκαιο προκρίνονται οι διατάξεις οι σχετικές με την προστασία της προσωπικότητας.

Το σημαντικότερο σχετικά με την ιστορία της κάμερας και της φωτογραφίας σε δημόσιο χώρο είναι ότι οι νόμοι και οι κανόνες μπόρεσαν να αντιμετωπίσουν τα προβλήματα εν τη γενέσει τους. Στο παρελθόν, οι περιορισμοί δεν θα επιβάλλονταν στη χρήση της φωτογραφικής μηχανής με βάση το υποθετικό σενάριο κακής χρήσης της. Αντιθέτως, υπήρχε η προσέγγιση του «βλέποντας και κάνοντας», αφήνοντας το χρόνο για τη διαμόρφωση της νομικής παρέμβασης, όταν αυτό απαιτούνταν. Το σημαντικό είναι ότι αυτοί οι νομικοί κανόνες αντανακλούσαν την εξέλιξη των κοινωνικών κανόνων σχετικά με την ευρεία χρήση της κάμερας. Κατ΄ επέκταση, όπως και στο παρελθόν, έτσι και σήμερα, οι κοινωνικοί κανόνες[67] που συνδέονται με τις δυνατότητες της εικονικής και της επαυξημένης πραγματικότητας (συμπεριλαμβανομένης και της χρήσης της αναγνώρισης προσώπου ή άλλων δυνατοτήτων βιομετρικής αναγνώρισης, όπως η μοναδική χροιά της φωνής ή η κίνηση των ματιών) θα προσαρμόζονται με το χρόνο, όσο οι άνθρωποι εξοικειώνονται μαζί τους και θα προκύπτουν νέοι κοινωνικά αποδεκτοί κανόνες

67 Στάμος Παπαστάμου, Γεράσιμος Προδρομίτης, Βασίλης Γ. Παυλόπουλος, «Κοινωνική Σκέψη, Νόηση και Συμπεριφορά. 29 Έλληνες Κοινωνικοί Ψυχολόγοι ανα-κρίνουν την επιστήμη τους», Πεδίο, (2010).

χρήσης. Η καθιέρωση της εικονικής και της επαυξημένης πραγματικότητας θα εξαρτηθεί από την απήχησή τους στο ευρύ κοινό. Κάποιοι ισχυρίζονται ότι τα γυαλιά της Google δεν έγιναν δημοφιλή, διότι η συσκευή έμοιαζε εκτός μόδας και επέμεναν στον εκσυγχρονισμό της για την αύξηση της δημοφιλίας της[68].

4 Εικονική πραγματικότητα

Ο όρος εικονική πραγματικότητα αναφέρεται σε ένα επιβλητικό τρισδιάστατο περιβάλλον που έχει δημιουργηθεί από κάποιον υπολογιστή[69]. Σε ένα εικονικό περιβάλλον οι κινήσεις του χρήστη παρακολουθούνται και το περιβάλλον που του έχει δοθεί ή έχει δημιουργηθεί ψηφιακά, εμφανίζεται στις αισθήσεις του σε συμφωνία με τις κινήσεις του[70]. Οι συσκευές της εικονικής πραγματικότητας μεταφέρουν τους χρήστες σε ένα φανταστικό ή πραγματικό περιβάλλον, το οποίο είναι απομακρυσμένο από το χρήστη, παράγοντας ρεαλιστικούς ήχους. Στα απτικά συστήματα της εικονικής πραγματικότητας όσοι ελέγχουν τα παιχνίδια ή άλλες συσκευές, επίσης μεταδίδουν απτικές αισθήσεις στους χρήστες.

Ο βασικός στόχος της τεχνολογίας της εικονικής πραγματικότητας είναι επιτυχία της «παρουσίας», «η αίσθηση της παρουσίας»[71]. Η «πραγματικότητα» της εικονικής πραγματικότητας είναι σημαντική όχι μόνο για τη ψυχαγωγική αξία των παιχνιδιών και την αληθοφάνεια των εκπαιδευτικών προγραμμάτων, αλλά και για τις εφαρμογές που σχετίζονται με τη διαχείριση του πόνου[72], την ενσυναίσθηση[73] και την

68 «Θα χρειαστεί χρόνος μέχρι η μορφή τους να τύχει επεξεργασίας, να φαίνονται μέσα στη μόδα και να είναι άνετα». Kevin Kelly, *The Inevitable*: *Understanding the 12 Technological Forces That Will Shape* our future, Penguin Books, N.Y. (2016).

69 Crystal Nwaneri, «Ready Lawyer One: Legal Issues in the Innovation of Virtual Reality», *Harvard Journal of Law & Technology,* Vol. 30/ 2, (2017): 601-627.

70 J. Fox, D. Arena και J.N. Bailenson, «Virtual Reality: A survival guide for the social scientist», *Journal of Media Psychology,* Vol. 21/ 3 (2009): 95-113.

71 James J. Cummings και Jeremy N. Bailenson, «How Immersive Is Enough? A Meta-Analysis of the Effect of Immersive Technology on User Presence», *Media Psychology,* Vol. 19/ 2 (2015): 272 - 309.

72 Angela Li, Zorash Montaño, Vincent J Chen και Jeffrey I Gold, «Virtual reality and pain management: current trends and future directions», (2011), διαθέσιμο σε https://pubmed.ncbi.nlm.nih.gov/21779307/ .

73 Özgür Gürerk και Alina Kasulke, «Does Virtual Reality Increase Charitable Giving? An Experimental Study», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072002 .

εκπαίδευση[74]. Παρόλα αυτά, υπάρχει ένα πιθανό μειονέκτημα σε αυτή την αίσθηση της συνεχούς παρουσίας. Οι ειδικοί ισχυρίζονται ότι οι τελευταίες εξελίξεις στην εικονική πραγματικότητα έχουν γίνει τόσο επιβλητικές που συχνά οι συμμετέχοντες συγχέουν τον εικονικό με τον αληθινό κόσμο[75]. Παρότι δεν είναι ακόμα γνωστοί οι ακριβείς λόγοι για τους οποίους η εικονική πραγματικότητα έχει τέτοιο αντίκτυπο στον τρόπο με τον οποίο αντιλαμβάνονται οι άνθρωποι την πραγματικότητα, οι ειδικοί υποθέτουν ότι το ανθρώπινο μυαλό εξαπατάται αποτελεσματικά, με το να θεωρεί ότι τα συμβάντα της εικονικής πραγματικότητας συμβαίνουν πραγματικά. Σύμφωνα με το Διευθύνοντα Σύμβουλο της εταιρίας Deep Stream VR, «το ανθρώπινο μυαλό κωδικοποιεί την εικονική πραγματικότητα ως ένα μέρος στο οποίο έχουμε βρεθεί και όχι ως κάτι που έχουμε δει»[76]. Σύμφωνα με τους ερευνητές της εικονικής πραγματικότητας «τα οφέλη της εκπαίδευσης μέσω της εικονικής πραγματικότητας δεν είναι άνευ κόστους: η ευκολία της δημιουργίας ζωντανών νοερών εικόνων μπορεί να προκαλέσει στη συνέχεια σύγχυση σχετικά με το εάν μία νοερή εικόνα που έχουμε ανακτήσει, την είχαμε αντιληφθεί ή φανταστεί, κάτι που στη συνέχεια προκαλεί και νέες λανθασμένες αναμνήσεις»[77].

Η τεχνολογία της εικονικής πραγματικότητας ενέχει τόσο σοβαρούς κινδύνους, όσο και ευκαιρίες για την εφαρμογή του δικαίου προστασίας της ιδιωτικής ζωής κι εποπτείας στον κυβερνοχώρο[78]. Στις ελεύθερες δημοκρατίες η κυβερνητική εποπτεία πηγάζει από την ανάγκη για δημόσια ασφάλεια κι ελέγχεται από το ατομικό δικαίωμα προστασίας της ιδιωτικής ζωής. Τα τελευταία χρόνια, δυστυχώς, η ισορροπία αυτή έχει αρχίσει να φθίνει, ως αποτέλεσμα της αύξησης των εθνικών και παγκόσμιων

74 Dylan Kreis, Daniel Magorrian και Gavin Moore, «Current and Future Virtual Reality Applications and the Application of User Experience Design Principles», (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3173934 .

75 Daniel Joseph Finnegan, «How to solve virtual reality's human perception problem», διαθέσιμο σε http://theconversation.com/how-to-solve-virtual-realitys-human-perception-problem-92128.

76 Mary Anne Franks, «The Desert of the Unreal: Inequality in Virtual and Augmented Reality», *UC Davis Law Review*, Vol. 51, University of Miami Legal Studies Research Paper No. 17-24 (2017).

77 Ann E. Schlosser, «Learning Through Virtual Product Experience: The Role of Imagery on True Versus False Memories», *Journal of Consumer Research*, Vol. 33/ 3, (2006): 377–383.

78 Gilad Yadin, «Virtual Reality Intrusion», *Willamette Law Review,* Vol. 53/ 1 (2016).

αναταραχών, της εξέλιξης των ικανοτήτων εποπτείας και τη διάβρωση της προστασίας της ιδιωτικής ζωής. Η ελευθερία έκφρασης στις ΗΠΑ[79] προστατεύει τους πολίτες από τα «κυβερνητικά αυτιά και μάτια» κατά την ιδιωτική τους ζωή εντός της οικίας τους ή κατά την εργασία τους, αλλά η προστασία αυτή φθίνει με την είσοδό τους στο Διαδίκτυο. Σε αντίθεση με άλλα είδη τεχνολογιών, η εικονική πραγματικότητα έχει δημιουργηθεί για να παρουσιάσει ένα ψυχολογικό αποτέλεσμα πιστευτό και όμοιο με το φυσικό κόσμο. Οι πολλαπλές έρευνες καταδεικνύουν ότι ο εικονικός κόσμος παράγει στους χρήστες νομικές προσδοκίες αντίστοιχες με αυτές του πραγματικού κόσμου και αντανακλά τις ανθρώπινες κοινωνικές αξίες. Τα άτομα στην πραγματικότητα εξισώνουν τις παραβάσεις της προστασίας της ιδιωτικής ζωής εντός της εικονικής πραγματικότητας, με τις παραβιάσεις της ιδιωτικής ζωής στο φυσικό κόσμο, εισάγοντας τις αξίες και τις προσδοκίες τους στο προσομοιωμένο περιβάλλον, ειδικότερα σε σχέση με την ιδιωτικότητα της πληροφορίας που διαμοιράζεται μέσα στο εικονικό περιβάλλον. Κατ' επέκταση η συνταγματική προστασία της ιδιωτικής ζωής του φυσικού κόσμου μπορεί δικαιολογημένα να επεκταθεί και στο εικονικό περιβάλλον[80] και στο πλαίσιο της τριτενέργειας[81].

79 Αντίστοιχες προβλέψεις υπάρχουν και σε άλλα νομοθετήματα, όπως για παράδειγμα το άρθρο 10 της Ευρωπαϊκής Σύμβασης των Ανθρωπίνων Δικαιωμάτων: «Παν πρόσωπον έχει δικαίωμα εις την ελευθερίαν εκφράσεως. Το δικαίωμα τούτο περιλαμβάνει την ελευθερίαν γνώμης ως και την ελευθερίαν λήψεως ή μεταδόσεως πληροφοριών ή ιδεών, άνευ επεμβάσεως δημοσίων αρχών και ασχέτως συνόρων». Στην Ελλάδα η ελευθερία του λόγου και του τύπου απαντάται στο άρθρο 14 του Συντάγματος: «Καθένας μπορεί να εκφράζει και να διαδίδει προφορικά, γραπτά και δια του τύπου τους στοχασμούς του, τηρώντας του νόμους του Κράτους», το οποίο αποτελεί εξειδίκευση του θεμελιώδους δικαιώματος του άρθρου 5, παρ. 1 του Συντάγματος περί ελεύθερης ανάπτυξης της προσωπικότητας και συμμετοχής στην κοινωνική, οικονομική και πολιτική της χώρας.

80 Βλ. σχετικά Georgios N. Yannopoulos, «Real Rights in Virtual Worlds and Virtual Rights in a Real World», στο Συνέδριο: 5th International Conference on Information Law “Equity, integrity and beauty in information law and ethics”, Ιόνιο Πανεπιστήμιο, Κέρκυρα, (2012) και Πελοπίδας Δόνος, Φίλιππος Βασιλόγιαννης, Τάκης Βιδάλης, Βασίλης Βουτσάκης, Ηλίας Καστανάς, Γιάννης Κτιστάκις, Ευάγγελος Κ. Μάλλιος, Χαράλαμπος Σαββάκης, Ανδρέας Τάκης, Κωνσταντίνος Τσιτσελίκης και Δημήτρης Χριστόπουλος, «Νέες τεχνολογίες και συνταγματικά δικαιώματα», Σάκκουλας, 2004.

81 «Τα ατομικά δικαιώματα ενεργούν [και] οριζόντια, αντιμετωπίζοντας τις ανθρώπινες σχέσεις πάνω στη γραμμή των βασικών αρχών του πολιτεύματος, της ελευθερίας και της ισότητας και κατευθύνονται στην προστασία του ανθρώπου τόσο από την δημόσια όσο και από την ιδιωτική εξουσίαση. «Τριτενέργεια» λέγεται η χρησιμοποίησή τους προς τη δεύτερη κατεύθυνση, δηλαδή για αποτροπή κινδύνων από την ανισορροπία των ιδιωτικών δυνατοτήτων μεταξύ των ατόμων, όπου υπάρχει τέτοια και όταν ο «απλός» νομοθέτης ή ο δικαστής του Ιδιωτικού Δικαίου δεν την έχει αποκαταστήσει». Βλ. σχετικά Αντώνης Μανιτάκης, «Η επίδραση του Συντάγματος στις ιδιωτικές έννομες σχέσεις», *Χαριστήρια Ι. Δεληγιάννη*, Επιστημονική Επετηρίδα Τμήματος Νομικής, Θεσσαλονίκη, (1992): 247-284.

Οι ειδικοί θεωρούν ότι η τεχνολογία της εικονικής πραγματικότητας θα εξελίξει τον κυβερνοχώρο με μία σταδιακή μετατόπιση από τις διεπαφές (interfaces) των δύο διαστάσεων, στο εικονικό περιβάλλον[82]. Αυτή η εξέλιξη θα δημιουργήσει σταδιακά έναν κυβερνοχώρο εικονικής πραγματικότητας, όπου θα είναι αναμενόμενη και δικαιολογημένη η ουσιαστική φυσική πρόσβαση και κατ' επέκταση θα μεταβάλει εφεξής τον τρόπο με τον οποίο ο νόμος αντιλαμβάνεται την εποπτεία του κυβερνοχώρου, αποκαθιστώντας την ισορροπία ανάμεσα στην ανάγκη για ασφάλεια κι επιβολή και την αξία της ιδιωτικής ζωής.

4.1 Εικονικοί Κόσμοι: έννοια

Ένας εικονικός κόσμος αποτελεί ένα ταυτόχρονο, διαρκές δίκτυο προσώπων, τα οποία_αναπαριστώνται από εικονικούς χαρακτήρες (avatars) και το οποίο καλύπτεται από δίκτυο υπολογιστών.

I. Ταυτόχρονο δίκτυο: πρόκειται για διαμοιρασμένες δραστηριότητες, οι οποίες απαιτούν ταυτόχρονη επικοινωνία[83]. Η έννοια του «κοινού χρόνου» προσφέρει την ευκαιρία για ομαδικές και συντονισμένες κοινωνικές δραστηριότητες. Οι εικονικοί κόσμοι επίσης προσφέρουν το χώρο, την απόσταση και τη συνύπαρξη με άλλους συμμετέχοντες, οι οποίοι βρίσκονται σε χώρους της πραγματικότητας, δίνοντάς τους την αίσθηση του περιβάλλοντος[84].

82 Gilad Yadin, «Virtual Reality Surveillance», *Cardozo Arts & Entertainment Law Journal,* Vol. 35/. 3, (2017).

83 «Ένα εικονικό διάστημα, το οποίο δεν στηρίζεται σε πραγματικό χρόνο, μοιάζει περισσότερο με ηλεκτρονική επικοινωνία που καθυστέρησε, παρά με εικονικό κόσμο». Βλ. σχετικά https://www.igi-global.com/dictionary/virtual-space/31800 .

84 Οι έννοιες του «κοντά» και του «μακριά» είναι δύσκολο να έχουν εφαρμογή σε ένα στατικό περιβάλλον ιστότοπου, αλλά όχι και σε ένα εικονικό περιβάλλον. Η μεγαλύτερη διαφορά μεταξύ αυτών είναι ότι οι σελίδες ενός ιστότοπου, ακόμη και όταν διαμοιράζονται, δεν αποτελούν ένα περιβάλλον περιήγησης, αλλά ένα στατικό περιτοιχισμένο χώρο. Από την άλλη πλευρά, οι εικονικοί κόσμοι, ανεξάρτητα από το επίπεδο, προσφέρουν στους συμμετέχοντες την αίσθηση της γεωγραφίας και του εδάφους. Carina Girvan, «What is a virtual world? Definition and classification», *Educational Technology Research and Development,* Vol. 66, (2018):1087–1100.

II. Διαρκές δίκτυο: ένας εικονικός κόσμος δεν μπορεί να παύσει (pause). Συνεχίζει να υπάρχει και να λειτουργεί ακόμη και μετά την αποχώρηση του συμμετέχοντος[85].

III. Δίκτυο προσώπων: τα πρόσωπα είναι κεντρικά στοιχεία του εικονικού κόσμου. Οι συμμετέχοντες επικοινωνούν και αλληλεπιδρούν μεταξύ τους και με το περιβάλλον[86].

IV. Αναπαράσταση με εικονικούς χαρακτήρες (avatars[87]): Οι ρόλοι του εικονικού χαρακτήρα και του εκπροσώπου του αναπαριστώνται ανάλογα με το πώς εμφανίζονται οι δράσεις τους σε άλλους. Οι εικονικοί χαρακτήρες λειτουργούν σαν μαριονέτες ελεγχόμενες από το χρήστη. Οι χρήστες παραγγέλλουν τις ενέργειες του εικονικού τους χαρακτήρα, αλλά ο ίδιος ο εικονικός χαρακτήρας είναι αυτός που τις πραγματοποιεί. Ακόμη και μορφές επικοινωνίας που προέρχονται απευθείας από το χρήστη, όπως η φωνητική συνομιλία (voice chat), παρουσιάζονται ως ενέργειες που έγιναν από τον εικονικό χαρακτήρα.

V. Κάλυψη από δίκτυο υπολογιστών: χωρίς δίκτυο υπολογιστών, ο εικονικός κόσμος θα μπορούσε να περιγραφεί ως ένα περιβάλλον το οποίο είναι παρόμοιο με το εικονικό[88]. Κανένα παιχνίδι δημιουργημένο με μολύβι και

85 Αυτό που διακρίνει τους εικονικούς κόσμους από τα βιντεοπαιχνίδια είναι η διάρκεια, η οποία μεταβάλλει τον τρόπο που οι άνθρωποι αλληλεπιδρούν με άλλους συμμετέχοντες και με το ίδιο το περιβάλλον. Ο συμμετέχων δεν είναι πλέον το κέντρο του κόσμου, αλλά ένα μέλος μίας δυναμικής κοινότητας και μίας εξελισσόμενης οικονομίας. Αντιλαμβάνεται ότι τα συστήματα υπάρχουν στο χώρο (περιβάλλον, οικολογία, οικονομία) ανεξάρτητα από την παρουσία του ή όχι. «What makes a virtual world more than a game?», (2019), διαθέσιμο σε https://decentraland.org/blog/technology/virtual-worlds/ .

86 Πρόκειται για ένα οικοσύστημα μέσα στο οποίο οι πράξεις ενός συμμετέχοντος επηρεάζουν κάθε άλλο τμήμα του συστήματος. Οι συμμετέχοντες μπορούν να διαμορφώσουν κοινωνικές ομάδες, μικρής ή μακράς διάρκειας, αλλά δεν είναι αναγκαίο να είναι ενεργά μέλη αυτού του οικοσυστήματος. Ένας χρήστης μπορεί να εισέλθει στο περιβάλλον ενός εικονικού κόσμου και να μην έρθει σε επαφή με άλλο χρήστη, αλλά συνεχίζει να αλληλεπιδρά με το περιβάλλον. Marc W. Bell, «Toward a Definition of Virtual Worlds», *Journal of Virtual Worlds Research,* Vol. 1 /1 (2008).

87 Ένα άβαταρ (avatar) είναι κάθε εικονική απεικόνιση (γραφική ή λεκτική), πέρα από ένα απλό έμβλημα ή όνομα, η οποία έχει αυτονομία (τη δυνατότητα να ενεργεί αυτοτελώς) και η οποία ελέγχεται από έναν ανθρώπινο εκπρόσωπο σε πραγματικό χρόνο. Βλ. σχετικά https://techterms.com/definition/avatar .

88 Ένα καλά διαχειριζόμενο βιντεοπαιχνίδι θα μπορούσε να περιλαμβάνει τις έννοιες του ταυτόχρονου, συνεχούς δικτύου ανθρώπων που αναπαριστώνται με εικονικούς χαρακτήρες, αλλά η διαφορά αυτού με έναν εικονικό κόσμο είναι ο τρόπος με τον οποίο τα δεδομένα και η επικοινωνία διευκολύνονται μέσω του δικτύου των υπολογιστών. «What makes a virtual world more than a game?», (2019), διαθέσιμο σε https://decentraland.org/blog/technology/virtual-worlds/ .

χαρτί δεν θα κατόρθωνε τη διαχείριση δεδομένων με όλα τα αντικείμενα, τα περιβάλλοντα, τις αλληλεπιδράσεις και τις συναλλαγές, συσσωρεύοντάς τα επ' αόριστον, όπως καθίσταται δυνατό μέσω ενός δικτύου υπολογιστών. Επίσης, ο υπολογιστής διατηρεί τα ίχνη από όλες τις συζητήσεις, τις κοινωνικές διασυνδέσεις και τα δίκτυα των προσώπων, επιτρέποντάς τους στιγμιαία επικοινωνία πέρα από εθνικά και γεωγραφικά σύνορα [89].

4.2 **Ιδιομορφίες και νομικοί προβληματισμοί επί των εικονικών κόσμων**

Οι εικονικοί κόσμοι συνδυάζουν περίπου κάθε πτυχή του σύγχρονου και δημοφιλούς πολιτισμού. Εν μέρει βιντεοπαιχνίδια, εν μέρει χώροι συζητήσεων (chat rooms), εν μέρει ιστοσελίδες δημοπρασιών, εν μέρει δίκτυα κοινωνικής δικτύωσης, έχουν την ικανότητα να καλύπτουν ένα μεγάλο εύρος των αναγκών των χρηστών. Παρόλο που τα θέματα και το περιβάλλον τους ποικίλουν, κάθε κόσμος χαρακτηρίζεται από ένα μεγάλο αριθμό χρηστών που κατοικούν σε αυτόν, όπως κατοικούν και στον αληθινό κόσμο[90]. Πρόκειται για τα avatars, «τους εκπροσώπους» των χρηστών του αληθινού κόσμου, οι οποίοι καταβάλλουν ένα ποσό μηνιαίως για αυτή τους τη διπλή αποίκιση. Ίσως η πιο σημαντική διαφορά ανάμεσα στους εικονικούς κόσμους και τα παραδοσιακά βιντεοπαιχνίδια είναι ότι «οι εικονικοί κόσμοι είναι ταυτόχρονα και επίμονοι και δυναμικοί. Ακόμη και όταν ο χρήστης δεν είναι παρών, το περιβάλλον υπάρχει και αλλάζει με την πάροδο του χρόνου». Τα αντικείμενα εντός των κόσμων αυτών υπάρχουν ανεξάρτητα από την παρουσία των χρηστών τους. Επομένως,

89 Ανεξάρτητα από τα χρήματα και το χρόνο που δαπανήθηκε από τους παίκτες για ένα συμβατικό παιχνίδι ρόλων, δεν θα μπορούσε ποτέ να φτάσει τα επίπεδα πολυπλοκότητας και διάρκειας που καθίστανται δυνατά μέσω του δικτύου υπολογιστών. Το δίκτυο των υπολογιστών επιτρέπει στους εικονικούς κόσμους να ξεπεράσουν τους ορίζοντες φαντασίας του παρελθόντος. Ό.π. υποσημ 89.

90 Κάποιος περιέγραψε τους, σε διαρκή σύνδεση, εικονικούς κόσμους ως «το ενδιάμεσο περιβάλλον, τις πρώτες εγκαταστάσεις στο τεράστιο και αχαρτογράφητο έδαφος που βρίσκεται ανάμεσα στους ανθρώπους και τα μηχανήματά τους». Marc W. Bell, «Toward a Definition of Virtual Worlds», *Journal of Virtual Worlds Research,* Vol. 1 /1 *(*2008).

μπορούν να αποτελέσουν αντικείμενο συναλλαγής ή πώλησης σε άλλους ανθρώπους με πραγματικά χρήματα[91].

Με δεκάδες εκατομμύρια χρήστες σε όλον τον κόσμο και συναλλαγές δισεκατομμυρίων πραγματικών δολαρίων ετησίως, οι εικονικοί κόσμοι δεν μπορούν να χαρακτηριστούν ως παιδικά παιχνίδια. Για το λόγο αυτό, πρέπει να γίνει σαφής διαχωρισμός ανάμεσα στα γεγονότα που συμβαίνουν στον εικονικό κόσμο, από την πραγματικότητα. Είναι εύλογες οι απαιτήσεις που προκύπτουν από τις ενέργειες στον αληθινό κόσμο και συνδέονται με τη συμπεριφορά στον εικονικό κόσμο, αλλά δεν υπάρχει αντίστοιχη αναγνώριση των αξιώσεων από τις ενέργειες στον εικονικό κόσμο που σχετίζονται με τη συμπεριφορά σε αυτόν[92]. Παρόλο που οι δράσεις εντός του εικονικού κόσμου πραγματοποιούνται από εικονικούς χαρακτήρες (avatars), οι οποίοι κατευθύνονται από πραγματικά πρόσωπα, οι εικονικοί χαρακτήρες δεν έχουν και δεν θα έπρεπε να έχουν ατομικά δικαιώματα. Όταν ένας εικονικός χαρακτήρας εξαπατάται, προσβάλλεται ή πλήττεται η ακεραιότητά του, σε κανένα πραγματικό δικαστήριο δεν θα στηριζόταν οποιουδήποτε είδους αξίωσή του ή παραπομπή του αυτουργού στη δικαιοσύνη. Ακόμη και αν το πρόσωπο που χειρίζεται τον εικονικό χαρακτήρα είναι αυτό που έχει υποστεί τη βλάβη, είναι σημαντική η διαφορά ανάμεσα σε πανομοιότυπες παραβάσεις απέναντι στο χρήστη και αυτές απέναντι στον εικονικό χαρακτήρα. Όταν ένα πρόσωπο αλληλεπιδρά σε έναν εικονικό κόσμο, βρίσκεται μέσα στο πλέγμα των φυσικών και κοινωνικών νόμων του κόσμου αυτού. Αν βιώσει μία αρνητική εμπειρία, υπάρχουν ενσωματωμένες επιλογές για την άμυνά του, όπως το να αναφέρει τις παραβάσεις στους ιδιοκτήτες του εικονικού κόσμου ή σε άλλους χρήστες. Παρομοίως, οι ενέργειες ενός προσώπου στον αληθινό κόσμο περιορίζονται από τους νόμους και τους κανόνες του κόσμου αυτού[93].

---

91 Σε κάποιες περιπτώσεις, όπως το Second Life, οι χρήστες μπορούν ακόμη και να δημιουργήσουν τα δικά τους αντικείμενα, από επιτραπέζια παιχνίδια, μέχρι εικονικά ελικόπτερα, πάνω στα οποία έχουν δικαιώματα πνευματικής ιδιοκτησίας.

92 Η αιτιολογία αυτής της διάκρισης είναι ότι οι ενέργειες που γίνονται στον αληθινό κόσμο εμπλέκουν πραγματικά άτομα, των οποίων οι σχέσεις ρυθμίζονται από πραγματικούς νόμους. «What makes a virtual world more than a game?», (2019), διαθέσιμο σε https://decentraland.org/blog/technology/virtual-worlds/

Δεδομένου ότι οι εικονικοί κόσμοι παρέχουν τη δυνατότητα συναλλαγών δισεκατομμυρίων δολαρίων ετησίως, κάτι το οποίο θα αυξάνεται με το χρόνο, πρέπει να αναπτυχθεί ένα νομικό πλαίσιο, για να επιλυθούν οι διαφορές που αναπόφευκτα θα προκύψουν. Προτείνεται οι εικονικοί κόσμοι να καλύπτονται από ένα νομικό σύστημα δύο όψεων. Αφενός μεν, ό,τι συμβαίνει αποκλειστικά μέσα στον εικονικό κόσμο πρέπει να οριοθετείται από μία σύμβαση όρων χρήσης, η οποία με τη σειρά της υπόκειται στο νόμο. Αφετέρου δε, οι συναλλαγές που θα προκύπτουν έξω από τον εικονικό κόσμο, δηλαδή στον αληθινό κόσμο, εάν περιλαμβάνουν και εμπλέκουν αγαθά και σχέσεις του εικονικού κόσμου, πρέπει να αντιμετωπίζονται όπως ακριβώς και οι συναλλαγές που αφορούν σε αγαθά και σχέσεις του αληθινού κόσμου[94].

4.2.1 Προστασία της ιδιωτικής ζωής στον εικονικό κόσμο

Καθώς οι άνθρωποι μεταφέρουν τις ζωές τους εντός του διαδικτύου, τα δικαστήρια πρέπει να αρχίσουν να αναγνωρίζουν ότι μαζί τους μεταφέρονται και τα δικαιώματά τους, διαμορφώνοντας έτσι μία δικαιολογημένη απαίτηση για διαδικτυακή προστασία της ιδιωτικής ζωής[95]. Το δικαίωμα στην προστασία της ιδιωτικής ζωής από προσβολές που σχετίζονται με το διαδίκτυο, δεν παύει να υφίσταται κατά τη διαφυγή στον εικονικό κόσμο. Καθώς οι άνθρωποι ζουν μεγαλύτερο κομμάτι της ζωής τους εντός του διαδικτύου, θα παρέχουν περισσότερα δεδομένα από αυτά που μπορούν να συγκεντρωθούν και να τύχουν επεξεργασίας. Σύντομα οι σχετικές νομοθετικές ρυθμίσεις και η νομολογία ως προς τους εικονικούς κόσμους θα

93 Jacob Rogers, «Note, A Passive Approach to Regulation of Virtual Worlds», *76 George Washington Law Review,* (2008): 405-409.

94 Οι εικονικοί κόσμοι είναι ανάλογοι του αληθινού, με τη διαφορά ότι οι «όροι» του αληθινού κόσμου ονομάζονται «νόμοι» και οι κάτοικοί του δεν έχουν τη δυνατότητα να «συμφωνήσουν» (agree) προτού συμμετάσχουν σε αυτόν. «What makes a virtual world more than a game?», (2019), διαθέσιμο σε https://decentraland.org/blog/technology/virtual-worlds/ .

95 «Η βασική ειρωνεία των εικονικών κόσμων είναι ότι οι άνθρωποι ψάχνουν να δημιουργήσουν νέα ζωή μακριά από τη δημοσιότητα και μεταφέρονται σε ένα περιβάλλον που βρίσκεται υπό συνεχή παρακολούθηση, από τους δημιουργούς των παιχνιδιών ή τις ιδιωτικές εταιρίες, οι οποίες σχεδιάζουν, διατηρούν και διαχειρίζονται τους εικονικούς κόσμους». Joshua Fairfield, «A.T. Escape into the Panopticon: Virtual Worlds and the Surveillance Society», 118 *Yale Law Journal Pocket* Part 131 (2009), διαθέσιμο σε http://thepocketpart.org/2009/01/19/fairfield.html

αφορούν και στην πραγματική ζωή, καθώς αυτά τα δύο (εικονικοί κόσμοι και πραγματικότητα) θα επικαλύπτονται. Κάθε κίνηση στον εικονικό κόσμο θα τυγχάνει επεξεργασίας από ιδιωτικές εταιρίες, οι οποίες οφείλουν να συμμορφώνονται στις απαιτήσεις της Πολιτείας σχετικά με τις τηλεφωνικές επικοινωνίες, τις ηχογραφήσεις, τις καταχωρημένες συνομιλίες ή άλλου είδους αρχεία. Η Πολιτεία θα ηγείται της προστασίας της ιδιωτικής ζωής των καταναλωτών, επεκτείνοντας την προστασία του νόμου και στη διαρροή δεδομένων μέσα στους εικονικούς κόσμους, επιβάλλοντας τους ήδη υπάρχοντες νόμους σχετικά με τη συναίνεση πριν από τη συλλογή των προσωπικών πληροφοριών και δημιουργώντας δικαιώματα πνευματικής ιδιοκτησίας πάνω στις πληροφορίες αυτές, ώστε οι καταναλωτές να έχουν επαρκή έλεγχο στην περίπτωση που τις μεταβιβάσουν[96].

4.2.2 Κυριότητα εικονικών κινητών πραγμάτων

Δεδομένου ότι εκατομμύρια κάτοικοι των εικονικών κόσμων ήδη θεωρούν την εικονική ιδιοκτησία ως πραγματική και μιας και δεν υπάρχει ισχυρή λογική διάκριση ανάμεσα στα δύο είδη ιδιοκτησιών, και οι δύο μορφές ιδιοκτησίας πρέπει να αντιμετωπιστούν νομοθετικά με τον ίδιο τρόπο. Δεν μπορεί κανείς να αμφισβητήσει το γεγονός ότι οι χρήστες έχουν αποκτήσει κυριότητα πάνω στα εικονικά αντικείμενα που έχουν δημιουργήσει, αγοράσει και πωλήσει, ανεξάρτητα από το αν η ιδιοκτησία αυτή εξαρτάται από τη σύμβαση των όρων χρήσης ανάμεσα στο χρήστη και τον ιδιοκτήτη του εικονικού κόσμου. Τα εικονικά αντικείμενα, αν και άυλα, ομοιάζουν με υπαρκτά κινητά πράγματα, μέσω του κώδικα του υπολογιστή[97]. Η υπάρχουσα τεχνολογία επιτρέπει στα εικονικά αντικείμενα να μιμούνται τα χαρακτηριστικά αυτά. Εάν ο εικονικός χαρακτήρας (avatar) ενός χρήστη κατέχει ένα αντικείμενο,

96 Ό.π. υποσημείωση 105.

97 Για παράδειγμα, εάν ένα άτομο έχει στην κατοχή του ένα αντικείμενο, όπως ένα στυλό, το κατέχει αποκλειστικά αυτό το άτομο και κανείς άλλος. Αν το αφήσει σε κάποιο χώρο και αποχωρήσει από αυτόν, το αντικείμενό του παραμένει εκεί και μπορούν να αλληλεπιδράσουν μαζί του όσοι το επιθυμούν. Wian Erlank, «Property in Virtual Worlds», (2013), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216481 .

όπως για παράδειγμα ένα συγκεκριμένο ζευγάρι μπότες, το ίδιο αντίγραφο του αντικειμένου δεν μπορεί να το έχει ο εικονικός χαρακτήρας κάποιου άλλου χρήστη. Εάν ο χαρακτήρας αυτός αποχωρήσει από το περιβάλλον του εικονικού κόσμου ή ο χρήστης αποσυνδεθεί από το δίκτυο ή κλείσει τον υπολογιστή του, το αντικείμενο βρίσκεται ακόμη εκεί. Περαιτέρω, και άλλοι εικονικοί χαρακτήρες του ίδιου περιβάλλοντος μπορούν να δουν το αντικείμενο και να αλληλεπιδράσουν με αυτό. Κατά συνέπεια, πολλοί θεωρητικοί ισχυρίζονται πλέον ότι για τα εικονικά αντικείμενα πρέπει να εφαρμοστούν οι ίδιοι κανόνες με την ιδιοκτησία στον αληθινό κόσμο, ενώ το Δίκαιο Πνευματικής Ιδιοκτησίας αναγνωρίζει ξεκάθαρα τη διάκριση ανάμεσα σε μία ιδέα[98] και την αποτύπωσή της[99].

Η ακμάζουσα αγορά των αντικειμένων των εικονικών κόσμων υποδεικνύει ότι υπάρχουν ήδη αξίες οικονομικά υπολογίσιμες, για μυριάδες εικονικά αντικείμενα. Υπάρχουν συμμετέχοντες σε εικονικούς κόσμους, οι οποίοι ουδέποτε μεταβιβάζουν κάποιο αντικείμενο. Περαιτέρω, μπορεί να ανακύψει και ζήτημα φορολόγησής τους. Εάν θεωρηθεί, τόσο από το αμερικανικό, όσο και από το ευρωπαϊκό δίκαιο, ότι τα εικονικά αντικείμενα συνιστούν ιδιοκτησία, η απόκτησή τους μπορεί να συνιστά

98 Κωνσταντίνος Χριστοδούλου, «Δίκαιο Πνευματικής Ιδιοκτησίας», Νομική Βιβλιοθήκη, Αθήνα, 2018.

99 Τα δικαιώματα που κάποιος έχει σε ένα αντίγραφο μίας ταινίας σε μορφή DVD, διαφοροποιούνται από τα δικαιώματα πάνω στην ίδια την ταινία. Ακόμη και αν μεταβιβάσει το DVD, η παραγωγός εταιρία εξακολουθεί να έχει τα δικαιώματα πάνω στην ταινία. Ο καθηγητής Fairfield έχει αναπτύξει μία παραπλήσια σκεπτική σχετικά με τα εικονικά αντικείμενα, διακρίνοντας τα αντίγραφα των εικονικών αντικειμένων σε ένα παιχνίδι εικονικού κόσμου, από τα πνευματικά δικαιώματα πάνω στο ίδιο το αντικείμενο. Υπό αυτή την προσέγγιση, τα δικαιώματα ως προς την εικονική ιδιοκτησία ενός παίκτη εικονικού παιχνιδιού πάνω σε ένα αντικείμενο που διατηρεί ο εικονικός του χαρακτήρας (avatar), δεν σχετίζονται ούτε με τα πνευματικά δικαιώματα που έχει ο ιδιοκτήτης της εικονικού κόσμου πάνω στο αντικείμενο αυτό, ούτε με τα δικαιώματα πάνω σε απτά περιουσιακά στοιχεία, όπως οι διάφοροι υπολογιστές που επιτρέπουν στους παίκτες να συμμετέχουν στον εικονικό αυτό κόσμο. Αντιθέτως, ο καθηγητής Fairfield θα απέδιδε στον παίκτη δικαιώματα ιδιοκτησίας στο αντίγραφο του αντικειμένου, αντίστοιχα με αυτά που έχει κάποιος πάνω στο DVD μίας ταινίας. Αυτή η θεωρία παρέχει προστασία σε εκείνον του οποίου τα εικονικά περιουσιακά στοιχεία έχουν αφαιρεθεί ή καταστραφεί από έναν εισβολέα (hacker), χωρίς να περιοριστούν τα δικαιώματα πνευματικής ιδιοκτησίας των ιδιοκτητών του παιχνιδιού. Joshua Fairfield, «A.T. Escape into the Panopticon: Virtual Worlds and the Surveillance Society», 118 *Yale Law Journal Pocket* Part 131 (2009), διαθέσιμο σε http://thepocketpart.org/2009/01/19/fairfield.html .

εισόδημα και η διάθεσή τους, ακόμη και μέσα στον εικονικό κόσμο, να πρέπει να τύχει φορολόγησης[100].

4.2.3 Φορολόγηση των παιχνιδιών στους εικονικούς κόσμους

Καθώς ο πολιτισμός μας «νομισματοποιεί» όλο και περισσότερο τις δραστηριότητας της καθημερινότητας, προκύπτουν ολοένα και περισσότερα φορολογικά ζητήματα, ιδίως και από τη νέα ανθρώπινη δραστηριότητα, τα επιγραμμικά (on-line) παιχνίδια ρόλων στους εικονικούς κόσμους. Περίπου τριάντα εκατομμύρια άνθρωποι συμμετέχουν σε τακτική βάση σε τέτοιου είδους παιχνίδια και ο αριθμός ολοένα και μεγαλώνει[101]. Η διερεύνηση της επέκτασης του Φορολογικού Δικαίου και στις συναλλαγές στους εικονικούς κόσμους δεν ανταποκρίνεται μόνο στις πρακτικές ανάγκες των εκατομμυρίων φορολογούμενων, αλλά επιτρέπει μία επανεκτίμηση των βασικών αρχών του φόρου εισοδήματος, όπως οι αρχές αυτές αλληλεπιδρούν με τις δραστηριότητες της ζωής κατά τον 21ο αιώνα. Ενόσω η δραστηριότητα των παικτών στους εικονικούς κόσμους αναμφισβήτητα παράγει μετρήσιμη οικονομική αξία στον παίκτη, αυτή η δραστηριότητα, η οποία προκύπτει αποκλειστικά στον εικονικό κόσμο, δεν θεωρείται ακαθάριστο εισόδημα υπό την υπάρχουσα θεωρία, ούτε αυτή η θεωρία θα έπρεπε να τροποποιηθεί. [102].

100 Leandra Lederman, «Stranger Than Fiction: Taxing Virtual Worlds», *New York University Law Review,* Vol. 82:1620, (2007).

101 Βλ. σχετικά Thomas Alsop, «Virtual Reality (VR) - statistics & facts», (2020), διαθέσιμο σε https://www.statista.com/topics/2532/virtual-reality-vr/ .

102 Οι παίκτες των οποίων η προστιθέμενη περιουσία αποτελείται αποκλειστικά και μόνο από «μονάδες παιχνιδιού» δεν πρέπει να φορολογηθούν, εκτός εάν προκύψει κι επιπλέον εισόδημα από αυτό του παιχνιδιού. Αντιστρόφως, οι παίκτες των οποίων η περιουσία στον αληθινό κόσμο μετατρέπεται από «μονάδες του παιχνιδιού» σε μέσο συναλλαγής, θα έπρεπε να υπολογίζουν και τις συναλλαγές τους στους εικονικούς κόσμους ως ακαθάριστο εισόδημα. Bryan Camp, «The Play's The Thing: A Theory of Taxing Virtual Worlds», *Hastings Law Journal*, Vol. 59/ 1 (2007).

4.2.4 Αδικοπραξίες εντός των εικονικών κόσμων

Η συνηθέστερη εφαρμογή της εικονικής πραγματικότητας είναι τα παιχνίδια, τα οποία αποτελούν ένα από τα σημαντικότερα κοινωνιολογικά φαινόμενα της εποχής, καθώς έχουν οικονομικές και κοινωνικές προεκτάσεις στον πραγματικό κόσμο[103]. Κατ' επέκταση, σημαντικά είναι τα νομικά ζητήματα που προκύπτουν με τη συμμετοχή σε αυτά, καθώς η διάδραση με άλλα άτομα μέσω ενός συστήματος εικονικής πραγματικότητας γίνεται με τρόπους που μέχρι σήμερα δεν ήταν γνωστοί. Αυτά τα νομικά ζητήματα που τίθενται, συχνά καλύπτονται στο αμερικανικό δίκαιο από τις υπάρχουσες διατάξεις περί αδικοπραξιών ή τις διατάξεις του Ποινικού Κώδικα, τις οποίες εφαρμόζουν και στις νέες τεχνολογίες.

Οι πιο ουσιώδεις, όμως, προκλήσεις που προκύπτουν από την εφαρμογή της τεχνολογίας της εικονικής πραγματικότητας έχουν να κάνουν με το γεγονός ότι η τεχνολογία αυτή θολώνει τη γραμμή ανάμεσα στο εικονικό και το πραγματικό, ανάμεσα στην πληροφορία και το φυσικό περιβάλλον, ανάμεσα στο λόγο και τη συμπεριφορά. Η εικονική πραγματικότητα δίνει την αίσθηση του πραγματικού, μόνο εάν τη βιώνει κανείς, ενώ σε διαφορετική περίπτωση δεν είναι εύκολο να γίνει αντιληπτή. Είναι καθησυχαστικό το γεγονός ότι, προς το παρόν τουλάχιστον, η φυσική απόσταση ανάμεσα στα άτομα με τα οποία ο χρήστης είναι σε διάδραση καθιστά εξαιρετικά δυσχερή την πραγματοποίηση των παράνομων πράξεων του εικονικού κόσμου και επί του φυσικού[104]. Από την άλλη πλευρά, ανεξάρτητα από τη φυσική απόσταση μπορούν να στοιχειοθετηθούν αδικήματα που ο νόμος ήδη αναγνωρίζει, όπως η δυσφήμιση ή η παραβίαση του νόμου περί πνευματικής ιδιοκτησίας, όπου η ευθύνη αναγνωρίζεται χωρίς να υφίσταται φυσική διάδραση. Οι κάτοχοι δικαιωμάτων πνευματικής ιδιοκτησίας και εμπορικών σημάτων θα

103 Οι ειδικοί του χώρου προβλέπουν κέρδη 45 δισεκατομμυρίων δολαρίων μέχρι το 2025, από την αγορά παιχνιδιών εικονικής πραγματικότητας. «VR in #Gaming. Ο θαυμαστός κόσμος του παιχνιδιού εικονικής πραγματικότητας», (2018), διαθέσιμο σε http://gadgetblog.gr/vr-in-gaming-o-thaymastos-kosmos-toy-paichnidioy-eikonikis-pragmatikotitas.

104 Mark Lemley και Eugene Volokh, «The Real Law of Virtual Reality», University of California, Davis, Vol. 51, (2017).

επιχειρήσουν ασφαλώς να επιβάλουν στον εικονικό κόσμο τα δικαιώματα που έχουν και στον πραγματικό.

4.2.5 **Δικαίωμα στη δημοσιότητα και ελευθερία έκφρασης.**

Εξίσου σημαντικό θέμα με τα ανωτέρω είναι ο τρόπος αντιμετώπισης του δικαιώματος στη δημοσιότητα (the right of publicity[105]) από την πλευρά του δικαίου. Το πρόβλημα τίθεται στις περιπτώσεις που οι χρήστες επιλέγουν να δώσουν μορφή διασήμων προσώπων στις εικονικές τους προσωπικότητες, τα avatars τους. Μία εταιρία δεν πρόκειται να δημιουργήσει avatars με τη μορφή διασήμων για εμπορικούς σκοπούς, αλλά ο ιδιώτης θα το πράξει για ιδία χρήση, οπότε προκύπτει το ερώτημα εάν αυτή του η πράξη αποτελεί παράβαση του δικαιώματος δημοσιότητας. Το συγκεκριμένο δικαίωμα υφίσταται αυτοτελώς στο αμερικανικό δίκαιο, ενώ γίνεται σταδιακά αποδεκτό στην ευρωπαϊκή και ελληνική έννομη τάξη στο πλαίσιο του δικαιώματος στην προσωπικότητα.

Γενικά, η πληροφορία (δεδομένα, εικόνες, ύβρεις) αντιμετωπίζεται ως ενέχουσα λιγότερους κινδύνους σε σχέση με την επαφή των προσώπων δια ζώσης. Εάν κάποιος εμφανιστεί δημόσια χωρίς ρούχα, αυτό αποτελεί αδίκημα και θα συλληφθεί για

105 «Το δικαίωμα της δημοσιότητας στις ΗΠΑ είναι αυτοτελώς προστατευόμενο περιουσιακό δικαίωμα που αφορά στο όνομα, την ταυτότητα και την προσωπικότητα. Κάθε πρόσωπο, δημόσιο, διάσημο ή μη, είναι φορέας του δικαιώματος της δημοσιότητας, δηλαδή του δικαιώματος προστασίας και οικονομικής εκμετάλλευσης του δικαιώματος της προσωπικότητας. Η γένεση του δικαιώματος της δημοσιότητας ερείδεται στο δικαίωμα της προσωπικότητας, ιδίως στον ιδιωτικό βίο (privacy). Η προστασία του δικαιώματος της δημοσιότητας διαφέρει από πολιτεία σε πολιτεία και σε επίπεδο ομοσπονδιακού δικαίου. Μετά θάνατον δικαιώματα προστατεύονται στο πλαίσιο του δικαιώματος της δημοσιότητας αλλά όχι σε όλες τις πολιτείες. Στο επίπεδο του ομοσπονδιακού δικαίου τα δικαστήρια τηρούν ισορροπία μεταξύ του δικαιώματος της δημοσιότητας και της ελευθερίας του τύπου, εξετάζοντας κάθε υπόθεση ξεχωριστά. Η ρήτρα αποκλειστικότητας είναι ουσιώδες στοιχείο των σχετικών συμβάσεων που υπογράφουν οι αθλητές όπως αυτοί του NBA. Το 2004, αμερικανικός Δικηγορικός Σύλλογος έκανε μία πρόταση για έναν ομοσπονδιακό νόμο που θα καθιερώνει το δικαίωμα της δημοσιότητας. Ένας τέτοιος νόμος θα μπορούσε να λειτουργήσει ως πρότυπο για το ελληνικό δίκαιο, αν και το ελληνικό δίκαιο δεν αναγνωρίζει το δικαίωμα της δημοσιότητας ως αυτοτελές δικαίωμα». Χ. Σταμέλος, «Το δικαίωμα της δημοσιότητας (right of publicity) του επαγγελματία αθλητή στις ΗΠΑ», *Δικαιο Μεσων Ενημερωσης & Επικοινωνιας,* Τεύχος 1, Ιανουάριος - Φεβρουάριος – Μάρτιος (2009). Βλ. επίσης Burkhard Hess, Σπυρίδων Β. Βλαχόπουλος, Λίλιαν Μήτρου, Βιργινία Τζώρτζη, Χρίστος Γεραρής, Κωνσταντίνος Μενουδάκος και Βασίλειος Σκουρής, «Προστασία των δεδομένων προσωπικού χαρακτήρα. Εξελίξεις ενόψει της θέσης σε εφαρμογή του νέου Γενικού Κανονισμού ΕΕ 2016/679», Σάκκουλας, Αθήνα, 2018.

προσβολή δημοσίας αιδούς. Το γυμνό, όμως, στην οθόνη αποτελεί προστατευόμενη ελευθερία έκφρασης, όπως και το γυμνό στον εικονικό κόσμο. Αυτές οι διακρίσεις υφίστανται διότι η φυσική παρουσία, σε αντίθεση με την εικονική, μπορεί να προκαλέσει φόβο, ο οποίος μπορεί να μετατραπεί και σε φόβο ως προς τις συνέπειες[106].

4.2.6 Σωματικές βλάβες και τόπος τέλεσης του αδικήματος.

Σε μια άλλη σχετική θεώρηση των πραγμάτων, έχει διαπιστωθεί ότι τόσο οι λέξεις, όσο και τα δεδομένα μπορούν να προκαλέσουν βλάβη, όπως για παράδειγμα από την παράνομη εισβολή κάποιου (hacking) στη συσκευή εικονικής πραγματικότητας ενός άλλου προσώπου ή τη μεταβολή του αλγορίθμου τοποθεσίας με αποτέλεσμα την πτώση του χρήστη. Σε αυτές τις περιπτώσεις, μέσω της αποστολής δεδομένων και πληροφοριών, θα έχουν προκληθεί σωματικές βλάβες ή ακόμα και θάνατος και κατά συνέπειες θα υπάρχει αντίκτυπος στον πραγματικό κόσμο[107]. Περαιτέρω, η ανάπτυξη των τεχνολογιών αφής[108] ενέχει τον κίνδυνο να αυξηθούν θεαματικά οι περιπτώσεις όπου οι αντιδράσεις των χρηστών στον εικονικό κόσμο θα έχουν συνέπειες στον πραγματικό, διότι η παρουσία των τεχνολογιών αυτών δυσχεραίνει ακόμα περισσότερο την εύρεση του ορίου ανάμεσα στον εικονικό και το φυσικό κόσμο. Μολαταύτα, τα δικαστήρια είναι πιο πιθανό να αντιληφθούν τη βλάβη ευκολότερα όταν υπάρχει φυσική επαφή, ακόμα και απομακρυσμένη. Μέχρι σήμερα δεν έχουν ληφθεί σοβαρά υπόψη τα προβλήματα που προκύπτουν εντός των εικονικών κόσμων και αυτό διότι τα προβλήματα αυτά πρωτίστως υπάρχουν μέσα στα παιχνίδια, τα

106 Μαρία Καρύδα, Σπύρος Κοκολάκης, Λίλιαν Μήτρου, Άννα-Μαρία Πισκοπάνη και Σπύρος Τάσσης, «Facebook, Blogs και δικαιώματα», Σάκκουλας, Αθήνα, 2013.

107 Ό.π. υποσημείωση 117.

108 Η τεχνολογίες αφής αναφέρονται στο είδος αυτό της τεχνολογίας που χρησιμοποιεί μεθόδους αφής για τον έλεγχο και τη διάδραση μεταξύ των υπολογιστών. Ο χρήστης μπορεί να αποκτήσει αίσθηση μέσω δονήσεων, ή μέσω της κίνησης και της δύναμης που ασκείται. Η τεχνολογία αυτή χρησιμοποιείται κυρίως στη δημιουργία εικονικών αντικειμένων, στον έλεγχο των αντικειμένων αυτών ή στη βελτίωση του απομακρυσμένου ελέγχου των μηχανών και των συσκευών. Βλ. σχετικά https://www.techopedia.com

οποία θεωρούν ανάξια λόγου. Σημαντικός παράγοντας βέβαια αυτής της απαξίωσης είναι και το πρόβλημα της εύρεσης του εναγομένου προσώπου και κατ' επέκταση της τοπικής δωσιδικίας[109].

4.2.7 Όροι χρήσης

Είναι γεγονός ότι η νομοθεσία που θα παραχθεί για την εικονική πραγματικότητα, θα εφαρμοστεί σε ένα πλαίσιο όπου ο,τιδήποτε συμβαίνει, αυτό συμβαίνει σε έναν ιδιωτικό διακομιστή. Δεν υπάρχει δημόσιο σύστημα εικονικής πραγματικότητας[110], οπότε κατ' επέκταση ό,τιδήποτε ενσκύψει θα υπόκειται στους όρους χρήσης (terms of use[111]) του συστήματος, στους οποίους ο χρήσης συμφωνεί a priori, με την τοποθέτηση και μόνο της συσκευής εικονικής πραγματικότητας επάνω στο σώμα του. Οι όροι αυτοί απαλλάσσουν από την ευθύνη την εταιρία που χειρίζεται το εικονικό περιβάλλον για τις δράσεις εντός αυτού[112], δεδομένο που πρέπει να αντιμετωπιστεί άμεσα από το Δίκαιο. Είναι γεγονός ότι αποτελεί μεγάλη αποτυχία του σύγχρονου συμβατικού δικαίου η είσοδος του προσώπου σε ένα περιβάλλον όπου δεσμεύεται από συμφωνίες άλλων προσώπων, στις οποίες απλά προσχωρεί, χωρίς να μπορεί να λάβει γνώση αυτών ή να τις τροποποιήσει, εάν έχει ενστάσεις.

Συμπερασματικά, ο συνδυασμός της αδυναμίας των δικαστηρίων να λάβουν σοβαρά υπόψη τα ανωτέρω θέματα και των ελλείψεων του δικαιικού συστήματος, έχει ως συνέπεια την ελλιπή παρουσία του νόμου στην τεχνολογία της εικονικής πραγματικότητας. Προς επίλυση αυτού, θα μπορούσαν να λάβουν δράση οι ίδιες οι

109 Ιωάννης Ιγγλεζάκης, «Δίκαιο πληροφορικής», 3η έκδ., Σάκκουλας, Αθήνα, 2018.

110 Οι σημαντικότερες πλατφόρμες εικονικής πραγματικότητας μέχρι τη συγγραφή της παρούσας είναι οι: Facebook's Oculus Rift, HTE's Vive, Sony's PlayStation VR και Microsoft's HoloLens.

111 «Terms of service» (επίσης γνωστοί ως terms of use ή terms and conditions, - TOS ή ToS ή ToU): κανόνες με τους οποίους πρέπει να συμμορφωθούν όσοι κάνουν χρήση μίας υπηρεσίας. Επίσης, ο όρος αυτός σε κάποιες περιπτώσεις υποδηλώνει την αποποίηση της ευθύνης του διαχειριστή ενός ιστότοπου ή μιας ιστοσελίδας κατά τη χρήση τους. https://en.wikipedia.org.

112 Με εξαίρεση τις περιπτώσεις που εμπίπτουν στις διατάξεις περί προστασίας του καταναλωτή.

εταιρίες που σχεδιάζουν τα συστήματα εικονικής πραγματικότητας, δημιουργώντας κανόνες και πρακτικές που θα απαγορεύουν συγκεκριμένες προβληματικές συμπεριφορές και θα παρέχουν τη δυνατότητα επίλυσης της διαφοράς εντός του συστήματος, με την αυτόματη αποβολή του χρήστη από το περιβάλλον.

4.3 Εφαρμογές των εικονικών κόσμων

Για τους φανατικούς της τεχνολογίας, η εικονική πραγματικότητα υπήρξε έως σήμερα ένα όνειρο που θα μπορούσε να μεταφερθεί από τις ταινίες επιστημονικής φαντασίας στην καθημερινότητα, μέσω ενός προϊόντος που ο καθένας θα μπορούσε να αποκτήσει. Είχε εισχωρήσει δειλά μόνο σε κάποιες βιομηχανικές και ιατρικές εφαρμογές, όπως για παράδειγμα την αντιμετώπιση του μετατραυματικού στρες στους βετεράνους πολέμων[113]. Η τεχνολογία αυτή αναπτύσσεται πλέον με τόσο γοργούς ρυθμούς, που είναι βέβαιο ότι θα επηρεάσει κάθε πτυχή της καθημερινότητας των ατόμων. Πρόκειται για τη φυσική και απόλυτη προέκταση άλλων σπουδαίων τεχνολογιών που χρησιμοποιούνται σήμερα, όπως της τηλεόρασης, των τηλεδιασκέψεων, των «έξυπνων» τηλεφώνων και του διαδικτύου και χρησιμοποιείται με τον ίδιο ακριβώς τρόπο, με στόχο την επικοινωνία, τη μάθηση, τη διασκέδαση και τη διαφυγή.

Για χρόνια, οι επιστήμονες ήταν επιφυλακτικοί σε σχέση με τις δυνατότητές της. Η επιφυλακτικότητα αυτή συνεχίζει να υφίσταται και σήμερα. Οι συσκευές εικονικής πραγματικότητας λειτουργούν μέσω της αποστολής μίας εικόνας που παράγεται από υπολογιστή, στα μάτια του χρήστη, ως απάντηση στις κινήσεις του. Η αξιοπιστία του προσομοιωτή εξαρτάται από την ακρίβεια με την οποία συλλαμβάνει τις κινήσεις του χρήστη και την ταχύτητα προσαρμογής της εικόνας στην κίνηση. Αν η τεχνολογία υστερεί, έστω και ελάχιστα, η προσομοίωση θα αποτύχει [114]. Αυτή η τεχνολογία, με

113 Nick Wingfield και Vindu Goel, «Facebook in $2 Billion Deal for Virtual Reality Company», διαθέσιμο σε https://www.nytimes.com.

114 Farhad Manjoo, «If You Like Immersion, You'll Love This Reality», διαθέσιμο σε https://www.nytimes.com/

την οποία δημιουργούνται περιβάλλοντα και αντικείμενα – φαντάσματα, δεν υπόσχεται μόνο εντυπωσιακά άλματα σε πεδία, όπως η ιατρική, η εκπαίδευση και η αρχιτεκτονική, αλλά δημιουργεί το υπόβαθρο για ένα μεγάλο άλμα προς την ελευθερία του ατόμου[115]. Η ελευθερία που παρέχει στα πρόσωπα τη δυνατότητα να βυθίζονται σε έναν κόσμο της επιλογής τους είναι αποκαλυπτική, διότι τους δίνει την ευκαιρία να βιώνουν, ζωντανά και απευθείας, δραστηριότητες, που διαφορετικά δεν θα ήταν σε θέση να βιώσουν[116].

Η τεχνολογία της εικονικής πραγματικότητας καθίσταται απαραίτητη και σε τομείς που στο παρελθόν η ανθρωπότητα δεν θα μπορούσε ούτε να φανταστεί. Για παράδειγμα, η Terre des Hommes μια διεθνής μη κυβερνητική οργάνωση (ΜΚΟ) προάσπισης των δικαιωμάτων των παιδιών με έδρα την Ολλανδία, κάλεσε τις αρμόδιες διωκτικές αρχές να συνεργαστούν μαζί της προκειμένου να αντιμετωπιστεί το αυξανόμενο πρόβλημα της προσέλκυσης ανηλίκων σε σεξουαλικές πράξεις, μέσω του διαδικτύου. Δημιουργώντας ένα ψηφιακό εικονικό προφίλ, ενός δεκάχρονου ανήλικου κοριτσιού από τις Φιλιππίνες με το όνομα Σουίτι, κατάφεραν να παγιδεύσουν αρκετούς ενδιαφερόμενους, οι οποίοι πίστευαν ότι συνομιλούσαν με τη Σουίτι, ενώ στην πραγματικότητα επικοινωνούσαν με μια ομάδα της ΜΚΟ στο Άμστερνταμ[117].

115 Χαράλαμπος Χρυσανθάκης, «Εισηγήσεις Συνταγματικού Δικαίου», Νομική Βιβλιοθήκη, Αθήνα 2007, Κώστας Χρυσόγονος και Σπύρος Βλαχόπουλος, «Ατομικά και Κοινωνικά Δικαιώματα», 4η έκδοση, Νομική Βιβλιοθήκη, Αθήνα, 2017 και Ιωάννης Ιγγλεζάκης (επιμ), «Δίκαιο πληροφορικής & διαδικτύου», 2η έκδ., Σάκκουλας, Αθήνα, 2020.

116 Ο Πολωνός συγγραφέας επιστημονικής φαντασίας Stanislaw Lem, όταν κατά το έτος 1964 προέβλεψε τη ραγδαία εξέλιξη της εικονικής πραγματικότητας, περιέγραψε ότι «η τεχνολογία αυτή μπορεί να αποκαταστήσει στους παραπληγικούς κατάκοιτους ασθενείς τη δύναμη της κίνησης, έστω και προσωρινά. Μπορεί να πραγματοποιήσει τα όνειρα των ηλικιωμένων που εύχονται να βιώσουν μία δεύτερη νεότητα». Πράγματι, όπως παρατηρεί ο Jaron Lanier, «η εικονική πραγματικότητα όχι μόνο ελευθερώνει τους ανθρώπους από τα δεσμά που τους επιβλήθηκαν από περιορισμούς λόγω τραυματισμών ή παθολογικών αιτίων, αλλά και από περιορισμούς σύμφυτους με την ανθρώπινη ύπαρξη». Ο Lanier υπενθύμισε στους ανθρώπους, διατρανώνοντας τις δυνάμεις της εικονικής πραγματικότητας, ότι «δεν χρειάζεται κάποιος να έχει την ανθρώπινη μορφή σε έναν κόσμο που έχει δημιουργηθεί για τον ίδιο – μπορεί κάλλιστα να φέρει τη μορφή μίας οροσειράς ή ενός γαλαξία. Μπορεί να μετατραπεί από έναν κομήτη στον ουρανό τη μία στιγμή, σε μία αράχνη μεγαλύτερη από έναν πλανήτη». Marc Jonathan Blitz, «The Freedom Of 3d Thought: The First Amendment In Virtual Reality», *Cardozo Law Review,* Vol. 30:3, (2008).

117 Ο Albert Jaap van Santbrink, διευθυντής της Terre des Hommes, δήλωσε ότι σε διάστημα 10 εβδομάδων, όσο δηλαδή διήρκεσε η έρευνα, περισσότεροι από 20.000 άνδρες επικοινώνησαν με τον

Πρόσφατα το Facebook εξαγόρασε την εταιρία Oculus VR, η οποία παρήγαγε μία συσκευή εικονικής πραγματικότητας, την Oculus Rift. Πρόκειται για έναν εικονικό κόσμο τριών διαστάσεων, όπου ο χρήστης έχει την αίσθηση ότι συναναστρέφεται τους φίλους του, αντί να έχει πρόσβαση μόνο στις φωτογραφίες τους[118]. Με αυτό τον τρόπο δίνεται μία άλλη διάσταση ως προς το πώς αλληλεπιδρούν οι άνθρωποι με την ίδια την πληροφορία ή με άλλες μορφές περιεχομένου. Η εν λόγω συσκευή αποτελείται από ένα ζεύγος γυαλιών που περιβάλλουν τα μάτια όσων τα φορούν και καλύπτουν ολοκληρωτικά το οπτικό τους πεδίο με οθόνες υψηλής ανάλυσης, οι οποίες παράγουν εικόνες τριών διαστάσεων. Αισθητήρες συλλαμβάνουν την κίνηση του κεφαλιού του χρήστη, προσαρμόζοντας το βλέμμα του με την οθόνη και δημιουργούν με αυτόν τον τρόπο την αίσθηση ότι ο χρήστης έχει ενεργή παρουσία στον εικονικό κόσμο[119].

Η εικονική πραγματικότητα δεν είναι, όμως, μόνο για παιχνίδια. Η ίδια τεχνολογία που επιτρέπει στους χρήστες να μάχονται τέρατα σε μυθικούς κόσμους, έχει αποδειχθεί χρήσιμη και σε άλλους τομείς, όπως για παράδειγμα στην ιατρική, στη θεραπεία φοβιών ή για πρακτικά ζητήματα σε χειρουργικές επεμβάσεις ή στην εκπαίδευση, με τις εικονικές περιηγήσεις σε μουσεία ή διαστημικούς σταθμούς. Πρόσφατο επίτευγμα της τεχνολογίας αυτής είναι η ευκαιρία που προσφέρει σε άτομα που διαβιούν σε μονάδες φροντίδας ηλικιωμένων να βιώσουν, μέσω των

εικονικό χαρακτήρα και «ήταν έτοιμοι να πληρώσουν για να την δουν να επιδίδεται σε σεξουαλικές πράξεις μπροστά σε μια διαδικτυακή κάμερα». Από αυτούς η ΜΚΟ κατάφερε να βρει τα αναλυτικά στοιχεία των χιλίων περίπου. Βλ. σχετικά σε www.lawnet.gr. Βλ. επίσης Maria Kanellopoulou- Bottis, «Disclosing Software Vulnerabilities» σε Jones and Bartlett Publishers, ed. Kenneth Einar Himma, (2006): 249-262.

118 Ο Mark Zuckerberg επεσήμανε ότι η εικονική πραγματικότητα θα αποτελέσει την επόμενη μεγάλη πλατφόρμα υπολογιστών, μετά το κινητό. Αρκεί να σκεφτεί κανείς ότι μέσω της τεχνολογίας αυτής ο χρήστης θα απολαμβάνει έναν αγώνα σε προνομιούχο θέση του γηπέδου, θα μελετά σε μία τάξη γεμάτη από φοιτητές και καθηγητές, οπουδήποτε κι εάν αυτή βρίσκεται στον κόσμο ή θα συμβουλεύεται έναν γιατρό σαν να βρίσκεται στο ιατρείο του και όλα αυτά μόνο μέσω της συγκεκριμένης συσκευής.

119 Ο Brendan Iribe, συνιδρυτής και Διευθύνων Σύμβουλος της εταιρίας Oculus VR, δήλωσε ότι το Facebook θα χρησιμοποιήσει την τεχνολογία της εικονικής πραγματικότητας, ώστε να επιτρέψει σε εικονικούς χαρακτήρες (avatars) να εκπροσωπούν τα μέλη του και να αλληλεπιδρούν μεταξύ τους, πιθανόν με την κοινωνικοποίησή τους σε ομάδες. Βλ. σχετικά Ben Popper, «This is how Facebook will animate you in VR», (2016), διαθέσιμο σε https://www.theverge.com/2016/10/6/13176906/oculus-connect-3-facebook-social-vr-avatars και https://www.oculus.com .

ειδικών οπτικοακουστικών μέσων εικονικής πραγματικότητας, αξιοθέατα και ήχους από μακρινά μέρη, να απολαύσουν στιγμές από το παρελθόν τους και να εξερευνήσουν εμπειρίες, οι οποίες θα ήταν απρόσιτες σε αυτούς στην πραγματικότητα, λόγω του γήρατος ή της κλονισμένης υγείας τους. Επίσης, η εικονική πραγματικότητα θα μπορούσε να φανεί χρήσιμη ως η εκδοχή υψηλής τεχνολογίας αυτού που ονομάζουμε «θεραπεία αναμνήσεων»[120], κατά την οποία άτομα με διαταραχές μνήμης ενθαρρύνονται να παρατηρούν παλιές φωτογραφίες, να ακούν μουσική ή να εξετάζουν οικογενειακά κειμήλια, ως τρόπους να απασχολούν το μυαλό τους και να ενισχύσουν τη διάθεσή τους[121].

Τέλος, η εικονική πραγματικότητα και ειδικότερα η συμμετοχή σε εικονικούς κόσμους παιχνιδιών, όπως το «Grand Theft Auto», το «Red Dead Redemption», το «Second Life» ή το «Minecraft», αποτελεί το νέο τρόπο συναντήσεων (meetings) ανάμεσα σε στελέχη επιχειρήσεων ανά τον κόσμο. Δεδομένου ότι η πανδημία του κορωνοϊου έχει αλλάξει τα εργασιακά δεδομένα και τα γεύματα ή οι άλλου είδους κοινωνικές εκδηλώσεις ανάμεσα στα στελέχη των επιχειρήσεων είναι απαγορευτικά, η τάση είναι ο στόχος αυτός να επιτευχθεί μέσω μίας «εκδρομής» σε εικονικό κόσμο, κάτι που πλέον φαίνεται ιδανικό για την ανάπτυξη κοινωνικών επαφών ή επαγγελματικών σχέσεων[122].

120 Πρόκειται για θεραπεία που χρησιμοποιεί όλες τις αισθήσεις: όραση, αφή, όσφρηση και ακοή, προς εξάσκηση των ατόμων που πάσχουν από άνοια, να θυμηθούν γεγονότα, πρόσωπα και μέρη από το παρελθόν τους. Μέρος της θεραπείας και προς βοήθεια για την ανάκτηση της μνήμης τους, αποτελεί η χρήση από τους φροντιστές των ατόμων αυτών, αντικειμένων σε διάφορες δραστηριότητες. Βλ. σχετικά «Benefits of Reminiscence Therapy», (2017), διαθέσιμο σε https://eldercarealliance.org/blog/benefits-reminiscence-therapy/.

121 Rebecca Heilweil, «How virtual reality is helping seniors breathe new life into old memories», (2019), διαθέσιμο σε https://www.nbcnews.com/mach/science/how-virtual-reality-helping-seniors-breathe-new-life-old-memories-ncna1069461.

122 David Segal, «Hey, You Free on Friday for a Meeting and a Bank Heist?», (2020), διαθέσιμο σε https://www.nytimes.com/2020/07/31/business/video-game-meetings.html.

5 Επαυξημένη πραγματικότητα

Το διαδίκτυο συνέδεσε στο παρελθόν την ανθρώπινη γνώση μέσω του απλού μηχανισμού της υπερσύνδεσης, αλλά σήμερα πλέον, η ίδια η πραγματικότητα έχει υπερσυνδεθεί και επαυξηθεί με εικονικές εμπειρίες. Αρκεί να σκεφτεί κάποιος ότι έχει τη δυνατότητα, για παράδειγμα, να ελέγξει το παρελθόν του επόμενου ραντεβού του μέσω ενός κινητού τηλεφώνου ή να βιώσει την εμπειρία ενός κρυμμένου κόσμου γιγάντων και ξωτικών όση ώρα κάνει περίπατο στο πάρκο. Όλα τα παραπάνω είναι η καλπάζουσα τεχνολογία της «επαυξημένης πραγματικότητας», η οποία επαυξάνει πραγματικά μέρη, ανθρώπους και πράγματα, με πλούσιες εικονικές εμπειρίες[123]. Η τεχνολογία της επαυξημένης πραγματικότητας υπάρχει ήδη και αναπτύσσεται με ταχύ ρυθμό[124].

Η επαυξημένη πραγματικότητα, αντί να μεταφέρει το χρήστη σε ένα φανταστικό ή μακρινό κόσμο, ενισχύει – επαυξάνει το φυσικό κόσμο που περιβάλλει το χρήστη, συνήθως σε πραγματικό χρόνο. Επιτρέπει στο ψηφιακό περιεχόμενο να υπερτεθεί στον πραγματικό κόσμο μέσω ειδικών γυαλιών ή πιο συχνά, μέσω της οθόνης ενός «έξυπνου» τηλεφώνου[125]. Η επαύξηση της πραγματικότητας έχει γίνει δυνατή μέσω εικονικών στοιχείων όπως τα δεδομένα GPS, τα γραφικά και τον ήχο. Για να γίνει αντιληπτός ο τρόπος με τον οποίο λειτουργεί η τεχνολογία αυτή, πρέπει να αρχικά να

123 Ουσιαστικά πρόκειται για τη συγχώνευση του διαδικτύου με το φυσικό κόσμο γύρω μας, «τον αληθινό κόσμο». Πολλοί σημερινοί ερευνητές θεωρούν ότι η μοντέρνα κοινωνία «εικονικοποιείται» συνεχώς. Είναι πιο ακριβές να σημειώσει κάποιος ότι τα εικονικά δεδομένα γίνονται συνεχώς «πραγματικά», καθώς ενώνονται με τα χαρακτηριστικά και τη γεωγραφία της πραγματικότητας. Joshua Rothman, «Are We Already Living in Virtual Reality?», (2018). διαθέσιμο σε https://www.newyorker.com/magazine/2018/04/02/are-we-already-living-in-virtual-reality .

124 Η τεχνολογία της επαυξημένης πραγματικότητας αποτελεί ήδη μία αρκετά παλαιά έννοια για τους τομείς της Τεχνολογίας της Πληροφορικής και της επιστήμης των υπολογιστών. Έκανε την εμφάνισή της τη δεκαετία του 1960 και συγκεκριμένα το 1968, όταν ο Αμερικανός καθηγητής Ivan Sutherland με τη βοήθεια ενός εκ των φοιτητών του, Bob Sproull κατασκεύασαν μία συσκευή την οποία ονόμασαν Sword of Damocles (Δαμόκλειος Σπάθη). Η συσκευή αυτή θεωρείται πλέον η πρώτη συσκευή επαυξημένης πραγματικότητας, ένα πρωτότυπο αυτού που ονομάζουμε HUD (head-up display), δηλαδή μία οθόνη στο κεφάλι του χρήστη. Σε αντίθεση με τις μοντέρνες και μινιμαλιστικές συσκευές που κυκλοφορούν σήμερα, η Δαμόκλειος Σπάθη ήταν ένα μεγάλο εξάρτημα τοποθετημένο στο ταβάνι προκειμένου να στηριχθεί στο κεφάλι του χρήστη – εξ ου και η ονομασία του (βλ. σχετικά Παράρτημα Β΄). Βλ. σχετικά Alexandru Tabusca, «Augmented Reality – A Possible Game-Changer in Education», *National Strategies Observer* No.2/Vol.1 (2015).

125 Roderick O'Dorisio, «Torts in the Virtual World», 94 *Denver Law Revew* Online 1, 1 (2017).

γίνει ανάλυση του τρόπου σύνδεσης (tagging) των δεδομένων. Στην έως σήμερα επιτυχημένη τεχνολογία GPS προστέθηκε ένας άλλος τύπος παρακολούθησης δεδομένων που ονομάζεται Υπηρεσίες Αναγνώρισης (Identification Services). Η διαφορά ανάμεσα στην τεχνολογία GPS και σε αυτή των IDS είναι ότι, ενώ η πρώτη στηρίζεται σε συντεταγμένες GPS, η δεύτερη στηρίζεται σε κάποιο οπτικό ή ακουστικό σύνθημα του περιβάλλοντος, όπως ένα εμπορικό σήμα, ένα πρόσωπο (για το λογισμικό αναγνώρισης προσώπων) ή ακόμη και σε ένα ίχνος μουσικού τόνου[126]. Η παρακολούθηση - σύνδεση του κινητού (mobile tagging) είναι ένας τρόπος επίσης υπερσύνδεσης της πραγματικότητας. Αν και συνδέεται στενά με την τεχνολογία IDS, στηρίζεται σε γραμμωτούς κώδικες (barcodes) ή άλλους κωδικούς που μπορούν να διαβαστούν με ειδικά εργαλεία για να ανακαλέσουν την εικονική πληροφορία. Ιδιαίτερα οι κωδικοί QR (Quick Response) χρησιμοποιούνται περισσότερο από την τεχνολογία IDS, διότι η πληροφορία δεν παρακολουθείται από ένα οπτικό ή ακουστικό σύνθημα, αλλά έχει ενσωματωθεί στο γραμμωτό κώδικα (barcode) ή στην ίδια την εικόνα. Το mobile tagging περιέχει των κωδικό που δημιουργεί την εικονική εμπειρία, εκεί που η τεχνολογία IDS με δυσκολία αναγνωρίζει το σημείο όπου η πληροφορία παρακολουθείται. Τα δεδομένα παρακολούθησης μέσω κινητού μπορούν να είναι μία ηλεκτρονική διεύθυνση, μία σύνδεση σε ασύρματο δίκτυο, ένα ελεύθερο ηλεκτρονικό βιβλίο ή ένα σταυρόλεξο Sudoku[127].

Η τεχνολογία «Near Field Communication» είναι ακόμη μία μορφή παρακολούθησης και σύνδεσης δεδομένων, η οποία προσομοιάζει στη θεωρίας της διάχυτης χρήσης υπολογιστή (pervasive computing) και στηρίζεται σε ολοκληρωμένα κυκλώματα υπολογιστών (computer chips) που είναι ενσωματωμένα σε ένα περιβάλλον ή σε αντικείμενα που μπορούν να μεταφέρουν την πληροφορία το ένα στο άλλο, μέσω εξαιρετικά περιορισμένης εμβέλειας (ορισμένων μέτρων) ραδιοφωνικών πεδίων. Ένα

126 Marco Gruteser και Baik Hoh, «Privacy Preservation of GPS». Βλ. επίσης Tracesσε Shashi Shekhar, Hui Xiong και Xun Zhou, «Encyclopedia of GIS», Springer, Boston, MA, 2008.

127 «Facts about GPS tracking using QR codes, RFID/NFC», Bluetooth & GSM/SMS, διαθέσιμο σε https://gocodes.com/facts-about-gps-tracking-using-qr-codes-rfid-bluetooth-sms/ .

παράδειγμα τεχνολογίας NFC μπορεί να θεωρηθεί μία εφαρμογή η οποία επιτρέπει σε μία κινητή συσκευή να λειτουργήσει ως πιστωτική κάρτα και η οποία με μόνη την κίνηση δίπλα σε κάποιον δέκτη σε ένα κατάστημα, να επιτρέψει την υποκλοπή. Παρ' όλα αυτά και δεδομένου ότι η τεχνολογία αυτή απαιτεί δύο ζεύγη ενσωματωμένων κυκλωμάτων για να λειτουργήσει, είναι λιγότερο εύχρηστη μέθοδος γεωγραφικής αναζήτησης δεδομένων, σε σχέση με τα GPS, τα IDS ή το mobile tagging[128]. Η επαυξημένη πραγματικότητα και η διάχυτη χρήση υπολογιστή (PerC) διαφέρουν θεμελιωδώς στο πού βρίσκονται αποθηκευμένα και τυγχάνουν επεξεργασίας τα δεδομένα[129].

Η «απορρόφηση» του πραγματικού κόσμου μέσω της επαυξημένης πραγματικότητας αποκαλύπτει νέους τρόπους αγορών, διασκέδασης και έρευνας. Παρέχοντας την πληροφορία σε πραγματικό χρόνο στο περιβάλλον γύρω μας, τα συστήματα της επαυξημένης πραγματικότητας προσφέρουν τη δυνατότητα της καινοτόμου δέσμευσης με το περιβάλλον μας και των στιγμιαίων αλληλεπιδράσεων με τους άλλους. Ταυτόχρονα, όμως, οι ίδιες ιδιότητες που καθιστούν την επαυξημένη πραγματικότητα ελκυστική, δημιουργούν κινδύνους, κυρίως σε σχέση με την προστασία της ιδιωτικής ζωής όσων βρίσκονται πέριξ του χρήστη[130]. Προϊόντα όπως τα γυαλιά της Google[131] καθιστούν πολύ εύκολη την καταγραφή των ανθρώπων,

128 Carla Tardi, «Near-Field Communication (NFC)», (2020), διαθέσιμο σε https://www.investopedia.com/terms/n/near-field-communication-nfc.asp

129 Η διάχυτη χρήση υπολογιστή (PerC) προβλέπει την ενσωμάτωση της επεξεργασίας στα αντικείμενα γύρω από το χρήστη, στο φυσικό του περιβάλλον. Αντιθέτως, η επαυξημένη πραγματικότητα χρησιμοποιεί δεδομένα αποθηκευμένα γενικά σε ένα νέφος, αλλά στα οποία υπάρχει τοπική πρόσβαση. Τα δεδομένα είναι συνδεδεμένα με υπαρκτές τοποθεσίες, άτομα ή αντικείμενα μέσω ασύρματης σύνδεσης και υπηρεσιών. Η τεχνολογία της επαυξημένης πραγματικότητας και η χρήση υπολογιστή μέσω νέφους (cloud computing) κινούνται παράλληλα. Joshua Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal,* Vol. 27:55. (2012).

130 Andreas Kotsios, «Privacy in an Augmented Reality», *International Journal of Law and Information Technology,* Vol. 23/ 2 (2015):157-185. Βλ. επίσης Michael S. Wagner, «Google Glass: A Preemptive Look at Privacy Concerns», S. 11 *Journal on Telecommunications & High Technology Law* (2013): 477-478.

131 Τα γυαλιά της Google (Google Glass) προσφέρουν μία εμπειρία επαυξημένης πραγματικότητας, με τη χρήση οπτικοακουστικών εισόδων (inputs) βασιζόμενων στην τοποθεσία, προκειμένου να παρέχουν τη σχετική πληροφορία. Για παράδειγμα, κατά την είσοδό του σε ένα αεροδρόμιο ο χρήστης θα μπορεί αυτομάτως να δεχθεί πληροφορίες σχετικές με την πτήση του. Επίσης, οι χρήστες θα μπορούν να χειριστούν τη συσκευή με φωνητικές εντολές και με τη χρήση μίας επιφάνειας αφής (touchpad), η οποία

διακριτικά και ακατάπαυστα, χωρίς τη γνώση ή τη συναίνεσή τους. Η τεχνολογία της επαυξημένης πραγματικότητας έχει ως στόχο να επιτρέπει στους χρήστες της να συγκεντρώνουν στιγμιαία μεγάλο όγκο δεδομένων που αφορούν σε άλλα άτομα, από τη δημιουργία προφίλ στα ποινικά αρχεία, βάσει της τεχνολογίας αναγνώρισης προσώπου – κάτι που στο Ευρωπαϊκό Δίκαιο δεν επιτρέπεται[132], έως τις αγοραστικές συνήθειες των καταναλωτών[133]. Παιχνίδια όπως το Pokémon Go έχουν ήδη κατηγορηθεί για παραβίαση της οικιακής ειρήνης και της ξένης ιδιοκτησίας[134].

5.1 **Εφαρμογές της επαυξημένης πραγματικότητας**

Η Επαυξημένη Εικονικότητα αποτελεί το σημείο εκείνο όπου η πραγματικότητα αρχίζει να εισέρχεται στους εικονικούς κόσμους. Οι εικονικοί κόσμοι μπορούν να εισαγάγουν πραγματικά γεγονότα μέσα στο εικονικό περιβάλλον, ώστε να μπορούν να τα δουν οι κάτοικοι του εικονικού κόσμου[135]. Το τεύχος του Νοεμβρίου 2009 του περιοδικού Esquire παρουσίασε για πρώτη φορά ένα δείγμα της τεχνολογίας της επαυξημένης πραγματικότητας, όταν με τη χρήση κάμερας υπολογιστή ή έξυπνου

βρίσκεται στο σκελετό των γυαλιών. Το λειτουργικό σύστημα των γυαλιών της Google στηρίζεται σε μία εκδοχή Android και χρησιμοποιεί εφαρμογές που καλούνται Glassware και έχουν βελτιστοποιηθεί για τη συγκεκριμένη συσκευή. Τα γυαλιά, επίσης, έχουν αναπτύξει συνδεσιμότητα Wi-Fi και Bluetooth και περιλαμβάνουν και μία κάμερα για τη λήψη φωτογραφιών και βίντεο. Η συγκεκριμένη τεχνολογία ανακοινώθηκε από την εταιρία Google X το 2012 και άρχισε να διατίθεται για δοκιμές σε προγραμματιστές στις αρχές του 2013. Βλ. σχετικά https://internetofthingsagenda.techtarget.com και «Μαγικά γυαλιά από την Google», 2012, διαθέσιμο σε https://www.naftemporiki.gr/video/406415/magika-gualia-apo-tin-google .

132 Σύμφωνα με το άρθρο 10 του ΓΚΠΔ δεν επιτρέπεται «η επεξεργασία προσωπικών δεδομένων σχετικά με τα εξής χαρακτηριστικά ενός προσώπου: [...] προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα, εκτός αν αυτό επιτρέπεται από τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία».

133 Sharon Nakar και Dove Greenbaum, «Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy», 23 B.U. School of Law, *Journal of Science & Technology Law* 88 (2017): 93-97 .

134 Samuel Mallick, «Note, Augmenting Property Law: Applying the Right to Exclude in the Augmented Reality Universe», *Vanderbilt Journal of Entertainment and Technology Law,* Vol. 19, Issue 4, Vanderbilt University, School of Law (2017): 1057- 1065.

135 Μία δημόσια συζήτηση υποψηφίων προέδρων στον αληθινό κόσμο μπορεί να παρουσιαστεί ζωντανά στους κατοίκους του εικονικού κόσμου. Οι εικονικοί χαρακτήρες (avatars) μπορούν να παρακολουθούν γεγονότα που διαδραματίζονται στον αληθινό κόσμο, μέσα σε μία αίθουσα του εικονικού περιβάλλοντος. David Pierce, «I Watched the Debate in Virtual Reality. Things Got Weird», (2015), διαθέσιμο σε https://www.wired.com/2015/10/dnc-debate-virtual-reality-gear-vr/ .

τηλεφώνου και μέσω ειδικών ετικετών, ο χρήστης μπορούσε να διαβάσει τόσο το εξώφυλλο, όσο και διαφημίσεις στο εσωτερικό του τεύχους. Σε άλλη εφαρμογή της που ονομάζεται «Hidden Park», η επαυξημένη πραγματικότητα παρέχει τη δυνατότητα στα παιδιά να δουν σε ένα πάρκο, μέσω ενός «έξυπνου» τηλεφώνου και σε συγκεκριμένες περιοχές του πάρκου, φανταστικούς δράκους, γίγαντες και νεράιδες. Εκτός από το ότι αυτές οι εφαρμογές της επαυξημένης πραγματικότητας δημιουργούν φανταστικές δράσεις κι ευκαιρίες για παιχνίδια, παρέχουν και νέες προοπτικές ως εκπαιδευτικά εργαλεία[136]. Αυτός ο συνδυασμός εκπαίδευσης και ευχάριστης τεχνολογίας δεν είναι καινούριος. Η διαφορά σήμερα έγκειται στο ότι η χρήση φορητού υπολογιστή σε οποιαδήποτε μορφή του, σε συνδυασμό με τα δεδομένα παρακολούθησης έχουν ως αποτέλεσμα τον εμπλουτισμό των δεδομένων με εικονικές εμπειρίες, καθιστώντας τα πιο κοινωνικά και δυναμικά από τα προγενέστερα μέσα. [137]

136 Ο συνδυασμός του «wikitude», μίας από τις πιο δημοφιλείς εφαρμογές της επαυξημένης πραγματικότητας και του «Hidden Park» έχει τη δυνατότητα να εκπληρώσει το σκοπό των γονέων και των δασκάλων να μεταδώσουν τη γνώση με τρόπο διασκεδαστικό. Με αυτή την τεχνολογία, η οποία παρέχει διαδραστικές εμπειρίες, πεδία λιγότερο ευχάριστα για τους μαθητές, όπως τα μαθηματικά ή η ιστορία, παρουσιάζονται με πιο διασκεδαστικό κι επιμορφωτικό τρόπο. Τα παιδιά είναι πιο πιθανό να εκπαιδευτούν στα μαθηματικά με το μέτρημα εικονικών δεινοσαύρων στο πάρκο ή να διδαχθούν ιστορία μέσω ενός εικονικού κόσμου που τα μεταφέρει στην Αρχαία Ρώμη ή την Αρχαία Αθήνα. Χάρη στη νέα αυτή τεχνολογία, οι μαθητές των Λυκείων θα μπορούν να πραγματοποιούν εκπαιδευτικές εκδρομές στην Αρχαία Αθήνα ή στη Βοστόνη κατά την εποχή της επανάστασης, να περπατούν στην επιφάνεια του φεγγαριού ή να επιπλέουν μέσα σε ένα δυναμικό μοντέλο κυτταρικού πυρήνα. Βλ. σχετικά «Mixed Reality Education», διαθέσιμο σε https://govrpro.com/services/mixed-reality-education#:~:text=Mixed%20Reality%20Education&text=Mixed%20reality%20offers%20students%20a,concepts%20being%20taught%20to%20them.&text=Mixed%20reality%20helps%20students%20to%20grasp%20complicated%20concepts%20and%20topics%20with%20ease και «Mixed Reality in Education: boosting students' learning experience», (2017), διαθέσιμο σε https://acerforeducation.acer.com/innovative-technologies/mixed-reality-in-education-boosting-students-learning-experience/, Lucinda Kerawalla, Rosemary Luckin, Simon Seljeflot και Adrian Woolard, «Making it real: exploring the potential of augmented reality for teaching primary school science», *Virtual-Reality,* Vol. 10 (2006): 163–174 και Eleni Demitriadou, Kalliopi - Evangelia Stavroulia και Andreas Lanitis, «Comparative evaluation of virtual and augmented reality for teaching mathematics in primary education», *Education and Information Technologies,* Vol. 25, (2020): 381–401.

137 Joshua Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal,* Vol. 27:55. (2012).

5.1.1 **Μουσεία**

Ήδη πριν από την άνθηση των σύγχρονων τεχνολογιών, τα μουσεία λειτουργούσαν ως προάγγελοι της εικονικής πραγματικότητας[138]. Ιδιαίτερα σε κάποια από αυτά υπήρχαν κόμβοι που μετέφεραν τους επισκέπτες σε μια άλλη διάσταση τέχνης, ιστορικής αναδρομής ή εκπαιδευτικών ταξιδιών[139] και χώροι όπου μπορούσε κάποιος να ξεφύγει για λίγα λεπτά από την πραγματικότητα και επιστρέφοντας σε αυτή να την κατανοήσει καλύτερα[140]. Στο Μουσείο Φυσικής Ιστορίας του Λος Αντζελες υπάρχουν ήδη χρονομηχανές εικονικής πραγματικότητας. Μέσω ειδικού εξοπλισμού - κράνους, οι επισκέπτες παρατηρούν απολιθώματα να ζωντανεύουν και σκελετούς από μαμούθ να αναβιώνουν. Στο Kennedy Space Center της Φλόριντα το κοινό ταξιδεύει στο Διάστημα και συγκεκριμένα στον πλανήτη Άρη, μέσω μιας σειράς εργαλείων εικονικής πραγματικότητας[141]. Ίσως, όμως, η πιο εντυπωσιακή τάση των

138 Το μουσείο Μοντέρνας Τέχνης (MoMA) της Νέας Υόρκης και το μουσείο Τέχνης της κομητείας του Λος Άντζελες προσέφεραν ήδη από το καλοκαίρι του 2013 εφαρμογές για έξυπνα τηλέφωνα και τα ευρωπαϊκά μουσεία ακολούθησαν αντιστοίχως. Το μουσείο Centre Pompidou στο Παρίσι έχει προχωρήσει στην έκδοση μίας εφαρμογής για «έξυπνα» τηλέφωνα, η οποία επιτρέπει στο χρήστη τη μελέτη των οδηγών εκθέσεων που πωλούνται στο μουσείο. Το μουσείο Reina Sofia στη Μαδρίτη και το Hamburger Bahnhof στο Βερολίνο έχουν αναπτύξει ιστοσελίδες κι εφαρμογές σχεδιασμένες για την κινητή τεχνολογία. Βλ. σχετικά www.nytimes.com .

139 Το μουσείο Stedelijk του Άμστερνταμ ήταν ένα από τα πρώτα μουσεία στον κόσμο που έκαναν χρήση της τεχνολογίας της επαυξημένης πραγματικότητας. Οι επισκέπτες του μουσείου έχουν τη δυνατότητα να χρησιμοποιήσουν τα «έξυπνα» τηλέφωνά τους για να εμπλουτίσουν τις επισκέψεις τους Οι συσκευές αυτές έχουν την ικανότητα να αναπαράγουν το ψηφιακό περιεχόμενό τους, όπως εικόνες ή ταινίες, παράλληλα με τον αληθινό κόσμο. Οι επισκέπτες χρησιμοποιούν τις συσκευές αυτές ως φακούς, οι οποίοι τους επιτρέπουν να βλέπουν τις, κατά τα άλλα, αόρατες εικόνες. Συγκεκριμένα, όσο περιηγούνται στο εν λόγω μουσείο και απευθύνουν τις κάμερες των τηλεφώνων τους επάνω στα εκθέματα, βλέπουν σε οθόνες, αγάλματα που κινούνται ή συνεντεύξεις με τους δημιουργούς. Charlotte Coates, «Virtual Reality is a big trend in museums, but what are the best examples of museums using VR?», (2020), διαθέσιμο σε https://www.museumnext.com/article/how-museums-are-using-virtual-reality/ .

140 Έπειτα από έρευνα που έδειχνε ότι τα δύο τρίτα των νέων Αμερικανών δεν γνώριζαν τι ήταν το στρατόπεδο συγκέντρωσης του Αουσβιτς, το Μουσείο Μνήμης του Ολοκαυτώματος στις ΗΠΑ προχώρησε στην ανάπτυξη μιας προσωπικής σύνδεσης των επισκεπτών με τις οικογένειες που έχασαν τη ζωή τους κατά τη διάρκεια του Ολοκαυτώματος. Στην αίθουσα του «Πύργου των Προσώπων», οι επισκέπτες μπορούν να συνδεθούν με τα θύματα του Ολοκαυτώματος μέσω μίας εφαρμογής που τους μεταφέρει στην εποχή του Β΄ Παγκοσμίου Πολέμου. Μέσω βίντεο και διαδραστικών πληροφοριών, καταγράφεται η ζωή κάθε οικογένειας που απεικονίζεται στην αίθουσα. Βλ. σχετικά «Υιοθετώντας τα νέα εργαλεία της επαυξημένης πραγματικότητας», (2018), διαθέσιμο σε https://www.kathimerini.gr/986719/article/politismos/eikastika/yio8etwntas-ta-nea-ergaleia-ths-epay3hmenhs-pragmatikothtas.

141 Στο μουσείο μοντέρνας τέχνης του Σαν Φρανσίσκο, σε μια αναδρομική έκθεση του Ρενέ Μαγκρίτ, μέσω ενός ειδικού δωματίου επαυξημένης πραγματικότητας, οι επισκέπτες έχουν την ευκαιρία να δουν από κοντά ψηφιακές ερμηνείες του έργου του. Ειδικές οθόνες με κάμερες ανίχνευσης βάθους και κίνησης

σύγχρονων μουσείων, είναι ο συγκερασμός της τέχνης με την εικονική πραγματικότητα και η αλληλεπίδραση με το έργο του καλλιτέχνη[142].

5.1.2 Τα γυαλιά της Google[143]

Τα γυαλιά της εταιρίας Google υπήρξαν η πρώτη συσκευή η οποία αποπειράθηκε να απελευθερώσει τα δεδομένα από τους υπολογιστές και τις φορητές συσκευές, όπως τα τηλέφωνα και τα tablets και να τα τοποθετήσει στο οπτικό πεδίο του χρήστη. Μέσω μίας κάμερας, μίας οθόνης, ενός χειριστηρίου αφής, μίας μπαταρίας κι ενός μικροφώνου τοποθετημένων επί του σκελετού των γυαλιών, δίνεται η δυνατότητα στο χρήστη να παρακολουθήσει ταινίες, να φωτογραφήσει πρόσωπα και αντικείμενα, ή να κάνει αναζητήσεις και μεταφράσεις εν κινήσει. Η δυνατότητα αυτή έχει σχεδιαστεί με τέτοιο τρόπο, ώστε να μην εμποδίζει την όραση[144].

Γενικά, η τοποθέτηση των δεδομένων μέσα στο οπτικό πεδίο των χρηστών έχει προφανή πλεονεκτήματα, πολλά από τα οποία γίνονται σαφή με την τεχνολογία των γυαλιών αυτών. Οι οδηγίες γίνονται πιο αντιληπτές στο χρήστη, ο οποίος μπορεί να δει σε παρόντα χρόνο μεταφράσεις ή απομαγνητοφωνήσεις όσων έχουν ειπωθεί, ενώ παράλληλα έχει τη δυνατότητα να παρακολουθήσει και να απαντήσει σε μηνύματα, εν κινήσει και στο λεπτό. Η ενσωματωμένη κάμερα δεν χρειάζεται νέα οθόνη, καθώς καταγράφει την προοπτική του χρήστη, ως πρώτου προσώπου, επιτρέποντάς του να λαμβάνει στιγμιότυπα ή αποσπάσματα από αυτά που βλέπει. Κάθε λειτουργία που γενικά απαιτεί να έχει πρόσβαση ο χρήστης σε οθόνη, γίνεται εντός του οπτικού του

μεταφέρουν τους θεατές στα τοπία του Μαγκρίτ αψηφώντας την προοπτική, την απόσταση ή το χρόνο, καθιστώντας τον επισκέπτη μέρος του πίνακα. Ό.π. υποσημείωση 149.

142 Jeppe Ugelvig, «8 Artists Pushing the Limits of Digital Effects and VR», (2019), διαθέσιμο σε https://www.artsy.net/article/artsy-editorial-8-artists-pushing-limits-digital-effects-vr .

143 Βλ. σχετικά www.google.com/glass/start/ και https://www.iti.gr/iti/about/labs/virtual-augmented-reality.html .

144 Τα τεχνικά χαρακτηριστικά της συσκευής είναι η προβολή επί οθόνης αντίστοιχης αυτής των 25ιντσών, υψηλής ευκρίνειας, από απόσταση 2,44μέτρων (8 ποδών), σε ανάλυση 640 x 360. Βλ. σχετικά υποσημ. 144.

πεδίου. Το να μπορέσει να ελέγξει ο χρήστης τα δεδομένα απαιτεί ειδικό χειρισμό. Με ένα μικρόφωνο και ένα χειριστή αφής στο ένα βραχίονα του σκελετού, του δίνεται η δυνατότητα να επιλέξει, με μία απαλή κίνηση ή με φωνητική εντολή, τι επιθυμεί να κάνει και η συσκευή θα ερμηνεύσει τις εντολές. Τα γυαλιά επίσης παρέχουν ήχο μέσω της τεχνολογίας επαγωγής οστών (bone conduction technology)[145]. Εκτός από τη λήψη φωτογραφιών και την παρακολούθηση ταινιών, ο χρήστης μπορεί να χρησιμοποιήσει το λογισμικό για τηλεδιασκέψεις με φίλους, όπου μπορεί να τους παρουσιάσει αυτό που έχει στο οπτικό του πεδίο ή μπορεί επίσης να χρησιμοποιήσει την υπηρεσία χαρτών της Google για να λάβει κατευθυντήριες οδηγίες[146].

Σημαντικό είναι να σημειώσει κάποιος ότι όπως σε κάθε νέα τεχνολογία, έτσι και στην περίπτωση της εφαρμογής των γυαλιών της Google υπάρχει πάντα η πιθανότητα ανορθόδοξης χρήσης της. Συγκεκριμένα για τη συσκευή αυτή προκύπτει το ζήτημα της προστασίας της ιδιωτικότητας[147], αν και η κατασκευάστρια εταιρία έχει τονίσει ότι επί της ουσίας χρησιμοποιεί τη λειτουργικότητα που υπάρχει ήδη σε όλες τις φορητές συσκευές και την κάνει πιο προσιτή[148].

Παρά την αρχική ενθουσιώδη υποδοχή της εφαρμογής αυτής, η κατασκευάστρια εταιρία σταμάτησε τη μαζική παραγωγή του προϊόντος αυτού, κυρίως λόγω της χαμηλής ζήτησης και της αντίδρασης των χρηστών που τα χρησιμοποίησαν, οι οποίοι δήλωσαν ότι τους κούραζαν ή ανησυχούσαν για θέματα υγείας, ασφάλειας και

145 Η τεχνολογία αυτή προκαλεί δονήσεις στο κρανίο με στόχο την παραγωγή ήχου, με πιο τραχύ αποτέλεσμα, αλλά λιγότερο βραδυκίνητο σε σχέση με τα παραδοσιακά ακουστικά. «How do bone conduction headphones work?», (2018), διαθέσιμο σε https://www.salusuhealth.com/Pennsylvania-Ear-Institute/Events/News-Stories/How-Do-Bone-Conduction-Headphones-Work.aspx .

146 Adam M. Gershowitz, «Google Glass While Driving», *William & Mary Law School Research Paper No. 09-280,* (2014).

147 Φερενίκη Παναγοπούλου – Κουτνατζή, «Διαδίκτυο των πραγμάτων και προστασία της ιδιωτικότητας», *ΔιΜΕΕ, τ.* 3, (2014): 346-358.

148 Πολλές συζητήσεις και προβληματισμοί έχουν ήδη προκύψει αναφορικά με την καταγραφή των κινήσεών μας από τους χρήστες των γυαλιών και με την τεχνολογία αναγνώρισης προσώπων. Η κατασκευάστρια εταιρία, σε μία προσπάθεια κατευνασμού των φόβων αυτών, πληροφόρησε το κοινό ότι η ένδειξη φωτισμού στη συσκευή αποτελεί δείγμα χρήσης αυτής, είτε με καταγραφή των δεδομένων είτε με τη λήψη φωτογραφιών. J. Rivington, «Google Glass: what you need to know», TechRadar, διαθέσιμο σε https://www.techradar.com/.

προστασίας της προσωπικής ζωής[149]. Ήδη από τον Ιούλιο του 2020, η εταιρία Google επανέλαβε την προσπάθειά της να κυκλοφορήσει ευρέως για το καταναλωτικό κοινό «έξυπνα» γυαλιά, εξαγοράζοντας την εταιρία North[150], η οποία από το 2012 παρήγαγε τα γυαλιά Focals[151].

Εφαρμογές των γυαλιών της Google

Παρά την εμπορική αποτυχία της συσκευής των γυαλιών της Google, υπήρξαν σημαντικές εφαρμογές τους, οι οποίες τα κατέστησαν δημοφιλή στο ευρύ κοινό. Η εφαρμογή «Preview» παρείχε τη δυνατότητα στο χρήστη να παρακολουθήσει το διαφημιστικό (trailer) των ταινιών στον κινηματογράφο, μέσω της αφίσας που αφορούσε στη συγκεκριμένη ταινία. Η εφαρμογή αυτή ενεργοποιούνταν αποκλειστικά και μόνο μέσω της φωνητικής εντολής «ok glass, preview the movie»[152]. Ενδιαφέρουσες, όμως, υπήρξαν και οι αναφορές σχετικά με τη συμβολή της συγκεκριμένης συσκευής στο ιατρικό πεδίο[153]. Το νοσοκομείο Beth Israel

149 Βλ. σχετικά «Τίτλοι τέλους για τα έξυπνα γυαλιά της Google», (2015), διαθέσιμο σε https://www.news247.gr/technologia/titloi-teloys-gia-ta-exypna-gyalia-tis-google.6319959.html. Σύμφωνα με δημοσίευμα του Guardian, όταν έκαναν την εμφάνισή τους οι πρώτοι προβληματισμοί για τη χρήση των γυαλιών της Google επεβλήθη στην Καλιφόρνια το πρώτο πρόστιμο για οδήγηση με ταυτόχρονη χρήση της συσκευής αυτής. Συγκεκριμένα, τροχονόμος σταμάτησε οδηγό για υπερβολική ταχύτητα και όταν διεπίστωσε ότι η οδηγός φορούσε τα γυαλιά αυτά, της επέβαλε και επιπλέον πρόστιμο για παρακολούθηση βίντεο κατά την οδήγηση. Βλ. σχετικά «Γυναίκα δέχεται κλήση για οδήγηση με τα Google Glasses», (2013), διαθέσιμο σε https://www.techgear.gr/woman-gets-ticket-for-driving-with-google-glass-21910 .

150 Ιδρύθηκε στον Καναδά το 2012 κι έκτοτε παρήγαγε προϊόντα τεχνολογίας μέχρι τη συγχώνευσή της με τη Google. Βλ. σχετικά https://www.bynorth.com/

151 Τα γυαλιά Focals της North αποτελούνται από επεξεργαστή, μπαταρία και σύστημα Bluetooth στους βραχίονές τους. Ελέγχονται μέσω ενός δαχτυλιδιού (Loop) και είναι συμβατά με την εφαρμογή Alexa της Amazon. Μέσω της οθόνης τους ο χρήστης μπορεί να βλέπει ενημερώσεις ή ακόμη και να καλεί ταξί. Βλ. σχετικά «Η Google επιστρέφει στα έξυπνα γυαλιά, χρόνια μετά το Google Glass, εξαγοράζοντας τη North», (2020), διαθέσιμο σε https://www.naftemporiki.gr/story/1615173/h-google-epistrefei-sta-eksupna-gualia-xronia-meta-to-google-glass-eksagorazontas-ti-north.

152 Βλ. σχετικά «Google Glass, εκπληκτική εφαρμογή που σας δείχνει trailers ταινιών κοιτώντας απλά τις αφίσες», (2014), διαθέσιμο σε https://www.techgear.gr/google-glass-preview-21812 .

153 Η πιο προφανής ιατρική χρήση των γυαλιών είναι ότι επιτρέπει στον πάροχο της ιατρικής φροντίδας την οπτική προβολή δεδομένων ή εικόνων που αφορούν τον ασθενή κατά τη διάρκεια της αξιολόγησης, της θεραπείας και γενικά της διαδικασίας ή τη διεξαγωγή γρήγορων διαγνωστικών τεστ και έρευνας στο διαδίκτυο για κωδικούς και ορολογία. Lloyd Price, «7 ways Google Glass is revolutionising healthcare», (2020), διαθέσιμο σε https://www.healthcare.digital/single-post/2017/08/23/7-ways-Google-Glass-is-revolutionising-healthcare .

Deaconess Medical Center στη Βοστόνη των Ηνωμένων Πολιτειών, αποφάσισε να ενσωματώσει για μία δοκιμαστική περίοδο στον εξοπλισμό του Τμήματος Επειγόντων Περιστατικών τη συσκευή αυτή, με την οποία εφοδίασε τους ιατρούς κατά τη διάρκεια των εφημεριών τους στους θαλάμους των έκτακτων περιστατικών. Κάθε ιατρός, αναγνώριζε, μέσω της συσκευής, από τον πίνακα ανακοινώσεων όπου βρίσκονταν αναρτημένοι κωδικοί QR[154], το δωμάτιο του ασθενούς στο οποίο έπρεπε να κατευθυνθεί, ενώ παράλληλα του αποστέλλονταν πληροφορίες από το κέντρο ελέγχου του νοσοκομείου, σχετικά με το ιστορικό του ασθενούς. Κατά την εξέτασή του ο ιατρός είχε πρόσβαση σε κρίσιμα δεδομένα, όπως τα αποτελέσματα των εργαστηριακών του εξετάσεων. Προκειμένου να προστατευθούν προσωπικά δεδομένα των ασθενών, η συσκευή προσαρμόστηκε με τέτοιο τρόπο, ώστε να εξασφαλιστεί ότι κανένα προσωπικό δεδομένο ασθενούς δεν θα μεταφερόταν στους διακομιστές (servers) της ιδιοκτήτριας εταιρίας. Οι αντιδράσεις των ασθενών προς τους ιατρούς υπήρξαν ποικίλες, καθώς κάποιοι εμφανίστηκαν επιφυλακτικοί, ενώ οι πιο εξοικειωμένοι με την τεχνολογία έδειξαν ενδιαφέρον για τον τρόπο λειτουργίας της συσκευής. Οι ιατροί, από την πλευρά τους, βρήκαν τη συσκευή χρήσιμη, γιατί τους βοήθησε να ανταπεξέλθουν άμεσα σε κρίσιμα περιστατικά ασθενών[155].

Μία άλλη εφαρμογή της συσκευής αυτής αποτέλεσε η πειραματική χρήση της από Βρετανούς ερευνητές σε ασθενείς με τη νόσο Πάρκινσον, με στόχο τη διερεύνηση αν και σε ποιο βαθμό ήταν δυνατό να τους παρέχει βοήθεια. Οι ερευνητές της Σχολής Επιστήμης των Υπολογιστών του Πανεπιστημίου του Newcastle, με επικεφαλής τον Δρ John Vince, που έκαναν τη σχετική ανακοίνωση σε συνέδριο στον Καναδά[156]

154 Ένας κώδικας QR (quick response code) είναι ένας γραμμικός κώδικας δύο διαστάσεων που χρησιμοποιείται για την πρόσβαση σε πληροφορίες μέσω των έξυπνων τηλεφώνων. Βλ. σχετικά σε https://whatis.techtarget.com/definition/QR-code-quick-response-code.

155 Οι συσκευές δέχθηκαν και τροποποιήσεις, όπως την προσθήκη εξωτερικού ζεύγους μπαταριών, τη δυνατότητας σύζευξης με τα έξυπνα τηλέφωνα που χρησιμοποιούσε το νοσοκομείο και ενδείξεων μπαταρίας και ασύρματου, με ταυτόχρονη αύξηση της ισχύος μετάδοσης του σήματος αυτού. Στο πρόγραμμα συμμετείχαν συνολικά τέσσερις ιατροί και ακόμη δέκα εργαζόμενοι του νοσοκομείου Βλ. σχετικά «Ιατρική εξέταση με το Google Glass», (2014), διαθέσιμο σε https://www.naftemporiki.gr/story/779540/iatriki-eksetasi-me-to-google-glass .

156 CHI 2014 - Human Factors in Computing Systems.

συνεργάστηκαν με μια ομάδα ασθενών ηλικίας 46 έως 70 ετών. Το ζητούμενο της έρευνας ήταν κατά πόσο μία τέτοιου είδους συσκευή θα μπορούσε να βοηθήσει τους ασθενείς να αυτοεξυπηρετηθούν και να διατηρήσουν την αυτονομία τους. Αν ο ασθενής είναι μόνος και χάσει την ισορροπία του, κάτι σύνηθες στη νόσο αυτή, μπορεί να συνδεθεί με υπολογιστές ή κινητά τηλέφωνα, χάρη στα συνδεδεμένα στο διαδίκτυο γυαλιά. Εναλλακτικά, ο ασθενής μπορεί να καλέσει κάποιο άλλο άτομο προς βοήθεια, με φωνητική εντολή[157].

Παρά τους ελάχιστους κινδύνους που εμφανίζουν οι τεχνολογικές καινοτομίες στον ιατρικό τομέα[158], έχουν παρατηρηθεί ταυτόχρονα και σημαντικά τρωτά σημεία[159]. Στο ανωτέρω παράδειγμα του αμερικανικού νοσοκομείου, παρόλο που όσοι από το ιατρονοσηλευτικό προσωπικό χρησιμοποίησαν τα γυαλιά της Google παρατήρησαν ότι η συσκευή τους βοήθησε να επικεντρωθούν στην εργασία που πραγματοποιούσαν με τα χέρια τους, διεπίστωσαν ταυτόχρονα ότι η τεχνολογία αυτή ενείχε τον κίνδυνο της απόσπασης της προσοχής τους από το έργο τους[160], λόγω της ενασχόλησής τους με πολλές εργασίες ταυτόχρονα (multi-tasking). Όταν μία συσκευή που μπορεί να φορεθεί (wearable device) δεν χρησιμοποιείται για την αλλαγή της διαγνωστικής μεθόδου, την πραγματοποίηση χειρουργικής διαδικασίας μέσω βιντεοσκόπησης ή τη

157 Μεταξύ άλλων, τα έξυπνα γυαλιά της Google θύμιζαν στους ασθενείς να λαμβάνουν έγκαιρα τα φάρμακά τους, να καταπίνουν τακτικά το σάλιο τους (οι μύες που ελέγχουν την κατάποση μπορεί να «παγώσουν») ή να κάνουν συγκεκριμένες κινήσεις. Η εν λόγω συσκευή θα μπορούσε να χρησιμοποιηθεί πειραματικά και σε ασθενείς με άνοια και άλλες νευροεκφυλιστικές ασθένειες. Βλ. σχετικά «Google Glass puts the focus on Parkinson's», (2014), διαθέσιμο σε https://www.ncl.ac.uk/press/articles/archive/2014/04/googleglassputsthefocusonparkinsons.html

158 Όπως έχει κριθεί, οι θεραπευτικές καινοτομίες προκαλούν ελάχιστες συνέπειες [...] κι ένας ιατρός θεωρείται ότι έχει τη γνώση και τις απαραίτητες δεξιότητες για τη χρήση των καινοτομιών ανάλογα με τις συνθήκες κάθε κλινικής περίπτωσης. Βλ. σχετικά Nicolas Terry, Chad S. Priest και Paul Szotek, «Google Glass and Health Care: Initial Legal and Ethical Questions», *Indiana University Robert H. McKinney School of Law Research Paper,* (2015):20.

159 Για παράδειγμα υπάρχει το ενδεχόμενο η συγκεκριμένη συσκευή να έχει μικρής διάρκειας μπαταρία, κάτι που παρατηρήθηκε στις πρώιμες εκδοχές των Google glasses. Steve Kovach, «It Sounds Like Google Glass Will Have Awful Battery Life», (2013), διαθέσιμο σε https://www.businessinsider.com/google-glass-poor-battery-life-2013-4 .

160 Για παράδειγμα, στην υπόθεση Halamka μελετήθηκε η περίπτωση ενός πολίτη, ο οποίος απέτυχε να ολοκληρώσει μία παραγγελία φαρμάκων μέσω μίας ηλεκτρονικής φόρμας, διότι αποσπάστηκε η προσοχή του από ένα μήνυμα στην έξυπνη συσκευή που χρησιμοποιούσε. Βλ. σχετικά John Halamka, «Order Interrupted by Text: Multitasking Mishap», AHRQ Morbidity & Mortality Rounds on the Web, 2011, διαθέσιμο σε https://aornjournal.onlinelibrary.wiley.com/doi/full/10.1016/j.aorn.2013.05.013 .

φωτογράφηση ενός περιστατικού, εμφανίζει την πιθανότητα και μόνο με την ελάχιστη παρουσία μίας εικόνας στο οπτικό πεδίο του ιατρού, να αποσπάσει την προσοχή του οδηγώντας σε δυσάρεστες συνέπειες[161].

Σε συνέχεια των ανωτέρω, άλλο μείζων ζήτημα που τίθεται κατά τη χρήση των γυαλιών επαυξημένης πραγματικότητας είναι αυτό του «δόγματος της ενημερωμένης συγκατάθεσης»[162] του ασθενούς. Έχοντας υπόψη το ευρύ φάσμα των κινδύνων που αντιμετωπίζουν οι ασθενείς στα σύγχρονα περιβάλλοντα ιατρικής φροντίδας, στο αμερικανικό δίκαιο δεν απαιτείται να αποκαλύπτεται κάθε είδους κίνδυνος[163], αλλά μόνο αυτοί που είναι πιθανό να επηρεάσουν την απόφαση των ασθενών να υποβληθούν σε μία συγκεκριμένη θεραπεία ή επέμβαση[164]. Στην Ευρώπη και την Ελλάδα, υφίσταται η έννοια του θεραπευτικού προνομίου, ως περιορισμός της υποχρέωσης ενημέρωσης του ασθενούς. Σύμφωνα με αυτό, «η ενημέρωση του ασθενούς μπορεί να περιοριστεί ή και να παραλειφθεί όταν η πράξη της ενημέρωσης θα μπορούσε να προκαλέσει βλάβη στον ασθενή. Ο περιορισμός μπορεί να αναφέρεται σε κάθε έκφανση της ενημέρωσης. Συνήθως απαντάται σε σχέση με την ενημέρωση για τη διάγνωση – πρόγνωση, όταν στον ασθενή θα πρέπει να αποκαλυφθεί ότι πάσχει από μία ανίατη, θανατηφόρα ασθένεια. Αλλά μπορεί να αναφέρεται και στους τυπικούς κινδύνους και τα ρίσκα της θεραπείας». Για το

161 Στην πράξη, πολλές πρόσφατες αγωγές για ιατρική αμέλεια στηρίζουν τη βάση τους στην απόσπαση της προσοχής του ιατρικού προσωπικού στο χειρουργείο από κινητά τηλέφωνα ή άλλες ηλεκτρονικές συσκευές. Βλ. σχετικά Eric Nicholson, Dallas Anesthesiologist Being Sued Over Deadly Surgery Admits to Texting, Reading iPad During Procedures, Unfair Park: The Dallas Observer Blog (2014) διαθέσιμο σε http://blogs.dallasobserver.com/unfairpark/2014/04/dallas_anesthesiologist_cops_t.php.

162 Ο ιατρός έχει την υποχρέωση να αποκαλύψει στον ασθενή σημαντικές πληροφορίες, για τις οποίες γνωρίζει ή όφειλε να γνωρίζει ότι θα ήταν κρίσιμες για ένα μέσο άνθρωπο στη θέση του ασθενή, προκειμένου αυτός να αποφασίσει για το εάν θα υποβληθεί σε μία συγκεκριμένη ιατρική θεραπεία ή διαδικασία. Βλ. σχετικά Μαρία Κανελλοπούλου - Μπότη, «Ιατρική ευθύνη για μη ενημέρωση ή πλημμελή ενημέρωση του ασθενούς κατά το ελληνικό και το αγγλοσαξωνικό δίκαιο», Σάκκουλας, (1999).

163 Το Ανώτατο Δικαστήριο του Rhode Island επεσήμανε δύο παράγοντες που καθορίζουν τη σημαντικότητα του κινδύνου: τη βαρύτητά του και την πιθανότητα να συμβεί. Βλ. σχετικά δικαστική απόφαση *Wilkinson v. Vesey,* 295 A.2d 676, 689 (R.I. 1972), διαθέσιμη σε https://www.courtlistener.com/opinion/2351299/wilkinson-v-vesey/.

164 Βλ. σχετικά Ζήσης Δουγαλής, «Ενημέρωση και συναίνεση του ασθενούς: Πότε δεν απαιτείται – Δικαίωμα μη γνώσης», (2016), σε πρακτικά συνεδρίου «Τα νέα φάρμακα στην τεχνολογία», Άγιος Σάββας (υπό έκδοση).

αμερικανικό δίκαιο, η χρήση των γυαλιών της Google θεωρείται ότι δεν αποτελεί ένα σημαντικό κίνδυνο για τον ασθενή, ώστε να απαιτείται πρόσθετη συγκατάθεση[165], αν και η χρήση οποιασδήποτε νέας τεχνολογίας στο χειρουργείο ως «χειρουργικό παρεπόμενο»[166] μπορεί να απαιτεί πρόσθετη ενημέρωση κινδύνου. Μία άλλη προβληματική εφαρμογή της συσκευής αυτής στον ιατρικό τομέα είναι τα θέματα εγγραφής και αναμετάδοσης. Τα γυαλιά αυτά έχουν την ικανότητα να μεταφέρουν «εξωτερικούς παρατηρητές» μέσα σε ένα εξεταστήριο ή στο χειρουργείο, είτε σε πραγματικό χρόνο είτε μέσω καταγεγραμμένων φωτογραφιών και βίντεο. Εάν οι εγγραφές αυτές έχουν ως στόχο τη διδασκαλία, τότε τα γυαλιά αυτά μπορεί να οδηγήσουν στη βελτιστοποίηση της χειρουργικής εκπαίδευσης[167]. Αν και είναι δεοντολογικά ορθό να βιντεοσκοπούνται και να μεταδίδονται οι ιατρικές διαδικασίες, όταν έχουν ως στόχο την προώθηση νόμιμων εκπαιδευτικών μεθόδων, πρέπει ταυτόχρονα η αναμετάδοση αυτή να υπόκειται σε δεοντολογικούς και νομικούς περιορισμούς[168]. Συγκεκριμένα, δεν επιτρέπεται η λήψη φωτογραφιών που λαμβάνονται χωρίς την εξουσιοδότηση των ασθενών, τόσο στην Ευρώπη[169], όσο και στις ΗΠΑ[170]. Ο ΓΚΠΔ στην παράγραφο 2 του άρθρου 9 παρέχει κατευθύνσεις ως

165 Σε αντίθεση με άλλες σημαντικές καινοτομίες που εμφανίζονται καθημερινά στη βιομηχανία της υγειονομικής περίθαλψης, οι κίνδυνοι από τη χρήση των γυαλιών φαίνεται να είναι υποδεέστεροι σε σημασία. Επιπλέον, η συσκευή αυτή θα μπορούσε να αντικαταστήσει πιθανές επισφαλείς τεχνικές, όπως την απομάκρυνση από τον ασθενή για να μελετηθεί μία εικόνα σε έναν υπολογιστή ή σε μία φωτιζόμενη επιφάνεια – τραπέζι (a light table). Βλ. σχετικά Nicolas Terry, Chad S. Priest και Paul Szotek, «Google Glass and Health Care: Initial Legal and Ethical Questions», *Indiana University Robert H. McKinney School of Law Research Paper,* (2015):20.

166 Η χρήση κάθε νέας χειρουργικής τεχνικής.

167 Το Μάιο του 2014, 13.000 φοιτητές από 115 χώρες παρακολούθησαν μία χειρουργική επέμβαση που πραγματοποιήθηκε από τον Δρ. Shafi Ahmed, χειρουργό στο Βασιλικό Νοσοκομείο του Λονδίνου. Βλ. σχετικά Rebecca Smith, «First Operation Streamed Live with Surgeon Wearing Google Glass», 2014, διαθέσιμο σε www.telegraph.co.uk/health/healthnews/10851116/First-operation-streamed-livewith-surgeon-wearing-Google-glass.html.

168 Βλ. Nicolas P. Terry, «Physicians and Patients Who Friend or Tweet: Constructing a Legal Framework for Social Networking in a Highly Regulated Domain», *43 Indiana Law Review 285,* (2010):301-05.

169 Το γραφείο της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κυπριακής Δημοκρατίας επέβαλε πρόστιμο δεκατεσσάρων χιλιάδων ευρώ σε ιατρό, έπειτα από καταγγελία για παράνομη επεξεργασία προσωπικών δεδομένων ασθενούς, μέσω της βιντεοσκόπησης χειρουργικής επέμβασης και ανάρτησής της σε μέσο κοινωνικής δικτύωσης. Βλ. σχετική από 6 Σεπτεμβρίου 2019 απόφαση της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κυπριακής Δημοκρατίας.

170 Βλ. σχετικά δικαστική απόφαση του Ανωτάτου Δικαστηρίου του Maine, *Estate of Berthiaume vs. Pratt*, 365 A.2d 792 (Me. 1976) περί φωτογράφησης ασθενούς από ιατρό, χωρίς τη συγκατάθεση του πρώτου, διαθέσιμη σε https://law.justia.com/cases/maine/supreme-court/1976/365-a-2d-792-0.html. Βλ. επίσης το

προς την κατ' εξαίρεση επεξεργασία δεδομένων υγείας[171] και ο ελληνικός εφαρμοστικός νόμος 4624/2019, στο άρθρο 22, εξειδικεύει τις διατάξεις του Γενικού Κανονισμού. Σε αντίστοιχες οδηγίες έχει προχωρήσει και η Αμερικανική Ιατρική Ένωση[172]. Κατά συνέπεια, η συσκευή των γυαλιών της Google για να γίνει επίσημα αποδεκτή από τα νοσηλευτικά ιδρύματα χρειάζεται να αναβαθμιστεί ως προς τα πρωτόκολλα ασφάλειας και ιδιωτικότητάς της. Μέχρι να επιτευχθεί αυτό, τα ιδρύματα αυτά έχουν κάθε λόγο να είναι επιφυλακτικά απέναντι σε οποιαδήποτε μη εγκεκριμένη συσκευή που έχει πρόσβαση σε προσωπικά δεδομένα και στο διαδίκτυο. Και όσο οι πάροχοι και τα νοσοκομεία διαχειρίζονται την ενσωμάτωση τέτοιου είδους τεχνολογιών σε ροές εργασίας και μοντέλα ρυθμιστικά ή διαχείρισης κινδύνων, είναι σημαντικό ν΄ αναγνωρίσει κανείς ότι τα γυαλιά της Google και άλλες πρώτης γενιάς συσκευές που μπορούν να φορεθούν είναι «πρώιμα ακατέργαστα πρωτότυπα των πιο ενδιαφερουσών και χρήσιμων συσκευών που θα χρησιμοποιούνται ευρέως μέχρι το 2025»[173].

Γενικά, το Ευρωπαϊκό νομοθετικό πλαίσιο διασφαλίζει την ασφάλεια και την αποτελεσματικότητα των ιατρικών συσκευών και διευκολύνει την πρόσβαση των ασθενών στις συσκευές αυτές στην Ευρωπαϊκή αγορά[174]. Προκειμένου να συμβαδίσει με τις καινοτομίες στην επιστήμη και την τεχνολογία σχετικά με τις ιατρικές

συμβιβασμό του νοσοκομείου John Hopkins, έπειτα από ισχυρισμούς ότι ιατρός είχε καταγράψει κρυφά γυναικολογικές εξετάσεις, Matt Pearce, «Johns Hopkins Gynecologist with Camera: Victims to Get $190 Million», 2014, διαθέσιμο σε www.latimes.com/nation/nationnow/la-na-nn-johns-hopkins-gynecologist-photos-settlement-20140721-story.html.

171 Σε εφαρμογή του ΓΚΠΔ ο ΙΣΑ έχει προχωρήσει σε ειδικές ενημερωτικές οδηγίες ως προς την προστασία των δεδομένων υγείας. Βλ. σχετικά https://www.isathens.gr/plirofories-gdpr .

172 AMA, Γνώμη 5.0591—Patient Privacy and Outside Observers to the Clinical Encounter, 2014, διαθέσιμη σε www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion50591.page και AMA, Γνώμη 5.046—Filming Patients for the Education of Health Professionals § 1, 2014, www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5046.page.

173 Janna Anderson και Lee Rainie, «The Internet of Things Will Thrive by 2025», (2014), Pew Reserch Center, Internet and Technology, διαθέσιμο σε www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

174 Βλ. σχετικά «Public Health, Medical Devices – Sector, Overview», διαθέσιμο σε https://ec.europa.eu/health/md_sector/overview_en .

συσκευές, το 2017 δύο νέοι Κανονισμοί[175] αντικατέστησαν τις υπάρχουσες έως τότε Οδηγίες[176]. Στο πλαίσιο αυτό και στην ίδια λογική με τη συσκευή των γυαλιών της Google, παρουσιάστηκε στην Ευρώπη η εφαρμογή Vostars (Video and Optical See-Through Augmented RealitySurgical Systems). Στόχος της εφαρμογής αυτής είναι η ανάπτυξη ενός εργαλείου βασισμένου στην τεχνολογία της επαυξημένης πραγματικότητας, το οποίο συνδράμει τους χειρουργούς στην πρακτική σύνθετων χειρουργικών μεθόδων. Πρόκειται για έργο του Ευρωπαϊκού προγράμματος Horizon 2020, με το Πανεπιστήμιο της Πίζα να ηγείται, και να έχει την ευθύνη για την ανάπτυξη του λογισμικού και το σχεδιασμό της συσκευής βάσει των χειρουργικών αναγκών. Στο πλαίσιο του προγράμματος θα πραγματοποιηθούν τρεις κλινικές δοκιμές, οι δύο στην Ιταλία και η μία στη Γερμανία[177].

5.1.3 **PokemonGo**

Όπως ήδη αναλυτικά περιγράφηκε, η επαύξηση της πραγματικότητας αποτελεί έναν ιδιαίτερα ανερχόμενο τομέα δραστηριοποίησης σε παγκόσμιο επίπεδο, καθώς

175 α) Κανονισμός (ΕΕ) 2017/745 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Απριλίου 2017 για τα ιατροτεχνολογικά προϊόντα, για την τροποποίηση της οδηγίας 2001/83/ΕΚ, του κανονισμού (ΕΚ) αριθ. 178/2002 και του κανονισμού (ΕΚ) αριθ. 1223/2009 και για την κατάργηση των οδηγιών του Συμβουλίου 90/385/ΕΟΚ και 93/42/ΕΟΚ και β) Κανονισμός (ΕΕ) 2017/746 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Απριλίου 2017 για τα in vitro διαγνωστικά ιατροτεχνολογικά προϊόντα και για την κατάργηση της οδηγίας 98/79/ΕΚ και της απόφασης 2010/227/ΕΕ της Επιτροπής

176 α) Οδηγία 90/385/ΕΟΚ του Συμβουλίου της 20ής Ιουνίου 1990 για την προσέγγιση των νομοθεσιών των κρατών μελών σχετικά με τα ενεργά εμφυτεύσιμα ιατρικά βοηθήματα, β), Οδηγία 93/42/ΕΟΚ του Συμβουλίου της 14ης Ιουνίου 1993 περί των ιατροτεχνολογικών προϊόντων και γ) Οδηγία 98/79/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Οκτωβρίου 1998 για τα ιατροτεχνολογικά βοηθήματα που χρησιμοποιούνται στη διάγνωση in vitro.
Πλέον από τον Απρίλιο 2020 ισχύει ο Κανονισμός (ΕΕ) 2020/561 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Απριλίου 2020 για την τροποποίηση του κανονισμού (ΕΕ) 2017/745 για τα ιατροτεχνολογικά προϊόντα, όσον αφορά τις ημερομηνίες εφαρμογής ορισμένων διατάξεών του. Με τον Κανονισμό αυτό τροποποιείται η ημερομηνία εφαρμογής των περισσοτέρων διατάξεων του Κανονισμού (ΕΕ) 2017/745 μέχρι την 26η Μαΐου 2021, ώστε οι εμπλεκόμενοι φορείς να εστιάσουν στα θέματα που άπτονται της πανδημίας του Κορωνοϊού.

177 Πρόκειται για μία συσκευή που μπορεί να φορεθεί, στόχος της οποίας είναι να παρέχει «χειρουργική πλοήγηση» απευθείας στα μάτια του χειρουργού, χρησιμοποιώντας τα δύο βασικά χαρακτηριστικά της επαυξημένης πραγματικότητας, την όραση μέσω βίντεο και την όραση μέσω των ματιών. Βλ. σχετικά «Augmented reality: the future of surgery», (2019), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/blogposts/augmented-reality-future-surgery .

χρησιμοποιείται, εκτός από τους ερευνητικούς σκοπούς και για την υλοποίηση διαφημίσεων και παιχνιδιών. Στη χώρα μας η τεχνολογία αυτή έγινε γνωστή στο μέσο χρήστη μέσω του παιχνιδιού «Pokémon Go»[178]. Η δημιουργός εταιρία παρήγαγε ένα παιχνίδι επαυξημένης πραγματικότητας βασισμένο στους χαρακτήρες των παιχνιδιών και ταινιών κινουμένων σχεδίων Pokemon, χαρακτήρων γνωστών σε μικρούς και μεγάλους, πράγμα που συνετέλεσε στη μαζική εγκατάσταση του σε κινητές συσκευές σε όλο τον κόσμο[179]. Η εφαρμογή αυτή, η οποία δημιουργήθηκε για «έξυπνα» τηλέφωνα (smartphones), ουσιαστικά τοποθετεί τον ψηφιακό χαρακτήρα του χρήστη (avatar) σε ένα χάρτη βάσει της τοποθεσίας του. Μόνο που αντί για εστιατόρια και ιστότοπους που αναδεικνύουν άλλες εφαρμογές της επαυξημένης πραγματικότητας, όπως το Monocle της Yelp, χρησιμοποιεί την τεχνολογία επαυξημένης πραγματικότητας για να αποκαλύψει εικονικά γυμναστήρια που ονομάζονται Pokéstops. [180].

178 David Streitfeld, «Chasing Pokémon, a Baby Step Toward Virtual Reality», (2016) διαθέσιμο σε https://www.nytimes.com/2016/07/22/technology/personaltech/chasing-pokemon-a-baby-step-toward-virtual-reality.html

179 Το «Pokémon Go» βασίζεται στην πλατφόρμα Google Maps και εντοπίζει τη θέση του χρήστη σε σχέση με κάποια ψηφιακά σημεία ενδιαφέροντος. Όταν ο χρήστης εισέλθει σε μια περιοχή στην οποία το σύστημα του παιχνιδιού έχει τοποθετήσει χαρακτήρες Pokémon, τότε αυτός ειδοποιείται και ενεργοποιείται η κάμερα βίντεο της συσκευής του, προβάλλοντας και συνθέτοντας τους χαρακτήρες του παιχνιδιού με τον πραγματικό χώρο στην οθόνη. Καθώς χρησιμοποιείται η πυξίδα, αλλά και το ψηφιακό γωνιόμετρο της συσκευής, ο χαρακτήρας φαίνεται να ακουμπά επάνω σε επιφάνειες οριζόντια και ο χρήστης, αν περιστραφεί στο χώρο, ειδοποιείται με βελάκια πως πρέπει να γυρίσει το κινητό του σε συγκεκριμένη διεύθυνση προκειμένου να εντοπίσει το χαρακτήρα. Ο επίδοξος παίκτης που επιθυμεί να ολοκληρώσει το παιχνίδι, μπορεί με έρευνα σχετικά με τη λειτουργία της εφαρμογής να κατανοήσει πώς θα μπορέσει να βρει τα Pokémon, ώστε να συμπληρώσει τη συλλογή του. Βλ. σχετικά «Από το Pokemon GO στην επαυξημένη πραγματικότητα», διαθέσιμο σε www.nooz.gr

180 Στα Pokéstops, ο χρήστης έχει τη δυνατότητα να συμμετάσχει σε ομάδες, εφόσον φτάσει στο επίπεδο πέντε (5) του παιχνιδιού, μπορεί να ανακαλύψει τα Pokéballs και να εκπαιδεύσει πλάσματα, τα Pokémon, τα οποία μπορεί να πιάσει σύροντας προς τα πάνω τους Pokéballs. Βλ. σχετικά Justin Sablich, «Let Pokémon Go Be Your Tour Guide», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/13/travel/pokemon-go-nyc-tourism.html.

Οφέλη, κίνδυνοι κι ερωτηματικά από τη χρήση της εφαρμογής Pokémon Go.

Η φρενίτιδα που προέκυψε με την εφαρμογή Pokémon Go ήγειρε διάφορα ζητήματα, πρακτικής και νομικής φύσεως. Κι επειδή και η αρνητική δημοσιότητα δεν παύει να αποτελεί δημοσιότητα, η δημοφιλία του παιχνιδιού έγκειτο σε μεγάλο βαθμό στα θέματα ασφαλείας που προέκυψαν κατά την περιήγηση των παικτών στο περιβάλλον δράσης του παιχνιδιού[181]. Αυτά τα περιστατικά οδήγησαν το Αμερικανικό Εθνικό Συμβούλιο Ασφαλείας στο να προειδοποιήσει τους παίκτες ώστε να θέσουν ως προτεραιότητα την ασφάλειά τους πάνω από τη βαθμολογία του παιχνιδιού, πριν χαθεί κάποια ζωή. Επίσης, προειδοποιήσεις εξέδωσαν και οι αμερικανικές Δημοτικές υπηρεσίες μέσω των μέσων κοινωνικής δικτύωσης, αλλά και κάποιοι σταθμοί μέσων μαζικής μεταφοράς, οι οποίοι προέβαλλαν προειδοποιητικές ανακοινώσεις κατά τη διάρκεια διάβασης των παικτών από πλατφόρμες με πολυκοσμία. Ως προς την ασφάλεια των ανηλίκων κατά την περιήγησή τους, οι γονείς έθεσαν όρια στην κυκλοφορία των δεκάχρονων παιδιών τους, τα οποία περνούσαν την ημέρα τους περιπλανώμενα στις γειτονιές της πόλης τους. Από την πλευρά της, η εταιρία που παρήγαγε το παιχνίδι δήλωσε ότι πρόθεσή της ήταν να δημιουργηθεί ένα ασφαλές, για τους παίκτες, περιβάλλον δράσης και ότι το παιχνίδι το ίδιο φροντίζει για την ασφάλεια του χρήστη, καθώς τον ενημερώνει, κατά την εγκατάστασή του, για τον περιβάλλοντα χώρο του[182].

181 Στις ΗΠΑ υπήρξαν, αφενός μεν αναφορές για απορροφημένους παίκτες που ενεπλάκησαν σε μία σειρά ατυχημάτων, τόσο πεζή, όσο και με οχήματα, αφετέρου δε καταγγελίες για επιθέσεις ή κλοπές κατά τη διάρκεια του παιχνιδιού, παρότι δεν ήταν πάντα ξεκάθαρη η σύνδεση της χρήσης της εφαρμογής με τα φαινόμενα βίας κατά των παικτών. Στην πολιτεία του Μισούρι, διαρρήκτες χρησιμοποίησαν τα γεωδεδομένα της εφαρμογής για να επιτεθούν σε παίκτες σε απομονωμένες τοποθεσίες. Zoë Bernard, «Maybe you shouldn't catch 'em all — A new study links 'Pokémon Go' to traffic deaths, injuries, and vehicle damage», (2017), διαθέσιμο σε https://www.businessinsider.com/pokemon-go-linked-to-traffic-deaths-accidents-and-hundreds-of-thousands-of-dollars-in-vehicular-damage-2017-11 .

182 Jonathan Soble, «Driver in Japan Playing Pokémon Go Kills Pedestrian», (2016), διαθέσιμο σε https://www.nytimes.com/2016/08/26/business/japan-driver-pokemon-go-kills-pedestrian.html. Ειδικά για την προστασία της ιδιωτικής ζωής Βλ. Laura Hudson, «How to Protect Privacy While Using Pokémon Go and Other Apps», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/14/technology/personaltech/how-to-protect-privacy-while-using-pokemon-go-and-other-apps.html .

Καθώς το Pokémon Go συγκέντρωσε ορδές παικτών από τη στιγμή της πρώτης του εμφάνισης, ήγειρε ανησυχίες σχετικά με το πόσο ευάλωτα είναι τα προσωπικά δεδομένα των χρηστών από τη συμμετοχή τους σε τέτοιου είδους εφαρμογές. Bloggers που ασχολούνται με την ασφάλεια στο διαδίκτυο παρατήρησαν ότι το συγκεκριμένο παιχνίδι, το οποίο είναι ελεύθερο στη χρήση, ζητούσε την άδεια να χρησιμοποιήσει, όχι μόνο την κάμερα και τα δεδομένα τοποθεσίας του τηλεφώνου του παίκτη, αλλά και να αποκτήσει πλήρη πρόσβαση στους λογαριασμούς Google, συμπεριλαμβανομένων των ηλεκτρονικών διευθύνσεων, των ημερολογίων, των φωτογραφιών, των αποθηκευμένων εγγράφων και κάθε άλλου σχετικού δεδομένου[183].

Κάθε επιτυχημένο διαδικτυακό παιχνίδι δίνει στους παίκτες του την ευκαιρία να αγοράσουν εικονικά αντικείμενα σε χαμηλές τιμές, για να επιταχύνουν την πρόοδο του παιχνιδιού[184]. Εν προκειμένω, καθώς το Pokémon Go κινήθηκε στην επαυξημένη πραγματικότητα, αν και παρείχετο δωρεάν στο χρήστη, η παραγωγός εταιρία απέκτησε μία ιδιαίτερα ενδιαφέρουσα δυνατότητα κέρδους, δίνοντας την ευκαιρία σε εστιατόρια, καφετέριες και άλλα καταστήματα λιανικής πώλησης, να γίνουν επί πληρωμή σπόνσορες του παιχνιδιού, στους οποίους θα οδηγούνταν οι παίκτες προκειμένου να αποκτήσουν εικονικά λάφυρα[185].

183 Οι κριτικοί του παιχνιδιού σύντομα το χαρακτήρισαν ως ένα τεράστιο ρίσκο ασφαλείας, το οποίο εισβάλλει στον ιδιωτικό χώρο των ατόμων. Η παραγωγός εταιρία απολογήθηκε ότι τα αιτήματα των αδειών δεν θα έπρεπε να είναι τόσο εκτεταμένα και ότι το Pokémon Go ουδέποτε χρησιμοποίησε από τους λογαριασμούς των παικτών άλλα δεδομένα, πλην των βασικών πληροφοριών του προφίλ της Google. Δήλωσε επίσης ότι επρόκειτο να ετοιμάσει μία διορθωμένη έκδοση της εφαρμογής που θα μετέβαλλε τα αιτήματα στο επίπεδο που οι άδειες θα ήταν σε συμφωνία με τα δεδομένα, στα οποία έχει πραγματικά πρόσβαση η εφαρμογή. «Pokemon Go Privacy Concerns», διαθέσιμο σε https://www.privacytrust.com/blog/pokemon-go-privacy-concerns.html .

184 Ο Jan Dawson, ένας αναλυτής τεχνολογιών στο ερευνητικό κέντρο Jackdaw, ανέφερε ότι «η επιτυχία του Pokémon Go ήταν μία πολύ σημαντική στιγμή για την επαυξημένη πραγματικότητα, κυρίως επειδή δεν απαιτείται επιπλέον εξοπλισμός, όπως για παράδειγμα ακουστικά ή κάθε άλλου είδους ακριβά αξεσουάρ, τα οποία είναι συχνά απαραίτητα για τα παιχνίδια εικονικής πραγματικότητας». Nick Wingfield και Mike Isaac, «Pokémon Go Brings Augmented Reality to a Mass Audience», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/12/technology/pokemon-go-brings-augmented-reality-to-a-mass-audience.html .

185 Η εφαρμογή, αν και ελεύθερη, με τις δυνατότητες αγορών που προσέφερε στους χρήστες της συνεισέφερε περισσότερο από 200εκ δολάρια στα παγκόσμια έσοδα κατά τον πρώτο μήνα παρουσίας της. Στις αρχές του 2017, τα συνολικά παγκόσμια έσοδα από το Pokemon GO υπερέβησαν το 1 δισεκατομμύριο δολάρια. Από μόνη της η εφαρμογή αντιπροσώπευε το 47% της αγοράς των παιχνιδιών

Ανεξάρτητα, πάντως, από τα ανωτέρω ζητήματα, οι χρήστες δήλωσαν ότι το «κυνήγι» των Pokémon θα μπορούσε να εξελιχθεί σε έναν πολύ ενδιαφέροντα τρόπο περιήγησης στην πόλη. Σε αντίθεση με άλλα διαδικτυακά παιχνίδια, τα οποία γίνονται δημοφιλή σε πολύ σύντομο χρονικό διάστημα, «φυλακίζοντας» τους παίκτες τους στα σπίτια τους για ημέρες, το Pokémon Go, από τη στιγμή που εμφανίστηκε, οδήγησε τους ανθρώπους στους δρόμους και τα πάρκα, σε παραλίες και στις θάλασσες[186][187]. Επιπλέον, το Pokémon Go αποδείχθηκε τελικά ένας σημαντικός νέος σύμμαχος για τους γονείς που αναζητούσαν έναν τρόπο να κατευθύνουν τα παιδιά τους μακριά από τον καναπέ του σπιτιού[188]. Οι μαρτυρίες των γονιών υπήρξαν καταλυτικές, κυρίως όταν πολλοί δήλωσαν ότι ανακάλυψαν μαζί με τα δεκάχρονα παιδιά τους ότι το να παίζει κάποιος Pokémon Go δεν είναι καθόλου στατικό (οι εκπαιδευτές Pokémon πρέπει να αναζητούν εικονικούς χαρακτήρες, κάτι που απαιτεί δράση, εγρήγορση και περιήγηση στο εξωτερικό περιβάλλον). Άλλοι γονείς σημείωναν ότι τα παιδιά και οι φίλοι τους χρειάστηκε να περπατήσουν και να

των ΗΠΑ ήδη τέσσερις ημέρες από την παρουσίασή της. Μέσα σε δύο εβδομάδες το παιχνίδι ξεπέρασε διεθνώς τις 30 εκατομμύρια λήψεις (downloads) και από το Νοέμβριο του 2017, ο αριθμός των λήψεων έφτασε περίπου τα 750 εκατομμύρια. Με μέτρο τους ενεργούς χρήστες ανά ημέρα, στο μέγιστο αριθμό τους, το Pokemon GO είναι το πιο δημοφιλές παιχνίδι για έξυπνα τηλέφωνα στην ιστορία των ΗΠΑ. Sara Gold, «When Pokémon GO(es) Too Far: Augmented Reality and Tort Law», *Whittier Law Review,* Vol. 38, (2018).

186 Το παιχνίδι αυτό, όπως αναφέρθηκε ανωτέρω, χρησιμοποιεί ένα συνδυασμό συνηθισμένων τεχνολογιών που υπάρχουν σε ένα έξυπνο τηλέφωνο (smartphone), όπως οι κάμερες και οι τεχνολογίες εντοπισμού θέσης (πχ GPS), για να ενθαρρύνει τους χρήστες να επισκεφθούν δημόσιους χώρους, αναζητώντας εικονικά λάφυρα και συλλέξιμους χαρακτήρες. Peter Clark, «Pokemon Go Creator on Augmented Reality's Massive Potential», (2019), διαθέσιμο σε https://variety.com/2019/gaming/features/pokemon-go-creator-on-augmented-realitys-massive-potential-1203169992/ .

187 Ο Boon Sheridan, κάτοικος της περιοχής Holyoke, έζησε τη δραστηριότητα αυτή από πολύ κοντά. Η οικία του, η οποία στο παρελθόν ήταν μία εκκλησία με κορυφή – αέτωμα που συγκέντρωνε προσκυνητές, έγινε, χωρίς να το γνωρίζει, ένα σημείο στάσης το παιχνιδιού – Pokestop, το μέρος όπου οι παίκτες, όταν φτάνουν στο επίπεδο πέντε, πρέπει να οδηγηθούν για να εκπαιδεύσουν τους χαρακτήρες τους. Όσο το παιχνίδι εξελισσόταν στην πιο δημοφιλή εφαρμογή, προέκυψε η ανάγκη να αιτιολογήσει στους περίοικους το λόγο της συγκέντρωσης πλήθους ατόμων στην περιοχή σε παράξενες ώρες. N. Wingfield και M. Isaac, «Pokémon Go Brings Augmented Reality to a Mass Audience», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/12/technology/pokemon-go-brings-augmented-reality-to-a-mass-audience.html.

188 Σε αντίθεση με τα περισσότερα διαδικτυακά παιχνίδια και παιχνίδια έξυπνων τηλεφώνων (Smartphone), το εξαιρετικά δημοφιλές Pokémon Go με εκατομμύρια χρήστες, απαιτεί από τον παίκτη να είναι ενεργός και δραστήριος. Η εφαρμογή χρησιμοποιεί τεχνολογία χαρτών και τοπικά ορόσημα, στα οποία τοποθετεί μυθικούς χαρακτήρες κινουμένων σχεδίων. Peter Clark, «Pokemon Go Creator on Augmented Reality's Massive Potential», (2019), διαθέσιμο σε https://variety.com/2019/gaming/features/pokemon-go-creator-on-augmented-realitys-massive-potential-1203169992/ .

ποδηλατήσουν με ευχαρίστηση κατά τη διάρκεια του παιχνιδιού, για πολλά χιλιόμετρα, σε συνθήκες ζέστης ή βροχής ή ότι μέρος της ευχαρίστησής τους ήταν ότι τα παιδιά απομακρύνθηκαν δελεαστικά από την Κυριακάτικη απογευματινή συνήθειά τους να παίζουν Wii[189]. Εξίσου σημαντικό, όμως, ήταν ότι πέρα από τις ιστορίες των «απολεσθέντων θερμίδων», κατά τη διάρκεια του παιχνιδιού προέκυψαν και απρόσμενα οφέλη για τις οικογένειες από το χρόνο που αξιοποίησαν μαζί τα μέλη τους. Η φύση του παιχνιδιού, με το κυνήγι των εικονικών πλασμάτων, σε συνδυασμό με την περιήγηση και τους περιπάτους στον πραγματικό κόσμο, φαίνεται ότι κατέστησαν ανούσιο το παιχνίδι κατά μόνας και οι έφηβοι προσκάλεσαν σε παιχνίδι τους γονείς και τα αδέλφια τους. Προσθέτοντας ότι τα Pokéstops υπήρξαν σημεία συνάντησης και άλλων παικτών, το παιχνίδι πήρε την έκταση μιας κοινωνικής εκδήλωσης. Η εφαρμογή φαίνεται ότι προσέδωσε νέα χρήση στην τεχνολογία των «έξυπνων» τηλεφώνων, η οποία προσέφερε διέξοδο στους φόβους των χρηστών των νέων τεχνολογιών ότι γίνονται στατικοί ή ότι συνδέονται περισσότερο με τα clouds, παρά με τις κοινωνικές επαφές τους. Υπήρξε μία ευφορία κατά τη διάρκεια του παιχνιδιού, η οποία ήταν μοναδική[190].

Αν και οι οικογένειες εξεπλάγησαν ευχάριστα από τη δράση και την αλληλεπίδραση του παιχνιδιού, προέκυψε το ζήτημα εάν θα μπορούσαν να εφαρμοστούν και στο παιχνίδι αυτό οι καθημερινές τους συνήθειες ως προς τη διάρκεια χρήσης του υπολογιστή. Επίσης, τέθηκε το ερώτημα εάν τα χιλιόμετρα που διανύθηκαν και ο κοινός χρόνος που αξιοποιήθηκε από την οικογένεια, καθιστούν το Pokémon Go διαφορετικό από τις άλλες ενέργειες που αποσπούν την προσοχή των χρηστών και στηρίζονται σε μία οθόνη[191]. Για κάποιες οικογένειες, το κυνήγι των Pokémon είχε

189 Kj. Dell' Antonia, «Pokémon Has Kids on the Move - and on their Phones», (2016), διαθέσιμο σε https://well.blogs.nytimes.com/2016/07/12/pokemon-has-children-on-the-move/?mtrref=www.google.com&gwh=33F88D0A1D440BBA2F5216E19A7A00FC&gwt=pay&assetType=REGIWALL.

190 Jonah Engel Bromwich, «Where Pokémon Should Not Go», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/13/technology/where-pokemon-should-not-go.html?searchResultPosition=1.

191 Το μέσο Αμερικανόπουλο ήδη καταναλώνει περισσότερο χρόνο μπροστά σε μία οθόνη, από ό,τι στο σχολείο. Και για τους ενήλικες τα στατιστικά είναι παραπλήσια. Σε μία έρευνα που έγινε, το 70% των

ήδη ξεκινήσει να υποκαθιστά τα ταξίδια τους[192]. Και πραγματικά η εφαρμογή αυτή παρότρυνε τα παιδιά να περπατήσουν και να κάνουν περισσότερο ποδήλατο, αλλά το ερώτημα παρέμενε σχετικά με το εάν θα θυμούνται τα αξιοθέατα της πόλης ή τα Pokémon και τις πύλες τους.

Καταλήγοντας, τέθηκε ο σοβαρός προβληματισμός ως προς το εάν υπάρχουν μέρη όπου δεν θα έπρεπε να παίζεται το Pokémon Go. Η εμφάνιση χαρακτήρων Pokémon στο πρώην στρατόπεδο συγκέντρωσης Auschwitz της Πολωνίας, στο Μουσείο Μνήμης του Ολοκαυτώματος στην Ουάσιγκτον και στο Εθνικό Μνημείο της 11ης Σεπτεμβρίου στη Ν. Υόρκη προκάλεσε οργισμένες αντιδράσεις[193] από τους εκπροσώπους των μνημείων αυτών. Συγκεκριμένα, εκπρόσωπος του Μνημείου του Auschwitz ανέφερε ότι κάθε παρουσία του παιχνιδιού εκεί ή σε άλλα μνημεία και μουσεία του Ολοκαυτώματος ήταν απολύτως ακατάλληλη. «Το να επιτρέψει κάποιος, ανέφερε, σε τέτοιου είδους παιχνίδια να είναι ενεργά σε τοποθεσίες, όπως το Μνημείο του Auschwitz, δείχνει ασέβεια στην μνήμη των θυμάτων των στρατοπέδων συγκεντρώσεως και εξοντώσεως των Γερμανών Ναζί, σε πολλά επίπεδα» και για το λόγο αυτό υπήρξε επικοινωνία με τους δημιουργούς του παιχνιδιού, από τους οποίους ζητήθηκε να μην συμπεριλαμβάνονται στο παιχνίδι τέτοιου είδους μνημεία ή τοποθεσίες[194]. Παράλληλα, κάτοικος της πόλης New Jersey άσκησε αγωγή κατά της εταιρίας δημιουργού του παιχνιδιού,με τον ισχυρισμό ότι το παιχνίδι ενθάρρυνε τους

ανηλίκων κάτω των 18 ετών δήλωσαν ότι οι γονείς τους καταναλώνουν πάρα πολύ χρόνο στο τηλέφωνο. Ο Richard Freed, ψυχολόγος και συγγραφέας του βιβλίου: «Ενσύρματο Παιδί: Ανακτώντας την Παιδική Ηλικία σε μία Ψηφιακή Εποχή» εξέφρασε το σκεπτικισμό του ως προς τις υποσχέσεις που δίνονται ότι η απάντηση στα προβλήματα που προκαλεί η υπερβολική χρήση της τεχνολογίας είναι ακόμα περισσότερη τεχνολογία είναι, αλλά και για το μέλλον του Pokémon Go. «Υπήρξαμε αισιόδοξοι στο παρελθόν ότι κάποια παιχνίδια, όπως το Wii, θα συνέβαλλαν στον κοινό οικογενειακό χρόνο και θα ωθούσαν τα παιδιά μακριά από τον καναπέ» αναφέρει, «αλλά τελικά απέτυχαν να διαρκέσουν παραπάνω από όσο διήρκεσε η διαφημιστική τους εκστρατεία». Richard Freed, Wired Child: Reclaiming Childhood in a Digital Age, (2018), διαθέσιμο σε http://richardfreed.com/ .

192 Jennifer Langston, «Parents who play 'Pokémon GO' with kids: 'It wasn't really about the Pokémon», (2017), διαθέσιμο σε https://www.washington.edu/news/2017/03/28/parents-who-play-pokemon-go-with-kids-it-wasnt-really-about-the-pokemon/ .

193 Andrea Peterson, «Holocaust Museum to visitors: Please stop catching Pokémon here», (2016), διαθέσιμο σε https://www.washingtonpost.com/ .

194 Jonah Engel Bromwich, «Where Pokémon Should Not Go», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/13/technology/where-pokemon-should-not-go.html?searchResultPosition=1.

παίκτες να καταπατούν ξένες περιουσίες κατά την αναζήτηση των Pokémon ή των PokéStops[195]. Κατά τη διάρκεια της εβδομάδας κατά την οποία το παιχνίδι παρουσιάστηκε στο κοινό, άγνωστοι παρέμεναν έξω από το σπίτι του ενάγοντος με τα τηλέφωνά τους ανά χείρας και τουλάχιστον πέντε άτομα ζήτησαν πρόσβαση στην αυλή του με σκοπό τη σύλληψη Pokémon που είχαν τοποθετηθεί από το παιχνίδι στο χώρο αυτό[196].

Σε μία αισιόδοξη θεώρηση των πραγμάτων, μετά την τεράστια συμμετοχή των ανθρώπων στην εφαρμογή PokémonGo, διαφάνηκε ένα μέλλον όπου η τεχνολογία θα μπορούσε να χρησιμοποιηθεί με στόχο την ενίσχυση των ταξιδιωτικών προορισμών. Είναι πιο εύκολο να φανταστεί κάποιος την εικονική αναζήτηση των μεγάλων συγγραφέων του Λονδίνου κατά την περιήγησή του στην πόλη, από την αναζήτηση των Pokémon σε αυτή.

Σε σχέση με τους κινδύνους της εφαρμογής, όπως σημειώνουν οι ειδικοί, είναι θέμα χρόνου το πότε θα προκύψουν αγωγές για σωματικές βλάβες που σχετίζονται με το παιχνίδι αυτό, είτε πρόκειται για παίκτες που κυκλοφορούν πεζή, στην προσπάθειά τους να «αιχμαλωτίσουν» Pokémon είτε για αυτοκινητικά ατυχήματα από οδηγούς των οποίων η προσοχή είναι στραμμένη στο «κυνήγι» των Pokémon. Έως τώρα,

195 Stephanie Fogel, «Pokemon Go creator Niantic will allow 130 foot buffer zones to protect private property from trespassing players», Variety, (2019), διαθέσιμο σε https://www.businessinsider.com/pokemon-go-new-rules-private-property-legal-settlement-2019-2. βλ, επίσης «Pokemon Go shines new attention on trespass laws», (2016) διαθέσιμο σε https://constitutioncenter.org/blog/pokemon-go-shines-new-attention-on-trespass-laws.

196 Η αγωγή αυτή μετατράπηκε σε ομαδική, με δώδεκα ενάγοντες, οι οποίοι αιτούνταν από την εναγομένη μέχρι 1000 δολάρια έκαστος. Η εταιρία Niantic κατέληξε σε συμβιβασμό, χωρίς να αποδεχτεί υπαιτιότητα και κατέβαλε 4 εκατομμύρια δολάρια σε δικαστικά έξοδα, όπως επίσης και το ποσό των 1000 δολαρίων σε καθέναν από τους ενάγοντες. Επιπλέον η εταιρία συμφώνησε να προσθέσει στο παιχνίδι μηνύματα κατά της παραβίασης ξένης ιδιοκτησίας και ότι στο μέλλον θα πάψει να τοποθετεί στάσεις (pokéstops) και γυμναστήρια (gyms) κοντά σε κατοικίες μονογονεϊκών οικογενειών ή σε άλλες πιθανόν προβληματικές τοποθεσίες. Ένας από τους όρους του συμβιβασμού ήταν ότι σε περίπτωση όπου μία στάση ή ένα γυμναστήριο έχει τοποθετηθεί στα 40μ από μία κατοικία, οι ιδιοκτήτες αυτής μπορούν να απαιτήσουν την απομάκρυνση αυτών. Δεδομένου ότι οι νόμοι που περιβάλλουν την επαυξημένη πραγματικότητα στους τομείς της παραβίασης ξένης ιδιοκτησίας είναι θολοί, η απόφαση της εταιρίας Niantic να συμβιβαστεί στη συγκεκριμένη υπόθεση οδήγησε στην αποφυγή δεδικασμένου. Επέλεξαν μία συμφωνία η οποία δεσμεύει τα δύο μέρη, μόνο όμως αναφορικά το συγκεκριμένο προϊόν και τη συγκεκριμένη υπόθεση. Sam Desatoff, «Niantic settles 2016 Pokemon Go class action trespassing lawsuit», διαθέσιμο σε https://finance.yahoo.com/news/niantic-settles-2016-pokemon-class-194800175.html.

έχουν προκύψει ατυχήματα μικρής σημασίας κατά τη διάρκεια του παιχνιδιού. Στην περίπτωση όμως που συμβεί κάτι σοβαρό, οι παίκτες που θα υποστούν τη βλάβη έχουν τη δυνατότητα στις ΗΠΑ να αμυνθούν με αγωγές στηριζόμενοι στο προηγούμενο των αυτοκινητικών ατυχημάτων που συνδέονται με το Snapchat[197][198]. Σε αντίθεση με την εφαρμογή Snapchat, κατά την οποία ενεργοποιείται φίλτρο ταχύτητας για την αποτροπή μεγάλων ταχυτήτων, στο Pokemon Go, αν και δεν υπάρχει κάτι αντίστοιχο, εντούτοις ενυπάρχουν προειδοποιήσεις και διασφαλίσεις για την αποτροπή της χρήσης του παιχνιδιού κατά την οδήγηση ή σε υψηλές ταχύτητες. Επίσης, οι όροι χρήσης του παιχνιδιού περιλαμβάνουν αποποιήσεις ευθύνης[199] και την προειδοποίηση σχετικά με την ασφαλή χρήση: «During game play, please be aware of your surroundings and play safely»[200].

Σχετικά με την προστασία της ιδιωτικότητας κατά τη συμμετοχή στο παιχνίδι, η εταιρία Niantic έχει συμπεριλάβει στην εφαρμογή ξεκάθαρα διατυπωμένες συνδέσεις (links) σχετικά με την πολιτική της ιδιωτικότητας. Οι πληροφορίες που περιγράφονται καλύπτουν τους παίκτες τόσο στις ΗΠΑ, όσο και στην Ευρωπαϊκή Ένωση, υπό το πρίσμα του ΓΚΠΔ, συμπεριλαμβανομένων και των απαιτούμενων μέτρων για την προστασία των ανηλίκων χρηστών[201].

Παρά τα αυστηρά μέτρα, παραμένει προβληματικό το γεγονός ότι η εφαρμογή συγκεντρώνει πολλές πληροφορίες των χρηστών. Κάποιες από αυτές είναι

197 Πρόκειται για προϊόν λογισμικού εφαρμογής μηνυμάτων εικόνας, μέσω των οποίων οι χρήστες επικοινωνούν με φίλους, δημιουργούν καινούριες σχέσεις, παίζουν και μαθαίνουν. Βλ. σχετικά https://www.snapchat.com/.

198 Οι ενάγοντες στήριξαν τις αγωγές τους στη θεωρία περί ελαττωματικού προϊόντος, με κύρια βάση της αγωγής ότι η εταιρία παρασκεύασε ένα προϊόν από το οποίο προέκυπταν εγγενείς κίνδυνοι για τους καταναλωτές κι επικουρικά ότι η εταιρία έθεσε σε κυκλοφορία ένα προϊόν χωρίς επαρκείς προειδοποιήσεις για πιθανές βλάβες. Στην ίδια νομική βάση και οι παίκτες του Pokémon Go θα μπορούσαν να ισχυριστούν ότι θα έπρεπε να είναι προβλέψιμο το γεγονός ότι οι παίκτες βαδίζοντας έχουν στραμμένη την προσοχή τους στα κινητά τους τηλέφωνα, αγνοώντας φυσικούς κινδύνους ή διερχόμενα αυτοκίνητα. Στην Ευρώπη και την Ελλάδα δεν υπάρχει σχετική νομολογία. Βλ. σχετικά Tiffany Li, «Pokémon Go and the Law: Privacy, Intellectual Property, and Other Legal Concerns», Yale Law School - Information Society Project, (2016).

199 Σύμφωνα με τα ΑΚ 332επ., το δίκαιο προστασίας του καταναλωτή όπως ισχύει και τους Γενικούς Όρους Συναλλαγών.

200 Βλ. σχετικά https://tldrlegal.com/license/pokemon-go-terms-of-service.

201 Beth Hill, «The important privacy lessons from 'Pokemon Go», διαθέσιμο σε https://iapp.org/news/a/beth-hill-the-important-privacy-lessons-from-pokemon-go/.

προσωπικά αναγνωριστικά, όπως το όνομα και η ηλεκτρονική διεύθυνση του χρήστη και άλλες σχετίζονται με αυτά που υποβάλει ο χρήστης στο παιχνίδι. Ο όγκος των πληροφοριών αυτών οδήγησε το Γερουσιαστή Al Franken στην αποστολή επιστολής στην κατασκευάστρια εταιρία, με την οποία απαιτούσε περισσότερη διαφάνεια ως προς την προστασία της ιδιωτικότητας που παρέχει το παιχνίδι[202]. Σοβαρή, όμως ανησυχία προκαλεί και η συνεχής παρακολούθηση των δεδομένων τοποθεσίας (location data), τα οποία στην Ευρώπη προστατεύονται ως προσωπικά δεδομένα υπό το ΓΚΠΔ, όπως επίσης και το γεγονός ότι η κατασκευάστρια εταιρία Niantic δεν παρέχει πολλές πληροφορίες σχετικά με το πού κοινοποιούνται τα δεδομένα των χρηστών. Η πολιτική του παιχνιδιού δίνει τη δυνατότητα στην εταιρία να μοιράζεται τις συγκεντρωτικές και μη αναγνωριστικές πληροφορίες με τρίτα μέρη προς έρευνα και ανάλυση, δημογραφικά προφίλ και άλλους παρόμοιους σκοπούς, κατά παράβαση και πάλι του ΓΚΠΣ και συγκεκριμένα της αρχής της διαφάνειας. Αυτό έχει ως αποτέλεσμα τα δεδομένα των χρηστών να πωλούνται σε εταιρίες για στοχευμένους διαφημιστικούς σκοπούς[203]. Για το λόγο αυτό, η κατασκευάστρια εταιρία έχει δεσμευτεί να μην κοινοποιεί τα δεδομένα αυτά χωρίς να τα ομαδοποιεί όλα μαζί, αφαιρώντας οποιαδήποτε αναγνωριστική πληροφορία (ονοματεπώνυμο, ηλεκτρονικό ταχυδρομείο κλπ)[204].

Στον τομέα της πνευματικής ιδιοκτησίας, η χρήση από την εταιρία Niantic φωτογραφιών τοποθεσιών στο παιχνίδι της Pokémon Go εμπίπτει στην εξαίρεση της «ελευθερίας του πανοράματος»[205], η οποία επιτρέπει την ελεύθερη χρήση

202 Βλ. σχετικά επιστολή του Γερουσιαστή Al Franken προς τον John Hanke, Διευθύνοντα Σύμβουλο της Niantic, την 12 Ιουλίου 2016, διαθέσιμο σε https://assets.documentcloud.org/documents/2991981/Al-Franken-Letter-On-Pokemon-Go.pdf.

203 Jedidiah Bracy, «Pokémon GO, augmented reality, and privacy», (2016), διαθέσιμο σε https://iapp.org/news/a/pokemon-go-augmented-reality-and-privacy/.

204 James Rogers, «Death by Pokemon? Public safety fears mount as 'Pokemon GO' craze continues», (2016), διαθέσιμο σε https://www.foxnews.com/tech/death-by-pokemon-public-safety-fears-mount-as-pokemon-go-craze-continues.

205 Πρόκειται για πρόβλεψη στους νόμους περί προστασίας της πνευματικής ιδιοκτησίας σε διάφορες δικαιοδοσίες που επιτρέπει τη λήψη φωτογραφιών ή βίντεο, ή δημιουργία άλλων εικόνων (όπως πίνακες ζωγραφικής), από κτίρια ή κάποιες φορές γλυπτά και άλλα καλλιτεχνικά έργα που είναι μόνιμα τοποθετημένα σε δημόσιο χώρο, χωρίς παραβίαση πνευματικών δικαιωμάτων που μπορεί να ισχύουν για αυτά τα έργα, και τη δημοσίευση αυτών των εικόνων. Αποτελεί εξαίρεση στον κανόνα ότι ο κάτοχος των

φωτογραφιών και βίντεο κτηρίων ή γλυπτών ή άλλων έργων, τα οποία βρίσκονται σε δημόσιους χώρους. Στην Ευρωπαϊκή Ένωση «ο όρος «παρουσίαση στο κοινό», κατά το άρθρο 3, παράγραφος 1, της οδηγίας 2001/29/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Μαΐου 2001, για την εναρμόνιση ορισμένων πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας, έχει την έννοια ότι καλύπτει την ανάρτηση σε ιστότοπο φωτογραφίας προηγουμένως δημοσιευθείσας σε άλλον ιστότοπο χωρίς περιορισμούς εμποδίζοντες την τηλεφόρτωσή της και με την άδεια του κατόχου του δικαιώματος του δημιουργού»[206]. Εξίσου σημαντική είναι και η χρήση των σημάτων στο παιχνίδι, κυρίως ως ορόσημα αυτού (ονομασίες καταστημάτων ή κτηρίων). Και σε αυτή την περίπτωση, όμως, έχει προβλεφθεί ότι η χρήση ενός εμπορικού σήματος που δηλώνει τοποθεσία ή προέλευση είναι γενικά αποδεκτή νομικά, ως «δίκαιη χρήση» (fair use), σύμφωνα με τον αμερικανικό νόμο περί εμπορικών σημάτων[207].

πνευματικών δικαιωμάτων έχει το αποκλειστικό δικαίωμα να επιτρέπει την δημιουργία και τη διανομή των παράγωγων έργων. Η φράση προέρχεται από τον Γερμανικό όρο Panoramafreiheit. Πολλές χώρες έχουν παρόμοιες διατάξεις που περιορίζουν το πεδίο εφαρμογής του νόμου περί πνευματικής ιδιοκτησίας προκειμένου να επιτρέπονται ρητά οι φωτογραφίες που περιλαμβάνουν σκηνές των δημόσιων χώρων ή σκηνές που έχουν φωτογραφηθεί από δημόσιους χώρους. Άλλες χώρες, όμως, διαφέρουν σε μεγάλο βαθμό στην ερμηνεία της αρχής. Στην Ευρωπαϊκή Ένωση, η Οδηγία 2001/29/ΕΚ προβλέπει, χωρίς να απαιτεί, τη δυνατότητα των κρατών μελών να μπορούν να έχουν ρήτρα ελευθερίας πανοράματος στους νόμους περί πνευματικής ιδιοκτησίας. https://el.wikipedia.org/wiki/%CE%95%CE%BB%CE%B5%CF%85%CE%B8%CE%B5%CF%81%CE%AF%CE%B1_%CF%80%CE%B1%CE%BD%CE%BF%CF%81%CE%AC%CE%BC%CE%B1%CF%84%CE%BF%CF%82

206 Βλ. σχετικά ΔΕΕ C-161/17 Renckhoff (Cordoba).

207 Brian D. Wassom, «How Pokémon GO Players Could Run Into Real-Life Legal Problems», (2016), διαθέσιμο σε https://www.hollywoodreporter.com/thr-esq/how-pok-mon-go-players-909869. Βλ. επίσης Natasha Lomas, «Pokemon Go T&Cs strip users of legal rights», (2016), διαθέσιμο σε https://techcrunch.com/2016/07/17/pokemon-go-tcs-strip-users-of-legal-rights/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEJiAr0pm33gSskRgQXoVzwZutNnIww-YCRfyuwdyJB2r7kbgYHL8xo7FnWtu3yiTAaSnnlHSGCRu8hXGI3OaPBdSC_PdhgQLikVE6mEmyqsHgOETRHQk9niJtsaPaJECanH92A9gMqWDzcVZErIAjiNf7M5g0Hy9oyy9_uCWNGE.

5.2 **Επαυξημένη Πραγματικότητα και ηλεκτρονικό εμπόριο**

Η τεχνολογία της επαυξημένης πραγματικότητας αποτελεί το παρόν και το μέλλον του ηλεκτρονικού εμπορίου, τη μεγαλύτερη ανακάλυψη μετά από την μηχανή αναζήτησης και ήδη οι κινητές συσκευές την τοποθετούν σε ένα εντελώς διαφορετικό επίπεδο. Όσο περισσότερες συσκευές και «έξυπνα» τηλέφωνα υποστηρίζουν την τεχνολογία αυτή και όσο οι άνθρωποι θα συνεχίζουν να τα αγοράζουν, η νέα εμπειρία της εικονικής δοκιμής ρούχων ή αξεσουάρ θα γίνεται πιο ελκυστική. Η εταιρία eBay παρουσίασε μία εφαρμογή, μέσω της οποίας οι χρήστες έχουν τη δυνατότητα να δοκιμάζουν γυαλιά ηλίου εικονικά, μέσω της κάμερας του κινητού τους τηλεφώνου και συγκεκριμένα μέσω της λήψης μίας φωτογραφίας τους και την προσαρμογή των γυαλιών σε αυτή, κάτι που μας προετοιμάζει για το άμεσο μέλλον και για άλλες παραπλήσιες εφαρμογές που άπτονται του ηλεκτρονικού εμπορίου. Ολοένα και μεγαλύτερος αριθμός ατόμων αποκτούν «έξυπνα» τηλέφωνα, αυτά και άλλες παρόμοιες συσκευές τελειοποιούνται καθημερινά και οι έμποροι αντιλαμβάνονται τις μοναδικές ευκαιρίες που παρουσιάζονται με τη νέα τεχνολογία[208]. Κάτι που, όπως ισχυρίζονται οι επικριτές της τεχνολογίας αυτής θα μειώσει σημαντικά τις ανάγκες και τις επιθυμίες των καταναλωτών ως προς τη φυσική τους παρουσία στα καταστήματα. Είναι φυσικό επόμενο ότι ο καταναλωτής θα παύσει να ταλαιπωρείται στα εμπορικά κέντρα, όταν θα μπορεί να δοκιμάσει τα ίδια εμπορεύματα από το σπίτι του ή από οποιονδήποτε άλλο χώρο αυτός επιθυμεί.

208 Ένα από τα μεγαλύτερα εμπόδια του ηλεκτρονικού εμπορίου ήταν μέχρι σήμερα η αδυναμία του καταναλωτή να δοκιμάσει το προϊόν πριν το αγοράσει. Το εμπόδιο αυτό καταρρίπτεται με την ύπαρξη της κάμερας σχεδόν σε κάθε ηλεκτρονική συσκευή και την ανακάλυψη εφαρμογών της επαυξημένης πραγματικότητας, με τις οποίες μεταφέρονται τα εικονικά προϊόντα στο περιβάλλον και τη ζωή του καταναλωτή. Joshua Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal,* Vol. 27:55 (2012).

6 Ζητήματα ασφάλειας των δεδομένων κατά τη χρήση των νέων τεχνολογιών και των ψηφιακών εφαρμογών

Μελετώντας και τις δύο όψεις του νομίσματος που ονομάζεται «νέες τεχνολογίες», πρέπει να ομολογήσει κανείς ότι κατά τη χρήση τους προκύπτουν ζητήματα ασφάλειας δεδομένων. Για παράδειγμα, το ψηφιακό αποτύπωμα του χρήστη μπορεί να χρησιμοποιηθεί ευρέως και με πολλούς τρόπους. Οι αντιδράσεις του στα μέσα κοινωνικής δικτύωσης διαμορφώνουν τις διαφημίσεις που παρουσιάζονται στο προφίλ του εκεί. Τα είδη των ταινιών και της μουσικής στα οποία έχει πρόσβαση επιτρέπουν σε διάφορες διαδικτυακές εταιρίες να σχολιάσουν τις πολιτικές και θρησκευτικές του πεποιθήσεις. Τίθενται λοιπόν τα βασικά ερωτήματα ως προς το εάν και ποιας μορφής έλεγχος ασκείται στις εταιρίες που συγκεντρώνουν όλα τα δεδομένα και χρησιμοποιούν όλες τις πληροφορίες που αφορούν τους χρήστες, αλλά κι εάν υφίστανται μηχανισμοί που να είναι σε θέση να προστατέψουν τα δεδομένα από την κακή χρήση τους από τρίτους.

Οι απαντήσεις στα ανωτέρω ερωτήματα διαφοροποιούνται ανάλογα με το πού τίθενται τα ζητήματα, στην Ευρώπη ή στις ΗΠΑ. Στις ΗΠΑ εφαρμόζονται ειδικές νομοθετικές ρυθμίσεις σε τομείς, όπως η υγεία και οι τραπεζικές συναλλαγές. Στην Ευρωπαϊκή Ένωση, η προστασία των δεδομένων θεωρείται θεμελιώδες δικαίωμα[209], το οποίο οδήγησε σε νομοθετικές ρυθμίσεις που επηρεάζουν όλα τα κράτη–μέλη[210]. Οι συζητήσεις για την προστασία της ιδιωτικής ζωής και των δεδομένων μπορεί να έχουν γίνει αιτία πολιτικών αντιπαραθέσεων, αλλά οι διαφορετικές προσεγγίσεις έχουν πρακτικές συνέπειες και για τα ίδια τα άτομα. Έστω ότι κάποιος έκανε ένα λάθος στο παρελθόν, κατά τη διάρκεια των σπουδών του, το οποίο οδήγησε στη

209 Βλ. σχετικά Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων), διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL

210 Βλ, σχετικά στην Ελλάδα Ν 4624/2019: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679.

σύλληψή του και στην απόδοση κατηγοριών σε βάρος του, από τις οποίες τελικά απαλλάχτηκε. Το ποινικό του μητρώο ήταν λευκό και πριν και μετά τη σύλληψη. Όμως το λάθος που διέπραξε τον ακολουθεί από τότε, ως άρθρο μιας τοπικής εφημερίδας η οποία αναφέρθηκε στη σύλληψη και το οποίο άρθρο εμφανίζεται κάθε φορά που γίνεται αναζήτηση του ονόματός του. Το ζήτημα αυτό αφορά στο δικαίωμα στη λήθη[211], το οποίο στην Ευρώπη δίνει τη δυνατότητα στα άτομα να αιτούνται από τις μηχανές αναζήτησης να αφαιρέσουν αναφορές στο πρόσωπό τους, από άρθρα που βρίσκονται στην ευρωπαϊκή εκδοχή των μηχανών αυτών, αν και τα άρθρα αυτά παραμένουν στις ιστοσελίδες των εφημερίδων όπου αρχικά δημοσιεύθηκαν. Αντιθέτως στις ΗΠΑ, η Πρώτη Τροπολογία του Αμερικανικού Συντάγματος προστατεύει την ελευθερία της έκφρασης[212], συμπεριλαμβανομένου του δικαιώματος του ατόμου να μιλά ελεύθερα. Εκεί δεν έχει θεσμοθετηθεί κάποια ρύθμιση που να επιτρέπει στα άτομα να διαγράφουν ή να αφαιρούν από το διαδίκτυο, αρνητικές, για τα ίδια, πληροφορίες.

Αναφορικά με την προστασία των δεδομένων των ανηλίκων[213] στις χώρες της Ευρωπαϊκής Ένωσης, ο Γενικός Κανονισμός Προστασίας Προστασίας Δεδομένων ΕΕ 2016/679 ρυθμίζει με το άρθρο 8 τις προϋποθέσεις που ισχύουν για τη συγκατάθεση του παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών. Κατά συνέπεια, στην περίπτωση δεκάχρονου παιδιού, το οποίο θέλει να δημιουργήσει προφίλ παίκτη για να συμμετάσχει σε διαδικτυακό παιχνίδι, το οποίο συγκεντρώνει προσωπικές πληροφορίες, όπως το πραγματικό όνομα του παιδιού, τοποθεσίες, φωτογραφίες και διευθύνσεις ηλεκτρονικού ταχυδρομείου ή να συμμετέχει σε μέσα κοινωνικής δικτύωσης, όπως το Facebook, το Snapchat και το

211 Δικαίωμα διαγραφής («δικαίωμα στη λήθη»). 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).

212 «What Does Free Speech Mean?», διαθέσιμο σε https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does .

213 Ευγενία. Αλεξανδροπούλου-Αιγυπτιάδου, «Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679», *ΔΙΤΕ (π. ΔΙΜΕΕ), τ.* 1, (2018): 5-20.

Instagram, οι υπηρεσίες αυτές θα ζητούν τη συναίνεση των γονέων για τη συλλογή δεδομένων σχετικά με αυτό[214].

Στις ΗΠΑ, ο ομοσπονδιακός νόμος Children's Online Privacy Protection Act απαιτεί από ιστότοπους και εφαρμογές που απευθύνονται σε παιδιά κάτω των 13 ετών, να αποκτήσουν πρώτα τη συναίνεση των γονέων πριν συγκεντρώσουν από αυτά προσωπικά δεδομένα, όπως ονόματα και ηλεκτρονικές διευθύνσεις[215].

Σχετικά με τις εφαρμογές που κατεβάζει κανείς διαδικτυακά, δίνει μηχανικά τη συναίνεσή του, μεταξύ άλλων, στο ότι τα προσωπικά του δεδομένα θα θεωρούνται και δεδομένα του παιχνιδιού και αποδέχεται πολλούς άλλους όρους, τους οποίους συχνά δεν διαβάζει, λόγω του μεγάλου τους όγκου και της πολυπλοκότητάς τους. Η αποδοχή όλων των αιτημάτων που εμφανίζονται όταν ο το άτομο εγκαθιστά μία

214 Για την Ελλάδα η συγκατάθεση του ιδίου του ανηλίκου απαιτείται για την ηλικία των 15 ετών και άνω. Βλ. άρθρο 21 Νόμου 4624/29-08-2019 - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις. Σύμφωνα με την Αιτιολογική Έκθεση του ανωτέρω νόμου, το άρθρο 21 αναφέρεται στο άρθρο 8 του ΓΚΠΔ. Το άμεσο πεδίο εφαρμογής του κανόνα που τίθεται με το άρθρο αυτό είναι η ικανότητα για την παροχή της συγκατάθεσης του ανηλίκου σε σχέση με τη χρήση υπηρεσιών της κοινωνίας της πληροφορίας καθώς επίσης και η νομική εκπροσώπηση μέσω των γονέων στο πλαίσιο αυτό. Με το άρθρο 21 τίθεται ως όριο συγκατάθεσης του ανηλίκου η ηλικία των δέκα πέντε (15) ετών (παράγραφος 1). Η νομοθετική αυτή επιλογή ως προς το όριο ηλικίας αντιστοιχεί σε αρκετές ρυθμίσεις του ελληνικού δικαίου, σύμφωνα με τις οποίες αναγνωρίζεται σε πρόσωπα δεκαπέντε (15) ετών περιορισμένη δικαιοπρακτική ικανότητα (Βλ. άρθρο 136 ΑΚ). Σε κάθε περίπτωση, η συγκατάθεση του ανηλίκου πρέπει να πληροί κατά μείζονα λόγο τους όρους που περιλαμβάνονται στον ορισμό της συγκατάθεσης και στους ειδικότερους όρους 13 που περιλαμβάνονται στο άρθρο 7 του ΓΚΠΔ. Για την ηλικία κάτω των 15 ετών απαιτείται η συγκατάθεση των νομίμων αντιπροσώπων του ανηλίκου (παράγραφος 2). Νόμιμοι αντιπρόσωποι του ανηλίκου θεωρούνται τα πρόσωπα που ασκούν κατά περίπτωση τη γονική μέριμνα αυτού (Βλ. άρθρ. 1510 ΑΚ επ.) ή ο επίτροπος (γενικός, ειδικός, προσωρινός ή μη) (Βλ. άρθρ. 1589 ΑΚ επ.). Τέλος, με την παράγραφο 3 ορίζεται ότι ο εκάστοτε υπεύθυνος επεξεργασίας φέρει το βάρος να επαληθεύσει ότι η συγκατάθεση στην περίπτωση ανηλίκου κάτω των 15 ετών παρασχέθηκε από το νόμιμο αντιπρόσωπό του. Μια τέτοια πρόβλεψη υπαγορεύεται από την αναγκαιότητα για προστασία της προσωπικότητας του ιδιαίτερα ευαίσθητου και ευάλωτου εν προκειμένω υποκειμένου των δεδομένων. Αντώνης Μπρούμας, «Η Προστασία των Προσωπικών Δεδομένων Παιδιού», (2019), διαθέσιμο σε https://lawandtech.eu/2019/10/09/children-data/ και Ευγενία. Αλεξανδροπούλου-Αιγυπτιάδου, Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679, *ΔΙΤΕ (π. ΔΙΜΕΕ), τ.* 1, (2018): 5-20.

215 Marc Scott και Natasha Singer, «How Europe Protects your Online Data Differently than the US», (2016), διαθέσιμο σε https://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html

εφαρμογή σε μία συσκευή κινητού συχνά απειλούν την ιδιωτικότητά του[216]. Οι εταιρίες οι οποίες κατασκευάζουν διαδικτυακά παιχνίδια στα οποία απαιτείται εγγραφή, δεν αποκτούν μόνο έσοδα από την πώληση του ίδιου του παιχνιδιού ή άλλων πραγμάτων σχετικών με το παιχνίδι, αλλά επιπρόσθετα συγκεντρώνουν δεδομένα σχετικά με τις συνήθειες των παικτών και με τη χρήση του τηλεφώνου τους, τα οποία πωλούν σε τρίτους[217]. Τίθεται, λοιπόν, το ερώτημα εάν και πώς θα μπορούσαν να μειωθούν στο ελάχιστο οι κίνδυνοι ασφαλείας που συνοδεύουν κάποιες εφαρμογές. Ο Ari Rubinstein, μηχανικός ασφαλείας στη Silicon Valley, προτείνει στους χρήστες να δίνουν ιδιαίτερη βαρύτητα στα όρια της πρόσβασης που οι εφαρμογές αυτές απαιτούν κατά την εγκατάστασή τους ή να εξετάζουν κάθε λεπτομέρεια και να απαντούν αρνητικά σε απαιτήσεις που τους κάνουν να νιώθουν άβολα[218].

Βέβαια, οι άδειες δεν είναι το μοναδικό θέμα το οποίο εγείρει ανησυχίες. Τα άτομα πρέπει να ενημερώνονται, επίσης, ως προς το τι είδους δεδομένα του τηλεφώνου τους συγκεντρώνει η εφαρμογή. Τέτοιου είδους πληροφορίες συνήθως εμπεριέχονται στις πολιτικές προστασίας της ιδιωτικότητας της εφαρμογής, οι οποίες είναι συχνά διαθέσιμες στις ρυθμίσεις αυτής ή μπορεί κάποιος να τις αναζητήσει διαδικτυακά. Καθώς οι εφαρμογές συχνά χρησιμοποιούν πλατφόρμες, όπως το Facebook και η Google για να επιβεβαιώσουν λογαριασμούς, προτείνεται ο συχνός και επαναλαμβανόμενος έλεγχος της πρόσβασης που έχει αποκτήσει ο χρήστης, μέσω των ρυθμίσεων αυτών των συστημάτων[219]. Όσον αφορά στη εφαρμογή Pokémon Go, παρότι δεν αναζητά τις ηλεκτρονικές διευθύνσεις των χρηστών, έχει τη δυνατότητα

216 N. Cameron Russell, Joel R. Reidenberg και Sumyung Moon, «Privacy in Gaming», *Fordham Intellectual Property, Media and Entertainment Law Journal,* Vol. 29, (2019): 61-180.

217 Ο Andrew Storms, αντιπρόεδρος της εταιρίας παροχής υπηρεσιών ασφαλείας New Context, αναφέρει σχετικά ότι «τελικά παραχωρούμε τα δικαιώματα για σχεδόν όλες τις πληροφορίες που μας αφορούν στις εταιρίες παραγωγής διαδικτυακών παιχνιδιών». Laura Hudson, «How to Protect Privacy While Using Pokémon Go and Other Apps», (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/14/technology/personaltech/how-to-protect-privacy-while-using-pokemon-go-and-other-apps.html.

218 Ο. π. υποσημείωση 212.

219 Ό.π. υποσημείωση 211.

να ανακαλύπτει τη θέση τους ή να μοιράζεται με τρίτα πρόσωπα μη αναγνωρίσιμες, ως προς το χρήστη, πληροφορίες για σκοπούς ερευνητικούς, δημογραφικούς ή άλλους σχετικούς.

7 Νέες τεχνολογίες: ζητήματα προστασίας κι εφαρμοστέο δίκαιο

Με τον ίδιο τρόπο με τους υπολογιστές, το διαδίκτυο και τα κινητά τηλέφωνα, και οι αναδυόμενες νέες τεχνολογίες, εκτός από τα οφέλη που παρέχουν στους χρήστες, ενέχουν και κινδύνους για την καθημερινότητά τους[220]. Παρά τις εξαιρετικές δυνατότητες που παρουσιάζουν οι τεχνολογίες της εικονικής κι επαυξημένης πραγματικότητας, ελοχεύουν πάντα κίνδυνοι σε σχέση με την ασφάλεια κατά τη χρήση ή την ανορθόδοξη χρήση αυτών των νέων εργαλείων[221].

7.1 Πνευματική Ιδιοκτησία

Οι εικονικοί κόσμοι κατά το αμερικανικό δίκαιο κυρίως διέπονται από τους νόμους περί Πνευματικής Ιδιοκτησίας και Αδειών Χρήσης[222]. Η εφαρμογή της τεχνολογίας της επαυξημένης πραγματικότητας έχει εγείρει ερωτήσεις σχετικά με τις νομοθετικές ρυθμίσεις που θα έπρεπε να εφαρμοστούν για την επίλυση όλων των νέων, για τη θεωρία και την πράξη, συγκρούσεων, όπως για παράδειγμα τα ζητήματα πνευματικής

220 «Η πρώτη τεχνολογική ανακάλυψη που υπήρξε καταστροφική για το κοινωνικό σύνολο και για την καθημερινότητα των ατόμων ήταν οι υπολογιστές, η δεύτερη τα κινητά τηλέφωνα, τα οποία έκαναν την επανάστασή τους μόλις σε λίγες δεκαετίες. Η επόμενη καταστροφική τεχνολογική ανακάλυψη που εμφανίζεται τώρα είναι η εικονική πραγματικότητα». Kevin Kelly, «The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future», New York: Viking, 231, (2016).

221 Anne Hobson, «Reality Check: The Regulatory Landscape for Virtual and Augmented Reality», Policy Study 69, R Street Institute, Washington, DC, (2016). Το Νοέμβριο του 2016 η Επιτροπή Εμπορίου, Επιστημών και Μεταφορών της Γερουσίας των ΗΠΑ προχώρησε στην πρώτη ακροαματική διαδικασία σχετικά με την τεχνολογία της επαυξημένης πραγματικότητας και τα θέματα ασφαλείας που μπορεί να προκύψουν. Βλ. σχετικά «Augmented Reality: Hearing Before the US Senate Committee on Commerce, Science, and Transportation», 114th Cong, (2016).

222 «Για αυτό που κάποτε μας ανήκε, στο μέλλον θα έχουμε μόνο την άδεια χρήσης του. Αυτό που κάποτε ήταν μόνο παραβίαση συμβατικών όρων, τώρα μπορεί να αποτελεί αδίκημα παραβίασης δεδομένων (hacking) ή δικαιωμάτων πνευματικής ιδιοκτησίας». Βλ. σχετικά Joshua Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal,* Vol. 27:55. (2012).

ιδιοκτησίας[223]. Εάν αυτές οι τεχνολογίες διαδοθούν ακόμα περισσότερο, το ευρύ κοινό θα αποκτήσει τη δύναμη και τη δυνατότητα να χρησιμοποιεί την εικονική και την επαυξημένη πραγματικότητα με στόχο την «αυτοπαραγωγή» νέου τύπου πληροφοριών και ψυχαγωγίας στο περιβάλλον του. Αυτό το σενάριο, όμως, εμφανίζει το ακανθώδες νομικό ζήτημα του της «κυριότητας» των εμπειριών. Ή πιο ορθά, της «κυριότητας» της καταγεγραμμένης αναπαράστασης ορισμένων εμπειριών. Με τις παραδοσιακές κάμερες οι πολίτες είναι ελεύθεροι να δημιουργούν και καταγράφουν τη δική τους μοναδική εμπειρία. Παρά ταύτα, με τις εμπειρίες οι οποίες παρουσιάζονται σε χώρο που δεν ανήκει στο καταγράφοντα ή σε άλλα ασφαλή περιβάλλοντα, μπορεί να προκύψουν ζητήματα πολιτικής ορθότητας. Χαρακτηριστικό παράδειγμα, η ταινία τρόμου του 2013 Escape from Tomorrow[224]. Η ταινία ολοκληρώθηκε κρυφά, από μία ανεξάρτητη ομάδα παραγωγής, στο θεματικό πάρκο του Walt Disney, στο Ορλάντο της Φλόριντα. Αν και οι ηθοποιοί και η ομάδα παραγωγής πραγματοποιούσε τις πρόβες των σκηνών εκτός του χώρου, η ταινία γυρίστηκε μέσα στην ιδιοκτησία της Disney, χωρίς τη γνώση ή την άδεια της εταιρίας[225]. Το αποτέλεσμα ήταν ότι προέκυψαν συζητήσεις σχετικά με το εάν και με ποιον τρόπο παραβιάστηκαν τα πνευματικά δικαιώματα ή τα εμπορικά σήματα της Disney ή εάν πρόκειται για καλλιτεχνική «ορθή χρήση» (fair use[226]), η οποία δεν διώκεται[227]. Μολονότι ορισμένοι νομικοί βιάστηκαν να προβλέψουν ότι η ταινία «δεν

223 Philipp Hacker, «Intellectual Property Quarterly. Lessons from IP markets for data markets: on moral rights, property rules, and resale royalties», 2018. Βλ. επίσης, Ευαγγελία Βαγενά, «Η τεχνολογική προστασία και η ψηφιακή διαχείριση της πνευματικής ιδιοκτησίας», Νομική Βιβλιοθήκη, 2011, Τατιάνα – Ελένη Συνοδινού, «Πνευματική ιδιοκτησία και νέες τεχνολογίες, η σχέση χρήστη και δημιουργού», Σάκκουλας, Αθήνα - Θεσσαλονίκη, 2008 και Bernt Hugenholtz, «The future of Copyright in the digital environment», Kluwer, Information law series -4, 1996.

224 Πρόκειται για ανεξάρτητη αμερικάνικη ψυχολογική ταινία τρόμου. Βλ. σχετικά https://www.imdb.com/title/tt2187884/ .

225 Matthew Carey, «Why Disney Might Want to "Escape from Tomorrow"», (2013), διαθέσιμο σε https://edition.cnn.com/2013/01/24/showbiz/movies/escape-tomorrow-sundance-disney/index.html.

226 Απαντάται κυρίως στο δίκαιο πνευματικής ιδιοκτησίας των ΗΠΑ.

227 Cory Doctorow, «More on 'Escape from Tomorrow,' the Guerrilla Art-House Movie Shot at Walt Disney World and Disneyland», (2013), διαθέσιμο σε https://boingboing.net/2013/01/21/more-on-escape-from-tomorrow.html. Βλ επίσης Tim Wu, «It's a Mad, Mad, Mad, Mad Disney World», διαθέσιμο σε https://www.newyorker.com/culture/culture-desk/its-a-mad-mad-mad-mad-disney-world.

θα έβλεπε ποτέ το φως της ημέρας»[228], προς έκπληξη όλων η Disney, μία εταιρία η οποία συνήθως αμύνεται με σθένος περί των πνευματικών της δικαιωμάτων, ποτέ δεν αναφέρθηκε στη συγκεκριμένη ταινία και η διαμάχη έληξε γρήγορα.

Τα προβλήματα που σχετίζονται με την πνευματική ιδιοκτησία μπορεί να αυξηθούν, ιδιαίτερα λόγω του εύρους διάδοσης των νέων τεχνολογιών, καθώς οι πολίτες κάνουν χρήση των «έξυπνων» τηλεφώνων τους και άλλων συσκευών για να «ανεβάσουν» βίντεο σε πλατφόρμες όπως το YouTube[229]. Επίσης, αναμένεται να προκύψουν ζητήματα σχετικά με τα εμπορικά σήματα. Το περιοδικό World Trademark Review, σε δημοσίευσή του το Μάιο του 2016, παρατήρησε ότι οι εφαρμογές της επαυξημένης πραγματικότητας που έχουν κάνει ήδη την εμφάνισή τους «προσφέρουν εικονικές εμπειρίες δανεισμένες από δημοφιλή ψυχαγωγικά προγράμματα, όπως το «Games of Thrones», το «Harry Potter», το «Minecraft», το «Super Mario», το «Legend of Zelda» και το «Final Fantasy». Δεδομένου ότι οι εφαρμογές αυτές διατίθενται δωρεάν, οι κάτοχοι των εμπορικών σημάτων βρίσκονται σε δίλημμα»[230]. Αντίστοιχα, «ονόματα χώρου» (domain names) που σχετίζονται με εφαρμογές εικονικής πραγματικότητας έχουν ήδη καταχωρισθεί αντιγράφοντας εμπορικές επωνυμίες, όπως το MinecraftVR.com και το HarryPotterVR.com.

Πέρα από τα εμπορικά σήματα, στο μέλλον θα μπορούσαν να προκύψουν και ζητήματα δικαιωμάτων στην προσωπικότητα ή προσβολής της εικόνας[231] και να εγερθούν αστικές αξιώσεις με βάση τα δικαιώματα αυτά. Τέτοιου είδους θέματα έχουν ήδη προκύψει σε βιντεοπαιχνίδια, τα οποία έχουν κάνει χρήση της εικόνας

228 Jonathan Franklin, Escape from Tomorrow' a Disney's Lawyers Nightmares, (2013), διαθέσιμο σε http://lawofficesofjonathanfranklin.blogspot.com/2013/01/escape-from-tomorrow-disneys-lawyers.html.

229 Steven Seidenberg, «Copyright in the Age of YouTube», (2009), διαθέσιμο σε https://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube.

230 Tim Lince, «Virtual Reality Is Set to Emerge as a New Trademark Battleground, Brand Owners Are Warned», (2016), διαθέσιμο σε https://www.worldtrademarkreview.com/brand-management/virtual-reality-set-emerge-new-trademark-battleground-brand-owners-are-warned.

231 «Using the Name or Likeness of Another», (2020), διαθέσιμο σε http://www.dmlp.org/legal-guide/using-name-or-likeness-another . Βλ. επίσης Μαρία Κανελλοπούλου – Μπότη, «Δικαίωμα στην προσωπικότητα και δικαίωμα στη φωτογραφία», σε Ειρήνη Σταματούδη (επιστημονική επιμέλεια), «Δημοσιογράφοι και Εκδότες, Ζητήματα πνευματικής ιδιοκτησίας», Σάκκουλας, Αθήνα (2009): 233-263.

γνωστών αθλητών[232]. Τέλος, θα μπορούσε να παραβιαστεί το εμπορικό απόρρητο[233], στην περίπτωση που οι εφαρμογές της εικονικής κι επαυξημένης πραγματικότητας χρησιμοποιούνται ανεύθυνα ή με ακατάλληλο τρόπο στο χώρο εργασίας.

7.2 Προστασία της ιδιωτικότητας

Η προστασία της ιδιωτικότητας και η ασφάλεια των ψηφιακών συσκευών και των διασυνδεδεμένων συστημάτων καταχώρισης, επεξεργασίας και μεταβολής πληροφοριών (platforms) έχουν καταστεί μέγιστο θέμα ανησυχίας τα τελευταία χρόνια[234]. Όσον αφορά στην προστασία της ιδιωτικότητας, η ανησυχία αυτή αφορά στη συλλογή και τη χρήση προσωπικών πληροφοριών από κυβερνήσεις ή εταιρικά σχήματα. Αναφορικά με την ασφάλεια, η ανησυχία έγκειται στις πιθανότητες παραβίασης (hacking) και διάρρηξης δεδομένων. Οι τάσεις αυτές οξύνθηκαν από το συνδυασμό της αύξησης της ισχύος της επεξεργασίας, της αδιάλειπτης διασύνδεσης, της αυξανόμενης ικανότητας αποθήκευσης και της συνεχιζόμενης ψηφιοποίησης προϊόντων και υπηρεσιών[235]. Η νέα αυτή τεχνολογική πραγματικότητα έχει ήδη δημιουργήσει την ανάγκη για νομοθετική ρύθμιση των πρακτικών συλλογής δεδομένων για το διαδίκτυο των Πραγμάτων[236] και τα Μεγάλα Δεδομένα (Big Data)[237]. Κατά τη διάρκεια της επεξεργασίας και της δημιουργίας των τεχνολογιών αυτών προέκυψαν σημαντικά ζητήματα σχετικά με την προστασία της ιδιωτικότητας

232 Steven McArthur, «Right of Publicity in Video Games: How You Can Legally Include a Celebrity in Your Game», (2014), διαθέσιμο σε https://www.gamasutra.com/blogs/StephenMcArthur/20141117/230361/Right_of_Publicity_in_Video_Games__How_You_Can_Legally_Include_a_Celebrity_in_Your_Game.php.

233 Ευδοκία Κορνηλάκη, «Η προστασία του εμπορικού απορρήτου», (2019), διαθέσιμο σε https://koumentakislaw.gr/arthra/prostasia-emporikoy-aporrhtoy/ .

234 Kacy Zurkus, «FTC Says Data and Privacy Are Top Security Concerns», (2015) διαθέσιμο σε https://www.csoonline.com/article/2983853/ftc-says-data-and-privacy-are-top-security-concerns.html.

235 Adam D. Thierer, «The Pursuit of Privacy in a World Where Information Control Is Failing», *Harvard Journal of Law and Public Policy 36*, no. 2 (2013): 424–436.

236 Scott R. Peppet, «Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent», *Texas Law Review* Vol. 93/ 1, (2014): 85–176.

237 Edith Ramirez, «The Privacy Challenges of Big Data: A View from the Lifeguard's Chair», Technology Policy Institute Aspen Forum, Aspen, (2013). Βλ. επίσης και Λίλιαν Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα», Σάκκουλας, Αθήνα, 2017.

και την ασφάλεια, τα οποία επιβάλουν την ανάγκη ελέγχου[238]. Η ίδια ανάγκη έχει ενσκήψει και για τις ανερχόμενες νέες τεχνολογίες της εικονικής κι επαυξημένης πραγματικότητας και τις εφαρμογές αυτής, όπως τα γυαλιά της Google[239] ή άλλες συσκευές που φοριούνται (wearables)[240]. Αυτές, αλλά και άλλες παρόμοιες τεχνολογίες επιτρέπουν τη συνεχή λήψη, σε πραγματικό χρόνο, φωτογραφιών ή βίντεο[241]. Ακόμη κι εάν αυτού του είδους τα προϊόντα δεν έχουν τύχει ευρείας εφαρμογής[242], η προοπτική του να επιτρέπουν μυστικές καταγραφές σε ιδιωτικά μέρη ή υποκλοπές σε εμπιστευτικές συνομιλίες, εγείρουν ενστάσεις[243], οι οποίες εντείνονται με τη διάδοση της χρήσης τους, καθώς «ανοίγουν την πόρτα» στη συλλογή περισσοτέρων δεδομένων για τους χρήστες και τα άτομα γύρω τους[244]. Η ανάγκη, λοιπόν, προστασίας της ιδιωτικότητας και της ασφάλειας θα καταστεί ακόμα πιο έντονη, όσο οι τεχνολογίες αυτές περιλαμβάνουν και βιομετρικές ικανότητες[245]. Οι βιομετρικές τεχνολογίες και ικανότητες έχουν εγείρει διάφορα ζητήματα

238 Adam D. Thierer, «Privacy Law's Precautionary Principle Problem», *Maine Law Review 66*, no. 2 (2014): 473–479.

239 Clive Thompson, «Googling Yourself Takes On a Whole New Meaning», (2013), διαθέσιμο σε https://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html.

240 Benny Evangelista, «Narrative Wearable Camera: Valuable Tool or Little Brother?», (2016), διαθέσιμο σε https://www.sfchronicle.com/business/article/Narrative-wearable-camera-valuable-tool-or-7294627.php .

241 Kevin Sintumuang, «This Pocketable Camera Gear Will Change the Way You Take Travel Photos», (2016), διαθέσιμο σε https://www.wsj.com/articles/this-pocketable-camera-gear-will-change-the-way-you-take-travel-photos-1467311630 .

242 Τα γυαλιά της Google απέτυχαν ως ευρύ καταναλωτικό προϊόν και είναι πλέον διαθέσιμα μόνο για βιομηχανική χρήση. Clara Yoon, «Assumptions that led to the failure of Google Glass», (2018), διαθέσιμο σε https://medium.com/nyc-design/the-assumptions-that-led-to-failures-of-google-glass-8b40a07cfa1e#:~:text=In%20an%20exploding%20digital%20market,on%20why%20this%20product%20exists.&text=This%20revolutionary%20product%20never%20succeeded,needed%20it%20in%20their%20lives.

243 Rachel Metz, «Google Glass Is Dead; Long Live Smart Glasses», *MIT Technology Review,* (2014), διαθέσιμο σε https://www.technologyreview.com/2014/11/26/169918/google-glass-is-dead-long-live-smart-glasses/ .

244 Καθώς παράγουμε επιβλητικές εμπειρίες μέσω των μέσων ενημέρωσης, είτε για την εργασία είτε για διασκέδαση, αυξάνει εκθετικά η ανάγκη διασφάλισής τους: είναι τόσο επιβλητικές και κατά συνέπεια πειστικές. Tim Weber, «How Real Is Virtual Reality», (2016), διαθέσιμο σε https://techonomy.com/2016/12/real-virtual-reality/ .

245 Οι βιομετρικές τεχνολογίες βοηθούν στην αναγνώριση των προσώπων, με τη χρήση μοναδικών προσωπικών χαρακτηριστικών, όπως η αναγνώριση προσώπου, η χροιά της φωνής, η κίνηση των ματιών και τα αποτυπώματα – τα τελευταία είναι τα παλαιότερα και τα πλέον κοινά αναγνωριστικά. Βλ. σχετικά σε https://www.dpa.gr/portal/page?_pageid=33,131182&_dad=portal&_schema=PORTAL

ασφαλείας[246] και για το λόγο αυτό κάποιες πολιτείες των ΗΠΑ, όπως το Ιλινόις, τείνουν να περιορίσουν τη χρήση τους[247]. Σε μία προσπάθεια αυτορύθμισης, η Google δήλωσε επίσημα ότι δεν θα επιτρέπει κάποιες εφαρμογές με βιομετρικά στοιχεία να χρησιμοποιηθούν στα Google Glass, όπως το λογισμικό αναγνώρισης προσώπου[248]. Η χρήση της εφαρμογής PokémonGo από εφήβους και προεφήβους ήγειρε επίσης ερωτηματικά ως προς την εφαρμογή του νόμου περί προστασίας της ιδιωτικότητας των παιδιών εντός του διαδικτύου (Children's Online Privacy Protection Act), ο οποίος ρυθμίζει τις πρακτικές συλλογής δεδομένων σε διαδικτυακούς τόπους και υπηρεσίες και απαιτεί τη γονική συναίνεση για δεδομένα που συλλέγησαν από παιδιά κάτω των 13 ετών[249].

7.3 **Ασφάλεια**

Οι τεχνολογίες της εικονικής κι επαυξημένης πραγματικότητας εγείρουν ανησυχίες και ως προς τα ζητήματα ασφαλείας, τα οποία μπορούν να διακριθούν σε σωματικά ή πνευματικά. Στην πρώτη κατηγορία συγκαταλέγονται οι κίνδυνοι που προκύπτουν, είτε για τους χρήστες είτε γι' αυτούς που τους περιβάλλουν, με τον εξοπλισμό της εικονικής ή επαυξημένης πραγματικότητας κατά τη χρήση μηχανημάτων ή κατά την κίνηση σε δημόσιους χώρους. Δεδομένου ότι οι τεχνολογίες αυτές εξ ορισμού προσθέτουν ακόμα ένα επίπεδο εμπειριών ή πληροφοριών στο αισθητήριο μέσο του χρήστη, εάν διασπάται σε μεγάλο βαθμό η προσοχή του όσο κάνει χρήση της τεχνολογίας αυτής, είτε περπατώντας στην άκρη του οδοστρώματος είτε

246 Claire Gartland, «Biometrics Are a Grave Threat to Privacy», (2016), διαθέσιμο σε https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy .

247 «Biometric Information Privacy Act», 740 Ill. Comp. Stat. 14 (2008).

248 Charles Arthur, «Google 'Bans' Facial Recognition on Google Glass — But Developers Persist», (2013), διαθέσιμο σε https://www.theguardian.com/technology/2013/jun/03/google-glass-facial-recognition-ban . Βλ. επίσης John Brodkin, «Google Forbids Facial Recognition Apps on Glass in the Name of Privacy», (2013), διαθέσιμο σε https://arstechnica.com/information-technology/2013/06/google-forbids-facial-recognition-apps-on-glass-in-the-name-of-privacy/ .

249 R. Atkinson, «Lessons Learned in Data Privacy Compliance from Pokemon Go», Driven, (2016).

κατεβαίνοντας μία σκάλα με κόσμο, θα μπορούσε αυτό να καταστεί επικίνδυνο[250]. Η εφαρμογή PokémonGo ήγειρε ανησυχίες σχετικά με τους κινδύνους που προέκυψαν για τα πλήθη ή τα μεμονωμένα άτομα κατά τη διάρκεια του παιχνιδιού σε συγκεκριμένα δημόσια μέρη[251].

Ένα άλλο ζήτημα ασφαλείας, το οποίο αφορά κυρίως παιδιά, έχει να κάνει με τη φύση του υλικού που παρακολουθεί ο χρήστης, κυρίως εάν πρόκειται για πορνογραφικό ή βίαιο[252]. Ο ρεαλισμός στη φωτογραφία και οι αλληλεπιδράσεις μέσω προσομοιωτή σε κάποια υπερβολικά βίαια παιχνίδια, όπως η σειρά του «Resident Evil»[253], προκαλούν ανησυχίες ως προς τα υψηλά επίπεδα άγχους που παρατηρούνται κατά τη διάρκεια του παιχνιδιού[254]. Ειδικά όσον αφορά στα παιχνίδια εικονικού κόσμου που περιλαμβάνουν όπλα, όπως οι προσομοιωτές ελεύθερων σκοπευτών[255], αυτά δημιουργούν προβληματισμούς, οι οποίοι εκφράζονταν και για τα παλαιότερα βιντεοπαιχνίδια που δεν περιελάμβαναν τεχνολογία εικονικής πραγματικότητας[256]. Επιπλέον, η διάσπαση προσοχής και ο εθισμός κατά τη χρήση των νέων τεχνολογιών αποτελούν ζητήματα προς διερεύνηση σε σχέση με τις τεχνολογίες αυτές και τους ανηλίκους που αφιερώνουν ολοένα και περισσότερο χρόνο σε εικονικά περιβάλλοντα. Τέλος, η παρενόχληση ή το trolling[257] θα μπορούσαν επίσης να θέσουν

250 Geoffrey A. Fowler, «Texting while Walking Isn't Funny Anymore», (2016), διαθέσιμο σε https://www.wsj.com/articles/texting-while-walking-isnt-funny-anymore-1455734501.

251 Lenore Skenazy, «Beware of Pokémon Go. Also, Rollerskates», (2016), διαθέσιμο σε https://www.wsj.com/articles/beware-of-pokemon-go-also-rollerskates-1468796256.

252 Jeff Grubb, «What Oculus Rift and Virtual Reality Mean for Sex, Death, Violence, and Identity», (2014), διαθέσιμο σε https://venturebeat.com/2014/06/05/what-oculus-rift-and-virtual-reality-mean-for-sex-death-violence-and-identity/. Βλ. επίσης Ben Kuchera, «How Should Parents Treat Violence in Virtual Reality?», (2016), διαθέσιμο σε https://www.polygon.com/2016/2/26/11120792/how-should-parents-treat-violence-in-virtual-reality, Stephen Balkam, «The New Realities: Virtual, Augmented and Mixed», διαθέσιμο σε https://www.fosi.org/good-digital-parenting/new-realities-virtual-augmented-and-mixed/ και Darrell M. West, «The Ethical Dilemmas of Virtual Reality», (2016), διαθέσιμο σε https://www.brookings.edu/blog/techtank/2016/04/18/the-ethical-dilemmas-of-virtual-reality/.

253 Πρόκειται για σειρά διαδικτυακών παιχνιδιών τρόμου με ζωντανούς νεκρούς – zombie.

254 Dennis Scimeca, «Resident Evil 7 in Virtual Reality Is a Heart Attack Waiting to Happen», (2016), διαθέσιμο σε https://www.dailydot.com/parsec/resident-evil-7-teaser-demo-e3-2016/.

255 Sam Machkovech, «Ars Tests The Nest, the HTC Vive's First VR Sniper Simulator», (2016), διαθέσιμο σε https://arstechnica.com/gaming/2016/06/ars-tests-the-nest-the-htc-vives-first-vr-sniper-simulator/.

256 Dave Grossman, «Videogames as 'Murder Simulators», (2013), διαθέσιμο σε https://variety.com/2013/voices/opinion/grossman-2640/ .

257 Πρόκειται για μία σειρά δραστηριοτήτων που εκτείνονται από έξυπνες φάρσες, σε παρενόχληση με βίαιες απειλές. Βλ. σχετικά «How Trolls Are Ruining the Internet», (2016), διαθέσιμο σε

σοβαρούς προβληματισμούς για κάποιες περιπτώσεις διαδικυακών τόπων[258] ή βιντεοπαιχνιδιών[259]. Ειδικοί εκφράζουν φόβους ότι το πρόβλημα του trolling θα γίνεται ολοένα και χειρότερο, εξαιτίας της διαδραστικής και ρεαλιστικής φύσης της τεχνολογίας της εικονικής πραγματικότητας[260].

7.4 Προστασία της ελευθερίας λόγου κι έκφρασης

Η ελευθερία της έκφρασης στο διαδίκτυο δεν είναι ένα νέο δικαίωμα, το οποίο δημιουργήθηκε με τη γέννηση του διαδικτύου, αλλά αποτελεί έκφανση του δικαιώματος στην ελευθερία της έκφρασης. Η τελευταία προστατεύεται από το άρθρο 19 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα, καθώς και από το άρθρο 10 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου, και όσον αφορά στην Ελλάδα προστατεύεται και από το άρθρο 14 του Συντάγματος. Η ελευθερία της έκφρασης όμως δεν είναι απεριόριστη. Ο καθένας μπορεί να εκφράζει ελεύθερα τη γνώμη του οπουδήποτε και οποτεδήποτε, αρκεί να μην παραβιάζει τα δικαιώματα άλλων ανθρώπων ή του κοινωνικού συνόλου. Συνεπώς, η ελευθερία της έκφρασης στο διαδίκτυο έχει ως όριο το σεβασμό των δικαιωμάτων των άλλων[261]. Οι δημιουργοί και οι χρήστες των τεχνολογιών της εικονικής κι επαυξημένης πραγματικότητας πρέπει να έχουν διευρυμένο περιθώριο ελευθερίας έκφρασης προς πλήρη αξιοποίηση των δυνατοτήτων αυτών. Όπως ισχύει για όλες τις

https://time.com/4457110/internet-trolls/.

258 Whitney Phillips, «This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture», Cambridge, MA: MIT Press (2015).

259 Scott Thacker και Marc D. Griffiths, «An Exploratory Study of Trolling in Online Video Gaming» *International Journal of Cyber Behavior, Psychology and Learning* 2, no. 4 (2012): 17–33.

260 Conor Cawley, «In Virtual Reality, Trolls Will Be Worse than Ever», (2017), διαθέσιμο σε https://virtualrealityinsider.com/index.php/2017/02/08/in-virtual-reality-trolls-will-be-worse-than-ever/.

261 Πελοπίδας Δόνος, Φίλιππος Βασιλόγιαννης, Τάκης Βιδάλης, Βασίλης Βουτσάκης, Ηλίας Καστανάς, Γιάννης Κτιστάκις, Ευάγγελος Κ. Μάλλιος, Χαράλαμπος Σαββάκης, Ανδρέας Τάκης, Κωνσταντίνος Τσιτσελίκης και Δημήτρης Χριστόπουλος, «Νέες τεχνολογίες και συνταγματικά δικαιώματα», Σάκκουλας, 2004. Βλ. επίσης Μαρία Καρύδα, Σπύρος Κοκολάκης, Λίλιαν Μήτρου, Άννα - Μαρία Πισκοπάνη και Σπύρος Τάσσης, «Facebook, Blogs και δικαιώματα», Σάκκουλας, Αθήνα, 2013 και Αριστείδης Γ. Ασκητής, «Ψηφιακή Ελεύθερη έκφραση. Κράτος, Μέσα Κοινωνικής Δικτύωσης & Μηχανές Αναζήτησης μεταξύ ιδιωτικοποίησης του ελέγχου & ελέγχου του ιδιώτη», Νομική Βιβλιοθηκη, Αθήνα, 2020.

διασυνδεδεμένες τεχνολογίες, έτσι και με τις ανωτέρω ισχύει ο χαρακτηρισμός «τεχνολογίες της ελευθερίας», διότι ενισχύουν με κάθε τρόπο το λόγο ή την έκφραση και κατά συνέπεια, οι νομοθέτες πρέπει να διασφαλίσουν ότι θα απολαμβάνουν του συνταγματικού δικαιώματος της ελευθερίας έκφρασης[262]. Περαιτέρω, το ενδιαφέρον των νομοθετών πρέπει να εστιάσει στη θωράκιση της απαγόρευσης πρόσβασης των ανηλίκων σε περιεχόμενο ακατάλληλο γι' αυτούς ή βίαιης θεματολογίας. Οι ανησυχίες αυτές δεν είναι καινούριες. Οι ίδιες ενστάσεις με τα βιντεοπαιχνίδια[263] οδήγησαν στο παρελθόν σε νομοθετικές ρυθμίσεις σχετικά με το διαδίκτυο και στον Ευρωπαϊκό χώρο[264]. Στην περίπτωση που ο νομοθέτης επιχειρήσει να επιβάλει περιορισμούς στο περιεχόμενο των τεχνολογιών αυτών, το πιο πιθανό είναι ότι αυτές οι πράξεις θα κριθούν δικαστικά και θα ανατραπούν, κάτι που αποτελεί μία λογική προέκταση της σύγχρονης νομολογίας στις ΗΠΑ για την ελευθερία λόγου στο διαδίκτυο[265] και τα βιντεοπαιχνίδια[266].

262 Jonathan W. Emord, «Freedom, Technology, and the First Amendment», *Harvard Journal of Law & Technology,* Vol. 5, (1992): 241-250.

263 «Αυτοί οι φόβοι σε πολλές περιπτώσεις είναι ανάλογοι με εκείνους που εκφράστηκαν για τα βιντεοπαιχνίδια στη δεκαετία του '70 - οι περισσότεροι δεν φαίνεται να δικαιολογούν ούτε νέους νόμους ούτε νέους κανονισμούς». Anne Hobson, «Reality Check», (2016), διαθέσιμο σε https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf .

264 Βλ. σχετικά απόφαση 276/1999/ΕΚ της 25ης Ιανουαρίου 1999 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου περί της θέσπισης προγράμματος Κοινοτικής Δράσης προς προώθηση της ασφαλέστερης χρήσης του Διαδικτύου (πρόγραμμα Safer Internet). Βλ. επίσης Σύμβαση της Βουδαπέστης της 23ης Νοεμβρίου του 2001 του Συμβουλίου της Ευρώπης περί του Κυβερνοεγκλήματος, Ν. 3064/2002 «Καταπολέμηση της Εμπορίας Ανθρώπων, των εγκλημάτων κατά της γενετήσιας ελευθερίας, της πορνογραφίας ανηλίκων και γενικότερα της οικονομικής εκμετάλλευσης της γενετήσιας ζωής και αρωγή στα θύματα των πράξεων αυτών», κοινή δράση 96/68/ΔΕΥ της 22ας Δεκεμβρίου 2003 περί της καταπολέμησης της σεξουαλικής εκμετάλλευσης παιδιών και της παιδικής πορνογραφίας του Συμβουλίου της ΕΕ, Ν.3625/2007 «Κύρωση, εφαρμογή του προαιρετικού Πρωτοκόλλου στη Διεθνή Σύμβαση για τα Δικαιώματα του παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία κι άλλες διατάξεις», άρθρο 348 Α του Ποινικού Κώδικα για την παιδική πορνογραφία κ.ο.κ.

265 *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997), διαθέσιμο σε https://supreme.justia.com/cases/federal/us/521/844/.

266 Brown, *Governor Of California, Et Al. V. Entertainment Merchants Association Et Al*. 564 U.S. 08–1448 (2011), διαθέσιμο σε https://www.supremecourt.gov/opinions/10pdf/08-1448.pdf.

7.5 EULAS (End-User License Agreement)[267]

Πολλές άδειες χρήσης παρουσιάζουν περιορισμούς ως προς την ευθύνη του δημιουργού. Συνηθέστερη περίπτωση είναι όταν μία άδεια έχει σκοπό να διατηρήσει ακέραια τα δεδομένα του χρήστη, αλλά κάποια λογισμικά περιλαμβάνουν και περιορισμούς ως προς την ευθύνη του για τη ζημία που προέκυψε από την κακή χρήση του λογισμικού[268]. Η διαφορά των αδειών EULAS από τις άδειες ελεύθερου λογισμικού (open source license[269]) έγκειται στο ότι μία τέτοια άδεια παραχωρεί στους χρήστες του λογισμικού όλα τα δικαιώματα που απορρέουν από αυτό, σε σχέση με τη χρήση του, την τροποποίησή του και την αναδιανομή δημιουργικής εργασίας και λογισμικού, κάτι που είναι απαγορευμένο σε άλλες περιπτώσεις δυνάμει των διατάξεων του δικαίου πνευματικής ιδιοκτησίας. Οι περισσότερες άδειες των λογισμικών που πωλούνται λιανικά περιορίζουν την ευθύνη για οποιαδήποτε ζημία μέχρι του ποσού αγοράς του λογισμικού.

Στις ΗΠΑ η εφαρμογή των EULAs είναι υποχρεωτική και εξαρτάται από διάφορους παράγοντες, ένας εκ των οποίων είναι το δικαστήριο στο οποίο έχει παραπεμφθεί η

---

267 Πρόκειται για τη σύμβαση ανάμεσα σε αυτόν που έχει την άδεια του λογισμικού και τον αγοραστή, με την οποία καταχωρείται στο δεύτερο το δικαίωμα στη χρήση του λογισμικού. Η άδεια μπορεί να προβλέπει τρόπους (ορθής) χρήσης του αντιγράφου, σε συνδυασμό με τα δικαιώματα που αποκτά αυτομάτως ο αγοραστής, συμπεριλαμβανομένης και της θεωρίας περί πρώτης αγοράς. Πολλές τέτοιου είδους συμβάσεις απαντώνται αποκλειστικά σε ηλεκτρονική μορφή και παρουσιάζονται στο χρήστη ως δυνατότητα μίας επιλογής (κλικ), όπου ο χρήστης πρέπει να «αποδεχθεί» τους όρους. Δεδομένου ότι ένας χρήστης μπορεί να μη δει το συμφωνητικό, παρά μόνο αφού έχει αγοράσει το λογισμικό, τα έγγραφα αυτά έχουν την έννοια της προσχώρησης. Οι εταιρίες παραγωγής λογισμικού συχνά δημιουργούν ειδικά συμφωνητικά με μεγάλες επιχειρήσεις και κυβερνητικούς φορείς, τα οποία περιλαμβάνουν συμβάσεις υποστήριξης και ειδικές εγγυήσεις. Βλ. σχετικά σε https://help.gnome.org/users/gnome-packagekit/stable/eula.html.el .

268 Ορισμένοι κάτοχοι πνευματικών δικαιωμάτων χρησιμοποιούν τέτοιου είδους άδειες χρήσης σε μία προσπάθεια παράκαμψης των περιορισμών που θέτει η εφαρμογή του δικαίου πνευματικής ιδιοκτησίας πάνω στα δικαιώματά τους ή με στόχο να επεκτείνουν τον έλεγχο και σε επίπεδα που δεν προβλέπονται από το δίκαιο πνευματικής ιδιοκτησίας. Jeff Langenderfer, «End-User License Agreements: A New Era of Intellectual Property Control», *Journal of Public Policy & Marketing,* Vol. 28/ 2, Sage Publications, Inc (2009): 202-211.

269 Δίνουν τη δυνατότητα της ελεύθερης χρήσης, τροποποίησης και διαμοιρασμού του λογισμικού. Αντίθετα με τις EULAs, οι άδειες ελεύθερου λογισμικού δεν λειτουργούν ως συμβατικές επεκτάσεις στην ήδη υπάρχουσα νομοθεσία. Δεν υπάρχει κάποιο συμφωνητικό ανάμεσα στα μέρη, διότι μία άδεια πνευματικής ιδιοκτησίας είναι μία δήλωση βάσει της οποίας κάτι επιτρέπεται, το οποίο σε άλλη περίπτωση θα εμποδιζόταν από τις διατάξεις περί πνευματική ιδιοκτησίας. Βλ. σχετικά σε https://opensource.org/licenses.

υπόθεση. Ορισμένα δικαστήρια στα οποία παραπέμφθηκαν υποθέσεις σχετικά με την εγκυρότητα της συρρίκνωσης των συμφωνητικών αδειών, έκριναν τις άδειες άκυρες, χαρακτηρίζοντάς τες ως συμβάσεις προσχώρησης, παράλογες και απαράδεκτες. Κανένα δικαστήριο δεν έκρινε υπέρ της καθολικής εγκυρότητας αυτών των αδειών χρήσης, αλλά μόνο σχετικά με συγκεκριμένες προβλέψεις και όρους[270].

Στην Ελλάδα[271] για να είναι νόμιμη η χρήση του προγράμματος Η/Υ πρέπει «ο δικαιούχος να παραχωρήσει στον αγοραστή την άδεια χρήσης του συγκεκριμένου προγράμματος. Η άδεια αυτή δίνεται μέσω μιας σύμβασης που ονομάζεται «άδεια χρήσης τελικού χρήστη» και δεν αποτελεί σε καμία περίπτωση μεταβίβαση του δικαιώματος. Ο αδειούχος αποκτά απλώς ένα περιορισμένο δικαίωμα χρήσης, όπως αυτό προβλέπεται στη σχετική άδεια»[272]. Παράλληλα, ο χρήστης δεσμεύεται από τους Γενικούς Όρους Συναλλαγών που έχουν τεθεί μέσω των EULAs, εφόσον οι όροι αυτοί δεν είναι αντίθετοι με τις διατάξεις αναγκαστικού δικαίου του Ν. 2121/1993 για την πνευματική ιδιοκτησία αναφορικά με την προστασία προγραμμάτων Η/Υ.

270 Η πιο κοινή κριτική των συμβάσεων αδειών χρήσης είναι ότι συνήθως είναι πολύ μακροσκελείς για να αφιερώσει ο χρήστης χρόνο στην ενδελεχή μελέτη τους. Το Μάρτιο του 2012 η άδεια χρήσης του PayPal αποτελούνταν από 36.275 λέξεις και το αντίστοιχο συμφωνητικό των iTunes το Μάιο του 2011 αποτελούνταν από 56 σελίδες, παραδείγματα που ενισχύουν το γεγονός ότι κανείς δεν αφιερώνει χρόνο στην ανάγνωσή τους, εξαιτίας του μεγέθους τους. Πολλές εταιρίες εκμεταλλεύθηκαν αυτήν την παραδοχή και πρόσθεσαν άχρηστους όρους στις συμβάσεις αδειών χρήσης τους έχοντας ως δεδομένο ότι λίγοι χρήστες θα τα διαβάσουν. Επίσης, οι συμβάσεις αδειών χρήσης EULA έχουν υποστεί κριτική για το γεγονός ότι περιλαμβάνουν όρους οι οποίοι επιβάλλουν επαχθείς υποχρεώσεις στους καταναλωτές. Ben Stegner, «8 Ridiculous EULA Clauses You May Have Already Agreed To», (2019), διαθέσιμο σε https://www.makeuseof.com/tag/10-ridiculous-eula-clauses-agreed/ .

271 Οι συμβατικές ρήτρες που θεωρούνται καταχρηστικές δε δεσμεύουν τους καταναλωτές. Ωστόσο, το υπόλοιπο συμβόλαιο εξακολουθεί να ισχύει σε περιπτώσεις που αυτό είναι νομίμως δυνατό. Οι χώρες της ΕΕ πρέπει να διασφαλίσουν την ύπαρξη μέσων έννομης προστασίας ώστε να προλαμβάνεται η χρήση καταχρηστικών ρητρών στις συμβάσεις. Βλ. σχετικά Οδηγία (ΕΕ) 2019/2161 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Νοεμβρίου 2019 για την τροποποίηση της οδηγίας 93/13/ΕΟΚ του Συμβουλίου, και των οδηγιών 98/6/ΕΚ, 2005/29/ΕΚ και 2011/83/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου όσον αφορά την καλύτερη επιβολή και τον εκσυγχρονισμό των κανόνων της Ένωσης για την προστασία των καταναλωτών.

272 Ομάδα Εργασίας ΤΕΕ, «Μελέτη των πνευματικών δικαιωμάτων του έργου που παράγεται και διακινείται στο ΤΕΕ», (2009), διαθέσιμο σε http://library.tee.gr/digital/m2386.pdf .

7.6 ToS (Terms of Service)[273]

Η σύμβαση που εμπεριέχει τους όρους αυτούς χρησιμοποιείται κυρίως για νομικούς λόγους από τους ιστότοπους και τους παρόχους υπηρεσιών διαδικτύου που συγκεντρώνουν προσωπικά δεδομένα, όπως το ηλεκτρονικό εμπόριο και τα μέσα κοινωνικής δικτύωσης. Η χρήση της σύμβασης των όρων λειτουργίας είναι νομικά δεσμευτική και δυνητικά μπορεί να υπόκειται σε αλλαγές. Μία σύμβαση όρων λειτουργίας συνήθως περιλαμβάνει ένα ή περισσότερα από τα παρακάτω θέματα:

i. Την αποσαφήνιση ή την απόδοση ορισμού λέξεων - κλειδιών και φράσεων.
ii. Δικαιώματα και υποχρεώσεις των χρηστών.
iii. Σωστή ή αναμενόμενη χρήση και πιθανή κακή χρήση.
iv. Οδηγίες ως προς την ευθύνη από ενέργειες και συμπεριφορές εντός του διαδικτύου.
v. Πολιτική ιδιωτικότητας, η οποία ρυθμίζει τη χρήση των προσωπικών δεδομένων.
vi. Λεπτομέρειες πληρωμών σχετικά με τα μέλη ή τέλη εγγραφής.
vii. Πολιτική αποκλεισμού (opt – out), η οποία περιγράφει τη διαδικασία λήξης του λογαριασμού, στις περιπτώσεις που αυτό παρέχεται.
viii. Άρνηση / περιορισμός ευθύνης με την οποία διευκρινίζεται η νομική ευθύνη του ιστότοπου για τυχόν ζημίες που προκλήθηκαν από τους χρήστες
ix. Ενημέρωση του χρήστη σε σχέση με την τροποποίηση των όρων, αν αυτό παρέχεται.
x. Πολιτική για τα cookies

273 Οι όροι λειτουργίας (συνήθως απαντώνται ως ToS ή TOS και αναφέρονται επίσης ως όροι χρήσης και όροι και προϋποθέσεις) είναι κανόνες τους οποίους πρέπει κάποιος να συμφωνήσει να τηρήσει ώστε να μπορέσει να χρησιμοποιήσει μία υπηρεσία. Πολλές φορές αυτοί οι όροι αποτελούν ουσιαστικά μία άρνηση (disclaimer), ειδικά για τη χρήση των ιστοτόπων. Βλ. σχετικά σε https://en.wikipedia.org/wiki/Terms_of_service

7.7 Εγκυρότητα των δικαιοπραξιών

Σε αντίθεση με την Ευρώπη και την Ελλάδα όπου δεν υπάρχει μέχρι στιγμής κάποιο αντίστοιχο προηγούμενο, τόσο στις ΗΠΑ, όσο και στην Αυστραλία, τα δικαστήρια απεφάνθησαν ότι είναι έγκυρες οι διαθήκες που έχουν συνταχθεί είτε σε τάμπλετ είτε σε «έξυπνο» τηλέφωνο, παρά την έλλειψη υπογραφής και του ιδιόχειρου χαρακτήρα που θα έπρεπε να έχει[274].

7.8 Αδικοπραξίες

Διερευνώντας το ζήτημα της αδικοπρακτικής ευθύνης ενός χρήστη των υπηρεσιών του διαδικτύου προέχει ο προσδιορισμός του τόπου τελέσεως του αδικήματος. Σύμφωνα με τον Ευρωπαϊκό Κανονισμό 864/2007[275] ο γενικός κανόνας είναι ότι «το εφαρμοστέο δίκαιο επί εξωσυμβατικής ενοχής η οποία απορρέει από αδικοπραξία, είναι το δίκαιο της χώρας στην οποία επέρχεται η ζημία, ανεξαρτήτως της χώρας στην οποία έλαβε χώρα το ζημιογόνο γεγονός, καθώς και της χώρας ή των χωρών στις οποίες το εν λόγω γεγονός παράγει έμμεσα αποτελέσματα, εκτός αν ορίζεται άλλως στον παρόντα κανονισμό». Επίσης, σύμφωνα με την απόφαση του ΔΕΕ *C-441/13 Pez Hejduk v EnergieAgentur NRW GmbH, «*το άρθρο 5, σημείο 3, του κανονισμού (ΕΚ) 44/2001 του Συμβουλίου, της 22ας Δεκεμβρίου 2000, για τη διεθνή δικαιοδοσία, την αναγνώριση και την εκτέλεση αποφάσεων σε αστικές και εμπορικές υποθέσεις, έχει την έννοια ότι, σε περίπτωση προβαλλόμενης προσβολής του δικαιώματος πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων που κατοχυρώνονται στο κράτος μέλος του δικαστηρίου ενώπιον του οποίου ασκήθηκε

274 Παρά την έλλειψη των βασικών αυτών προϋποθέσεων, το Δικαστήριο έκρινε πως ο διαθέτης βρισκόταν σε πλήρη συνείδηση, είχε σαφή πρόθεση σύνταξης της τελευταίας του βούλησης και ως εκ τούτου η διαθήκη του είναι νομικά έγκυρη. Βλ. σχετικά «ΗΠΑ: Κήρυξη διαθήκης γραμμένης σε ταμπλέτα ως έγκυρης», (2013), διαθέσιμο σε https://lawnet.gr/law-news/dikeo-technologia/hpa-kiruxi-dia8ikis-grammenis-se-tampleta-os-egkuris/ και «Έγκυρη διαθήκη γραμμένη σε iphone», (2013), διαθέσιμο σε https://lawnet.gr/law-news/dikeo-technologia/egkuri-dia8iki-grammeni-se-iphone/ .

275 Κανονισμός (ΕΚ) Αριθ. 864/2007 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Ιουλίου 2007 για το εφαρμοστέο δίκαιο στις εξωσυμβατικές ενοχές («Ρώμη ΙΙ»).

σχετική αγωγή, το τελευταίο έχει δικαιοδοσία, ως δικαστήριο του τόπου επελεύσεως της ζημίας, να κρίνει επί της αγωγής εφόσον ζητείται να αναγνωριστεί ευθύνη για την προσβολή των ως άνω δικαιωμάτων λόγω αναρτήσεως προστατευόμενων φωτογραφιών σε διαδικτυακό ιστότοπο προσβάσιμο στην περιφέρειά του. Το δικαστήριο αυτό είναι αρμόδιο να κρίνει μόνον επί της ζημίας που προκλήθηκε εντός του κράτους μέλους όπου έχει την έδρα του»[276]. Στις ΗΠΑ ισχύει οι κανόνες του «Proper Law of a Tort» και του «Internet Analysis».

7.9 **Ειδικά ζητήματα κυριότητας**

Η τεχνολογία της επαυξημένης πραγματικότητας επαυξάνει αντικείμενα, τοποθεσίες και πρόσωπα του υπαρκτού κόσμου με εικονικές εμπειρίες. Η επαύξηση αυτή των αντικειμένων και των τοποθεσιών εμπλέκει αναγκαστικά το εμπράγματο δίκαιο (ή το αμερικανικό δίκαιο ιδιοκτησίας)[277]. Ένα διηνεκές χαρακτηριστικό του ψηφιακού τοπίου είναι ο πόλεμος για την «ψηφιακή γη»[278]. Ο νόμος περί προστασίας των καταναλωτών από τον κυβεροσφετερισμό[279] (Anticybersquatting Consumer

276 ΔΕΕ *C-441/13 Pez Hejduk v EnergieAgentur NRW GmbH.*

277 Ας φανταστούμε ότι κάποιος «επαυξάνει» το γειτονικό του σπίτι με μία εικονική ετικέτα, η οποία εμπεριέχει μία προσβλητική λέξη που είναι ορατή μέσω μίας εφαρμογής της επαυξημένης πραγματικότητας. Με αυτόν τον τρόπο προκύπτει το ζήτημα εάν μπορεί αυτός που υφίσταται την προσβολή να διεκδικήσει δικαιώματα, ως ιδιοκτήτης του σπιτιού, με στόχο την αφαίρεση της προσβλητικής εικονικής επιγραφής. Joshua A.T. Fairfield, Mixed Reality: «How the Laws of virtual worlds govern everyday life», Berkeley Technology Law Journal, Vol. 27 (2012) .

278 Για παράδειγμα, στις αρχές της ανάπτυξης του διαδικτύου υπήρχαν λίγα και διαφορετικά ονόματα χώρου ανώτερου επιπέδου (top level domain names). Κάποια από αυτά ήταν περιορισμένα, όπως οι καταλήξεις .mil και .edu. Άλλα ήταν γενικά, όπως τα .net, .org, και .com. Δεν έγινε άμεσα αισθητό ότι ένα όνομα χώρου με κατάληξη .com θα μεταβαλλόταν στο πιο πολύτιμο τμήμα «γης» στο διαδίκτυο, παρά μόνο όταν έγινε η πρώτη επιλογή των αναζητήσεων των καταναλωτών και στη συνέχεια προέκυψαν νομικές διαμάχες για τα ονόματα χώρου με την ίδια κατάληξη. Οι διαμάχες αυτές προκάλεσαν τη νομοθέτηση του Κογκρέσου προς ενίσχυση των δικαιωμάτων των ιδιοκτητών σημάτων, επιτρέποντάς τους να έχουν ονόματα χώρου για τα άτομα που τα είχαν κατοχυρώσει. David E. Weslow, «Cybersquatting & Internet IP», https://www.wiley.law/practices-cybersquatting-and-internet-IP .

279 Το ζήτημα του «κυβερνοσφετερισμού» ανέκυψε για πρώτη φορά στην ελληνική νομολογία με την υπόθεση Amazon και στη συνέχεια με την υπόθεση του «Αθήνα 2004». Όταν το γνωστό αμερικανικό βιβλιοπωλείο επιχείρησε να κατοχυρώσει στην Ελλάδα την ηλεκτρονική διεύθυνση http://www.amazon.gr διεπίστωσε ότι το σχετικό όνομα πεδίου είχε καταχωρηθεί από ελληνική επιχείρηση βιβλιοπωλείου σε κάποιο νησί. Η σχετική υπόθεση εκδικάσθηκε από το Μονομελές Πρωτοδικείο Σύρου, το οποίο με την υπ' αριθ. 637/1999 απόφαση ασφαλιστικών μέτρων δικαίωσε την

Protection Act) επιτρέπει στον δικαιούχο ενός καταχωρημένου σήματος να λάβει όνομα χώρου που διαχωρίζει το εν λόγω σήμα από τα υπόλοιπα.

Οι διαμάχες για τη διαδικτυακή «γη» συνεχίζονται και στη σφαίρα της επαυξημένης πραγματικότητας, όπως για παράδειγμα σε σχέση με τις ετικέτες δεδομένων αναγνώρισης της γεωγραφικής θέσης του χρήστη (geolocated data tags[280]) στην περίπτωση των εφαρμογών Google Earth[281] και Google Maps[282], σε βάρος των οποίων πολλές ευρωπαϊκές χώρες ανέπτυξαν ενστάσεις, εξαιτίας της έλλειψης ελέγχου των εικονικών απεικονίσεων των κατοικιών και των ιδιοκτησιών σε αυτές. Πόλεμοι σχετικά με την «ψηφιακή» γη θα ανακύψουν και στο μέλλον στους αντανακλαστικούς κόσμους (mirror worlds[283]). Για παράδειγμα η εφαρμογή της πλήρους έκδοσης τριών διαστάσεων (3D) του Google Earth παρέχει στους χρήστες

αμερικανική εταιρία και απαγόρευσε στους καθ' ων την χρήση του ονόματος πεδίου amazon.gr. Την προστασία της δικαιοσύνης ζήτησε και ο Οργανισμός «Αθήνα 2004», όταν διαπίστωσε ότι ελληνική εταιρία παροχής τηλεπικοινωνιακών υπηρεσιών είχε κατοχυρώσει υπέρ αυτής το domain name www.olympicgames2004.gr . Η ενέργεια αυτή κρίθηκε προσβλητική του δικαιώματος στο σήμα καθ' όσον με τον Ν. 2598/1998 προστατεύτηκαν ως σήματα υπέρ του Οργανισμού «Αθήνα 2004», εκτός των άλλων, και οι όροι «Ολυμπιακός», «Ολυμπιάδα», «Ολυμπιακοί Αγώνες 2004», «Ολυμπιακοί Αγώνες – Ελλάδα», η επωνυμία και ο διακριτικός της τίτλος «Αθήνα 2004» και κάθε άλλος συναφής όρος στα Ελληνικά ή σε οποιαδήποτε ξένη γλώσσα. Με την υπ' αριθ. 9485/2000 απόφασή του το Μον. Πρωτ. Αθηνών δικαίωσε τον αιτούντα Οργανισμό και απαγόρευσε στην καθ' ης την χρήση του επίμαχου ονόματος χώρου στο διαδίκτυο, υποχρέωσε το Ι.Τ.Ε. να διακόψει τη σύνδεση της καθ' ης εταιρίας στο διαδίκτυο με domain name «Olympicgames2004» και να προβεί επιπλέον σε ακύρωση της καταχώρισης του εν λόγω domain name, διέταξε δημοσίευση περιλήψεως της αποφάσεως αυτής και του διατακτικού της σε δύο ημερήσιες εφημερίδες, και απείλησε χρηματική ποινή σε περίπτωση εκ νέου παραβίασης του δικαιώματος του αιτούντος. Βλ. σχετικά https://greeklaw.wordpress.com.

280 Η διαδικασία της πρόσθεσης γεωγραφικών αναγνωριστικών – μεταδεδομένων σε διάφορα μέσα, όπως μία γεωγραφικά προσδιορισμένη φωτογραφία ή βίντεο, ιστότοποι, μηνύματα κινητών κλπ. Τα δεδομένα αυτά συνήθως αποτελούνται από συντεταγμένες γεωγραφικού πλάτους και μήκους, όπως επίσης μπορεί να περιλαμβάνουν στοιχεία ύψους, απόστασης, δεδομένα ακριβείας και ονόματα τοποθεσιών, ακόμα και χρονοσημάνσεις. Βλ. σχετικά https://fpf.org/2020/05/22/understanding-the-world-of-geolocation-data/ .

281 Πρόκειται για πρόγραμμα γραφικής απεικόνισης της Γης, το οποίο είναι διαθέσιμο στο διαδίκτυο. Κατασκευάστηκε από την εταιρεία Keyhole Inc. με το όνομα «Earth Viewer 3D». Πήρε το σημερινό του όνομα το 2004, όταν η εταιρεία αγοράστηκε από την Google. Βλ. σχετικά https://www.google.com/earth/

282 Πρόκειται για υπηρεσία χαρτογράφησης στο διαδίκτυο. Η εφαρμογή και η τεχνολογία της παρέχεται από την Google και υποστηρίζει πολλές υπηρεσίες που βασίζονται σε χάρτες, συμπεριλαμβανομένης της ιστοσελίδας Χάρτες Google. Παρέχει οδικούς χάρτες και τη δυνατότητα σχεδιασμού διαδρομών για μεταφορά με τα πόδια, το αυτοκίνητο, ποδήλατο ή μέσα μαζικής μεταφοράς. Περιλαμβάνει επίσης τον εντοπισμό των επιχειρήσεων που βρίσκονται σε διάφορες πόλεις σε όλο τον κόσμο. Οι δορυφορικές εικόνες των Χαρτών Google δεν ανανεώνονται σε πραγματικό χρόνο, ωστόσο η Google προσθέτει τακτικά νέα δεδομένα στη κύρια βάση δεδομένων της και οι περισσότερες από τις εμφανιζόμενες εικόνες δεν είναι παλαιότερες των τριών ετών. Βλ. σχετικά σε https://www.google.com/maps

283 Πρόκειται για εικονικούς κόσμους στους οποίους αντανακλάται ο πραγματικός. «Mirror Worlds: The Universe in a Box?», *(IN)VISIBLE,* Springer, Vienna (2008): 36-72.

της τη δυνατότητα να βλέπουν αναπαραστάσεις τριών διαστάσεων από κτίρια και ταυτόχρονες αναμεταδόσεις από κάμερες σε συγκεκριμένες τοποθεσίες.

Με τις αντιδικίες αυτές σε σχέση με την «ψηφιακή» γη τίθενται πολλά νομικά ζητήματα, με κυριότερο το αν στην περίπτωση αυτή το δίκαιο πνευματικής ιδιοκτησίας είναι το σωστό νομικό πλαίσιο το οποίο πρέπει να εφαρμοστεί. Η τεχνολογία της επαυξημένης πραγματικότητας θα εντείνει την τάση του ελέγχου από τις εταιρίες. Δεδομένου ότι η τεχνολογία αυτή συγκλίνει πραγματικές και εικονικές εμπειρίες προκύπτει ο κίνδυνος οι κάτοχοι «εικονικών» δικαιωμάτων[284] να υπερισχύσουν έναντι των κατόχων των «πραγματικών» δικαιωμάτων[285], οι οποίοι θα εξαφανισθούν. Περαιτέρω, η τεχνολογία της επαυξημένης πραγματικότητας θεωρείται πολυ-καναλική (multi-channel) άσκηση. Μόνο να υποθέσει μπορεί κάποιος ποιες εφαρμογές και ποια κανάλια θα κυριαρχήσουν σε αυτές τις εφαρμογές. Παρόλα αυτά, από τη στιγμή που μία εφαρμογή ή ένα κανάλι καθίσταται πράγματι κυρίαρχο, οι χρήστες που υιοθετούν πρώτοι την τεχνολογία αυτή διατρέχουν τον κίνδυνο να τεθούν στην άκρη προς ενίσχυση των κατόχων των πνευματικών δικαιωμάτων. Και στη συνέχεια, τα δικαιώματα των κατόχων της απτής ιδιοκτησίας δεν θα ενισχύονται εξίσου με αυτά των κατόχων δικαιωμάτων πνευματικής ιδιοκτησίας.[286]

7.10 Δικαίωμα στην ιδιωτική ζωή

Η έλευση των φορητών υπολογιστών ενεργοποίησε το απόλυτο όνειρο (ή εφιάλτη) του αδιάλειπτου εντοπισμού των πολιτών. Τις περισσότερες φορές, πάντως, δεν είναι η Πολιτεία που εντοπίζει τους πολίτες, αλλά η ίδια η τεχνολογία που χρησιμοποιούν. Πρόκειται για την τεχνολογία του εντοπισμού, η οποία είναι αρκετά διαδεδομένη και

284 Κάτοχοι πνευματικών δικαιωμάτων.

285 Πραγματικά πρόσωπα και κάτοχοι απτών ιδιοκτησιών.

286 Granit Curri, «Intellectual Property Law – Age of Internet», *Academic Journal of Interdisciplinary Studies,* Vol 5/ 3, MCSER Publishing, Rome-Italy, (2016): 364-367.

προβληματική. Τα αυτοκίνητα που χρησιμοποιεί η υπηρεσία Google Street view[287] κατά καιρούς εντόπισαν μη κρυπτογραφημένα προσωπικά δεδομένα, καθώς εισέβαλαν στην ιδιωτική ζωή των κατοικιών των καταναλωτών. Το Facebook δημιούργησε μία εφαρμογή που επιτρέπει σχεδόν στον καθένα να συλλαμβάνει μεγάλο όγκο πληροφοριών μέσω της εγκατάστασής της από ένα προφίλ σε ένα άλλο. Με την τεχνολογία GPS που περιλαμβάνουν τα κινητά τηλέφωνα καταγράφονται συνεχώς οι θέσεις των χρηστών εντός του πραγματικού κόσμου. Οι πάροχοι υπηρεσιών του διαδικτύου κάνουν ακριβώς το ίδιο, εντοπίζοντας τους πελάτες τους στο ψηφιακό τοπίο. Αντιστοίχως οι ευρυζωνικοί πάροχοι κινητών τεχνολογιών, όχι μόνο εντοπίζουν τη θέση των χρηστών τους, αλλά τη συσχετίζουν και με τις συνήθειες διαδικτυακής αναζήτησης των χρηστών. Με τον ίδιο τρόπο, οι φίλοι και οι οικογένειες των χρηστών μπορούν να τους εντοπίσουν με τη χρήση μίας ευρέως διαδεδομένης τεχνολογίας[288]. Από τη στιγμή που ένα πρόσωπο λαμβάνει μία φωτογραφία και την ανεβάζει σε μέσο κοινωνικής δικτύωσης, η υπηρεσία αναγνώρισης προσώπων[289] μπορεί να αναγνωρίσει και να συνδέσει το πρόσωπο της φωτογραφίας με μεταδεδομένα, τα οποία συνήθως περιλαμβάνουν ημερομηνίες και τη θέση του στον πραγματικό κόσμο. Οι κυβερνήσεις δεν χρειάζονται κάτι παραπάνω

287 Το «Street View» των Χαρτών Google αποτελεί μια ψηφιακή αναπαράσταση του περιβάλλοντος χώρου στους Χάρτες Google, η οποία απαρτίζεται από εκατομμύρια πανοραμικές εικόνες. Το περιεχόμενο του «Street View» προέρχεται από δύο πηγές, την Google και τους χρήστες. Βλ. σχετικά https://www.google.com/streetview/ .

288 «Στο πλαίσιο του συμμετοχικού διαδικτύου υπάρχει (και) μία μεγάλη κατηγορία πληροφοριών που μπορεί να μην αντίκειται ευθέως στο νόμο, αλλά εντάσσονται στην κατηγορία των ενοχλητικών. Πρόκειται για όλες αυτές τις πληροφορίες της καθημερινότητάς μας που δεν επιθυμούμε να εμφανίζονται: μία φωτογραφία με πρόσωπα ή τόπους που δεν θέλουμε να συσχετιζόμαστε, μία συμμετοχή σε εκδήλωση αντίθετη με αρχές που διακηρύσσουμε, ακόμα και αν δεν είμαστε πρόσωπα της επικαιρότητας. Για όλες αυτές τις κατηγορίες ενοχλητικών πληροφοριών η ανεύρεση του δράστη δεν ωφελεί. Χρησιμότερη εμφανίζεται η δυνατότητα για άμεσα αφαίρεση και – στο μέτρο που είναι εφικτό στο Internet - η παύση της περαιτέρω διάδοσης ... Στην προσπάθεια για την αναζήτηση της ευθύνης των παρόχων – ενδιάμεσων, τις πρώτες κρίσιμες κατευθύνσεις θα δώσει το Ιδιωτικό Διεθνές Δίκαιο, αφού στο Ίντερνετ εξ ορισμού υπάρχει στοιχείο αλλοδαπότητας». Βλ. σχετικά Γιώργος Ν. Γιαννόπουλος, «Η ευθύνη των παρόχων υπηρεσιών στο Internet», Νομική Βιβλιοθήκη, Αθήνα (2013): 29, 31.

289 Inioluwa Deborah Raji, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee και Emily Denton, «Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing», AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, (2020): 145–151.

από το να αναζητήσουν τις πληροφορίες από τα τρίτα μέρη που τις έχουν ήδη συλλέξει και ευρετηριάσει[290].

Η διαδικτυακή ιδιωτικότητα αποτελεί μείζον θέμα σε ό,τι έχει σχέση με την τεχνολογία της επαυξημένης πραγματικότητας, μιας και αυτή η τεχνολογία επιτρέπει σε κυβερνητικούς φορείς και ιδιώτες να γνωρίζουν τόσο το ψηφιακό προφίλ ενός προσώπου, όσο και τις συνήθειές του στον πραγματικό κόσμο. Έξω από το διαδίκτυο, οι δραστηριότητες του πραγματικού κόσμου είναι πλέον κωδικοποιημένες και καταγεγραμμένες, αναλυμένες και προς μεταπώληση, χάρη στην ολοκλήρωση των εφαρμογών της επαυξημένης πραγματικότητας στην καθημερινότητα, όπως ακριβώς συμβαίνει και με τις διαδικτυακές δραστηριότητες[291]. Η τεχνολογία της επαυξημένης πραγματικότητας καθιστά ολοένα και περισσότερο την ιδιωτικότητα απατηλή και ανέφικτη. Στην πραγματικότητα κάποιοι παροτρύνουν όσους ενδιαφέρονται για την ιδιωτικότητα να εγκαταλείψουν τις διαδικτυωμένες τεχνολογίες[292].

Από τη στιγμή που οι άνθρωποι συνεχώς προσπαθούν να κρατήσουν κάποιες πληροφορίες εμπιστευτικές και άλλοι συνεχώς ψάχνουν να τις ανακαλύψουν ή να τις αποκαλύψουν, η ιδιωτικότητα χρειάζεται περιχαράκωση. Είναι ακόμη σχεδόν αδύνατο να περιηγηθεί κάποιος στο διαδίκτυο με ασφάλεια ή να χρησιμοποιήσει ένα κινητό τηλέφωνο χωρίς να αποκαλύπτει συνέχεια τη φυσική του θέση ή προσωπικές

290 Sam duPont, «Facial Recognition Is Here But We Have No Laws. Without legal safeguards, this technology will undermine democratic values and fundamental rights», (2020), διαθέσιμο σε https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/ .

291 Η οδική διαδρομή ενός χρήστη μπορεί να διασταυρωθεί με τις συνήθειές του κατά την περιήγησή του στο διαδίκτυο. Η περιήγηση ενός καταναλωτή κατά τη διάρκεια της ημέρας είναι εξίσου εμπορεύσιμο αγαθό με το ποιες ιστοσελίδες έχει επισκεφθεί και ο συνδυασμός των δύο είναι ακόμη πιο ισχυρός. CMA, «The commercial use of consumer data Report on the CMA's call for information», (2015), διαθέσιμο σε https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf .

292 Ο πρώην Διευθύνων Σύμβουλος της Google Eric Schmidt υπονόησε ότι οι χρήστες οι οποίοι δεν θέλουν να εντοπίζονται από τη Google μέσα στο διαδίκτυο, συμπεριλαμβάνοντας και κάθε ιστότοπο που εξυπηρετεί η Google και αναφέρεται σε αυτή, δεν πρέπει να χρησιμοποιούν το διαδίκτυο. Jared Newman, «Google's Schmidt Roasted for Privacy Comments», (2009), διαθέσιμο σε https://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html .

και οικονομικές πληροφορίες[293]. Και η περιχαράκωση αυτή έχει επιτευχθεί στις χώρες της Ευρωπαϊκής Ένωσης μέσω του ΓΚΠΔ και των σχετικών εφαρμοστικών νόμων.

7.11 **Εφαρμοστέο Δίκαιο**

Με τη σύγκλιση των εικονικών κόσμων και του αληθινού, οι νόμοι που διέπουν τις εικονικές εμπειρίες θα καταλήξουν να διέπουν την καθημερινότητα, κυρίως διότι οι νόμοι εκτός κι εντός διαδικτύου απομακρύνονται αισθητά οι μεν από τους δε. Ας αναλογιστεί κάποιος το απλό παράδειγμα της αγοράς ενός αντικειμένου. Αν αγοράσει ένα βιβλίο εκτός διαδικτύου, το βιβλίο αυτό του ανήκει. Αν αντιθέτως, αγοράσει ένα ηλεκτρονικό βιβλίο, δεν αποκτά το εμπράγματο δικαίωμα της κυριότητας. Καθώς, λοιπόν, οι τεχνολογίες της επαυξημένης πραγματικότητας επιτυγχάνουν τη σύγκλιση του αληθινού περιβάλλοντος και του κυβερνοχώρου, η ερώτηση η οποία προκύπτει είναι αν οι εντός ή εκτός διαδικτύου νόμοι θα καθορίσουν τα δικαιώματα των καταναλωτών πάνω στην ιδιοκτησία τους και τα δεδομένα[294].

Οι εικονικοί κόσμοι δεν μπορούν να διαχωριστούν νομικά από τον αληθινό. Όλοι οι εικονικοί κόσμοι είναι, έως ένα βαθμό, επαυξημένοι. Τους βιώνουν αληθινοί άνθρωποι, οι οποίοι παρεμβάλλουν σε αυτούς στοιχεία της πραγματικότητας. Ο κόσμος μπορεί να είναι εικονικός, αλλά οι οικονομικές, καλλιτεχνικές, ακόμη και ρομαντικές ζωές των συμμετεχόντων είναι πραγματικές[295]. Η παρούσα κατάσταση

293 Joshua A.T. Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal*, Vol. 27 (2012).

294 «Οι ολοένα και αυξανόμενες νομικές ρυθμίσεις, ως απάντηση στην επαυξημένη πραγματικότητα, θα λύσουν τις υπάρχουσες νομικές έριδες, ενώ ταυτόχρονα θα εγείρουν και νέες ερωτήσεις. Για παράδειγμα, η αναπτυσσόμενη θεωρία της επαυξημένης πραγματικότητας θα θέσει τέλος στη θεωρητική ιδέα του «Μαγικού Κύκλου», ενός μεταφορικού νομικού συνόρου, το οποίο οι σχολιαστές υπέθεσαν ότι διακρίνει τον αληθινό κόσμο από τους εικονικούς». Joshua A.T. Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal*, Vol. 27 (2012).

295 Οι νόμοι που διέπουν τον αληθινό κόσμο θα εφαρμοστούν και στα δύο κύρια στοιχεία που συνοδεύουν την εμπειρία της επαυξημένης πραγματικότητας: η πνευματική ιδιοκτησία και οι συμβάσεις του ηλεκτρονικού εμπορίου θα συνεχίσουν να διέπουν το λογισμικό και το υλικολογισμικό (firmware) στις συσκευές και το κοινό δίκαιο θα εξακολουθήσει να ρυθμίζει τις κινήσεις και τις πράξεις των χρηστών στον αληθινό κόσμο. Μολαταύτα, το κύριο θέμα ανάμεσα σε αυτές τις δύο σφαίρες είναι η παραβίαση των συμβάσεων του ηλεκτρονικού εμπορίου και της πνευματικής ιδιοκτησίας στον αληθινό κόσμο. Τίθεται λοιπόν, το ερώτημα εάν οι νόμοι περί πνευματικής ιδιοκτησίας πρόκειται να ρυθμίσουν μέχρι ποια έκταση μπορούν οι χρήστες να χρησιμοποιήσουν την ιδιοκτησία τους, όπως προς το παρόν

της τεχνολογίας οριοθετεί, στην πράξη, τις ενέργειες στις οποίες μας επιτρέπεται να προχωρήσουμε, τα αντικείμενα τα οποία επιτρέπεται να δημιουργήσουμε και τις σχέσεις τις οποίες μας επιτρέπεται να διαμορφώσουμε[296]. Δεδομένου ότι οι τεχνολογικές αλλαγές αποτελούν συχνά την αφορμή για νομικά προβλήματα, για τέσσερις κατά βάση λόγους οι τεχνολογικές αλλαγές θα πρέπει απαραιτήτως να προκαλέσουν και νομικές αλλαγές:

i. Νέες ρυθμίσεις. Πρέπει να ρυθμιστούν νέες μορφές συμπεριφοράς και για το λόγο αυτό κρίνεται απαραίτητο να υπάρξουν ειδικοί νόμοι.
ii. Αβεβαιότητα. Όταν ο νόμος εφαρμόζεται σε νέες μορφές συμπεριφοράς, οι υπάρχοντες κανόνες πρέπει να διευκρινιστούν για να μην προκύψουν ασαφή σημεία.
iii. Έκταση των ρυθμίσεων. Οι υπάρχοντες κανόνες δεν συμπεριέλαβαν στις διατάξεις τους τις νέες τεχνολογίες. Κατά συνέπεια, οι νέες μορφές συμπεριφοράς περιλαμβάνουν ή αποκλείουν κάποιους κανόνες με την παρούσα τους μορφή.
iv. Αιτιολόγηση των ρυθμίσεων. Κάποιοι υπάρχοντες κανόνες βασίζονται ρητά ή έμμεσα σε μία υπόθεση η οποία δεν υπάρχει πλέον και για το λόγο αυτό θα πρέπει να αιτιολογηθούν[297].

Αν γίνει αντιληπτός ο τρόπος με τον οποίο οι νομικοί κανόνες αποτυγχάνουν το στόχο τους μπροστά στις τεχνολογικές αλλαγές, θα μπορούσε αυτό να συνδράμει στη βελτίωση της τεχνικής της δημιουργίας τους και να προκύψει ένα σχέδιο

ρυθμίζουν τις εφαρμογές που χρησιμοποιούν στις συσκευές τους. Χωρίς την ανάπτυξη μίας θεωρίας για την επαυξημένη πραγματικότητα, η πνευματική ιδιοκτησία και οι συμβάσεις ηλεκτρονικού εμπορίου θα αντικαταστήσουν το κοινό δίκαιο. Ό.π. υποσημ. 238.

296 Είναι κοινός τόπος το γεγονός ότι οι τεχνολογικές αλλαγές έχουν επιρροή στο νόμο. Πριν κάτι καταστεί δυνατό, δεν υπάρχει η ανάγκη να προσδιοριστεί το πώς θα τύχει αντιμετώπισης από νομικούς κανόνες ή το αν θα είναι επιτρεπτό ή απαγορευμένο. Οι προβληματισμοί ξεκινούν (με αυξανόμενη επιτακτικότητα) από τη στιγμή που συλλαμβάνεται, αναπτύσσεται και διαχέεται ένα τεχνολογικό επίτευγμα στην κοινωνία . Lyria Bennett Moses, «Agents of Change: How the Law Copes with Technological Change», *Griffith Law Revew,* Vol. 20/ 4 (2011): 763-794.

297 Δεν θεωρείται δεδομένο ότι κάθε νέα τεχνολογία θα δημιουργήσει νομικά ζητήματα. Μολαταύτα, καθώς η τεχνολογία αλλάζει, καθώς δημιουργούνται νέες οντότητες, δραστηριότητες και σχέσεις, υπάρχει πάντα το ενδεχόμενο αυτά να προκύψουν. «The Rule of Law in the Technological Age Challenges and opportunities for the EU», ACELG's Annual Conference 2016.

αναμόρφωσης των ρυθμίσεων στα αρχικά στάδια ανάπτυξης της τεχνολογίας[298]. Τις περισσότερες φορές θα εφαρμοστεί στις νέες συνθήκες ένας νόμος προγενέστερος των τεχνολογικών αλλαγών[299]. Η τεχνολογική αλλαγή είναι μία μορφή κοινωνικής αλλαγής. Αν η κοινωνική αλλαγή αφορά στον τρόπο με τον οποίο οι άνθρωποι σκέφτονται και πράττουν, η τεχνολογική αλλαγή αφορά στο τι έχουν την τεχνική ικανότητα να πράξουν. Τα δύο είναι στενά συνδεδεμένα. Οι φιλόσοφοι και οι κοινωνιολόγοι έχουν πολλές φορές σχολιάσει την έκταση με την οποία η τεχνολογία έχει εισχωρήσει στις ζωές των ανθρώπων και στον τρόπο σκέψης τους. Δείγματα ενθουσιασμού και φόβου για τις ικανότητες της τεχνολογίας μπορεί κανείς να δει στα μέσα ενημέρωσης και στον πολιτισμό. Ωστόσο, οι φόβοι σχετικά με τις ικανότητες της τεχνολογίας δημιουργούν επίσης την ανάγκη για έλεγχο μέσω των ρυθμίσεων[300]. Η ιδέα του κρατικού ελέγχου στην τεχνολογία είναι γενικά πιο δημοφιλής από τον κρατικό έλεγχο στην κοινωνική ζωή. Το ενδεχόμενο ύπαρξης νομικών προβλημάτων από τις τεχνολογικές αλλαγές έρχεται πρώτο σε σχέση με την απόλυτη κοινωνική αποδοχή, τη διάδοση της τεχνολογίας και τις επερχόμενες κοινωνικές επιπτώσεις. Τα

298 Παρόμοια προβλήματα θα μπορούσαν να προκύψουν κατά την επίδραση της εξελισσόμενης τεχνολογίας στην κοινωνία. Για παράδειγμα, μοιάζει πιο εύλογο να συμπεράνει κανείς ότι το διαδίκτυο προκαλεί, κατά μέσο όρο, κατάθλιψη, από το να πει ότι η συζήτηση, κατά μέσο όρο έχει το ίδιο αποτέλεσμα, ακόμη και αυτό στατιστικά είναι ορθό. Οι δικαστές συχνά πέφτουν στην παγίδα να θεωρήσουν ότι ο νόμος πρέπει να είναι διαφορετικός όταν τα γεγονότα λαμβάνουν χώρα στο διαδίκτυο. Brian Christopher Jones, «The Online/Offline Cognitive Divide: Implications for Law», *SCRIPT-ed*, Vol. 13/ 1, (2016): 83-94.

299 Ο αποστολέας μηνύματος μέσω ηλεκτρονικού ταχυδρομείου (e-mail) συνιστά και εκδότη του κειμένου που συνοδεύει το μήνυμα, καθόσον η μοναδική για κάθε χρήστη ηλεκτρονική διεύθυνση που έχει οριστεί και εφαρμοστεί από τον ίδιο τον αποστολέα έχει το χαρακτήρα της ιδιόχειρης υπογραφής. Η μηχανική απεικόνιση του μηνύματος σε έντυπο εμπίπτει στην έννοια του ιδιωτικού εγγράφου με αποδεικτική δύναμη εις βάρος του εκδότη του (συνδυασμός των άρθρων 443, 444 και 445 ΚΠολΔ). Βλ. σχετικά ΜΠρΑθ 1963/2004 [Σύγκληση Γ. Σ. σωματείου μέσω e-mail] (σημ. Γ. Γιαννόπουλος), *ΔΙΤΕ (π. ΔΙΜΕΕ),* Τεύχος 3/2004, σελ. 404. Επίσης, ένα δικαστήριο στην Πολιτεία της Μασαχουσέτης δεν δυσκολεύτηκε να αποφασίσει ότι το όνομα που αποτυπώνεται στο τέλος μίας ηλεκτρονικής αλληλογραφίας αποτελεί υπογραφή, όπως αναλογικά το όνομα που αποτυπωνόταν στο τέλος ενός τηλεγραφήματος είχε γίνει αποδεκτό ως υπογραφή σε προγενέστερες υποθέσεις. Lyria Bennett Moses, «Why Have a Theory of Law and Technological Change?», *Minnesota Journal of Law, Science & Technology,* 8, 2 (2007):589-606.

300 Όταν ιδιαίτερα τεχνολογικά επιτεύγματα εγείρουν ισχυρές αντιδράσεις, όπως στην περίπτωση της ανθρώπινης κλωνοποίησης, το ενδιαφέρον της κοινωνίας μπορεί να οδηγήσει σε απαγορεύσεις. Ακόμη και όταν τα οφέλη ξεπερνούν τις βλάβες, όπως στην περίπτωση της εξωσωματικής αναπαραγωγής, προκύπτει μερικές φορές η ανάγκη να λειτουργήσει ο νόμος ως όριο για να καθησυχάσει τις ανησυχίες του κόσμου. Νικόλαος Ματσανιώτης, «Βιοηθικά διλήμματα: πρόσφατα και μελλοντικά», (2005), διαθέσιμο σε https://www.iatrikionline.gr/Deltio_52d/07.htm .

νομικά προβλήματα που συνδέονται με τις τεχνολογικές αλλαγές είναι έτσι πιο επείγοντα και πιο δύσκολο να προβλεφθούν από ότι τα νομικά προβλήματα που συνδέονται με τις κοινωνικές αλλαγές. Σαφώς και όταν η τεχνολογία γίνει ευρέως αποδεκτή και σε χρήση, τα νομικά προβλήματα που συνδέονται με αυτή καθίστανται πιο σημαντικά[301].

Η «θεωρία του Μαγικού Κύκλου» αποτελεί μία θεωρία δημοφιλή στο παρελθόν για την αντιμετώπιση των ανωτέρω περιγραφομένων ζητημάτων. Πρόκειται για τη νοητή γραμμή ανάμεσα στους εικονικούς κόσμους και αυτόν που θεωρείται ως αληθινός[302]. Η προστασία του εικονικού παιχνιδιού είναι η πρώτη λειτουργία του «Μαγικού Κύκλου». Τα άτομα κατά τη συμμετοχή τους στο εικονικό παιχνίδι συχνά ενεργούν με σενάρια που θα ήταν εκτός των ορίων του νόμου στον αληθινό κόσμο. Στα βιντεοπαιχνίδια, για παράδειγμα, οι παίκτες μπορούν να αφαιρέσουν τη ζωή των εικονικών χαρακτήρων των άλλων παικτών. Οι υποστηρικτές του «Μαγικού Κύκλου» θεωρούν ότι δεν εφαρμόζονται νομοθετικές ρυθμίσεις εντός του παιχνιδιού, παρά μόνο όταν παραβιάζονται οι κανόνες του, όπως, για παράδειγμα, όταν ένας παίκτης προκαλέσει ζημία σε άλλον παίκτη[303]. Άλλη εφαρμογή της θεωρίας του «Μαγικού Κύκλου» είναι αυτό που αποκαλείται «ξεκίνημα από την αρχή», οι «ίσοι όροι ανταγωνισμού», το «λευκό μητρώο». Κυριαρχεί η αντίληψη, η οποία

301 Lyria Bennett Moses, «Why Have a Theory of Law and Technological Change?», *Minnesota Journal of Law, Science & Technology,* 8, 2 (2007):589-606.

302 Ο στόχος του «Μαγικού Κύκλου» είναι να προστατευθεί ο εικονικός κόσμος από εξωτερικές επιρροές, όπως ο νόμος, τα οικονομικά θέματα του αληθινού κόσμου, τα πραγματικά χρήματα κλπ. Η έννοια του «Μαγικού Κύκλου» έγκειται στο ότι οι πράξεις που συμβαίνουν στον εικονικό κόσμο δεν είναι πραγματικές και για το λόγο αυτό δεν μπορεί να εφαρμοστούν κατ' αντιστοιχία οι νόμοι του αληθινού κόσμου. Με αυτό το σκεπτικό, οι νόμοι του αληθινού κόσμου έχουν μείνει εκτός εικονικών κόσμων. Ο «Μαγικός Κύκλος», όμως, θα έπρεπε να απομυθοποιηθεί, διότι δεν υπάρχει «αληθινός» κόσμος διαχωρισμένος από τον «εικονικό». Όλες οι υποτιθέμενες «εικονικές» ενέργειες προέρχονται από πραγματικά πρόσωπα και έχουν επίδραση πάνω σε πραγματικά πρόσωπα μέσα από ένα περιβάλλον διαχειριζόμενο από υπολογιστή. Κατά συνέπεια, η διάκριση ανάμεσα μίας «εικονικής» και μίας «πραγματικής» ενέργειας δεν έχει σημασία. Θα ήταν πιο ορθό αν η έννοια του «Μαγικού Κύκλου» αντικαθίστατο από την έννοια της «συναίνεσης». Αυτό που έχει σημασία είναι εάν η ενέργεια που πραγματοποιήθηκε – ένα δάγκωμα σε αγώνα πυγμαχίας, ένα χτύπημα στο κεφάλι σε αγώνα ποδοσφαίρου ή μία κλοπή σε εικονική ιδιοκτησία, είναι μέσα στο εύρος της συναίνεσης των άλλων παικτών. Joshua A.T. Fairfield, «The Magic Circle», 14 Vand. J. Ent. & Tech. L. 545 (2012).

303 Douglas Brown, «Games and the Magic Circle», Newton Lee, Encyclopedia of Computer Graphics and Games, Springer, 2015.

τροφοδοτείται κυρίως από τα μέσα ενημέρωσης ότι κάποιοι παίκτες των εικονικών κόσμων, κοινωνικά περιθωριοποιημένοι, επιθυμούν μία νέα ζωή στο εικονικό κόσμο. Η θεωρία του «Μαγικού Κύκλου», όμως, έχει τεθεί σε λανθασμένη βάση. Πρέπει να γίνει αντιληπτό από τους υποστηρικτές της ότι τα σενάρια που θα ήταν εκτός των ορίων του νόμου στον αληθινό κόσμο, είναι παράνομα και στον εικονικό, στον οποίο αντανακλώνται εντέλει οι αξίες του πραγματικού κόσμου. Δικαιώματα όπως η ισότητα, η προσωπική και θρησκευτική ελευθερία, η απαγόρευση των βασανιστηρίων, η προστασία της ανηλικότητας και των προσωπικών δεδομένων, τα οποία προστατεύονται ρητά τόσο από το ελληνικό Σύνταγμα, όσο και από το Χάρτη των Θεμελιωδών Δικαιωμάτων και την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, πρέπει να τύχουν προστασίας μέσω της θεωρίας της τριτενέργειας των ατομικών δικαιωμάτων[304], η οποία στην περίπτωση των εικονικών κόσμων μπορεί να εφαρμοστεί στην ιδιωτικής φύσεως σχέση του παρόχου με το χρήστη[305].

Κρίνοντας από μία άλλη σκοπιά, για τους παίκτες που επιθυμούν να δουν τις διασυνδεδεμένες κοινωνίες να θέτουν τους δικούς τους κανόνες, δεν έχουν χαθεί τα πάντα. Φαίνεται απίθανο στον αληθινό κόσμο να αναγνωριστούν οι διασυνδεδεμένες κοινωνίες ως ξεχωριστές και ισότιμες, αλλά είναι πιθανό τα δικαστήρια του αληθινού κόσμου να επεξεργαστούν σοβαρά τους κανόνες που παράγονται από τις διασυνδεδεμένες κοινωνίες, καθώς αναλαμβάνουν το καθήκον να εφαρμόσουν το νόμο στους εικονικούς κόσμους. Η βασική ερώτηση δεν είναι το αν οι ενέργειες είναι πραγματικές ή εικονικές, αλλά το αν η συγκεκριμένη ενέργεια ξεφεύγει από την έκταση συναίνεσης των μερών[306]. Οι κανόνες του παιχνιδιού προκύπτουν από το

304 Ό.π. υποσημείωση 81 περί τριτενέργειας.

305 βλ. χαρακτηριστικά Πρόταση ψηφίσματος του Ευρωπαϊκού Κοινοβουλίου σχετικά με την απαγόρευση της πώλησης και της διανομής στην Ευρώπη του βιντεοπαιχνιδιού «Rule of Rose» (όπου «παρουσιάζονται παιδιά και διεστραμμένες, βίαιες και σαδιστικές εικόνες, οι οποίες θίγουν την ανθρώπινη αξιοπρέπεια και [...] ο μόνος απώτερος στόχος είναι η υποκίνηση στη βία, στην επίδειξη ισχύος και στην κακομεταχείριση των πλέων αδύναμων») και τη δημιουργία ενός Ευρωπαϊκού Παρατηρητηρίου για την παιδική ηλικία και τους ανήλικους, διαθέσιμο σε https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B6-2007-0023+0+DOC+XML+V0//EL.

306 Ό.π. υποσημ. 269.

συνδυασμό τουλάχιστον τεσσάρων νομικών πηγών: i) από τις συμβάσεις άδειας του τελικού χρήστη (EULAs) που σχεδιάζονται από τους δημιουργούς του παιχνιδιού (τις εταιρίες που δημιουργούν και συντηρούν τους εικονικούς κόσμους), ii) από τους κανόνες που διαπραγματεύονται οι κοινότητες, iii) από τη συναίνεση του παίκτη[307] και iv) από τους ήδη υπάρχοντες νόμους. Επιπρόσθετα, οι παίκτες μπορεί να συναινέσουν σε ενέργειες οι οποίες είναι πέρα από τα όρια των EULAs και των προτύπων των κοινοτήτων. Για παράδειγμα, οι κανόνες συναίνεσης του χρήστη απαγορεύουν την εισβολή (hacking) σε λογαριασμούς άλλων παικτών και οι κανόνες των κοινοτήτων συμφωνούν. Κατά συνέπεια, η παράνομη αυτή εισβολή εμπίπτει και στο συμβατικό δίκαιο και στις διατάξεις περί αδικοπραξιών. Σε άλλες περιπτώσεις, οι κανόνες συναίνεσης του χρήστη και οι κανόνες των κοινοτήτων μπορεί να μην συγκλίνουν.

Οι συμβάσεις αδειών τελικού χρήστη δημιουργούν νομικές υποχρεώσεις ανάμεσα στο δημιουργό του παιχνιδιού και τον παίκτη και ταυτόχρονα προτείνουν κανόνες οι οποίοι θα μπορούσαν να υιοθετηθούν ως πρότυπα κοινοτήτων. Οι άδειες αυτές έχουν μεγάλο αντίκτυπο στα πρότυπα των κοινοτήτων και παρ' όλα αυτά δεν είναι η μοναδική πηγή νόμου στους εικονικούς κόσμους, αλλά αλληλεπιδρούν με τα πρότυπα των κοινοτήτων, τη συναίνεση του προσώπου και τον ήδη υπάρχοντα νόμο για να παράγουν νομικά αποτελέσματα και κανόνες που λειτουργούν στους εικονικούς κόσμους. Το αν θα πραγματοποιηθεί μία ενέργεια στον εικονικό κόσμο εξαρτάται από το εύρος της συναίνεσης ανάμεσα στα μέρη. Τα δικαιώματα θα αλλάξουν και αυτό εξαρτάται από τις σχέσεις ανάμεσα στα μέρη[308]. Κάτω από αυτό

307 Αντίθετα από τη συμβατική έννοια της συναίνεσης, ως προς την αδικοπραξία, η παραβίαση των κανόνων του παιχνιδιού μπορεί να εμπεριέχεται στη συναίνεση των παικτών προς το παιχνίδι. Μία ενέργεια στο ποδόσφαιρο που αποτελεί offside είναι ενάντια στους κανονισμούς, αλλά μέσα στα όρια της αναμενόμενης συμπεριφοράς στο παιχνίδι και δεν είναι αξιόποινος. Υπάρχει ένα φάσμα επιτρεπτής συμπεριφοράς: εάν κάτι είναι τεχνικά εκτός των κανόνων, αλλά μέσα στο πλαίσιο της συναίνεσης, δεν θα επιφέρει νομικές ευθύνες. Αντί, λοιπόν, οι νομικοί να εξετάσουν αν οι πράξεις οι σχετιζόμενες με τους εικονικούς κόσμους είναι «πραγματικές» ή «εικονικές», θα έπρεπε να εξεταστεί το εύρος της συγκατάθεσης των συμμετεχόντων. Joshua A.T. Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal*, Vol. 27 (2012).

308 Για παράδειγμα, το πρόβλημα σχετικά με την εικονική ιδιοκτησία. Σε πολλές άδειες χρήσης υποστηρίζεται ότι ο παίκτης δεν έχει δικαιώματα κυριότητας στην εικονική ιδιοκτησία. Παρόλα αυτά, οι

το πρίσμα, οι παίκτες στους εικονικούς κόσμους είναι αληθινοί, οι ενέργειές τους είναι πραγματικές και ακόμη και τα εικονικά αντικείμενα είναι πραγματικά. Η κρίσιμη ερώτηση δεν είναι εάν η ιδιοκτησία είναι πραγματική ή όχι, ούτε εάν ο αφαιρών αυτή είναι πραγματικός ή εικονικός, αλλά εάν η δεδομένη πράξη που συνδέεται με την ιδιοκτησία είναι εντός ή εκτός της έκτασης της συναίνεσης των μερών. Επομένως, δεν είναι η φύση του παιχνιδιού ως αληθινού ή εικονικού που καθορίζει εάν η παραβίαση των κανόνων επισύρει νομική ευθύνη ή όχι, αλλά το κατά πόσο η πράξη του παίκτη ξεπερνά την έκταση της συναίνεσης που δόθηκε από τους άλλους παίκτες. Τα πρόσωπα που εισέρχονται στους εικονικούς κόσμους είναι πραγματικά, οι πράξεις τους μέσα σε αυτούς τους κόσμους είναι πραγματικές και οι συνέπειες αυτών των πράξεων πάνω σε άλλα άτομα είναι και αυτές πραγματικές. Έτσι είναι αβάσιμο να πει κάποιος ότι οι εικονικοί κόσμοι δεν υπόκεινται στους νόμους του αληθινού κόσμου, από τη στιγμή που η αληθινή συναίνεση που δόθηκε από αληθινά πρόσωπα είναι η πηγή του νόμου στους εικονικούς κόσμους[309].

αξιώσεις μεταξύ παικτών εξακολουθούν να εκδικάζονται από τα δικαστήρια ανά τον κόσμο σαν να πρόκειται για υπαρκτά δικαιώματα. Σύμφωνα με τους ισχύοντες κανόνες, το δικαίωμα κυριότητας στην εικονική ιδιοκτησία δεν αντιτίθεται στους δημιουργούς του παιχνιδιού, αλλά μπορεί να έρχεται σε αντίθεση με άλλους παίκτες. Ανάμεσα στο δημιουργό του παιχνιδιού και τον παίκτη η κυριότητα θα θεωρηθεί ότι ανήκει στο δημιουργό, αλλά εάν κάποιος παίκτης αφαιρέσει την εικονική περιουσία κάποιου άλλου παίκτη, θα ευθύνεται γι΄ αυτό. Michael Zhou, Mark A.A.M. Leenders και Ling Mei Cong, «Ownership in the virtual world and the implications for long-term user innovation success», *Technovation,* Vol. 78, (2018): 56-65.

309 F. Gregory Lastowka και Dan Hunter, «The Laws of the Virtual Worlds», *California Law Review,* Vol. 92/ 1 (2004):1-73.

ΤΕΤΑΡΤΟ ΚΕΦΑΛΑΙΟ: Τεχνητή Νοημοσύνη

1 Εισαγωγικά

Αν και τα άτομα και η κοινωνία έχουν επωφεληθεί από την πρόοδο σε τομείς όπως η ανθρώπινη γονιδιωματική[1], η ανθρώπινη εξέλιξη ή οι τεχνολογίες της τεχνητής νοημοσύνης και της ρομποτικής, αυτού του είδους οι τεχνολογίες παρουσιάζουν ηθικές προκλήσεις και έχουν τη δυνατότητα να αμφισβητήσουν τις ανθρώπινες αξίες και τον τρόπο ζωής, αλλά και να έχουν αρνητική επιρροή πάνω στα ανθρώπινα δικαιώματα. Πρόσφατη έρευνα[2] ανέδειξε τις δυσμενείς επιπτώσεις των τεχνολογιών της τεχνητής νοημοσύνης και της ρομποτικής, οι οποίες είναι ποικίλες και συμπεριλαμβάνουν ενδεικτικά τη μείωση του ελέγχου του ατόμου πάνω στα δεδομένα του, τις αρνητικές επιδράσεις στην ιδιωτική του ζωή, την αύξηση των διακρίσεων, την επιβολή και επικράτηση της κυρίαρχης τάξης και του πλούτου, τον κίνδυνο βλαβών από τα αυτόνομα συστήματα και τα όπλα και την αύξηση της επιτήρησης[3]. Κατ' επέκταση, τίθενται ερωτήματα, όπως το ποια είναι η ανθεκτικότητα των κοινοτήτων που δυνητικά θα επηρεαστούν και το πόσο ευάλωτες είναι οι κοινότητες αυτές σε τόσο δυσμενείς επιδράσεις[4]. Σύμφωνα με την έρευνα, μεγαλύτερη ανθεκτικότητα παρατηρείται στις κοινωνίες της Δύσης, όπου οι τεχνολογίες της τεχνητής νοημοσύνης και της ρομποτικής έχουν εξελιχθεί και οι επιπτώσεις τους είναι ελεγχόμενες. Επίσης, το ίδιο παρατηρείται και στις κοινότητες

1 Πρόκειται για τη δυνατότητα της επιστήμης να «διαβάζει» ολόκληρο τον γενετικό κώδικα ενός ατόμου και να εξάγει χρήσιμα συμπεράσματα. Ιωάννα Α. Σουφλέρη, «Το ελληνικό Κέντρο Γονιδιωματικής», (2016), διαθέσιμο σε https://www.tovima.gr/2016/05/20/science/to-elliniko-kentro-gonidiwmatikis/ .

2 Βλ. σχετικά πρόγραμμα SIENNA σε https://www.sienna-project.eu/.

3 Βλ. σχετικά https://www.trilateralresearch.com/work/sienna/

4 Οι αρνητικές συνέπειες των τεχνολογιών της τεχνητής νοημοσύνης και της ρομποτικής θα επηρεάσουν εξαιρετικά κάποιες κοινότητες, ενώ μία μερίδα αυτών θα προσαρμοστεί καλύτερα. Τα ανθεκτικά μέρη μπορεί να έχουν συγκεκριμένες αξίες ή πόρους, τα οποία εάν παρέχονταν και στους ευάλωτους, θα μπορούσαν να αυξήσουν την ευημερία τους και να μειώσουν τις βλάβες από τις αρνητικές συνέπειες. Εάν η επιστήμη λάβει υπόψη της τα ζητήματα της ανθεκτικότητας και της ευπάθειας, μπορεί να βοηθήσει στο μέλλον στην έρευνα και την πολιτική των τεχνολογιών της τεχνητής νοημοσύνης και της ρομποτικής. Βλ. σχετικά Rowena Rodrigues, «AI and robotics adverse impacts – how resilient or vulnerable are we?», (2020), διαθέσιμο σε https://www.trilateralresearch.com/ai-and-robotics-adverse-impacts-how-resilient-or-vulnerable-are-we/ .

που στηρίζονται σε ισχυρές αξίες που τις ενοποιούν, αλλά και στα άτομα που είναι ανοιχτά στις εξελίξεις κι έχουν την ικανότητα να προσαρμόζονται με ταχύτητα στις αλλαγές[5]. Χωρίς θεσμικές ρυθμίσεις που να καθοδηγούν την εξέλιξη και την εφαρμογή των τεχνολογιών της τεχνητής νοημοσύνης και της ρομποτικής, θα αυξηθεί η ευπάθεια στον ανθρώπινο τρόπο ζωής και η ανοχή θα μειωθεί ή θα παραμείνει η ίδια, κάτι που χρειάζεται μελλοντική έρευνα και συζήτηση. Απαιτείται, επίσης και η εκτίμηση του είδους των ρυθμίσεων που θα είναι οι πιο κατάλληλες ώστε να επωφεληθεί η ανθρώπινη κοινωνία από τς ανωτέρω τεχνολογίες.

Σε έρευνα σχετικά με το ποια περιοχή στον κόσμο θεωρείται η πιο ευάλωτη από τις τεχνολογίες αυτές, ως τέτοια αναγνωρίζεται το νότιο ημισφαίριο. Παρότι οι ανησυχίες είναι παρόμοιες παντού, υπογραμμίζεται ότι οι κίνδυνοι από τον τρόπο που επηρεάζονται οι νότιοι πολιτισμοί μπορεί να επιδεινωθούν για τους ευάλωτους πληθυσμούς τους, κυρίως αυτούς που δεν έχουν πρόσβαση στις καθιερωμένες διατάξεις των ανθρωπίνων δικαιωμάτων[6]. Έχουν εκφραστεί, επίσης, ανησυχίες σχετικά με το ενδεχόμενο η τεχνολογία της τεχνητής νοημοσύνης να εκτοπίσει εκατομμύρια θέσεων εργασίας στο μέλλον ή να καταστρέψει την ανάπτυξη περιοχών όπως η Αφρική[7].

Σημαντική ευάλωτη ομάδα αποτελούν οι εργαζόμενοι, κυρίως οι νέοι, οι οποίοι είτε χάνουν τη θέση εργασίας τους είτε πρέπει να αλλάξουν εργασία[8]. Η ομάδα αυτή είναι ευάλωτη στις συνέπειες της τεχνολογίας της τεχνητής νοημοσύνης, όταν τα μέλη της δεν έχουν την απαιτούμενη εκπαίδευση ή τις κατάλληλες δεξιότητες που θα τους επιτρέψουν να προσαρμοστούν στις μεταβαλλόμενες τεχνολογίες και τους εξαιρετικά αυτοματοποιημένους χώρους εργασίας. Αλλά και οι κοινωνίες, στις οποίες τα άτομα

5 Βλ. σχετικά https://www.sienna-project.eu/digitalAssets/787/c_787382-l_1-k_sienna-d4.1-state-of-the-art-review--final-v.04-.pdf .

6 Chinmayi Arun, «AI and the Global South: Designing for Other Worlds», (2019), σε Markus D. Dubber, Frank Pasquale και Sunit Das (eds.), «The Oxford Handbook of Ethics of AI», Oxford University Press.

7 Ian Goldin, «Will AI kill developing world growth?» (2019), διαθέσιμο σε https://www.bbc.com/news/business-47852589 .

8 Euan Cameron, «How will automation impact jobs?», διαθέσιμο σε https://www.pwc.co.uk/services/economics/insights/the-impact-of-automation-on-jobs.html .

στερούνται παιδείας και ευκαιριών για επανεκπαίδευση, είναι πιο ευάλωτες. Τέλος, επηρεάζονται σημαντικά τα παιδιά και οι ηλικιωμένοι. Μία αναφορά της UNISEF[9] καταδεικνύει τα αυξημένα τρωτά σημεία των παιδιών, λόγω της έκθεσής τους και της έλλειψης έγκρισης κατάλληλων μέτρων ασφαλείας και προειδοποίησης από τις εταιρείες που πωλούν προϊόντα τεχνολογίας τεχνητής νοημοσύνης και ρομποτικής και προσφέρουν τέτοιου είδους υπηρεσίες. Οι ηλικιωμένοι είναι εξίσου ευάλωτοι, βάσει των πιθανών δυσμενών συνεπειών των τεχνολογιών της τεχνητής νοημοσύνης και ρομποτικής πάνω στην αξιοπρέπειά τους, την αυτονομία τους, την ιδιωτικότητά τους και την αποστασιοποίησή τους από άλλα άτομα, λόγω της αντικατάστασης των ανθρωπίνων υπηρεσιών από μηχανές[10].

2 Ορισμοί

Τεχνητή Νοημοσύνη (Artificial intelligence): η επιστήμη και μηχανική των μηχανών με ικανότητες νοημοσύνης αντίστοιχης με την ανθρώπινη. Μπορεί να διαχωριστεί σε δύο τομείς: στην «ισχυρή» τεχνητή νοημοσύνη[11] και την «αδύναμη»[12]. Στην πρώτη περίπτωση η τεχνολογία αυτή μπορεί να ανταπεξέλθει σε οποιαδήποτε πνευματική εργασία που απαιτεί ανθρώπινη ιδιότητα και θεωρείται ότι είναι ικανή να περιέλθει σε γνωσιακές καταστάσεις παραπλήσιες του ανθρωπίνου εγκεφάλου. Η «αδύναμη» τεχνητή νοημοσύνη μπορεί να εκτελεί «έξυπνες» εργασίες

9 Βλ. σχετικά «Executive Summary Artificial Intelligence and Childrens Rights», (2019), διαθέσιμο σε https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf .

10 Sarah Knapton, «Care-bots' for the elderly are dangerous, warns artificial intelligence professor», (2016), διαθέσιμο σε https://www.telegraph.co.uk/science/2016/05/30/care-bots-for-the-elderly-are-dangerous-warns-artificial-intelli/ .

11 Βλ. σχετικά https://www.ocf.berkeley.edu/~arihuang/academic/research/strongai3.html#:~:text=Strong%20AI%20is%20a%20term,functionally%20equal%20to%20a%20human's

12 Βλ. σχετικά https://www.investopedia.com/terms/w/weak-ai.asp#:~:text=Weak%20artificial%20intelligence%20(AI)%E2%80%94,that%20humans%20sometimes%20can't .

αποκλειστικά σε συγκεκριμένους τομείς, όπως η οπτική ταξινόμηση ψηφιακών εικόνων)[13].

Η τεχνολογία της τεχνητής νοημοσύνης εμφανίστηκε για πρώτη φορά τη δεκαετία του 1950 και οι ρίζες της εκτείνονται στους τομείς της Φιλοσοφίας, των Μαθηματικών, της Υπολογιστικής, της Βιολογίας και της Ψυχολογίας. Περιλαμβάνει τις τεχνολογίες της μηχανικής μάθησης, των νευρωνικών δικτύων, της εξελιγκτικής υπολογιστικής[14], της ρομποτικής, των συστημάτων των εμπειρογνωμόνων[15], του σχεδιασμού, της επεξεργασίας της ομιλίας[16], της επεξεργασίας της φυσικής γλώσσας[17], της υπολογιστικής όρασης[18] και άλλες. Οι βασικοί στόχοι της έρευνας της τεχνολογίας της τεχνητής νοημοσύνης είναι η συστηματική έρευνα του φαινομένου της νοημοσύνης και η ανάπτυξη χρήσιμων προγραμμάτων και εργαλείων που θα εκτελούν τις εργασίες που υπό άλλες συνθήκες θα απαιτούσαν νοημοσύνη.

Μηχανική μάθηση (machine learning): Όταν κάποιος μελετά την τεχνητή νοημοσύνη ο πρώτος όρος που συναντά είναι η «μηχανική μάθηση» (machine learning). Πρόκειται για υποπεδίο της επιστήμης των υπολογιστών που ασχολείται με

13 Λεωνίδας Κανέλλος, «Εφαρμογές Τεχνητής Νοημοσύνης, Νομική Βιβλιοθήκη», (2021). Βλ. επίσης πρόγραμμα SIENNA, D4.1: State-of-the-art Review, (2018), διαθέσιμο σε https://www.sienna-project.eu/digitalAssets/787/c_787382-l_1-k_sienna-d4.1-state-of-the-art-review--final-v.04-.pdf .

14 Αποτελεί ένα νέο αλλά εξελισσόμενο τομέα της Υπολογιστικής Νοημοσύνης και περικλείει ένα σύνολο από ισχυρά εργαλεία βελτιστοποίησης και αναζήτησης λύσεων σε δύσκολα πραγματικά προβλήματα, όπου δεν υπάρχουν αναλυτικές ή άλλες μέθοδοι επίλυσης. Βλ. σχετικά http://informatics.teicm.gr/index.php?option=com_content&view=article&id=95:2010-05-22-09-18-55&catid=24:courses&Itemid=127 .

15 Πρόκειται για συστήματα υπολογιστών τα οποία μιμούνται την ικανότητα λήψης αποφάσεων ενός ανθρώπινου εμπειρογνώμονα. Έχουν σχεδιαστεί για να επιλύουν σύνθετα προβλήματα μέσω σωμάτων γνώσης που αναπαριστώνται κυρίως με τους κανόνες if–then, παρά μέσω του συμβατικού κώδικα διαδικασίας. Βλ. σχετικά https://onlinelibrary.wiley.com/journal/14680394

16 Πρόκειται για τομέα της επιστήμης των υπολογιστών που πραγματεύεται το σχεδιασμό των υπολογιστικών συστημάτων που αναγνωρίζουν τον προφορικό λόγο. Βλ. σχετικά https://www.sciencedirect.com/topics/neuroscience/speech-processing .

17 Πραγματεύεται την αλληλεπίδραση μεταξύ των υπολογιστών και των ανθρώπων με τη χρήση της φυσική γλώσσας. Michael J. Garbade, «A Simple Introduction to Natural Language Processing», (2018), διαθέσιμο σε https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32 .

18 Πρόκειται για το πεδίο εκείνο που αναζητά την ανάπτυξη τεχνικών, με στόχο την υποβοήθηση των υπολογιστών να δουν και να καταλάβουν το περιεχόμενο των ψηφιακών εικόνων, όπως των φωτογραφιών και των βίντεο. Jason Brownlee, «A Gentle Introduction to Computer Vision», (2019), διαθέσιμο σε https://machinelearningmastery.com/what-is-computer-vision/ .

τα προγράμματα των υπολογιστών που έχουν την ικανότητα να μαθαίνουν μέσω της εμπειρίας και να βελτιώνουν συνεχώς, με την πάροδο του χρόνου, τις επιδόσεις τους[19]. Η έκφραση ότι οι υπολογιστές «μαθαίνουν» αποτελεί περισσότερο μία μεταφορά, καθώς δεν υπονοείται ότι τα υπολογιστικά συστήματα αναπαράγουν τεχνητά τα προηγμένα γνωστικά συστήματα που πιστεύεται ότι εμπλέκονται στην ανθρώπινη μάθηση[20]. Περισσότερο μπορούμε να θεωρήσουμε ότι οι αλγόριθμοι αυτοί μαθαίνουν με μία λειτουργική έννοια: έχουν την ικανότητα να μεταβάλλουν τη συμπεριφορά τους μέσω της εμπειρίας, με στόχο την ενίσχυση της απόδοσής τους σε κάποια εργασία. Συνήθως, οι αλγόριθμοι μηχανικής μάθησης χρησιμοποιούνται για την ανίχνευση μοτίβων των δεδομένων για την αυτοματοποίηση σύνθετων εργασιών ή την παραγωγή προβλέψεων. Τέτοιου είδους αλγόριθμοι χρησιμοποιούνται σε ποικιλία σε εμπορικές εφαρμογές του πραγματικού κόσμου, όπως είναι τα αποτελέσματα της έρευνας στο διαδίκτυο, η αναγνώριση προσώπου[21], η ανίχνευση της απάτης και η εξόρυξη δεδομένων. Επίσης, η μηχανική μάθηση συνδέεται στενά με την ευρύτερη βιομηχανία των προγνωστικών ανάλυσης (predictive analytics[22]),

19 Stuart Russell και Peter Norvig, «Artificial Intelligence: A Modern Approach», (2010).

20 Ian H. Witten, «Data Mining: Practical Machine Learning Tools And Techniques» (2011).

21 Τα τελευταία χρόνια οι εταιρίες αναζητούν στο διαδίκτυο δημόσιες φωτογραφίες που συνδέονται με ονοματεπώνυμα, τις οποίες μπορούν να χρησιμοποιήσουν με στόχο τη δημιουργία μία τεράστιας βάσης δεδομένων προσώπων και τη βελτίωση των συστημάτων αναγνώρισης προσώπων. Όπως χαρακτηριστικά λέγεται, «η ιδιωτικότητα χάνεται bit με το bit». Για παράδειγμα, η ανερχόμενη εταιρία Clearview AI συνέλεξε δισεκατομμύρια διαδικτυακές φωτογραφίες για τη δημιουργία ενός εργαλείου που θα οδηγούσε την αστυνομία από ένα πρόσωπο σε λογαριασμό στο Facebook, στην αποκάλυψη της ταυτότητάς του. Οι νέοι ερευνητές επιχειρούν να αποδυναμώσουν τα συστήματα αυτά. Συγκεκριμένα, μία ομάδα μηχανικών υπολογιστών του Πανεπιστημίου του Σικάγο ανέπτυξε ένα εργαλείο, το οποίο μεταμορφώνει τις φωτογραφίες μέσω αλλαγών στα επίπεδα των πίξελ, οι οποίες αλλαγές μπλοκάρουν τα συστήματα αναγνώρισης προσώπων. Ήδη το λογισμικό αυτό, το οποίο ονομάστηκε Fawkes, προς τιμήν του ομώνυμου επαναστάτη, ανέβηκε στον ιστότοπο των ερευνητών τον Ιούλιο του 2020 και ο στόχος είναι να κυκλοφορήσει μία δωρεάν εκδοχή της εφαρμογής. Το λογισμικό αυτό δεν στοχεύει μόνο στην υπεράσπιση των εραστών της ιδιωτικότητας, αλλά θα τεθεί απέναντι στα συστήματα αναγνώρισης προσώπων, παραμορφώνοντας την ακρίβεια των δεδομένων που συγκεντρώνονται από το διαδίκτυο. βλ. σχετικά Kashmir Hill, «This Tool Could Protect Your Photos From Facial Recognition», 2020, https://www.nytimes.com/2020/08/03/technology/fawkes-tool-protects-photos-from-facial-recognition.html, ημερομηνία πρόσβασης 04-08-2020.

22 Πρόκειται για τη χρήση δεδομένων, στατιστικών αλγορίθμων και τεχνικών μηχανικής μάθησης για την εξακρίβωση της πιθανότητας μελλοντικών αποτελεσμάτων που βασίζονται σε ιστορικά δεδομένα. Ο στόχος είναι να οδηγηθεί κάποιος ένα βήμα πιο πέρα από αυτό που γνωρίζει, ώστε να παρέχει μία καλύτερη αξιολόγηση ως προς το τι θα συμβεί στο μέλλον. βλ. σχετικά https://www.sas.com/el_gr/insights/analytics/predictive-analytics.html, ημερομηνία πρόσβασης 15-06-2020.

κατά την οποία οι ερευνητές συχνά χρησιμοποιούν μεθόδους μηχανικής μάθησης για την ανάλυση δεδομένων, με στόχο την πρόβλεψη της πιθανότητας αβέβαιων αποτελεσμάτων. Εάν οι αλγόριθμοι μηχανικής μάθησης έχουν καλή απόδοση, έχουν τη δυνατότητα να παράγουν αυτοματοποιημένα αποτελέσματα που προσεγγίζουν αυτά που θα παρήγαγε ένα ανθρώπινο μυαλό στην ίδια θέση. Για το λόγο αυτό, η μηχανική μάθηση θεωρείται συχνά κλάδος της τεχνητής νοημοσύνης, καθώς ένας αλγόριθμος, με την κατάλληλη απόδοση μπορεί να παράγει αυτοματοποιημένα αποτελέσματα που θεωρούνται «έξυπνα»[23].

Ρομποτική (Robotics): Πρόκειται για το πεδίο της επιστήμης και της μηχανικής που σχετίζεται με το σχέδιο, την κατασκευή, τη λειτουργία και την εφαρμογή των ρομπότ[24]. Οι κυριότερες εφαρμογές τους αφορούν ενδεικτικά τους τομείς των μεταφορών, της βιομηχανίας, της υγείας, της επιστήμης, της διασκέδασης, της εξερεύνησης του διαστήματος, της άμυνας, των λιανικών πωλήσεων και του νοικοκυριού[25]. Τα ρομπότ αποτελούν μηχανικά αντικείμενα που προσλαμβάνουν δεδομένα από τον εξωτερικό κόσμο, επεξεργάζονται αυτό που αντιλαμβάνονται - «αισθάνονται» και στη συνέχεια επενεργούν προς τον κόσμο. Ο κύκλος «αισθάνομαι – σκέφτομαι – ενεργώ»[26] στηρίζει τη διαφοροποίηση της τεχνολογίας των ρομπότ από τις άλλες. Ένας φορητός υπολογιστής με κάμερα έχει την ικανότητα, έως ένα βαθμό, να «αισθάνεται» και να επεξεργάζεται τον εξωτερικό κόσμο, αλλά δεν μπορεί να επενεργήσει προς τον εξωτερικό κόσμο. Ένα όχημα απομακρυσμένης κίνησης με κάμερα «αισθάνεται» κι επηρεάζει με φυσικό τρόπο το περιβάλλον του, αλλά η

23 Harry Surden, «Machine Learning and Law», *Washington Law Review, Vol. 89, No. 1,* (2014).

24 Οποιαδήποτε μηχανή με αυτόματη λειτουργία, η οποία αντικαθιστά την ανθρώπινη προσπάθεια, ακόμα και αν δεν έχει ανθρωπόμορφη μορφή, ούτε εκτελεί τις εργασίες όπως ο άνθρωπος. βλ. σχετικά https://www.britannica.com/technology/robot-technology.

25 Σημαντικά υποπεδία της ρομποτικής αποτελούν η ρομποτική μηχανική, η αισθητηριακή ρομποτική, ο ρομποτικός έλεγχος, η ρομποτική μετακίνηση, η βιοεμπνευσμένη ρομποτική, η ανθρωποειδής ρομποτική, η μικρορομποτική, η νανορομποτική, η ρομποτική δέσμης, η ρομποτική νέφους, η ρομποτική σμήνους, η τηλερομποτική, η κοινωνική ρομποτική και η ανθρωποδιαδραστική ρομποτική. βλ. σχετικά https://en.wikipedia.org/wiki/Robotics.

26 Ο κύκλος αισθάνομαι – σκέφτομαι – ενεργώ αναπαριστά έναν τρόπο μοντελοποίησης της ανθρώπινης νοημοσύνης, ο οποίος επηρέασε ιδιαίτερα τις κοινότητες της ρομποτικής και της τεχνητής νοημοσύνης. Rolf Pfeifer και Christian Scheier, «Understanding Intelligence», (1999).

επεξεργασία εξαρτάται από το χειριστή του. Σε αντίθεση αυτών, η τεχνολογία των ρομπότ ή των ρομποτικών συστημάτων συνδυάζει και τις τρεις παραμέτρους[27]. Καθένα από τα ανωτέρω χαρακτηριστικά της αίσθησης, επεξεργασίας και δράσης υπάρχει σε ένα φάσμα[28]. Τα ρομπότ μπορούν να «δράσουν» με διάφορους τρόπους, όπως επίσης μπορούν να έχουν ευρύτερη ή πιο περιορισμένη ικανότητα κίνησης ή να χειρίζονται τον εξωτερικό κόσμο. Αυτή η «δράση» τους, όμως, εγείρει θεμελιώδη ερωτήματα, όπως για παράδειγμα εάν έχει τη δυνατότητα η τεχνολογία αυτή να ενεργεί μη μηχανικά. Ένα σύστημα θεωρείται ότι ενεργεί πάνω στο περιβάλλον του όταν το μεταβάλλει ευθέως. Η τεχνολογία δεν ενεργεί και κατά συνέπεια δεν αποτελεί ρομπότ μόνο όταν παρέχει πληροφορίες σε κατανοητή μορφή – πρέπει να «υπάρχει» με κάποιον τρόπο. Ένα ρομπότ στην απόλυτη ερμηνεία του όρου «υπάρχει» στον κόσμο ως ενσώματο αντικείμενο αποκτώντας την ικανότητα της σωματικής άσκησης. Αλλά και αυτό πρέπει να έχει μία συνέχεια. Τα ρομπότ αποτελούν τα καλύτερα τεχνητά αντικείμενα ή συστήματα που αισθάνονται, επεξεργάζονται και δρουν πάνω στον εξωτερικό κόσμο έως ένα βαθμό, αλλά και αυτό αποτελεί μία τεχνική ερμηνεία που θα μπορούσε να περιγράφει τα δίκτυα ή τα πρωτόκολλα που συμπεριλαμβάνονται στο διαδίκτυο. Αυτό που τελικά καθίσταται σημαντικό ως προς τις νομικές και πολιτικές συζητήσεις δεν είναι η ακριβής αρχιτεκτονική των ρομπότ, αλλά οι δυνατότητες κι εμπειρίες που παρέχει και οριοθετεί η αρχιτεκτονική αυτή. Με άλλα λόγια, οι συζητήσεις περιστρέφονται γύρω από τη μαζική, ασύγχρονη και από απόσταση επικοινωνία που επιτρέπει αυτού του είδους η τεχνολογία[29].

27 Ryan Calo, «Robotics and the Lessons of Cyberlaw», *California Law Review,* Vol. 103, No. 3, (2015): 513-63.

28 Κάποια ρομπότ έχουν περιορισμένη αίσθηση του χώρου, άλλα μπορούν να αξιοποιήσουν τα δεδομένα από οποιονδήποτε αισθητήρα. Επίσης κάποια μπορούν έχουν τηλεχειρισμό, ώστε αυτό που βλέπει ο άνθρωπος να μεταφέρεται σε αυτό που βλέπει η μηχανή με ελεγχόμενες ενέργειες και παράλληλα έχουν την ικανότητα της σκέψης έως ένα περιορισμένο βαθμό. Στην άλλη πλευρά του φάσματος, τα αυτοκινούμενα οχήματα, για παράδειγμα, έχουν την ικανότητα να κινούνται απεριόριστα σε συνθήκες αστικών τοπίων, στα προάστια ή σε αυτοκινητοδρόμους χωρίς την ανθρώπινη παρέμβαση. Brian Jeffrey Fogg, «Persuasive Technology: Using Computers To Change What We Think And Do», (2003).

29 Harry Surden, «Machine Learning and Law», *Washington Law Review, Vol. 89, No. 1,* (2014).

Αυτοματοποιημένες διαδικασίες λήψης αποφάσεων (autom decision-making): Πρόκειται για αποφάσεις που λαμβάνονται αποκλειστικά μέσω αυτοματοποιημένης επεξεργασίας, όπως η δημιουργία προφίλ, οι οποίες παράγουν νομικά αποτελέσματα αναφορικά με το υποκείμενο των δεδομένων ή το επηρεάζουν σημαντικά[30]. Οι διαδικασίες λήψης αποφάσεων προκύπτουν από αυτοματοποιημένα μέσα, χωρίς την ανθρώπινη παρέμβαση[31].

3 Τεχνητή νοημοσύνη και ανθρώπινη αυτονομία.

Σύμφωνα με τους ερευνητές, ο μεγαλύτερος κίνδυνος κατά τη χρήση της τεχνολογίας της τεχνητής νοημοσύνης είναι η μεγάλη πίεση στα μέλη της κοινωνίας να προσαρμόσουν τις ζωές τους σύμφωνα με τις υποδείξεις του συστήματος, σχετικά με το τι είναι καλό για τον καθένα και τι όχι, κάτι που σταδιακά θα έχει ως αποτέλεσμα την απώλεια της αυτονομίας του ανθρώπου[32] να αποφασίζει τον τρόπο με τον οποίο θέλει να ζήσει τη ζωή του. Το γεγονός αυτό είναι ουσιώδες, εάν λάβει κανείς υπόψη του ότι οι επιπτώσεις της τεχνολογίας στην αυτονομία είναι συχνά αόρατες και ελάχιστα είναι γνωστά σχετικά με αυτές.

Αν και κάθε είδους τεχνολογία έχει επιπτώσεις στην ανθρώπινη αυτονομία, ειδικά η τεχνητή νοημοσύνη και οι εφαρμογές της τείνουν να οξύνουν τις επιπτώσεις αυτές

30 Βλ. σχετικά άρθρο 22 ΓΚΠΔ: Αυτοματοποιημένη ατομική λήψη αποφάσεων.

31 Για παράδειγμα η ηλεκτρονική απόφαση περί χορήγησης δανείου ή ο έλεγχος ικανότητας με στόχο την πρόσληψη, μέσω προ-προγραμματισμένων αλγορίθμων και κριτηρίων. βλ. σχετικά https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ .

32 Πρόκειται για το δικαίωμα του ατόμου στην αυτοδιάθεση και την αυτοδιακυβέρνηση, τα οποία προσδιορίζουν τη δυνατότητα των προσώπων να λαμβάνουν ανεξάρτητα αποφάσεις σχετικά με τη ζωή τους. Η αυτονομία αποτελεί θεμελιώδη ανθρώπινη αξία και ηθική αρχή. Ο σεβασμός στην ανθρώπινη αυτονομία κατοχυρώνεται και νομικά με διάφορους τρόπους, όπως για παράδειγμα στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου στα άρθρα 2 (δικαίωμα στη ζωή), 3 (απαγόρευση των βασανιστηρίων) και 8 (Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής). βλ. σχετικά Μιχάλης Ν. Πικραμένος, «Τι σημαίνει ότι μπορώ να αναπτύξω ελεύθερα την προσωπικότητά μου;», (2019), διαθέσιμο σε https://www.syntagmawatch.gr/my-constitution/ti-simainei-oti-boro-na-anaptyxo-eleftheratin-prosopikotita-mou/ .

είτε προς το θετικότερο είτε προς το αρνητικό[33]. Η ανθρώπινη αυτονομία συγκρούεται με άλλες αξίες, οι οποίες συνεχώς κερδίζουν έδαφος στις μοντέρνες κοινωνίες, όπως η ασφάλεια και η πρόσβαση σε υπηρεσίες και προϊόντα. Στην ποινική δίκη, για παράδειγμα, όταν χρησιμοποιούνται εργαλεία και τεχνικές εκτίμησης κινδύνου της τεχνητής νοημοσύνης, μπορούν μεν να αμβλύνουν τις διαφορές στον τρόπο που οι πολίτες εξετάζονται και αντιμετωπίζονται από τη δικαιοσύνη, αλλά μπορούν επίσης και να επιδεινώσουν τις υπάρχουσες ανισότητες[34], οι οποίες έχουν τη βάση τους στο κοινωνικοοικονομικό υπόβαθρο των ατόμων ή την προέλευσή τους. Στο ίδιο πλαίσιο, μελέτη του οργανισμού Partnership on AI[35] εκφράζει ανησυχίες σχετικά με την εγκυρότητα, την ακρίβεια και τις ανισότητες των ίδιων των εργαλείων, τα ζητήματα που προκύπτουν από τις διεπαφές των εργαλείων και την αλληλεπίδραση των ατόμων με αυτά και θέτει ερωτήματα σχετικά με τη διακυβέρνηση, τη διαφάνεια και τη λογοδοσία κατά την ποινική δίκη[36]. Στο πλαίσιο αυτό η ανθρώπινη αυτονομία πλήττεται με δύο τρόπους. Ο πρώτος αφορά στην αυτονομία των δικαστών και το επίπεδο ελευθερίας που έχουν κατά τη διαδικασία έκδοσης απόφασης, σε συνάρτηση με την αξιολόγηση που παρέχει το σύστημα της τεχνητής νοημοσύνης, όταν είναι ισχυρή η πίεση που υφίστανται να συμμορφωθούν με την απόφαση που το σύστημα το ίδιο προτείνει. Ο δεύτερος τρόπος συνδέεται με την προσωπική αυτονομία του δράστη, ο οποίος δεν θα κριθεί σε αυστηρά ατομική

33 Janna Anderson, Lee Rainie και Alex Luchsinger, «Artificial Intelligence and the Future of Humans», (2018), διαθέσιμο σε https://www.elon.edu/docs/e-web/imagining/surveys/2018_survey/AI_and_the_Future_of_Humans_12_10_18.pdf .

34 «Criminal justice system should be cautious when approaching risk assessment», (2019), διαθέσιμο σε https://phys.org/news/2019-04-criminal-justice-cautious-approaching.html .

35 Αποστολή του συγκεκριμένου οργανισμού είναι η διεξαγωγή έρευνας, η οργάνωση συζητήσεων, η διοχέτευση πληροφοριών, η παροχή ηγετικής σκέψης, η διαβούλευση με σχετικά τρίτα μέρη, η απάντηση σε ερωτήσεις του κοινού και των μέσων ενημέρωσης και η δημιουργία εκπαιδευτικού υλικού που προωθεί την κατανόηση τεχνολογιών τεχνητής νοημοσύνης, συμπεριλαμβανομένης της μηχανικής αντίληψης, της μηχανικής μάθησης και της αυτοματοποιημένης συλλογιστικής. βλ. σχετικά https://www.partnershiponai.org/about/#!

36 βλ. σχετικά «Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System», διαθέσιμο σε https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/ .

βάση, αλλά σε σχέση με το πώς κρίθηκαν άλλοι δράστες με το ίδιο προφίλ και ποια ήταν η απόφαση που τους επεβλήθη[37].

Η έρευνα σε ειδικές κατηγορίες ατόμων, όπως οι υπερήλικες ή οι ανήλικοι, θα οδηγήσει στη διαπίστωση ότι αυτοί είναι πιο ευπαθείς στις δυσμενείς επιδράσεις της τεχνολογίας της τεχνητής νοημοσύνης στην αυτονομία τους, λόγω των ειδικών αναγκών τους ή της έλλειψης επιλογών και συναίνεσης, καθώς και των περιορισμένων πόρων τους να περιορίσουν τις αρνητικές επιπτώσεις. Για παράδειγμα, οι υπερήλικες πλήττονται από συγκεκριμένες εφαρμογές όπως είναι η απομακρυσμένη ηλεκτρονική παρακολούθησή τους, για λόγους ατομικής τους ασφάλειας, κατά τις καθημερινές τους συνήθειες. Παράλληλα, όμως, η ίδια τεχνολογία τους βοηθάει να αυξήσουν την αυτονομία τους, ελαχιστοποιώντας την εξάρτησή τους από έναν άνθρωπο – φροντιστή. Στους ανήλικους οι εφαρμογές της τεχνητής νοημοσύνης επηρεάζουν τις αξίες και τις σχέσεις τους με τα άλλα άτομα και το περιβάλλον τους[38].

Όσο τα συστήματα της τεχνητής νοημοσύνης γίνονται πιο αυτόνομα και υποκαθιστούν τα πρόσωπα και τις ανθρώπινες αποφάσεις με ολοένα και αυξανόμενους τρόπους, οι άνθρωποι κινδυνεύουν να απωλέσουν τη δυνατότητα να θέτουν τους κανόνες με βάση τους οποίους θα ζουν, θα λαμβάνουν αποφάσεις ή θα διαμορφώνουν γενικά τον τρόπο ζωής τους. Εάν κάποιος επιλέξει να λάβει ιατρική συμβουλή μέσω εφαρμογής της τεχνητής νοημοσύνης[39], επιλέγει επίσης να περιορίσει την ικανότητα να αναγνωρίζει και να κατανοεί το σώμα του και την ασθένειά του, να επιτρέψει σε ένα αυτόματο σύστημα να αντικαταστήσει το γενικό

37 Rowena Rodrigues και Anaïs Rességuier, Trilateral Research, «The underdog in the AI ethical and legal debate: human autonomy», (2019), διαθέσιμο σε https://www.ethicsdialogues.eu/2019/06/12/the-underdog-in-the-ai-ethical-and-legal-debate-human-autonomy/ .

38 Nicholas A. Christakis, «How AI Will Rewire Us», (2019), διαθέσιμο σε https://www.theatlantic.com/magazine/archive/2019/04/robots-human-relationships/583204/ .

39 Όπως για παράδειγμα η εφαρμογή ADA, η οποία αποτελεί μία ιατρική εταιρία παγκοσμίου βεληνεκούς, η οποία ιδρύθηκε από ιατρούς, επιστήμονες και πρωτοπόρους της βιομηχανίας, με στόχο να δημιουργήσει νέες δυνατότητες στον τομέα της προσωπικής υγείας. Το κεντρικό σύστημα της εταιρίας συνδέει την ιατρική γνώση με τις έξυπνες τεχνολογίες για να προσφέρει αποτελεσματική βοήθεια και φροντίδα στα άτομα που συνδέονται με αυτή. Από την ίδρυση της εταιρίας το 2016 έως σήμερα, έχουν γίνει περίπου είκοσι εκατομμύρια διαγνώσεις. Βλ. σχετικά https://ada.com/about/ .

ιατρό του ή άλλες ιατρικές υπηρεσίες, ίσως δύσκολα προσβάσιμες ή δαπανηρές, και να λάβει αποφάσεις αντ' αυτού. Μία εφαρμογή που υποκαθιστά το διαιτολόγο[40], επιβάλλει στο άτομο τι πρέπει να καταναλώνει και τι όχι και δυνητικά μπορεί για παράδειγμα να επιτρέψει τη διαμόρφωση της διατροφής του μέσω ενός «έξυπνου» ψυγείου[41]. Το άτομο τελικά ενδέχεται να παραδώσει τη διαχείριση της διατροφής του σε ένα σύστημα ή μία εφαρμογή και να χάσει το ενδιαφέρον του για τον ίδιο του τον οργανισμό, εξαιτίας της υπερβολικής εξάρτησής του από τα συστήματα αυτά. Τέτοιου είδους κίνδυνοι ενδεχομένως να εντείνουν την ανθρώπινη παθητικότητα και άγνοια και τελικά με τη σειρά τους να θέσουν σε κίνδυνο την αυτονομία του ατόμου. Πρόκειται για ένα φαύλο κύκλο, ο οποίος προϋπήρχε της τεχνολογίας της τεχνητής νοημοσύνης, αλλά και τον οποίο, πιθανόν, η τεχνολογία αυτή να επιδεινώσει[42].

4 Νομικό πλαίσιο.

Είναι κοινά αποδεκτό ότι τεχνολογίες όπως αυτή της τεχνητής νοημοσύνης, με λανθασμένους χειρισμούς μπορεί να έχουν απρόβλεπτες νομικές συνέπειες, όπως για παράδειγμα να προκαλέσουν κλυδωνισμό σε εκλογικά συστήματα[43], να οδηγήσουν σε διακρίσεις[44] ή να εμποδίσουν την ελευθερία έκφρασης[45] και την πρόσβαση στην

40 Βλ. σχετικά Hitesh Pruthi, Hardik Parvadiya,Varun Rawool και Joel Philip, «Artificial Intelligence Dietician», (2017), διαθέσιμο σε https://www.ijrter.com/papers/volume-3/issue-2/artificial-intelligence-dietician.pdf .

41 https://www.lg.com/us/refrigerators/lg-LNXS30996D-door-in-door .

42 Rowena Rodrigues και Anaïs Rességuier, Trilateral Research, «The underdog in the AI ethical and legal debate: human autonomy», (2019), διαθέσιμο σε https://www.ethicsdialogues.eu/2019/06/12/the-underdog-in-the-ai-ethical-and-legal-debate-human-autonomy/ .

43 Vyacheslav W. Polonski, «How artificial intelligence conquered democracy», (2017), διαθέσιμο σε https://www.independent.co.uk/news/long_reads/artificial-intelligence-democracy-elections-trump-brexit-clinton-a7883911.html .

44 Jordan Weissmann, «Amazon Created a Hiring Tool Using A.I. It Immediately Started Discriminating Against Women», (2018), διαθέσιμο σε https://slate.com/business/2018/10/amazon-artificial-intelligence-hiring-discrimination-women.html .

45 «AI tools threaten right to privacy and freedom of expression — report», (2018), διαθέσιμο σε https://medium.com/@privacyint/ai-tools-threaten-right-to-privacy-and-freedom-of-expression-report-443be95f3b75 .

πληροφορία[46]. Επίσης έχει παρατηρηθεί ότι η πλημμελής ανάπτυξη των αλγορίθμων στο δικαστικό σύστημα των ΗΠΑ έχει οδηγήσει σε πλημμελείς αποφάσεις προφυλάκισης πολιτών[47], ενώ δικαιολογημένα αναπτύσσονται ενστάσεις για τις επιβλαβείς συνέπειες από τη συνεχιζόμενη ανάπτυξη θανατηφόρων αυτόνομων όπλων[48]. Είναι πλέον πραγματικότητα το γεγονός ότι οι αλγόριθμοι και η τεχνητή νοημοσύνη μπορούν να προκαλέσουν σοβαρές ρωγμές στην προστασία των ανθρωπίνων δικαιωμάτων. Είναι κοινά αποδεκτό ότι ο νόμος δυσκολεύεται να συμβαδίσει με την τεχνολογία, φαινόμενο που συχνά απαντάται ως «καθυστέρηση του νόμου» (law lag)[49]. Μολονότι δεν υφίστανται ειδικοί νόμοι ρύθμισης της τεχνολογίας - στην Ευρώπη, πλην των σχετικών εκθέσεων της Ευρωπαϊκής Επιτροπής, δεν απαντώνται ειδικοί νόμοι για την τεχνητή νοημοσύνη ή τη ρομποτική[50], στην ουσία δεν υφίσταται νομικό κενό: οι τεχνολογίες αυτές καλύπτονται από τις γενικές διατάξεις, συμπεριλαμβανομένων των διεθνών νομοθετημάτων για τα ανθρώπινα δικαιώματα, με τα οποία οφείλουν να συμβαδίζουν και τα οποία πρέπει να σέβονται.

Από έρευνες που έχουν πραγματοποιηθεί από διεθνείς οργανισμούς (όπως ο οργανισμός του Ελσίνσκι για τα ανθρώπινα δικαιώματα[51]) και προγράμματα (όπως το πρόγραμμα SIENNA[52]) προκύπτει ότι η τεχνητή νοημοσύνη θα έχει ευρείες κοινωνικές επιπτώσεις και προβλέπεται να επηρεάσει τα ανθρώπινα δικαιώματα που

46 Michael Deane, «AI and the Future of Privacy», (2018), διαθέσιμο σε https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4 .

47 Jason Tashea, «Courts Are Using AI to Sentence Criminals. That Must Stop Now», (2017), διαθέσιμο σε https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/ .

48 «The threat of fully autonomous weapons», (2020), διαθέσιμο σε https://www.stopkillerrobots.org/learn/ .

49 «Dealing with the Law Lag», (2018), διαθέσιμο σε https://legalvision.com.au/dealing-with-the-law-lag/ .

50 Βλ. σχετικά Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, σχετικά με τις επιπτώσεις της τεχνητής νοημοσύνης, του διαδικτύου των πραγμάτων και της ρομποτικής στην ασφάλεια και την ευθύνη, Βρυξέλλες, (2020), διαθέσιμο σε https://ec.europa.eu/transparency/regdoc/rep/1/2020/EL/COM-2020-64-F1-EL-MAIN-PART-1.PDF

51 Βλ. σχετικά https://www.hfhr.pl/en/ .

52 Ό.π. υποσημ. 2.

σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα[53], την ισότητα[54], την ανθρώπινη αυτονομία και τον αυτοπροσδιορισμό[55], την ανθρώπινη αξιοπρέπεια[56], την ανθρώπινη ασφάλεια[57], τη δικαιοσύνη και την αμεροληψία[58], την απουσία διακρίσεων[59] και την ιδιωτική ζωή[60]. Το Δικαστήριο Ανθρωπίνων Δικαιωμάτων έχει αποδείξει ότι μπορεί να συμβαδίσει με τις νέες κοινωνικές και τεχνολογικές εξελίξεις[61] και τα ανθρώπινα δικαιώματα πρέπει να παραμείνουν η βάση πάνω στην οποία θα στηριχθεί το κανονιστικό οικοδόμημα, σε ό,τι αφορά στις τεχνολογικές εξελίξεις τις σχετικές με τους αλγορίθμους και την τεχνητή νοημοσύνη. Αυτό δεν σημαίνει ότι όσο η τεχνολογία αναπτύσσεται και διευρύνεται, δεν εξελίσσονται και οι κοινές αντιλήψεις και οι κανόνες του πώς αντιλαμβάνεται κάποιος και εκτιμά την αυτονομία και την ιδιωτική του ζωή. Ωστόσο, αυτή η

53 Άρθρο 8 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
54 Άρθρο 20 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
55 Άρθρο 3 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
56 Άρθρο 1 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
57 Άρθρο 6 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
58 Άρθρο 47 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
59 Άρθρο 21 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
60 Άρθρο 7 Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.
61 Βλ. υπόθεση *Bărbulescu v. Romania* (αίτηση 61496/08), σχετικά με την παρακολούθηση των εργαζομένων στον εργασιακό τους χώρο, διαθέσιμη σε https://hudoc.echr.coe.int/eng . Το 2007 μία εταιρεία στη Ρουμανία αποφάσισε να απολύσει τον εργαζόμενό της, κ. Barbulescu, έπειτα από παρακολούθηση των επικοινωνιών του μέσω του λογαριασμού Yahoo!Messenger, τον οποίο είχε δημιουργήσει, έπειτα από αίτημα της εταιρείας, προκειμένου να επικοινωνεί με πελάτες. Ο Barbulescu είχε χρησιμοποιήσει το λογαριασμό, πέρα από επαγγελματικούς και για προσωπικούς σκοπούς, με αποτέλεσμα η εταιρεία να αποφασίσει την απόλυσή του. Έπειτα από την εξάντληση των δικαστικών μέσων στη Ρουμανία, χωρίς να κατορθώσει να δικαιωθεί, ο Barbulesu προσέφυγε στο ΕΔΔΑ, όπου αρχικώς και πάλι κρίθηκε ότι, ενόψει της προστασίας των συμφερόντων του εργοδότη, δεν υπήρξε παραβίαση της ιδιωτικής του ζωής. Η υπόθεση έφτασε τελικώς ενώπιον της μείζονος σύνθεσης του ΕΔΔΑ, το οποίο διαφώνησε με τις προηγούμενες αποφάσεις, κρίνοντας (ψήφοι 11 υπέρ και 6 κατά) ότι εν προκειμένω υπήρξε πράγματι παραβίαση του δικαιώματος στην ιδιωτική ζωή του Barbulescu και ειδικότερα ότι οι Αρχές της Ρουμανίας δεν κατάφεραν να επιτύχουν μια δίκαιη ισορροπία μεταξύ των συμφερόντων της εταιρείας και του Barbulescu. Όπως επισημαίνει το ΕΔΔΑ, τα εθνικά δικαστήρια αφενός δεν κατόρθωσαν να εξακριβώσουν αν ο Bărbulescu είχε λάβει προηγουμένως ειδοποίηση από τον εργοδότη του σχετικά με το ενδεχόμενο παρακολούθησης των επικοινωνιών του και αφετέρου δεν έλαβαν υπόψη το γεγονός ότι δεν είχε ενημερωθεί για τη φύση ή την έκταση της παρακολούθησης ή τον βαθμό «εισβολής» στην ιδιωτική ζωή και αλληλογραφία του. Επιπλέον, τα εθνικά δικαστήρια δεν καθόρισαν ούτε τους ειδικούς λόγους που δικαιολογούσαν τα μέτρα παρακολούθησης ούτε το αν ο εργοδότης μπορούσε να χρησιμοποιήσει πιο ήπια μέσα για την παρακολούθηση. «Ευρωπαϊκό Δικαστήριο: Παραβίαση της ιδιωτικής ζωής η παρακολούθηση των emails εργαζομένου», (2017), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/eyropaiko-dikastirio-paraviasi-tis-idiotikis-zois-i-parakoloythisi-ton-emails-ergazomenoy .

επεξεργασία δεν πρέπει να οδηγήσει σε αποπροσανατολισμό σε σχέση με τις υπάρχουσες σταθερές των διεθνών διατάξεων των σχετικών με τα ανθρώπινα δικαιώματα[62].

Όσο η τεχνολογία εξελίσσεται, έχουν εμφανιστεί διάφοροι μηχανισμοί ηθικής και δεοντολογίας που αφορούν στην τεχνητή νοημοσύνη, ως απάντηση στη μαζική ανάπτυξη και χρήση της τεχνολογίας της τεχνητής νοημοσύνης από την κοινωνία και τους κινδύνους που σχετίζονται με αυτή. Οι μηχανισμοί αυτοί περιλαμβάνουν αρχές, κώδικες δεοντολογίας, υποδείξεις και κατευθυντήριες γραμμές. Αυτή όμως η εξέλιξη στους κανόνες δεοντολογίας, αν και ελπιδοφόρα, είναι παράλληλα και προβληματική. Πρέπει να αποδειχθεί η αποτελεσματικότητα των κανόνων, δεδομένου ότι είναι ιδιαίτερα επιρρεπείς στη χειραγώγηση, κυρίως από τη βιομηχανία, κάτι που αποτελεί μειονέκτημα για την τεχνητή νοημοσύνη και περιορίζει όσα θα μπορούσαν να επιτευχθούν για την κοινωνία και τα άτομα. Ο προβληματισμός δεν έγκειται, όμως, στο ότι οι κανόνες δεοντολογίας στερούνται αξίας μπροστά στην ανάπτυξη της τεχνητής νοημοσύνης, αλλά στο ότι χρησιμοποιούνται ή χειραγωγούνται με τέτοιον τρόπο που τελικά καθίστανται αναποτελεσματικοί.

Δεδομένου ότι είναι κοινά αποδεκτό ότι η εξάπλωση της τεχνητής νοημοσύνης χωρίς επίβλεψη θα μπορούσε να επιφέρει καταστροφικά αποτελέσματα, τόσο σε συγκεκριμένες κοινότητες, όσο και στο σύνολο της κοινωνίας, όπως κυρίως ανισότητες και διακρίσεις, παραβίαση της ιδιωτικότητας, αύξηση της επιτήρησης, έλλειψη αυτονομίας ή υπερβολική εξάρτηση από την τεχνολογία[63], παρατηρείται μία στροφή, αν και προβληματική, προς τους κανόνες δεοντολογίας προς διασφάλιση του

62 Zuzanna Warso, «Harnessing existing human rights jurisprudence to guide AI», (2019), διαθέσιμο σε https://digitalfreedomfund.org/harnessing-existing-human-rights-jurisprudence-to-guide-ai/ .

63 Το χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση ερευνητικό πρόγραμμα SIENNA παρείχε μία επισκόπηση των θεμάτων που προκύπτουν από την εφαρμογή της τεχνολογίας της τεχνητής νοημοσύνης και της ρομποτικής. Βλ. σχετικά Jansen P, Brey P, Fox A, Maas J, Hillas B, Wagner N, Smith P, Oluoch I, Lamers L, van Gein H, Resseguier A, Rodrigues R, Wright D, Douglas D, «Ethical analysis of AI and robotics technologies», (2019), SIENNA D4.4, διαθέσιμο σε https://www.sienna-project.eu/digitalAssets/801/c_801912-l_1-k_d4.4_ethical-analysis .

σεβασμού στις κοινωνικές αξίες και τους κανόνες. Οι κανόνες αυτοί κυριαρχούνται από αυτό που ο Βρετανός φιλόσοφος G.E.M. Anscombe ονομάζει «σύλληψη του νόμου της δεοντολογίας», δηλαδή την προσπάθεια για διαμόρφωση ενός είδους δεοντολογίας που θα αποτελεί υποκατάστατο του νόμου[64], κάτι για το οποίο η δεοντολογία δεν έχει σχεδιαστεί[65]. Στόχος των κανόνων δεοντολογίας γενικά, δεν είναι να επιβάλουν συγκεκριμένες συμπεριφορές και να διασφαλίσουν ότι αυτές θα τύχουν εφαρμογής, όπως λανθασμένα παρατηρείται με τους κανόνες δεοντολογίας της τεχνητής νοημοσύνης. Κάποιοι στη νομική θεωρία ισχυρίζονται ότι αυτή η λανθασμένη εφαρμογή των κανόνων δεοντολογίας είναι εσκεμμένη, προκειμένου να διασφαλιστεί ότι η τεχνητή νοημοσύνη δεν θα ρυθμιστεί από το νόμο, ώστε κατ' αυτόν τον τρόπο να υπάρχει μεγαλύτερη ευελιξία και να μην τεθούν αυστηροί περιορισμοί στους τομείς της βιομηχανίας και του εμπορίου που σχετίζονται με την τεχνολογία αυτή[66]. Αυτού του είδους, όμως, λανθασμένη χρήση θα οδηγήσει, όπως έχει σημειωθεί, σε «εξαγορά δεοντολογίας» ή «αποφυγή της δεοντολογίας»[67].

Η σωστή χρήση των κανόνων δεοντολογίας πρέπει να περιλαμβάνει μία στενή σύνδεση με τις κοινωνικές επιστήμες. Πρέπει να ωθήσουν την κοινωνία να

64 G.E.M. Anscombe, «Modern moral philosophy», *Philosophy* Vol. 33/124, Cambridge University Press, (1958): 1–19.

65 «Article 19, Governance with teeth: How human rights can strengthen fat and ethics initiatives on artificial intelligence», (2019), διαθέσιμο σε https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf. Βλ. επίσης Daniel Greene, Anna Lauren Hoffmann και Luke Stark, «Better, nicer, clearer, fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning», σε Proceedings of the 52nd Hawaii international conference on system sciences, Maui, Hawaii, (2019): 2122–2131. Thilo Hagendorff, «The ethics of AI ethics. An evaluation of guidelines», *Minds and Machines*, Vol. 30, (2020): 99–120. Chris Klöver και Alexander Fanta, «No red lines: Industry defuses ethics guidelines for artificial intelligence», (2019) διαθέσιμο σε https://algorithmwatch.org/en/industry-defuses-ethics-guidelines-for-artificial-intelligence/. Brent Mittelstadt, «Principles alone cannot guarantee ethical AI», *Nature Machine Intelligence*, Vol. 1, (2019): 501–507. Anna Jobin, Marcello Ienca και Effy Vayena, «The global landscape of AI ethics guidelines», *Nature Machine Intelligence, Vol.* 1/9, (2019): 389–399. Ben Wagner, «Ethics as an escape from regulation: From ethics-washing to ethics-shopping», σε Emre Bayamlioglu, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens και Mireille Hildebrandt «Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen», Amsterdam, Amsterdam University Press, (2018): 84–89.

66 Chris Klöver και Alexander Fanta, «No red lines: Industry defuses ethics guidelines for artificial intelligence», (2019) διαθέσιμο σε https://algorithmwatch.org/en/industry-defuses-ethics-guidelines-for-artificial-intelligence/.

67 Luciano Floridi, «Translating principles into practices of digital ethics: Five risks of being unethical», *Philosophy & Technology,* Vol. 32 (2019): 185–193.

κατανοήσει τον τρόπο με τον οποίο μεταμορφώνονται ο κόσμος και τα πράγματα, μεταμορφώσεις που σε μεγάλο βαθμό οφείλονται και στην τεχνολογία της τεχνητής νοημοσύνης[68]. Έχοντας ως δεδομένες αυτές τις ριζικές, μαζικές και ευρείες επιπτώσεις που έχει η τεχνολογία της τεχνητής νοημοσύνης στην κοινωνία, είναι κρίσιμο τελικά να διατηρηθούν ζωντανοί οι κανόνες δεοντολογίας, ως μία βαθιά και ζωτική ανάγκη συνεχούς ανανέωσης της διαδικασίας αμφισβήτησης του κόσμου και του τρόπου με τον οποίο αυτός γίνεται, συνειδητά, επαναλαμβανόμενα και με συνέχεια, αντιληπτός[69]. Νέες χρήσεις των ρομπότ, νέες ευκαιρίες για τις κυβερνήσεις και τις εταιρίες να καταγράφουν τους πολίτες, νέοι τρόποι εξάρτησης από την τεχνολογία, νέοι κίνδυνοι ανισοτήτων και διακρίσεων και πολλές άλλες νέες προκλήσεις εμφανίζονται καθημερινά και είναι απρόβλεπτες[70].

Όπως και στην υπόλοιπη Ευρώπη, έτσι και στην Ελλάδα δεν υπάρχουν σημαντικά νομοθετικά κείμενα και ρυθμίσεις σχετικά με την τεχνητή νοημοσύνη και τη ρομποτική. Οι νομικές ακαδημαϊκές συζητήσεις εστιάζουν κυρίως στην απομακρυσμένη τεχνητή νοημοσύνη και τη ρομποτική. Το κενό της σχετικής νομοθεσίας καλούνται να καλύψουν, μέσω ερμηνείας, οι υπάρχοντες νόμοι, όπως ο ελληνικός Αστικός Κώδικας. Επίσης, οι εξελίξεις σε αυτού του είδους τις τεχνολογίες έχουν οδηγήσει σε επιστημονικές συζητήσεις, οι οποίες δεν έχουν καταλήξει ακόμα στην Ελλάδα στην τροποποίηση της νομοθεσίας περί ανθρωπίνων δικαιωμάτων.
Ειδικά και σε σχέση με το νόμο 4624/2019, ο οποίος θέτει σε εφαρμογή στην Ελλάδα το Γενικό Κανονισμό Προστασίας των Δεδομένων (2016 /679), δεν γίνεται κάποια ρητή αναφορά στις έννοιες της «τεχνητής νοημοσύνης» ή της «ρομποτικής», αλλά

68 Thilo Hagendorff, «The ethics of AI ethics. An evaluation of guidelines», *Minds and Machines*, Vol. 30, (2020): 99–120. Βλ. επίσης Anaïs Rességuier και Rowena Rodrigues, «AI ethics should not remain toothless! A call to bring back the teeth of ethics», (2020), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/2053951720942541 . Evgeni Aizenberg και Jeroen van den Hoven, «Designing for human rights in AI», (2020), διαθέσιμο σε https://bigdatasoc.blogspot.com/2020/09/evgeni-aizenberg-and-jeroen-van-den.html .

69 Pär Segerdahl, «Ethical frameworks for research», (2020), διαθέσιμο σε https://ethicsblog.crb.uu.se/2020/08/19/ethical-frameworks-for-research/ .

70 Pär Segerdahl, «Ethics as renewed clarity about new situations», (2020), διαθέσιμο σε https://ethicsblog.crb.uu.se/2020/08/26/ethics-as-renewed-clarity-about-new-situations/ .

ρυθμίζονται οι «αυτοματοποιημένες διαδικασίες λήψης αποφάσεων» και η «αυτοματοποιημένη επεξεργασία» των προσωπικών δεδομένων, τα οποία περιλαμβάνουν τη χρήση των προσωπικών δεδομένων στην τεχνητή νοημοσύνη και τη μηχανική μάθηση. Αυτή η πρόβλεψη εξασφαλίζει στα πρόσωπα την επεξεργασία των δεδομένων τους μέσω αυτοματοποιημένων διαδικασιών μόνο στις περιπτώσεις που απαιτείται ή επιβάλλεται από το νόμο. Παράλληλα, περιγράφονται οι προϋποθέσεις για τέτοιου είδους επεξεργασία. Επίσης, διευκρινίζεται ότι δεν επιτρέπεται να λαμβάνονται σημαντικές αποφάσεις για τα πρόσωπα που να βασίζονται αποκλειστικά στις αυτοματοποιημένες διαδικασίες. Περαιτέρω, στην Ελλάδα εσχάτως θεσμοθετήθηκαν ρυθμιστικές Αρχές που, μεταξύ άλλων, θα είναι αρμόδιες για τα πεδία της τεχνητής νοημοσύνης και της ρομποτικής[71]. Αναμένεται να εκδοθούν σχετικές αποφάσεις από διάφορους φορείς, όπως, ενδεικτικά, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[72], η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ[73]), η οποία είναι αρμόδια για τις ραδιοσυχνότητες στην Ελλάδα, στις οποίες συμπεριλαμβάνονται θέματα που

71 Βλ. σχετικά Ν 4780/2021 – Εθν. Αρχή Προσβασιμότητας, Εθν.Επιτροπή α) για τα Δικαιώματα του Ανθρώπου, β) Βιοηθικής και Τεχνοηθικής.

72 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή που ιδρύθηκε με τον νόμο 2472/1997, ο οποίος είχε ενσωματώσει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Με τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Γενικός Κανονισμός Προστασίας Δεδομένων), ο οποίος τέθηκε σε εφαρμογή στις 25/5/2018 σε όλες τις χώρες της ΕΕ, η Οδηγία 95/45/ΕΚ καταργήθηκε. Πλέον από 29/8/2019 ισχύει ο νόμος 4624/2019 («Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»). Επίσης, όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η Αρχή εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002.

73 Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) είναι Ανεξάρτητη Διοικητική Αρχή. Αποτελεί τον Εθνικό Ρυθμιστή που ρυθμίζει, εποπτεύει και ελέγχει: (α) την αγορά ηλεκτρονικών επικοινωνιών, στην οποία δραστηριοποιούνται οι εταιρίες σταθερής και κινητής τηλεφωνίας, ασύρματων επικοινωνιών και διαδικτύου και (β) την ταχυδρομική αγορά, στην οποία δραστηριοποιούνται οι εταιρίες παροχής ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφοράς. Επιπλέον, η ΕΕΤΤ αποτελεί την αρχή ανταγωνισμού στις ανωτέρω αγορές της αρμοδιότητας της και διαθέτει όλες τις εξουσίες και τα δικαιώματα της Επιτροπής Ανταγωνισμού κατά την εφαρμογή της νομοθεσίας του ελεύθερου ανταγωνισμού στις εν λόγω αγορές (Ν.3959/2011 (Α' 93), άρθρα 101/102 ΣΛΕΕ και Κανονισμός 1/2003 ΕΚ του Συμβουλίου).

άπτονται των «έξυπνων» συστημάτων μεταφοράς, το Συμβούλιο Επικρατείας, το οποίο παρακολουθεί περιπτώσεις διακρίσεων, στις οποίες συγκαταλέγονται και οι υποθέσεις αλγοριθμικών διακρίσεων, η Ελληνική Εταιρία Τεχνητής Νοημοσύνης[74], η οποία δεδομένου ότι αποτελεί νομικό πρόσωπο ιδιωτικού δικαίου, δεν έχει την εξουσία να ρυθμίζει θέματα ή να εκδώσει κώδικα δεοντολογίας της τεχνητής νοημοσύνης, το Ινστιτούτο Συστημάτων Επικοινωνιών και Υπολογιστών του Εθνικού Μετσοβείου Πολυτεχνείου[75], το οποίο επίσης αποτελεί έναν μη κερδοσκοπικό ακαδημαϊκό ερευνητικό οργανισμό, μη δυνάμενο επίσης να νομοθετήσει επί θεμάτων τεχνητής νοημοσύνης, ο μη κερδοσκοπικός Οργανισμός Εκπαιδευτικής Ρομποτικής κι Επιστήμης (WRO Hellas)[76], του οποίου αντικείμενο αποτελούν η ανάπτυξη των μεθόδων και εφαρμογών της αυτοματοποίησης και της ρομποτικής στην εκπαίδευση και γενικότερα στην κοινωνία ή το Πανεπιστήμιο Μακεδονίας, το οποίο έχει ιδρύσει Ακαδημία Ρομποτικής. Όλες αυτές οι πρωτοβουλίες έχουν εκπαιδευτικό και ερευνητικό προσανατολισμό, αλλά δεν επηρεάζουν άμεσα την πολιτική και τη μελλοντική νομοθεσία της τεχνητής νοημοσύνης[77].

74 Πρόκειται για έναν μη κερδοσκοπικό επιστημονικό οργανισμό, ο οποίος ιδρύθηκε το 1988, με στόχο την οργάνωση και προώθηση της έρευνας σχετικά με την τεχνητή νοημοσύνη στην Ελλάδα και το εξωτερικό. Από την ίδρυσή του κι έπειτα έχει συμμετάσχει στην οργάνωση εγχώριων και διεθνών εκδηλώσεων που σχετίζονται με την τεχνητή νοημοσύνη και τα υποπεδία της. Το ενδιαφέρον του οργανισμού επίσης στρέφεται στην προώθηση της τεχνητής νοημοσύνης στην ανώτερη εκπαίδευση και την εκμετάλλευση των ερευνητικών αποτελεσμάτων από εμπορικούς οργανισμούς. βλ. σχετικά https://www.eetn.gr/index.php/about-eetn/about-eetn.

75 Το Ερευνητικό Πανεπιστημιακό Ινστιτούτο Συστημάτων Επικοινωνιών και Υπολογιστών (ΕΠΙΣΕΥ) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών (ΣΗΜΜΥ) του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ) ιδρύθηκε το 1989. Ο ιδρυτικός του «Χάρτης» ήταν η διεξαγωγή υψηλής ποιότητας έρευνας, οι αναπτυξιακές δραστηριότητες και η παροχή επιστημονικών υπηρεσιών σε ιδιωτικούς και δημοσίους φορείς. Ουσιαστικά ο ρόλος του ΕΠΙΣΕΥ ήταν να στηρίξει την ανάπτυξη και υλοποίηση των ερευνητικών προτεραιοτήτων της ΣΗΜΜΥ και σε μεγάλο βαθμό να επιδιώξει τη χρηματοδότηση της έρευνας μέσω της υποβολής ανταγωνιστικών ερευνητικών προτάσεων στο πλαίσιο προκήρυξης προγραμμάτων της Ευρωπαϊκής Επιτροπής. βλ. σχετικά https://www.iccs.gr/.

76 Ο μη κερδοσκοπικός Οργανισμός Εκπαιδευτικής Ρομποτικής & Επιστήμης με διακριτικό τίτλο WRO Hellas είναι ο κύριος φορέας διεξαγωγής διαγωνισμών εκπαιδευτικής ρομποτικής στην Ελλάδα και στην ευρύτερη περιοχή της Νοτιοανατολικής Ευρώπης. βλ. σχετικά https://wrohellas.gr/wro-hellas/.

77 Λίλιαν Μήτρου, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα», Σάκκουλας (2017). βλ. επίσης Φερενίκη Παναγοπούλου – Κουτνατζή, «Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων», Σάκκουλας, (2018).

Η Επιτροπή Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών του Ευρωπαϊκού Κοινοβουλίου (ΕΚ) ενέκρινε ψήφισμα[78] σχετικά με την αντιμετώπιση των προκλήσεων που προκύπτουν από την ταχεία ανάπτυξη των τεχνολογιών της τεχνητής νοημοσύνης και των αυτοματοποιημένων διαδικασιών λήψης αποφάσεων, σε συνδυασμό με την προστασία των δικαιωμάτων των καταναλωτών[79]. Το ψήφισμα αναφέρει ότι τα εν λόγω συστήματα πρέπει να χρησιμοποιούν μόνο υψηλής ποιότητας και αντικειμενικές βάσεις δεδομένων με «εξηγήσιμους και αμερόληπτους αλγορίθμους» και ότι πρέπει να δημιουργηθούν δομές επανεξέτασης για την αντιμετώπιση πιθανών λαθών στις αυτοματοποιημένες αποφάσεις. Πρέπει επίσης οι καταναλωτές να έχουν τη δυνατότητα να ζητούν την αναθεώρηση των αυτοματοποιημένων αποφάσεων που είναι οριστικές και μόνιμες[80]. Τα μέλη του Ευρωπαϊκού Κοινοβουλίου αιτήθηκαν από την Επιτροπή να υποβάλει προτάσεις για την προσαρμογή των κανόνων ασφαλείας της ΕΕ στα προϊόντα, όπως για παράδειγμα οδηγίες για τα μηχανήματα και την ασφάλεια των παιχνιδιών, ώστε να ενημερώνονται οι καταναλωτές σχετικά με τη χρήση αυτών των προϊόντων και να προστατεύονται από πιθανές βλάβες, ενώ πρέπει να είναι σαφείς οι υποχρεώσεις των κατασκευαστών. Σημειώθηκε, επίσης, ότι η Οδηγία για τη νομική ευθύνη λόγω ελαττωματικών προϊόντων[81], η οποία ισχύει τα τελευταία 30 χρόνια, πρέπει να αναθεωρηθεί για να επανακαθορίσει έννοιες όπως το «προϊόν», η «ζημία», το

78 Βλ.σχετικά https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/OJ/2020/01-22/1195401EL.pdf .

79 Τα μέλη της Επιτροπή του Ευρωπαϊκού Κοινοβουλίου δήλωσαν ότι «Όταν οι καταναλωτές χρησιμοποιούν ένα σύστημα το οποίο βασίζεται σε αυτοματοποιημένες διαδικασίες λήψης αποφάσεων, πρέπει να είναι κατάλληλα ενημερωμένοι σχετικά με τη λειτουργία του, σχετικά με τη δυνατότητα πρόσβασης σε άνθρωπο με αποφασιστικές εξουσίες, καθώς και σχετικά με τη δυνατότητα ελέγχου και διόρθωσης των αποφάσεων που λαμβάνει το σύστημα». Ό.π. ανωτέρω υποσημ. 76.

80 Βλ. σχετικά https://www.europarl.europa.eu/news/el/press-room/20200206IPR72015/kanones-gia-asfali-kai-dikaii-technologia-technitis-noimosunis .

81 Οδηγια του Συμβουλιου της 25ης Ιουλίου 1985 για την προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών σε θέματα ευθύνης λόγω ελαττωματικών προϊόντων (85/374/ΕΟΚ), διαθέσιμη σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31985L0374&from=EN .

«ελάττωμα» και τους κανόνες που διέπουν το βάρος της απόδειξης[82]. Υπογραμμίζεται ότι «ο άνθρωπος πρέπει να φέρει την ευθύνη σε τελευταίο βαθμό και ότι πρέπει να έχει τη δυνατότητα να ανατρέπει αποφάσεις», οι οποίες θα λαμβάνονται μέσω αυτοματοποιημένων διαδικασιών λήψης αποφάσεων, ιδίως σε σχέση με τα ιατρικά, νομικά και λογιστικά επαγγέλματα, αλλά και με τον τραπεζικό κλάδο. Τέλος, με το ψήφισμα υπενθυμίζεται ότι, δυνάμει του ενωσιακού δικαίου, οι έμποροι πρέπει να ενημερώνουν τους καταναλωτές σε περιπτώσεις που οι τιμές των προϊόντων ή των υπηρεσιών προσωποποιούνται, βάσει αυτοματοποιημένων διαδικασιών λήψης αποφάσεων, ενώ παράλληλα απευθύνεται αίτημα προς την Ευρωπαϊκή Επιτροπή να παρακολουθεί στενά την εφαρμογή των συγκεκριμένων κανόνων. Πρέπει επίσης να ελέγχεται ότι το ρυθμιστικό πλαίσιο της Ένωσης, όσον αφορά την απαγόρευση του αδικαιολόγητου γεωγραφικού αποκλεισμού («geo-blocking[83]»), εφαρμόζεται με τέτοιο τρόπο, ώστε να διασφαλίζεται ότι οι αυτοματοποιημένες διαδικασίες λήψης αποφάσεων δεν χρησιμοποιούνται ως εργαλεία διακριτικής μεταχείρισης λόγω υπηκοότητας, τόπου κατοικίας ή προσωρινής διαμονής. Η Πρόεδρος της Επιτροπής Εσωτερικής Αγοράς και Προστασίας των Καταναλωτών του Ευρωπαϊκού Κοινοβουλίου, δήλωσε ότι[84] «Η τεχνολογία στον τομέα της τεχνητής νοημοσύνης και των αυτοματοποιημένων διαδικασιών λήψης αποφάσεων εξελίσσεται με απίστευτους ρυθμούς. [....] Πρέπει να διασφαλίσουμε ότι η προστασία και η εμπιστοσύνη των καταναλωτών δεν διακυβεύονται, ότι οι κανόνες της Ευρωπαϊκής Ένωσης για την ασφάλεια και την

82 Βλ. σχετικά https://www.europarl.europa.eu/news/el/headlines/society/20200206STO72030/techniti-noimosuni-antimetopisi-ton-kindunon-kai-prostasia-ton-katanaloton .

83 Πρόκειται για διακρίσεις μεταξύ των καταναλωτών εντός της Ευρωπαϊκής Ένωσης για τμηματοποίηση των αγορών κατά μήκος των εθνικών συνόρων, προς αύξηση των κερδών εις βάρος ξένων καταναλωτών. Βλ. σχετικά Κανονισμό (ΕΕ) 2018/302 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 28ης Φεβρουαρίου 2018 για την αντιμετώπιση του αδικαιολόγητου γεωγραφικού αποκλεισμού και άλλων μορφών διακριτικής μεταχείρισης με βάση την ιθαγένεια, τον τόπο διαμονής ή τον τόπο εγκατάστασης των πελατών εντός της εσωτερικής αγοράς και για την τροποποίηση των κανονισμών (ΕΚ) αριθ. 2006/2004 και (ΕΕ) 2017/2394 και της οδηγίας 2009/22/ΕΚ, διαθέσιμος σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32018R0302&from=EN .

84 Βλ. σχετικά https://www.europarl.europa.eu/doceo/document/CRE-9-2020-02-10-INT-1-135-0000_EN.html .

ευθύνη σχετικά με τα προϊόντα και τις υπηρεσίες είναι προσαρμοσμένοι στην ψηφιακή εποχή, καθώς και ότι οι ομάδες δεδομένων που χρησιμοποιούνται στα συστήματα που βασίζονται σε αυτοματοποιημένες διαδικασίες λήψης αποφάσεων είναι υψηλής ποιότητας και δεν παραβιάζουν την απαίτηση της αμεροληψίας»[85].

Οι αλγόριθμοι και τα ρομπότ δυνητικά μπορούν να προκαλούν ζημίες στα άτομα καθημερινά και όταν αυτό συμβαίνει, ανακύπτουν ζητήματα από την πλευρά του δικαίου, ως προς το ποιος φέρει την ευθύνη. Δεδομένου ότι οι αλγόριθμοι δεν είναι ούτε πρόσωπα, αλλά ούτε και προϊόντα, στις ζημίες που προκαλούνται δεν μπορούν πάντα να εφαρμοστούν οι διατάξεις περί ευθύνης, πράγμα που ουσιαστικά εμποδίζει το ζημιωθέντα από την απονομή της δικαιοσύνης[86]. Οποιοδήποτε σύστημα ευθύνης αναφορικά με τις ζημίες που προκαλούνται από τους αλγορίθμους πρέπει να καλύπτει ένα ευρύ φάσμα περιπτώσεων. Τόσο σωματικές[87], όσο και συστημικές βλάβες[88]. Τίθεται λοιπόν το ερώτημα εάν αυτού του είδους οι ζημίες είναι τελικά παράπλευρες απώλειες της τεχνολογικής προόδου, τις οποίες πρέπει να υφίστανται τα πρόσωπα ή πρέπει κάποιος να φέρει την αστική ή ποινική ευθύνη. Ο νόμος δεν έχει πάντα την απάντηση στα ερωτήματα αυτά και η παραδοσιακή νομική θεωρία αναπτύχθηκε την εποχή όπου τέτοιου είδους ζημίες σχετίζονταν αποκλειστικά με την

85 Γεώργιος Π. Κανέλλος, «AI: Δέσμη δικαιωμάτων για την προστασία των καταναλωτών στα πλαίσια της τεχνητής νοημοσύνης ζητάει το Ευρωκοινοβούλιο», (2020), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/ai-desmi-dikaiomaton-gia-tin-prostasia-ton-katanaloton-sta-plaisia-tis-tehnitis .

86 Mihailis Diamantis, «Algorithms Acting Badly: A Solution from Corporate Law», *89 George Washington Law Review,* (forthcoming 2020), U Iowa Legal Studies Research Paper No. 2020-12.

87 Conner Forrest, «Robot kills worker on assembly line, raising concerns about human-robot collaboration», (2017), διαθέσιμο σε https://www.techrepublic.com/article/robot-kills-worker-on-assembly-line-raising-concerns-about-human-robot-collaboration/ . Βλ. επίσης, Daisuke Wakabayashi, «Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam», (2018), διαθέσιμο σε https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html .

88 «White & Case LLP, Algorithms and bias: What lenders need to know», (2017), διαθέσιμο σε https://www.lexology.com/library/detail.aspx?g=c806d996-45c5-4c87-9d8a-a5cce3f8b5ff . Βλ. επίσης Enrique Mart´ınez-Miranda και Peter McBurney and Matthew J. Howard, «Learning Unfair Trading: a Market Manipulation Analysis From the Reinforcement Learning Perspective», (2015), διαθέσιμο σε https://arxiv.org/pdf/1511.00740.pdf και Emilio Calvano, Giacomo Calzolari, Vincenzo Denicolò, Sergio Pastorello, «Artificial intelligence, algorithmic pricing, and collusion», (2019), διαθέσιμο σε https://voxeu.org/article/artificial-intelligence-algorithmic-pricing-and-collusion .

ευθύνη του αντιπροσώπου[89]. Αυτού του είδους η ευθύνη δεν μπορεί πλέον να καλύψει την τεχνολογική και οικονομική εξέλιξη της επιστήμης, όπου τα πρόσωπα ενεργούν καλή τη πίστει και σύμφωνα με το νόμο, αλλά τελικά οι μηχανές είναι αυτές που έχουν την παραβατική συμπεριφορά. Είναι προβληματικό το γεγονός ότι οι αλγόριθμοι αποτελούν για το νόμο άγνωστες παραμέτρους, με αποτέλεσμα, τα ένδικα βοηθήματα και μέσα που έχουν ασκηθεί κατά καιρούς για τις σωματικές βλάβες ή κάθε άλλη ζημία από τους αλγορίθμους στις ΗΠΑ, να έχουν απορριφθεί[90]. Από την πλευρά του δικαίου, οι σωματικές βλάβες ή η προσβολή της προσωπικότητας ή της ιδιοκτησίας δεν πρέπει να είναι ήσσονος σημασίας, επειδή ένας αλγόριθμος αντικατέστησε τον άνθρωπο. Επίσης, λόγω της εξέλιξης των αλγορίθμων και των ρομπότ δεν μπορεί να απαιτηθεί από μία μερίδα της κοινωνίας, αυτής που υφίσταται τις ζημίες που προκαλούνται από τους αλγόριθμους, να φέρει ένα δυσανάλογο μερίδιο του βάρους[91]. Οι ζημίες αυτές είναι πράγματι παρεπόμενες της τεχνολογικής προόδου και τις περισσότερες φορές είναι δύσκολο να ανακαλύψει κάποιος τις νομικές πρακτικές που θα επιτρέπουν στους ζημιωθέντες να υπερασπίζονται τον εαυτό τους. Σε κάποιες περιπτώσεις αυτό είναι εφικτό, όταν για παράδειγμα το θύμα φέρει την ευθύνη για τη ζημία που υπέστη, όπως εάν το ατύχημα με το αυτοκινούμενο όχημα είναι υπαιτιότητα του πεζού. Σε άλλες περιπτώσεις, οι υπάρχοντες νόμοι καλύπτουν την ευθύνη, όταν ουσιαστικά υπεύθυνος για τη ζημία είναι άνθρωπος, όπως για παράδειγμα όταν ένας κατασκευαστής σχεδιάζει έναν

89 Άμεση αντιπροσώπευση: Δήλωση βούλησης από κάποιον (αντιπρόσωπο) στο όνομα άλλου (αντιπροσωπευομένου) μέσα στα όρια της εξουσίας αντιπροσώπευσης ενεργεί αμέσως υπέρ και κατά του αντιπροσωπευομένου. Το αποτέλεσμα αυτό επέρχεται είτε η δήλωση γίνει ρητά στο όνομα του αντιπροσωπευομένου είτε συνάγεται από τις περιστάσεις ότι έγινε στο όνομά του. Η διάταξη αυτή εφαρμόζεται αναλόγως και όταν η δήλωση της βούλησης απευθύνεται προς τον αντιπρόσωπο. Βλ. σχετικά άρθρα 211επ. ΑΚ. Περί αντιπροσώπευσης.

90 Robot Maker «Escapes Liability In Fatal Auto Factory Accident», (2019), διαθέσιμο σε https://www.law360.com/articles/1192734/robot-maker-escapes-liability-infatal-auto-factory-accident . Βλ. επίσης Angie Schmitt, «Uber Got Off the Hook for Killing a Pedestrian with its Self-Driving Car», (2019), διαθέσιμο σε https://usa.streetsblog.org/2019/03/08/uber-got-off-the-hook-for-killing-a-pedestrian-with-its-self-driving-car/ .

91 Mihailis Diamantis, «The Extended Corporate Mind: When Corporations Use AI to Break the Law», 97 *North Carolina Law Review,* (2020): 893.

αλγόριθμο τιμολόγησης, ο οποίος συνδέεται δολίως με άλλους[92]. Σε αυτή την περίπτωση ο νόμος βλέπει τον αλγόριθμο ως μέσο που ενέχει την ευθύνη του αντιπροσώπου. Αλλά το μεγαλύτερο ποσοστό των ζημιών προκύπτει χωρίς την ανθρώπινη παρέμβαση, είτε από την πλευρά του ζημιωθέντος είτε του προγραμματιστή. Η δύναμη της σύγχρονης τεχνολογίας μηχανικής μάθησης αναπτύσσεται με τρόπους που δεν θα μπορούσαν να προβλέψουν ούτε οι χρήστες, ούτε και οι προγραμματιστές και αυτή η ίδια η δύναμη είναι που καθιστά τις ζημίες αναπόφευκτες. Ακόμα και στις περιπτώσεις όπου «έξυπνοι» αλγόριθμοι προκαλούν ζημία χωρίς την ανθρώπινη παρέμβαση, κάτι που ήδη συμβαίνει και θα συνεχίσει να αυξάνεται προοδευτικά, όσοι υφίστανται τη ζημία δεν έχουν πρόσβαση σε ένδικα βοηθήματα[93].

Οι εσωτερικές νομοθεσίες των Κρατών γενικά διαθέτουν ισχυρό αστικό και ποινικό πλαίσιο προς εξισορρόπηση των δικαιωμάτων των ζημιωθέντων με τα δικαιώματα όσων τους ζημιώνουν - των πιθανών εναγομένων. Ειδικά στην περίπτωση των αλγορίθμων η λύση είναι να βρεθεί ο «κατάλληλος» εναγόμενος που θα εισέλθει στο πλαίσιο αυτό και θα καλύψει το νομικό κενό της απουσίας ευθύνης. Μία προσέγγιση θα ήταν να δημιουργήσει ο ίδιος ο νόμος έναν. Έχει διατυπωθεί η άποψη ότι θα μπορούσε κατά πλάσμα δικαίου[94], να αποδοθεί σε έναν εκλεπτυσμένο αλγόριθμο η ικανότητα δικαίου του φυσικού προσώπου και κατ' επέκταση να δημιουργηθεί η δυνατότητα να εναχθεί ως πρόσωπο. Η άποψη αυτή, όμως, αφενός μεν εγείρει φιλοσοφικά ερωτήματα, όπως εάν οι αλγόριθμοι μπορούν πραγματικά να θεωρηθούν

92 Βλ. σχετικά «Acting Assistant Attorney General Andrew Finch Delivers Keynote Address at Annual Conference on International Antitrust Law and Policy», (2017), διαθέσιμο σε https://www.justice.gov/opa/speech/acting-assistant-attorney-general-andrew-finch-delivers-keynote-address-annual-conference .

93 Mihailis E. Diamantis, «Who Pays for AI Injury?», (2020), διαθέσιμο σε https://www.law.ox.ac.uk/business-law-blog/blog/2020/05/who-pays-ai-injury .

94 Πρόκειται για δημιούργημα του ρωμαϊκού δικαίου, το οποίο προσδιορίζεται εννοιολογικά με αυτόν τον όρο (δικαιικό πλάσμα - fictio juris), επειδή οι Ρωμαίοι νομικοί πίστευαν ότι στην περίπτωσή του ο νομοθέτης μορφοποιεί κάτι, που δέν ανταποκρίνεται στην εμπειρική πραγματικότητα, έτσι που ο νόμος να πειθαναγκάζει στην παραδοχή οτι το φανταστικό δημιούργημα -το πλάσμα- είναι τάχα κάτι το αληθινό. Γεώργιος Γ. Μητσόπουλος, «Το πρόβλημα της εννοίας του δικαιικού πλάσματος», Εκδόσεις Αντ.Ν. Σάκκουλα, 1998:185.

πρόσωπα, αφετέρου δε παρουσιάζει πρακτικά εμπόδια, όπως ο τρόπος με τον οποίο θα επιβληθεί η ποινή σε έναν αλγόριθμο, αλλά ενέχει και απρόβλεπτες συνέπειες, όπως το εάν ο αλγόριθμος, ως πρόσωπο, θα μπορούσε να αμυνθεί με την άσκηση ενδίκων βοηθημάτων και μέσων[95].

Μία πιο ρεαλιστική πρόταση είναι η κατ' αναλογία εφαρμογή του εταιρικού δικαίου. Σε αυτή την περίπτωση, στις περιπτώσεις των ατόμων που θα μπορούσε να επιβληθεί η καταβολή αποζημίωσης λόγω της ζημίας που προκλήθηκε από τους αλγόριθμους, περιλαμβάνονται, πέρα από τους ζημιωθέντες, ως συνυπαίτιους, τους προγραμματιστές ή τους ίδιους τους αλγόριθμους και οι εταιρίες που σχεδιάζουν και θέτουν σε εφαρμογή τους αλγόριθμους. Οι ισχύουσες διατάξεις του εταιρικού δικαίου[96] αναγνωρίζουν την ευθύνη των εταιριών ως προσώπων, τα οποία δρουν μέσω των εκπροσώπων τους[97], πάνω στους οποίους ασκούν έλεγχο, αλλά και επωφελούνται και από τη δράση τους. Ο ίδιος έλεγχος, αλλά και τα ίδια οφέλη θα μπορούσαν να εκτείνονται και στους εταιρικούς αλγόριθμους. Εάν ο νόμος είχε τη δυνατότητα να αναγνωρίσει την αλγοριθμική «συμπεριφορά» ως εταιρική ενέργεια, θα άλλαζε όλο το πλαίσιο της αστικής και ποινικής ευθύνης. Με αυτόν τον τρόπο θα αποκτούσαν οι ζημιωθέντες έναν πιθανό διάδικο, από τον οποίο θα αναζητούσαν την αποκατάσταση της βλάβης. Περαιτέρω, όταν μία εταιρία θα ήλεγχε έναν αλγόριθμο, η προοπτική απόδοσης ευθύνης θα ωθούσε το νομικό πρόσωπο να δώσει μεγαλύτερη προσοχή στο σχεδιασμό, την παρακολούθηση και την τροποποίηση του αλγορίθμου, κάτι που θα είχε ως αποτέλεσμα περιορισμό των ζημιών. Σε αυτή την περίπτωση, με

95 Joanna Bryson, Mihailis Diamantis και Thomas D. Grant, «Of, for, and by the People: The Legal Lacuna of Synthetic Persons», *25 Artificial Intelligence & Law*, University of Cambridge Faculty of Law Research Paper No. 5 (2018): 273.

96 Ιωάννης Ρόκας, «Εισαγωγή στο δίκαιο των εταιριών του εμπορικού δικαίου», 6η έκδοση, Νομική Βιβλιοθήκη, Αθήνα, 2019.

97 Ελένη Θ. Πασαμιχάλη, «Η αλληλέγγυα ευθύνη διοικούντων νομικά πρόσωπα και νομικές οντότητες», (2019), διαθέσιμο σε http://www.nsk.gr/documents/15678/84519/%CE%95%CE%99%CE%A3%CE%97%CE%93%CE%97%CE%A3%CE%95%CE%99%CE%A3_18-12-2019.pdf/3388c219-a316-49cb-a836-d7f0c2986e74 .

την άσκηση του ελέγχου που ήδη έχει ο νόμος πάνω στις εταιρίες, θα υπήρχε η δυνατότητα διασφάλισης της ορθής και υπεύθυνης λειτουργίας των αλγορίθμων[98].

5 Εφαρμογές της Τεχνητής Νοημοσύνης

Στην Ελλάδα η Ανεξάρτητη Αρχή Δημοσίων Εσόδων πρωτοπορεί κι έρχεται να εφαρμόσει την τεχνολογία της τεχνητής νοημοσύνης για την ταυτοποίηση ύποπτων συναλλαγών και προσώπων, με στόχο την καταπολέμηση της φοροδιαφυγής. Συγκεκριμένα, από το έτος 2021 θα γίνεται στο σύνολο της φορολογίας (φόρος εισοδήματος, ΦΠΑ, ειδικοί φόροι κατανάλωσης, δασμοί κοκ) χρήση της διαδικασίας του Data mining[99], δηλαδή της εξόρυξης χρήσιμων πληροφοριών από μεγάλες βάσεις δεδομένων. Μέχρι σήμερα η τεχνολογία της τεχνητής νοημοσύνης εφαρμόζεται στο Υπουργείο Οικονομικών είτε με την ταυτοποίηση των προσώπων μέσω ειδικών αλγορίθμων, σε συνδυασμό με τη διαδικασία της αμοιβαίας συνδρομής[100], δηλαδή την ανταλλαγή πληροφοριών από τις χώρες του εξωτερικού όπου δραστηριοποιείται ο φορολογούμενος ή ενδεχομένως παρουσιάζει εισοδήματα είτε με τον έλεγχο των τραπεζικών συναλλαγών και τη ροή του χρήματος[101].

Η βρετανική εταιρεία DeepMind, θυγατρική της Google, ανέπτυξε ένα σύστημα τεχνητής νοημοσύνης με την ονομασία AlphaFold, το οποίο κατάφερε για πρώτη φορά, εδώ και δεκαετίες να προβλέψει με ταχύτητα και ακρίβεια τον τρόπο

98 Ό.π. υποσημείωση 93.

99 Η εξόρυξη δεδομένων είναι η διαδικασία εύρεσης ανωμαλιών, προτύπων και συσχετισμών σε μεγάλα σύνολα δεδομένων, με στόχο την πρόβλεψη των αποτελεσμάτων. «Data Mining. What it is & why it matters», διαθέσιμο σε https://www.sas.com/en_us/insights/analytics/data-mining.html#:~:text=Data%20mining%20is%20the%20process,relationships%2C%20reduce%20risks%20and%20more .

100 βλ. σχετικά ΠΟΛ.1120/27.5.2013.

101 Στο εξωτερικό και συγκεκριμένα στη Γαλλία, οι αντίστοιχες φορολογικές Αρχές κάνουν χρήση των συστημάτων τεχνητής νοημοσύνης ήδη από το 2018, με συστήματα εξόρυξης δεδομένων και αξιολόγηση αυτών, έπειτα από διαδοχικό έλεγχο και συστηματική επαλήθευση. Τα στοιχεία έχουν αντληθεί, πέρα από τα αρχεία του Δημοσίου και από ιδιωτικές εταιρίες, από το ηλεκτρονικό εμπόριο, αλλά και από τα μέσα κοινωνικής δικτύωσης. Προκόπης Χατζηνικολάου, «Με τεχνητή νοημοσύνη η εφορία στη μάχη κατά της φοροδιαφυγής», (2020), διαθέσιμο σε https://www.kathimerini.gr/economy/561186367/me-techniti-noimosyni-i-eforia-sti-machi-kata-tis-forodiafygis/ .

αναδίπλωσης των πρωτεϊνών, το τρισδιάστατο σχήμα που θα λάβουν και κατ' επέκταση τη λειτουργία τους. Η συγκεκριμένη εφαρμογή προέβλεψε σωστά τουλάχιστον τα δύο τρίτα της δομής των πρωτεϊνών, με βάση μόνο την αρχική αλληλουχία (αλυσίδα) των αμινοξέων τους, μέσα σε λίγες ημέρες, κάτι που για τους επιστήμονες απαιτεί χρόνια δαπανών και διαδικασιών στα εργαστήρια. Ο επιστημονικός κόσμος χαιρέτησε το επίτευγμα αυτό με ενθουσιασμό, διότι θα βοηθήσει στην κατανόηση ασθενειών και στην ταχύτερη ανάπτυξη νέων φαρμάκων, μεταξύ αυτών και για τον Covid-19[102].

Περαιτέρω, ένας απρόσμενος τομέας στον οποίο έχει εισέλθει η τεχνολογία της τεχνητής νοημοσύνης είναι ο χώρος της Δικαιοσύνης[103], όπου κατάλληλα διαμορφωμένες πλατφόρμες διαχείρισης αρχείων, δεδομένων ή εικόνων βασιζόμενων στην τεχνολογία αναγνώρισης προσώπου δίνουν τη δυνατότητα στις διωκτικές Αρχές να προχωρήσουν στην αστυνόμευση συγκεκριμένων περιοχών, όπως τα προγράμματα HART στο Ηνωμένο Βασίλειο[104], CAS στην Ολλανδία και PredPol στις ΗΠΑ[105] ή ειδικές εφαρμογές με αλγόριθμους παρέχουν τη δυνατότητα στους δικαστικούς λειτουργούς στις ΗΠΑ να κατατάσσουν τους παραβάτες σε κλίμακες, ανάλογα με την πιθανότητα υποτροπής τους[106]. Στο Αγγλοσαξωνικό Δίκαιο, σε

102 Ήδη ο αλγόριθμος AlphaFold έχει προβλέψει τα σχήματα αρκετών πρωτεϊνών του κορωνοϊού SARS-CoV-2 και οι επιστήμονες τρέφουν την ελπίδα ότι στο μέλλον θα έχει την ικανότητα να προβλέπει, με τα ελάχιστα δυνατά πειράματα, ποια από τα υπάρχοντα φάρμακα συνδέονται σωστά με αυτές τις πρωτεΐνες και κατά συνέπεια μπορούν να έχουν θεραπευτική δράση. Βλ. σχετικά «Εμβόλιο κορονοϊού: Η τεχνητή νοημοσύνη έλυσε βιολογικό μυστήριο δεκαετιών», (2020), διαθέσιμο σε https://www.news247.gr/good-news/emvolio-koronoioy-i-techniti-noimosyni-elyse-viologiko-mystirio-dekaetion.9067074.html .

103 Λεωνίδας Κανέλλος, «Η Τεχνητή Νοημοσύνη στην υπηρεσία μιας έξυπνης Δικαιοσύνης», (2020), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis#footnote10_c75t8oh .

104 Matt Burgess, «UK police are using AI to inform custodial decisions – but it could be discriminating against the poor», (2018), διαθέσιμο σε https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit .

105 Βλ. σχετικά https://www.predpol.com/how-predictive-policing-works/ .

106 Για παράδειγμα, το λογισμικό «COMPAS» (Correctional Offender Management Profiling for Alternative Sanctions) παρέχει της δυνατότητα στο χρήστη, δικαστικό λειτουργό ή υπεύθυνο αναστολών, να εξετάζει την πιθανότητα των παραβατών να γίνουν υπότροποι. Jeff Larson, Surya Mattu, Lauren Kirchner και Julia AngwinMay, «How We Analyzed the COMPAS Recidivism Algorithm», (2016), διαθέσιμο σε https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm .

αντίθεση με χώρες της Ευρώπης[107], δίνεται η δυνατότητα πρόβλεψης της έκβασης των δικαστικών υποθέσεων, μέσω της ανάλυσης της σχετικής νομολογίας και της δημιουργίας του προφίλ των δικαστών[108]. Ιδιαίτερα ενδιαφέρον, επίσης, είναι το γεγονός ότι σε διάφορες χώρες του κόσμου χρησιμοποιούνται ρομπότ που υποκαθιστούν του δικηγόρους, ως προς την παροχή νομικών συμβουλών (legal chatbots[109]), τους δικαστές, σε απλές υποθέσεις [110] ή τους υπαλλήλους της εισαγγελίας, ως προς την προετοιμασία της δικογραφίας[111]. Οι τεχνολογικές αυτές εξελίξεις, αν και έχουν γίνει δεκτές με ενθουσιασμό από τους πολίτες, απαιτούν γρήγορα αντανακλαστικά από το νομικό κόσμο. Σύμφωνα με το Συμβούλιο των Ευρωπαϊκών Δικηγορικών Συλλόγων (CCBE[112]) και την Ευρωπαϊκή Επιτροπή για την Αποτελεσματικότητα της Δικαιοσύνης (CEPEJ[113]), η χρήση της τεχνολογίας της τεχνητής νοημοσύνης στο δικαστικό σύστημα απαιτεί το κατάλληλο πλαίσιο κανόνων ηθικής και δεοντολογίας[114], οι οποίοι θα συμβαδίζουν με την Ευρωπαϊκή

107 Η Γαλλία απαγόρευσε τις αναλύσεις των δικαστικών αποφάσεων προς αποφυγήν του forum shopping, δηλαδή των ευνοϊκών προς τους διαδίκους, αποφάσεων. Επιπλέον, δεν επιτρέπεται πλέον η χρήση της ταυτότητας των δικαστών για την αξιολόγηση, την ανάλυση, τη σύγκριση ή την πρόβλεψη των επαγγελματικών τους πρακτικών. Βλ. σχετικά το Γαλλικό νόμο 2019-222 της 23ης Μαρτίου 2019, περί αναμόρφωσης της δικαιοσύνης, διαθέσιμο σε https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038261631 .

108 Bernard Marr, «How Big Data Is Disrupting Law Firms And The Legal Profession», (2016), διαθέσιμο σε https://www.forbes.com/sites/bernardmarr/2016/01/20/how-big-data-is-disrupting-law-firms-and-the-legal-profession/?sh=157daecf7c23 .

109 SnatchBot Team, «How Legal Chatbots Will Automate Lawyer Services in the Future», (2020), διαθέσιμο σε https://snatchbot.me/amp/blog/130/legal-chatbots .

110 «Beijing Internet court launches AI judge», (2019), διαθέσιμο σε http://www.chinadaily.com.cn/a/201906/28/WS5d156cada3103dbf1432ac74.html .

111 «Δικαστής με τεχνητή νοημοσύνη αποφασίζει για τον κατηγορούμενο», (2018), διαθέσιμο σε https://www.ethnos.gr/kosmos/1691_dikastis-me-tehniti-noimosyni-apofasizei-gia-ton-katigoroymeno .

112 Πρόκειται για το αντιπροσωπευτικό όργανο περίπου ενός (1) εκατομμυρίου δικηγόρων, μέσω των δικηγορικών συλλόγων – μελών, από τριάντα μία (31) χώρες-πλήρη μέλη και έντεκα (11) συνεργαζόμενες χώρες και παρατηρητές. https://www.dsa.gr/page/.

113 Η Ευρωπαϊκή Επιτροπή για την Αποτελεσματικότητα της Δικαιοσύνης (CEPEJ) του Συμβουλίου της Ευρώπης υποστηρίζει τα κράτη μέλη του Οργανισμού στην προσπάθειά τους για βελτίωση της αποτελεσματικότητας και της ποιότητας των δικαστικών συστημάτων τους, έτσι ώστε να διασφαλίζεται ότι λειτουργούν σύμφωνα με τα πρότυπα του Συμβουλίου της Ευρώπης και ανταποκρίνονται στις ανάγκες όσων ζητούν δικαιοσύνη. https://rm.coe.int/cepej-10-06-2020-declaration-in-greek-covid-19/16809ee8de .

114 «CCBE Considerations on the Legal Aspects of Artificial Intelligence», (2020), διαθέσιμο σε https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf . Βλ. επίσης «Τεχνητή νοημοσύνη, β) Συμπεράσματα σχετικά με το συντονισμένο σχέδιο για την τεχνητή

Σύμβαση των Δικαιωμάτων του Ανθρώπου, το Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και το Γενικό Κανονισμό για την Προστασία των Δεδομένων[115].

5.1 Αναγνώριση προσώπου (facial recognition)

Μετά την 11η Σεπτεμβρίου 2001, τα συστήματα βιντεοεπιτήρησης[116] έχουν εισέλθει στην καθημερινότητα των πολιτών σε παγκόσμιο επίπεδο. Σε πολλά κράτη η Πολιτεία έχει μετατραπεί σε «Κράτος παρακολούθησης» που στοχεύει στην εικόνα, την κίνηση και την ιδιωτική ζωή των πολιτών[117]. Η ανίχνευση των προσώπων, είτε σε διασυνδεδεμένο περιβάλλον είτε σε εξωτερικό χώρο, είναι εξαιρετικά αποτελεσματική, λόγω της ευκολότερης συλλογής δείγματος σε σχέση με άλλα βιομετρικά στοιχεία[118], όπως τα δαχτυλικά αποτυπώματα ή το DNA, τα οποία απαιτούν φυσική επαφή. Αλλά και η ίδια η τεχνολογία αναγνώρισης προσώπου έχει καταστεί πλέον προσιτή και εύκολη στη χρήση, κυρίως για τα όργανα δημόσιας τάξης. Η βιντεοεπιτήρηση, σε συνδυασμό με τις τεχνολογίες αναγνώρισης προσώπου, οι οποίες χρησιμοποιούν βιομετρικά δεδομένα, παρέχουν στο χρήστη, τόσο τη δυνατότητα παρακολούθησης, όσο και αυτή της μοναδικής ταυτοποίησης

νοημοσύνη», (2019), διαθέσιμο σε https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/el/pdf .

115 Λεωνίδας Κανέλλος, «The GDPR Handbook», Νομική Βιβλιοθήκη, 2020: 364-370.

116 Πρόκειται για τα συστήματα εκείνα που είναι μόνιμα εγκατεστημένα σε έναν χώρο και έχουν τη δυνατότητα λήψης ή/και μετάδοσης εικόνας ή και ήχου προς οθόνες προβολής ή μηχανήματα καταγραφής (όπου οι κάμερες μπορούν να συνδέονται με την οθόνη ή το μηχάνημα καταγραφής είτε απευθείας είτε μέσω δικτύου/διαδικτύου). Η συνηθέστερη περίπτωση ενός συστήματος είναι το κλειστό κύκλωμα τηλεόρασης. Βλ. σχετικά «Θεματική ενότητα: Συστήματα βιντεοεπιτήρησης», διαθέσιμο σε https://www.dpa.gr/portal/page?_pageid=33,124801&_dad=portal&_schema=PORTAL .

117 Μαγδαληνή Σκόνδρα, «Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα», (2020), διαθέσιμο σε https://www.ddikastes.gr/node/5271 .

118 Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από βιομετρικά συστήματα, με τη χρήση ειδικών μεθόδων της επιστήμης της στατιστικής κι έχουν ιδιαίτερο χαρακτήρα, καθώς αφορούν είτε τα φυσικά χαρακτηριστικά ενός ανθρώπου (όπως δακτυλικά αποτυπώματα, γεωμετρία της παλάμης, ανάλυση της κόρης του ματιού, των χαρακτηριστικών του προσώπου, του DNA) είτε τα στοιχεία της συμπεριφοράς του (όπως υπογραφή, φωνή, τρόπο πληκτρολόγησης, τρόπο βαδίσματος) και τα οποία τον προσδιορίζουν μοναδικά. βλ. σχετικά «Θεματική ενότητα: Νέες τεχνολογίες – βιομετρικά», διαθέσιμο σε https://www.dpa.gr/portal/page?_pageid=33,131221&_dad=portal&_schema=PORTAL .

του πολίτη σε πραγματικό χρόνο. Όσο εντυπωσιακή και αν δείχνει, όμως, αυτή η τεχνολογική πρόοδος, ελοχεύουν κίνδυνοι για τα προσωπικά δεδομένα των πολιτών, όπως είναι οι φυλετικές διακρίσεις ή τα λάθη στις ταυτοποιήσεις, οι οποίοι μεγιστοποιούνται όταν η παρακολούθηση των πολιτών γίνεται σε απολυταρχικά καθεστώτα και οδηγεί στην καταπάτηση του συνόλου των θεμελιωδών ανθρωπίνων δικαιωμάτων[119].

Για να χρησιμοποιηθεί ένα ανθρώπινο χαρακτηριστικό ως βιομετρικό πρέπει να πληρούνται οι προϋποθέσεις της καθολικότητας - κάθε άτομο πρέπει να έχει το χαρακτηριστικό, της μονιμότητας - το χαρακτηριστικό πρέπει να είναι αμετάβλητο για ένα χρονικό διάστημα, της μετρησιμότητας - το χαρακτηριστικό πρέπει να μπορεί να μετρηθεί ποσοτικά και του διακριτικού χαρακτήρα - κάθε δύο άτομα πρέπει να είναι αρκετά διαφορετικά από την άποψη των χαρακτηριστικών[120]. Το ανθρώπινο πρόσωπο καλύπτει τις ανωτέρω παραμέτρους, ώστε με τη σάρωσή του από μία κάμερα και την επεξεργασία του από ειδικούς αλγορίθμους, να αποτελεί δείγμα και έπειτα από την ταυτοποίησή του με άλλα αντίστοιχα δείγματα σε μία βάση δεδομένων, να μπορεί να οδηγήσει στην αναγνώριση του ατόμου.

Κατ' εφαρμογήν των ανωτέρω, στις ΗΠΑ, η εταιρία Clearview AI[121] έχει ως αντικείμενο τη δημιουργία μίας βάσης δεδομένων, έπειτα από συλλογή

119 Στην Κίνα, για παράδειγμα, σύμφωνα με δημοσιεύματα του τύπου καθημερινά, αναγνωρίζονται και εντοπίζονται 1,4 δισεκατομμύρια πολίτες. Σαρωτές αναγνώρισης προσώπου προστατεύουν τις εισόδους κτηριακών συγκροτημάτων, κάμερες ανιχνεύουν σιδηροδρομικούς σταθμούς προς εντοπισμό υποδίκων, οθόνες απεικονίζουν τα πρόσωπα περαστικών και απαριθμούν τα ονόματα των οφειλετών του Δημοσίου. Στόχος των μέτρων αυτών είναι ένα σύστημα κοινωνικής αξιολόγησης που θα βαθμολογεί τους πολίτες. Η δε παρακολούθηση των μειονοτήτων, συνοδεύεται από την επιβολή σοβαρών περιορισμών στις μετακινήσεις τους, αλλά και σοβαρών κυρώσεων, που οδηγούν σταδιακά σε αφανισμό τους συγκεκριμένους πληθυσμούς, ώστε να γίνεται λόγος ακόμη και για γενοκτονία. Konstantin Salomatin και Shura Burtin, «Beyond Orwell's Worst Nightmares: How China Uses Artificial Intelligence to Commit Genocide», (2019), διαθέσιμο σε https://bylinetimes.com/2019/11/18/beyond-orwells-worst-nightmares-how-china-uses-artificial-intelligence-to-commit-genocide/ .

120 Φερενίκη Παναγοπούλου - Κουτνατζή, «Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)», *ΔιΜΕΕ*, 4/2013: 482.

121 Πρόκειται για μία εταιρία που παρέχει ερευνητικά εργαλεία στις υπηρεσίες επιβολής του νόμου με στόχο την ταυτοποίηση θυτών και θυμάτων εγκλημάτων. Βλ. σχετικά https://clearview.ai/ .

δισεκατομμυρίων φωτογραφιών από το διαδίκτυο, συμπεριλαμβανομένων και των πλατφορμών LinkedIn και Instagram, με στόχο την παροχή πρόσβασης σε αυτές στις υπηρεσίες επιβολής του νόμου. Για την εφαρμογή που έχει αναπτύξει βρίσκεται σε δικαστική διαμάχη με ενώσεις, οι οποίες ισχυρίζονται ότι η μεταβίβαση των δεδομένων των πολιτών στις υπηρεσίες επιβολής του νόμου αποτελεί μία μεγάλη νέα απειλή σε βάρος του απορρήτου, διότι καθιστά εφικτό στην εκάστοτε κυβέρνηση και σε οργανισμούς να ταυτοποιήσουν από μία φωτογραφία σχεδόν κάθε πολίτη[122]. Επιπλέον, το λογισμικό της εταιρίας, εκτός από το ότι συλλέγει τις φωτογραφίες των πολιτών χωρίς τη συγκατάθεσή τους, τις αναλύει, δημιουργώντας ένα μοναδικό βιομετρικό αποτύπωμα κάθε προσώπου. Στον αντίποδα, οι υποστηρικτές της εταιρίας θεωρούν ότι η διαμάχη αυτή αφορά την αλληλεξάρτηση και αλληλεπίδραση απορρήτου και ελευθερίας έκφρασης και ότι η χρήση της εφαρμογής αυτής αποτελεί μία μορφή έκφρασης, η οποία προστατεύεται από το Σύνταγμα των ΗΠΑ.

Περαιτέρω, κατά τη διάρκεια μίας διαδήλωσης στην πλατεία Lafayette στην Ουάσινγκτον, τον Ιούνιο του 2020, η τοπική αστυνομία αναγνώρισε και συνέλαβε ένα διαδηλωτή έπειτα από επίθεση σε αστυνομικό, με τη βοήθεια της τεχνολογίας αναγνώρισης προσώπου πάνω σε μία φωτογραφία του στο Twitter. Η δικογραφία που σχηματίστηκε σε βάρος του αποτελεί την πρώτη δημόσια αναγνώριση της χρήσης της τεχνολογίας της αναγνώρισης προσώπου από τις δημόσιες Αρχές και συγκεκριμένα του συστήματος National Capital Region Facial Recognition Investigative Leads System (NCRFRILS), του οποίου η ύπαρξη δεν ήταν γνωστή, όχι μόνο στο ευρύ κοινό, αλλά ούτε και στους δικαστικούς λειτουργούς και τους ειδικούς[123]. Η χρήση της συγκεκριμένης εφαρμογής δημιουργεί ερωτηματικά για την

122 Όταν ο αρμόδιος υπάλληλος/αξιωματικός ανεβάζει μία φωτογραφία ή μία λήψη βίντεο που περιέχει κάποιο πρόσωπο, η εφαρμογή προσπαθεί να ταιριάξει ως προς την ομοιότητα και να εμφανίσει και άλλες φωτογραφίες του ιδίου προσώπου που υπάρχουν στο διαδίκτυο. Kashmir Hill, «Facial Recognition Start-Up Mounts a First Amendment Defense», (2020), διαθέσιμο σε https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html .

123 Σύμφωνα με τους αξιωματούχους της αστυνομίας, η συγκεκριμένη τεχνολογία έχει χρησιμοποιηθεί περισσότερες από 12.000 φορές από το έτος 2019, περιλαμβάνει μία βάση δεδομένων με 1,4 εκατομμύρια εγγραφές προσώπων, αλλά λειτουργεί εξ ολοκλήρου εκτός δημόσιας προβολής. Πρόσβαση σε αυτή έχουν δεκατέσσερις τοπικές και ομοσπονδιακές υπηρεσίες. Martins Bruveris, «Have you heard

προστασία των συνταγματικών δικαιωμάτων των πολιτών, κυρίως ως προς την αδυναμία των κατηγορουμένων να αμφισβητήσουν την μέθοδο ταυτοποίησή τους, δεδομένου ότι στο μεγαλύτερο ποσοστό των υποθέσεων ο τρόπος ταυτοποίησης δεν αποκαλύπτεται. Το πρόβλημα μεγεθύνεται, καθώς έρευνες έχουν δείξει ότι τα σχετικά συστήματα είναι περισσότερο επιρρεπή στα λάθη, όσον αφορά στις μειονότητες. Μία ομοσπονδιακή μελέτη το 2019 σημείωσε ότι οι αλγόριθμοι που χρησιμοποιούνται στην αναγνώριση προσώπου, συμπεριλαμβανομένων και αυτών του συστήματος NCRFRILS, αποδείχθηκαν απόλυτα ακριβείς ως προς τους λευκούς άντρες, αλλά ανακριβείς ως προς τα έγχρωμα και ασιατικά πρόσωπα. Επίσης, η μελέτη υπέδειξε προβλήματα και στην αναγνώριση των γυναικών[124]. Στον αντίποδα των ενστάσεων, ο υπεύθυνος του προγράμματος υποστήριξε ότι η συγκεκριμένη εφαρμογή αποτελεί ένα αποτελεσματικό εργαλείο, το οποίο προσφέρει στοιχεία σε υποθέσεις που σε διαφορετικές περιπτώσεις θα παρέμεναν άλυτες, ότι το συγκεκριμένο πρόγραμμα ουδέποτε χρησιμοποιήθηκε σε ειρηνικές διαδηλώσεις, αλλά μόνο όπου διαπιστώνονται αδικήματα, ότι έχει ρυθμιστεί προσεκτικά, ώστε να προστατεύει την ιδιωτική ζωή και να αποφεύγει τις λανθασμένες ταυτοποιήσεις και τέλος ότι δεν αποκαλύπτεται η χρήση του στους κατηγορουμένους, διότι χρησιμοποιείται αποκλειστικά για την παροχή ενδείξεων και όχι αποδείξεων για τη σύλληψη του προσώπου[125]. Στον απόηχο των ανωτέρω, οι εταιρίες IBM[126], Microsoft[127] και

of NCRFRILS?», (2020), διαθέσιμο σε https://martinsbruveris.com/2020/11/have-you-heard-of-ncrfrils/#more-659 .

124 Βλ. σχετικά Drew Harwell, «Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use», (2019), διαθέσιμο σε https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ .

125 Justin Jouvenal και Spencer S. Hsu, «Facial recognition used to identify Lafayette Square protester accused of assault», (2020), διαθέσιμο σε https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html .

126 Hannah Denham, «IBM's decision to abandon facial recognition technology fueled by years of debate», (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/ .

127 Jay Greene, «Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM», (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ .

Amazon[128] ανακοίνωσαν ότι αναστέλλουν τις πωλήσεις τους σε εφαρμογές αναγνώρισης προσώπου, εστιάζοντας στις πρόσφατες διαδηλώσεις κατά των φυλετικών διακρίσεων που προκύπτουν από τα συστήματα αυτά και την απουσία εθνικής νομοθεσίας που να ρυθμίζει τη σχετική τεχνολογία.

Περιπτώσεις σαν την ανωτέρω είναι πλέον συνηθισμένες. Στο Μαϊάμι, τα μέσα μαζικής ενημέρωσης ανέφεραν ότι η τοπική αστυνομία χρησιμοποίησε λογισμικό αναγνώρισης προσώπου για την ταυτοποίηση γυναίκας, έπειτα από επίθεση σε αστυνομικούς κατά τη διάρκεια διαδήλωσης[129], στη Φιλαδέλφεια η τοπική αστυνομία χρησιμοποίησε φωτογραφίες από τα μέσα κοινωνικής δικτύωσης και αντίστοιχο λογισμικό για τον εντοπισμό διαδηλωτών που βανδάλισαν αστυνομικά αυτοκίνητα[130] και στη Νέα Υόρκη, η δημοτική αρχή απηύθυνε συστάσεις στην αστυνομία, έπειτα από καταγγελία τοπικού ειδησεογραφικού πρακτορείου ότι η έρευνα με τη χρήση λογισμικού αναγνώρισης προσώπου για τον εντοπισμό ενός διοργανωτή του κινήματος Black Lives Matter[131], ο οποίος παρενόχλησε αστυνομικό, οδήγησε στον εντοπισμό του και στην εισβολή της αστυνομίας στο διαμέρισμά του[132].

Στην Ευρώπη η χρήση της τεχνολογίας αναγνώρισης προσώπου πραγματοποιείται διστακτικά, ελλείψει κυρίως κατάλληλων εθνικών νομοθετημάτων και υπό τους περιορισμούς του Γενικού Κανονισμού Προστασίας Δεδομένων, ο οποίος απαγορεύει

128 Jay Greene, «Amazon bans police use of its facial-recognition technology for a year», (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/ .

129 Connie Fossi και Phil Prazan, «Miami Police Used Facial Recognition Technology in Protester's Arrest», (2020), διαθέσιμο σε https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ .

130 Katie Shepherd, «An artist stopped posting protest photos online to shield activists from police. Then, he was arrested», (2020), διαθέσιμο σε https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/ .

131 Το κίνημα αυτό προέκυψε το 2013 ως απάντηση στην απαλλαγή από τις κατηγορίες του φυσικού αυτουργού της ανθρωποκτονίας του Trayvon Martin. Το σχετικό ίδρυμα είναι ένας διεθνής οργανισμός με παραρτήματα στις ΗΠΑ, το Ηνωμένο Βασίλειο και τον Καναδά. Σκοπό του αποτελεί η εξάλειψη της λευκής υπεροχής και η οικοδόμηση τοπικής εξουσίας προς επέμβαση στη βία που προκαλείται στις κοινότητες των έγχρωμων από το κράτος και τους τιμωρούς. Βλ. σχετικά https://blacklivesmatter.com/about/ .

132 Jake Offenhartz και George Joseph, «De Blasio Will Reassess NYPD's Use Of Facial Recognition Tech After Protester Arrest», (2020), διαθέσιμο σε https://gothamist.com/news/de-blasio-will-reassess-nypds-use-facial-recognition-tech-after-protester-arrest .

την επεξεργασία βιομετρικών δεδομένων, εκτός εάν συντρέχει κάποια από τις εξαιρέσεις που προβλέπει το άρθρο 9 παρ. 2. Για παράδειγμα, στο Ηνωμένο Βασίλειο, όπου η βάση δεδομένων της Αστυνομίας περιλαμβάνει περί τα 23 εκατομμύρια πρόσωπα προς ταυτοποίηση, υπάρχουν σοβαρές ενστάσεις ως προς τη χρήση της τεχνολογίας αναγνώρισης προσώπου και τη βιντεοεπιτήρηση δημοσίων χώρων, λόγω της έλλειψης επιστημονικής έρευνας για την αξιοπιστία των συστημάτων και του ανάλογου νομοθετικού πλαισίου εγγυήσεων[133]. Στην Σουηδία τον Αύγουστο του 2019 επιβλήθηκε το πρώτο πρόστιμο που αφορούσε την επεξεργασία αναγνώρισης προσώπου μέσω βιντεοεπιτήρησης σε σχολείο, κατά παράβαση του ΓΚΠΔ[134], στη Γαλλία γίνονται ενέργειες για τη δημιουργία νομοθετικού πλαισίου που θα επιτρέψει την χρήση της τεχνολογίας αναγνώρισης προσώπου από τις δημόσιες Αρχές και την αστυνομία[135], ενώ ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων εκφράζει σοβαρές ανησυχίες για τη χρήση της νέας τεχνολογίας[136].

133 Ο Βρετανός Επίτροπος Βιομετρικών (Biometrics Commissioner) Paul Wiles επεσήμανε στην ετήσια έκθεσή του το 2018 τον κίνδυνο από την ανάθεση στην αστυνομία, χωρίς νομικό πλαίσιο, της στάθμισης της προστασίας των δεδομένων και του δημόσιου συμφέροντος. Βλ. σχετική ετήσια έκθεση, διαθέσιμη σε https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf . Παράλληλα παρατηρήθηκε ότι η τεχνολογία αυτή λειτουργεί με διακρίσεις, αναγνωρίζοντας εσφαλμένα περισσότερο γυναίκες και έγχρωμα άτομα. Συγκεκριμένα, έρευνα του Πανεπιστημίου του Κάρντιφ σχετικά με δοκιμές τεχνολογίας αναγνώρισης προσώπου από την αστυνομία της Νότιας Ουαλίας, υπογράμμισε ότι το σύστημα σημείωσε 2.900 πιθανούς υπόπτους, αλλά οι 2.755 ήταν εσφαλμένες αναγνωρίσεις και συνακόλουθα, λάθος συλλήψεις. Οι συλλήψεις αυτές παραμένουν κι εμφανίζονται στα ποινικά μητρώα των ατόμων, γεγονός που μπορεί να επηρεάσει, για παράδειγμα, το επαγγελματικό τους μέλλον. Ian Sample, «Watchdog criticises 'chaotic' police use of facial recognition», (2019), διαθέσιμο σε https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition .

134 Βλ. σχετικά «Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students», (2019), διαθέσιμο σε https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf .

135 Luana Pascu, «France looks to establish legal framework to deploy biometric video surveillance», (2020), διαθέσιμο σε https://www.biometricupdate.com/202001/france-looks-to-establish-legal-framework-to-deploy-biometric-video-surveillance .

136 Wojciech Wiewiórowski, «Facial recognition: A solution in search of a problem?», (2019), διαθέσιμο σε https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en .

Στην Ελλάδα, το Δεκέμβριο του 2019 η Ελληνική Αστυνομία προχώρησε στη σύναψη σύμβασης που αφορά στην προμήθεια συστημάτων για «έξυπνη» αστυνόμευση (Smart Policing)[137]. Πρόκειται για ένα λογισμικό αναγνώρισης φωτογραφιών προσώπου, μέσω του οποίου θα γίνεται η σύγκριση με ψηφιακά αρχεία φωτογραφιών προσώπων, προκειμένου να αναγνωριστεί - ταυτοποιηθεί ένα υπό εξέταση άτομο. Σε εφαρμογή τέθηκε το Μάρτιο του 2021 και το πρόγραμμα σχετικά με τη χρήση κάμερας στις στολές των υπηρετούντων στις Μονάδες Αποκατάστασης Τάξης της Ελληνικής Αστυνομίας[138], ήδη και μετά την έκδοση του του προεδρικού διατάγματος 75/2020 περί χρήσης συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους, την έκδοση του οποίου προέβλεπε το άρθρο 14 παρ. 4 του νόμου 3917/11. Επιπλέον, με πρόσφατη τροποποίηση του άρθρου 41Δ του αθλητικού νόμου 2725/1999, είναι επιτρεπτή, κατόπιν άδειας του Εισαγγελέα, η χρήση από την αστυνομία κινητών συσκευών καταγραφής ήχου ή εικόνας ή οποιωνδήποτε άλλων ειδικών τεχνικών μέσων, ψηφιακών ή μη, οπτικής ή ηχητικής καταγραφής, εντός και εκτός των αθλητικών εγκαταστάσεων κατά τη διάρκεια και μετά τη λήξη της αθλητικής εκδήλωσης[139]. Η εκτεταμένη χρήση της τεχνολογίας αναγνώρισης προσώπου υπό αμφισβητούμενες ακόμα πρακτικές, έχει οδηγήσει στη δημιουργία κινημάτων από τους πολίτες προς απαγόρευσή της[140] ή στην ανάπτυξη εφαρμογών με στόχο το μπλοκάρισμα των σχετικών αλγορίθμων[141].

137 Βλ. σχετικά «Σύμβαση που αφορά στην προμήθεια Συστημάτων για έξυπνη Αστυνόμευση (Smart Policing)», (2019), διαθέσιμο σε http://www.astynomia.gr/images/stories/2019/prokirikseis19/14122019anakoinosismartpolicing.pdf .

138 Γιάννης Σουλιώτης, «Σε τελική ευθεία το σχέδιο για τις κάμερες στις διμοιρίες των ΜΑΤ», (2020), διαθέσιμο σε https://www.kathimerini.gr/society/561085486/se-teliki-eytheia-to-schedio-gia-tis-kameres-stis-dimoiries-ton-mat/ .

139 Άρθρο τρίτο - Νόμος 4639/2019 - Τροποποίηση του άρθρου 41Δ του ν. 2725/1999 (Α΄ 121) «Υποχρεώσεις αθλητικών φορέων - Μέτρα αστυνόμευσης αθλητικών εκδηλώσεων», (2019), διαθέσιμο σε https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4639-2019/arthro-trito-nomos-4639-2019-tropopoiisi-toy-arthroy-41d .

140 Samuel Sigal, «Activists want Congress to ban facial recognition. So they scanned lawmakers' faces», (2019), διαθέσιμο σε https://www.vox.com/future-perfect/2019/11/15/20965325/facial-recognition-ban-congress-activism .

141 Aaron Holmes, «All it takes to fool facial recognition at airports and border crossings is a printed mask, researchers found», (2020), διαθέσιμο σε https://www.businessinsider.com/facial-recognition-fooled-with-mask-kneron-tests-2019-12 . Βλ. επίσης Stephen Johnson, «How designers are fighting the rise of facial recognition technology», (2019), διαθέσιμο σε https://bigthink.com/technology-innovation/facial-

Έπειτα από τις ανωτέρω παραθέσεις, διαφαίνεται ότι ο στόχος για τα κράτη είναι η εφαρμογή εξειδικευμένης εθνικής νομοθεσίας, προκειμένου να αναχαιτιστεί η γενικευμένη χρήση της αναγνώρισης προσώπου και της βιντεοεπιτήρησης[142]. Δεδομένου ότι «η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο» και ότι »το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο - πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας»[143], κάθε νέα τεχνολογία, πριν τεθεί σε εφαρμογή, πρέπει να αξιολογείται προσεκτικά και να εξετάζεται κατά πόσον η χρήση της είναι απολύτως αναγκαία, είναι κατάλληλη προς εφαρμογή και ποιες θα είναι οι επιπτώσεις της στα δικαιώματα των πολιτών[144]. Τέλος, απαραίτητη είναι η προηγούμενη γνώμη της Αρχής Προστασίας Δεδομένων, όπως ρητά προβλέπεται από τον ΓΚΠΔ[145] για κάθε μέτρο που εισάγει περιορισμό στην προστασία των προσωπικών δεδομένων, αλλά και η μελέτη εκτίμησης αντικτύπου στα δικαιώματα και τις ελευθερίες των πολιτών[146].

5.2 Ειδικά ζητήματα για τις εφαρμογές της τεχνητής νοημοσύνης.

Όπως μπορεί να διαπιστώσει κάποιος από τα ανωτέρω, υπάρχει πληθώρα νομικών ζητημάτων που αφορούν τις τεχνολογίες της τεχνητής νοημοσύνης και της ρομποτικής. Συχνά παρουσιάζονται προβλήματα κοινά με τις τεχνολογίες πληροφοριών και επικοινωνίας, τα οποία είτε διευκολύνονται είτε επιδεινώνονται,

recognition?rebelltitem=2#rebelltitem2 .

142 Steven Feldstein, «The Global Expansion of AI Surveillance», (2019), διαθέσιμο σε https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 .

143 Άρθρο 4 αιτιολογικής σκέψης ΓΚΠΔ.

144 Μαγδαληνή Σκόνδρα, «Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα», (2020), διαθέσιμο σε https://www.ddikastes.gr/node/5271 .

145 Άρθρο 57 παρ. 1, εδ. γ΄ ΓΚΠΔ: 1. Με την επιφύλαξη των άλλων καθηκόντων που ορίζονται στον παρόντα κανονισμό, κάθε εποπτική αρχή στο έδαφός της: [...] γ) συμβουλεύει, σύμφωνα με το δίκαιο του κράτους μέλους, το εθνικό κοινοβούλιο, την κυβέρνηση και άλλα όργανα και οργανισμούς για νομοθετικά και διοικητικά μέτρα που σχετίζονται με την προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας,

146 Άρθρο 35 ΓΚΠΔ.

ενώ άλλα είναι νέα και εξελισσόμενα, όπως για παράδειγμα η απόδοση ικανότητας δικαίου στα συστήματα τεχνητής νοημοσύνης και ρομποτικής. Κάποια από τα ζητήματα αυτά έχουν συνέπειες ευρείας κλίμακας για τα ανθρώπινα κοινωνικά και ατομικά δικαιώματα, όπως την προστασία των δεδομένων, την ισότητα, τις ελευθερίες, την ανθρώπινη αυτονομία, τον αυτοπροσδιορισμό, την ανθρώπινη αξιοπρέπεια, την ασφάλεια, την πληροφορημένη συναίνεση, την ακεραιότητα, τη δικαιοσύνη και την αμεροληψία, την απουσία διακρίσεων, την ιδιωτικότητα και την αυτοδιάθεση[147].

Διαφάνεια στην αυτοματοποιημένη λήψη αποφάσεων.

Η έλλειψη αλγοριθμικής διαφάνειας[148] στις τεχνολογίες της τεχνητής νοημοσύνης αποτελεί μείζον ζήτημα στη νομική θεωρία. Από τη στιγμή που η τεχνολογία αυτή αναπτύσσεται σε τομείς υψηλού κινδύνου, αυξάνεται και η πίεση για το σχεδιασμό και τη ρύθμισή της με τέτοιο τρόπο, ώστε να είναι υπεύθυνη, δίκαιη και διαφανής[149]. Βασικά συστατικά της διαφάνειας αυτής είναι η προσβασιμότητα στην πληροφορία και η κατανόησή της. Οι πληροφορίες που σχετίζονται με τη λειτουργικότητα των αλγορίθμων είναι συχνά κι εσκεμμένα, ελάχιστα προσβάσιμες[150]. Παρά τους

147 Philip Jansen, Stearns Broadhead, Rowena Rodrigues, David Wright, Philip Brey, Alice Fox, Ning Wang, Owen King, Raja Chatila και Virginia Romano, SIENNA D4.1: State-of-the-art Review: AI and robotics, (2018).

148 Ο όρος «αλγοριθμική διαφάνεια» αναφέρεται στην αρχή σύμφωνα με την οποία οι παράγοντες που επηρεάζουν τις αποφάσεις που προέρχονται από αλγορίθμους πρέπει να είναι ορατοί ή διαφανείς από τα πρόσωπα που χρησιμοποιούν, ρυθμίζουν και επηρεάζονται από τα συστήματα που εμπλέκουν τους αλγορίθμους αυτούς. Bruno Lepri, Nuria Oliver, Emmanuel Letouzé, Alex Pentland και Patrick Vinck, «Fair, transparent, and accountable algorithmic decision-making processes», *Philosophy & Technology,* Vol. 31/ 4 (2018): 611-627. Βλ. επίσης Cary Coglianese και David Lehr, «Transparency and algorithmic governance», *Administrative Law Review,* Vol. 71/ 1 (2019): 18-38 και B. Bodo, N Helberger, K Irion, K Zuiderveen Borgesius, J Moller, B van de Velde, N Bol, B van Es και C de Vreese, «Tackling the Algorithmic Control Crisis-the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents», *Yale Journal of Law and Technology*, Vol. 19/ 1 (2018): 3.

149 Corinne Cath, «Governing artificial intelligence: ethical, legal and technical opportunities and challenges», (2018), διαθέσιμο σε https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080 .

150 Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter και Luciano Floridi, «The ethics of algorithms: Mapping the debate», (2016), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/2053951716679679 .

περιορισμούς της[151], η διαφάνεια είναι σημαντική ως στοιχείο της λογοδοσίας. Ειδικά στο Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, δίνεται έμφαση στη διαφάνεια σε συνδυασμό με την επεξεργασία των προσωπικών δεδομένων, παρέχοντας στα άτομα κατάλληλες πληροφορίες και έλεγχο.

Μεροληψία, προκαταλήψεις, διακρίσεις και έλλειψη ανταγωνιστικότητας.

Η μεροληψία[152], οι προκαταλήψεις[153] και οι διακρίσεις[154] έχουν χαρακτηριστεί ως μέγιστη πρόκληση[155], όταν σχετίζονται με τη χρήση των αλγορίθμων και τα συστήματα λήψης αυτοματοποιημένων αποφάσεων. Μεταξύ άλλων, τομείς που επηρεάζονται είναι η υγεία[156], η εργασία, η ποινική δικαιοσύνη[157] και η ασφάλιση. Σε έκθεσή του ο Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης αναγνωρίζει την πιθανότητα ύπαρξης διακρίσεων σε βάρος των ατόμων μέσω των αλγορίθμων ως «πιεστική πρόκληση» και δηλώνει ότι «η αρχή της απουσίας διακρίσεων, όπως περιγράφεται στο άρθρο 21 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, πρέπει να ληφθεί σοβαρά υπόψη, όταν γίνεται χρήση των

151 Mike Ananny και Kate Crawford, «Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability», (2016), διαθέσιμο σε https://journals.sagepub.com/doi/abs/10.1177/1461444816676645 .

152 Lauren Smith, «Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making», (2017), διαθέσιμο σε https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automateddecision-making/ .

153 Rachel Courtland, «Bias detectives: the researchers striving to make algorithms fair», (2018), διαθέσιμο σε https://www.nature.com/articles/d41586-018-05469-3 . Επίσης, Sara Hajian, Francesco Bonchi και Carlos Castillo, «Algorithmic bias: From discrimination discovery to fairness-aware data mining», KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, California (2016) και Ricardo Baeza-Yates, «Data and algorithmic bias in the web», Proceedings of the 8th ACM Conference on Web Science, (2016).

154 Ό.π. υποσημείωση 44.

155 Philipp Hacker, «Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law», *Common Market Law Review,* Vol. 55/ 4 (2018): 1143-1185.

156 David Danks και Alex John London, «Algorithmic bias in autonomous systems», Proceedings of the 26th International Joint Conference on Artificial Intelligence, AAAI Press, 2017: 4, διαθέσιμο σε https://www.cmu.edu/dietrich/philosophy/docs/london/IJCAI17-AlgorithmicBias-Distrib.pdf .

157 Richard Berk, «Accuracy and fairness for juvenile justice risk assessments», (2017), διαθέσιμο σε https://crim.sas.upenn.edu/sites/default/files/Berk_FairJuvy_1.2.2018.pdf .

αλγορίθμων στην καθημερινή ζωή»[158]. Το 2016, το Ευρωπαϊκό Κοινοβούλιο δημοσίευσε μία αναφορά του σχετικά με τις επιπτώσεις των μεγάλων δεδομένων (big data) πάνω στα θεμελιώδη δικαιώματα του ανθρώπου[159], όπως είναι η ιδιωτικότητα, η προστασία των δεδομένων, η απουσία διακρίσεων, η ασφάλεια και η επιβολή του νόμου. Σε αυτήν κατέδειξε ότι εξαιτίας των συνόλων των δεδομένων και των αλγοριθμικών συστημάτων που χρησιμοποιούνται κατά την πραγματοποίηση αξιολογήσεων και προβλέψεων στα διάφορα στάδια της επεξεργασίας δεδομένων, τα μεγάλα δεδομένα (big data) μπορούν να οδηγήσουν, όχι μόνο σε παραβιάσεις των θεμελιωδών δικαιωμάτων των ατόμων, αλλά και στη διαφορική μεταχείριση και έμμεση διάκριση ομάδων ανθρώπων με παρόμοια χαρακτηριστικά. Αυτό μπορεί να συμβεί κυρίως σε τομείς όπως η απονομή της δικαιοσύνης και η ισότητα στις ευκαιρίες πρόσβασης στην εκπαίδευση και την απασχόληση, κατά την πρόσληψη ή την αξιολόγηση ατόμων ή κατά τον προσδιορισμό των νέων καταναλωτικών συνηθειών των χρηστών των κοινωνικών μέσων. Συνεπεία των ανωτέρω, το Ευρωπαϊκό Κοινοβούλιο κάλεσε την Ευρωπαϊκή Επιτροπή, τα Κράτη – Μέλη και τις Αρχές προστασίας προσωπικών δεδομένων να αναγνωρίσουν και να λάβουν οποιαδήποτε πιθανά μέτρα για την ελαχιστοποίηση των διακρίσεων και των προκαταλήψεων μέσω των αλγορίθμων και να αναπτύξουν ένα δυνατό και κοινό δεοντολογικό πλαίσιο για τη διαφανή επεξεργασία των προσωπικών δεδομένων και των αυτοματοποιημένων λήψεων αποφάσεων, με στόχο την ορθή χρήση των δεδομένων και τη συνεχιζόμενη επιβολή του δικαίου της Ένωσης[160].

Αναφορικά με την έλλειψη ανταγωνιστικότητας στα αλγοριθμικά συστήματα, την απουσία, δηλαδή, του προφανούς μέσου, το οποίο θα μπορούσε να ανταγωνιστεί τους αλγορίθμους, όταν αυτοί παράγουν απρόσμενα, καταστροφικά, άδικα ή

158 EU Agency for Fundamental Rights (FRA), «#BigData: Discrimination in data-supported decision making», (2018), διαθέσιμο σε http://fra.europa.eu/en/publication/2018/big-data-discrimination .

159 Βλ. σχετικά http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0044+0+DOC+XML+V0//EN .

160 Ό.π. υποσημείωση 182.

μεροληπτικά αποτελέσματα[161], επισημαίνεται ότι η αδιαφάνεια των συστημάτων μηχανικής μάθησης μπορεί να οδηγήσει στον περιορισμό τόσο της λογοδοσίας των χρηστών τους, όσο και της ανταγωνιστικότητας των αποφάσεών τους[162].

Πνευματική ιδιοκτησία.

Δικαιώματα που προστατεύονται σύμφωνα με τις διατάξεις του δικαίου Πνευματικής Ιδιοκτησίας απαντώνται στο άρθρο 27 της Οικουμενικής Διακήρυξης των Δικαιωμάτων του Ανθρώπου (UDHR)[163], στο άρθρο 15 του Διεθνούς Συμφώνου για τα Οικονομικά, Κοινωνικά και Μορφωτικά Δικαιώματα (ICESCR)[164], στο άρθρο 19 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR)[165] και στη Διακήρυξη και το πρόγραμμα Δράσης της Βιέννης του 1993 (VDPA)[166]. Τα δικαιώματα αυτά σχετίζονται με την προστασία των ανθρωπίνων δικαιωμάτων και εμπεριέχονται σε διάφορους τομείς της ανθρώπινης δραστηριότητας[167]. Τα ζητήματα που άπτονται του δικαίου πνευματικής ιδιοκτησίας σχετίζονται με τα έργα που δημιουργήθηκαν με την τεχνολογία της τεχνητής νοημοσύνης, όπως για παράδειγμα κι ενδεικτικά αναφέροντας, η κυριότητα των έργων και των εφευρέσεων κι εάν αυτά

161 Lilian Edwards και Michael Veale, «Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for», *Duke Law and Technology Review,* 16/1 (2017):1-65.

162 Mireille Hildebrandt, «The New Imbroglio - Living with Machine Algorithms», σε Liisa Janssens, «The Art of Ethics in the Information Society», Amsterdam University Press (2016): 55-60.

163 1. Κάθε άτομο έχει το δικαίωμα να συμμετέχει ελεύθερα στην πνευματική ζωή της κοινότητας, να απολαμβάνει τις καλές τέχνες και να μοιράζεται την επιστημονική πρόοδο και τα αγαθά της. 2. Κάθε άτομο έχει το δικαίωμα προστασίας των ηθικών και υλικών αποκτημάτων του που απορρέουν από κάθε είδους επιστημονική, λογοτεχνική ή καλλιτεχνική παραγωγή. Βλ. σχετικά https://www.amnesty.gr/universal-declaration-of-human-rights .

164 1 γ) Να ωφελούνται από την προστασία των ηθικών και υλικών συμφερόντων τα οποία προκύπτουν από κάθε επιστημονικό, φιλολογικό ή καλλιτεχνικό έργο τους. Βλ. σχετικά https://unric.org/el/.

165 2. Κάθε πρόσωπο έχει δικαίωμα στην ελευθερία της έκφρασης. Το δικαίωμα αυτό περιλαμβάνει την ελευθερία της αναζήτησης, της λήψης και της μετάδοσης πληροφοριών και απόψεων κάθε είδους, ανεξαρτήτως συνόρων, προφορικά, γραπτά, σε έντυπα, σε κάθε μορφή τέχνης ή με κάθε άλλο μέσο της επιλογής του. Βλ. σχετικά https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4bd686e52 .

166 Βλ. σχετικά https://www.ohchr.org/en/professionalinterest/pages/vienna.aspx .

167 WIPO, «Intellectual Property and Human Rights», proceedings of a panel discussion, organized by the World Intellectual Property Organization in collaboration with the Office of the United Nations High Commissioner for Human Rights, (1998), διαθέσιμο σε http://www.wipo.int/edocs/pubdocs/en/intproperty/762/wipo_pub_762.pdf .

μπορούν να θεωρηθούν τέχνη, η κυριότητα του συνόλου των δεδομένων, από τα οποία μαθαίνει μία εφαρμογή τεχνητής νοημοσύνης, η ιδιότητα του δημιουργού ή του εφευρέτη έργων τεχνητής νοημοσύνης, οι συγκρούσεις με δικαιώματα άλλων ή άλλες νομικές διατάξεις[168].

Ικανότητα Δικαίου.

Η νομική θεωρία ερευνά το κατά πόσο η τεχνητή νοημοσύνη και/ή τα ρομποτικά συστήματα μπορούν να υπαχθούν στις ήδη υπάρχουσες νομικές οντότητες ή πρέπει να δημιουργηθεί νέα κατηγορία που να τις εμπεριέχει, με συγκεκριμένα χαρακτηριστικά και προϋποθέσεις[169]. Κατ΄ επέκταση προκύπτει το ερώτημα, εάν τα συστήματα αυτά μπορούν να είναι υποκείμενα δικαίου[170]. Κι ενώ συζητάται πλέον η πιθανότητα να δοθεί νομική προσωπικότητα στις οντότητες αυτές, για κάποιους μία τέτοιου είδους νομοθετική πράξη, θα είναι ηθικά περιττή και νομικά προβληματική[171]. Αντίστοιχα, στην περίπτωση της διερεύνησης της ύπαρξης ευθύνης από τις αυτόνομες μηχανές, κρίθηκε από τα αμερικανικά δικαστήρια, παρά τις αντίθετες προτάσεις, ότι δεν μπορούν να υπαχθούν στο υπάρχον νομικό καθεστώς της αντιπροσωπείας[172].

168 Βλ. σχετικά «Νομικά Προβλήματα των Διαδικτυακών Συναλλαγών» (συλλογικό), 2ο Συνέδριο ΕΜΕΟΔ, Νομική Βιβλιοθήκη, (2018). Βλ. επίσης «Innovation Law - Δίκαιο & Καινοτομία» (συλλογικό), 5ο Πανελλήνιο Συνέδριο e-ΘΕΜΙΣ, Νομική Βιβλιοθήκη, (2014) και CEIPI, Artificial Intelligence and Intellectual Property, διαθέσιμο σε http://www.ceipi.edu/en/training-seminars/artificialintelligence-and-intellectual-property/ .

169 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)) (2018/C 252/25), διαθέσιμο σε https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017IP0051&from=EN

170 Paulius Čerka, Jurgita Grigienė και Gintarė Sirbikytė, «Is it possible to grant legal personality to artificial intelligence software systems?», *Computer Law & Security Review,* Vol. 33/5 (2017): 685-699.

171 Joanna J. Bryson, Mihailis E. Diamantis και Thomas D. Grant, «Of, for, and by the people: the legal lacuna of synthetic persons», *Artificial Intelligence and Law,* Vol. 25/ 3 (2017): 273-291.

172 Bartosz Brożek και Marek Jakubiec, «On the legal responsibility of autonomous machines», *Artificial Intelligence and Law,* Vol. 25/ 3 (2017): 293-300.

Ευπάθειες της τεχνητής νοημοσύνης στην κυβερνοασφάλεια.

Ο οργανισμός RAND[173], σε μία έκθεση προοπτικών του, υπογραμμίζει ότι έχουν προκύψει ζητήματα εθνικής ασφάλειας που σχετίζονται με την τεχνητή νοημοσύνη, όπως η απόλυτα αυτοματοποιημένη τεχνολογία λήψης αποφάσεων που οδηγεί σε λάθη και θανάτους, η χρήση των όπλων τεχνητής νοημοσύνης χωρίς την ανθρώπινη παρέμβαση, οι ευπάθειες της τεχνητής νοημοσύνης σε σχέση με την κυβεροασφάλεια ή οι μέθοδοι παρέμβασης στα δίκτυα από αλλοδαπούς χρήστες τεχνολογιών τεχνητής νοημοσύνης[174]. Η ίδια έκθεση επίσης υπογραμμίζει τα ζητήματα που σχετίζονται και με την εσωτερική ασφάλεια, όπως για παράδειγμα την αυξανόμενη χρήση μεθόδων τεχνολογίας τεχνητής νοημοσύνης για την επιτήρηση των πολιτών από τις κυβερνήσεις, οι οποίες προκαλούν ανησυχίες με το ενδεχόμενο καταπάτησης των θεμελιωδών δικαιωμάτων των πολιτών. Ενδεικτικά αναφέροντας, το χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση πρόγραμμα SHERPA επίσης ερευνά τα θέματα που σχετίζονται με την τεχνητή νοημοσύνη και την κυβερνοασφάλεια[175].

Περιβάλλον εργασίας και εργαζόμενοι.

Το IBA Global Employment Institute[176] επισημαίνει σε έκθεσή του τις επιπτώσεις της τεχνητής νοημοσύνης και της ρομποτικής στον εργασιακό χώρο[177]. Μεταξύ άλλων διερευνώνται ζητήματα όπως η προετοιμασία των εργαζομένων για την απόκτηση των απαιτούμενων προσόντων, η ανάγκη σχετικής προσαρμογής του εκπαιδευτικού συστήματος, η δημιουργία νέων δομών και μορφών εργασίας, ο κίνδυνος απολύσεων

173 Πρόκειται για μη κερδοσκοπικό οργανισμό που βοηθά στη βελτίωση της πολιτικής και της λήψης των αποφάσεων, μέσω της έρευνας και της ανάλυσης. Βλ. σχετικά https://www.rand.org/about/history.html .

174 Osonde A. Osoba και William Welser IV, «The Risks of Artificial Intelligence to Security and the Future of Work», Santa Monica, CA: RAND Corporation, (2017), διαθέσιμο σε . https://www.rand.org/pubs/perspectives/PE237.html .

175 Βλ.σχετικά https://www.project-sherpa.eu/about/ .

176 Πρόκειται για μία διεθνή οργάνωση νομικών, δικηγορικών συλλόγων και νομικών εταιρειών, με στόχο τη συμβολή τους στην παγκόσμια σταθερότητα και την ειρήνη μέσω της απονομής της δικαιοσύνης. Βλ. σχετικά https://www.ibanet.org/About_the_IBA/About_the_IBA.aspx .

177 International Bar Association, Global Employment Institute, «Artificial Intelligence and Robotics and Their Impact on the Workplace», Απρίλιος 2017.

εργαζομένων, οι υπάρχουσες ανισότητες στη νέα αγορά εργασίας, η ενσωμάτωση των μη εκπαιδευμένων εργαζομένων στη νέα αγορά εργασίας, οι εργασιακές σχέσεις, θέματα υγείας και ασφαλείας, οι επιπτώσεις στο ωράριο εργασίας και στις αμοιβές, και θέματα κοινωνικής ασφάλισης. Η έκθεση σημειώνει ότι οι εθνικοί νομοθέτες ήδη υστερούν και το χάσμα μεταξύ πραγματικότητας και νομικού πλαισίου αυξάνει. Όλα τα υποδεικνυόμενα ζητήματα δεν έχουν μόνο σημαντικές, δυνητικά αρνητικές επιπτώσεις στα ανθρώπινα δικαιώματα, αλλά εγείρουν και ηθικά ζητήματα και διλήμματα που δεν μπορούν εύκολα να επιλυθούν.

Ιδιωτικότητα και ζητήματα προστασίας δεδομένων

Οι θεωρητικοί της νομικής επιστήμης και οι Αρχές προστασίας των δεδομένων εκφράζουν την άποψη ότι η τεχνητή νοημοσύνη θα επιφέρει μεγάλους κλυδωνισμούς στην ιδιωτικότητα και την προστασία των δεδομένων[178]. Οι προκλήσεις που θα προκύψουν αφορούν κυρίως στη συναίνεση, την επιτήρηση, τα δικαιώματα των ατόμων για την προστασία των δεδομένων τους, όπως το δικαίωμα πρόσβασης στα προσωπικά δεδομένα[179], το δικαίωμα να αποτρέψουν την επεξεργασία σε βάρος τους[180] ή το δικαίωμα να μην υπόκεινται σε αποφάσεις οι οποίες βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία[181]. Επίσης, εκφράζονται συχνά ανησυχίες σχετικά με την αλγοριθμική λογοδοσία και τον τρόπο που οι τεχνολογίες της τεχνητής νοημοσύνης παράγουν μη επαληθεύσιμα τεκμήρια, κατά παράβαση της ιδιωτικότητας, τα οποία δεν μπορούν να προβλεφθούν, να γίνουν κατανοητά ή να τύχουν αντίκρουσης[182]. Τα υποκείμενα των δικαιωμάτων έχουν περιορισμένο έλεγχο κι ελάχιστη επίβλεψη στον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα τους,

178 Stephen Gardner, «AI poses big privacy and data protection challenges», (2016), διαθέσιμο σε https://www.bna.com/artificial-intelligence-poses-n57982079158/ .

179 Βλ. σχετικά άρθρο 15 ΓΚΠΔ.

180 Βλ. σχετικά άρθρο 19 ΓΚΠΔ.

181 Βλ. σχετικά άρθρο 22 ΓΚΠΔ.

182 Sandra Wachter και Brent Mittelstadt, «A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI», Columbia Business Law Review, (2019), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829# .

κι εξάγονται συμπεράσματα από αυτά. Για το λόγο αυτό καθίσταται επιτακτική η ανάγκη για τη δημιουργία ενός καινούριου δικαιώματος προστασίας δεδομένων που να αφορά τα λογικά συμπεράσματα, ώστε να περιοριστεί το χάσμα της λογοδοσίας που οδηγεί σε υψηλού ρίσκου αποτελέσματα, τα οποία παραβιάζουν την ιδιωτικότητα ή βλάπτουν τη φήμη κι έχουν χαμηλή επαλήθευση[183]. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων σε άρθρο του στο 38ο Διεθνές Συνέδριο των Επιτρόπων για την Προστασία των Δεδομένων και την ιδιωτικότητα το 2016, τόνισε την πιθανότητα αύξησης της επιτήρησης και των επιπτώσεων στην προστασία της ιδιωτικής ζωής[184]. Καίριο ερώτημα παραμένει ο τρόπος με τον οποίο οι Αρχές προστασίας των δεδομένων θα μπορούσαν να επιτηρούν με τα κατάλληλα μέσα τους οργανισμούς που χρησιμοποιούν εντατικά τα μεγάλα δεδομένα, την τεχνητή νοημοσύνη και τη μηχανική μάθηση. Η βρετανική Αρχή Προστασίας Δεδομένων σε έγγραφό της το 2017, σχετικά με τα μεγάλα δεδομένα, την τεχνητή νοημοσύνη, τη μηχανική μάθηση και την προστασία των δεδομένων, εξέτασε τις επιπτώσεις των τεχνολογιών αυτών στην προστασία των δεδομένων κι εξέφρασε, μεταξύ άλλων, την άποψη ότι τα οφέλη από τις νέες τεχνολογίες δεν πρέπει επιτευχθούν σε βάρος του δικαιώματος απορρήτου των δεδομένων και ότι η επίτευξη των απαιτήσεων για την προστασία των δεδομένων θα ωφελήσει τόσο τους οργανισμούς, όσο και τους ιδιώτες[185].

183 Ό.π. υποσημειώση 205.

184 EDPS, «Artificial Intelligence, Robotics, Privacy and Data Protection Background document for the 38th International Conference of Data Protection and Privacy Commissioners», (2016), διαθέσιμο σε https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en .

185 ICO, «Big data, artificial intelligence, machine learning and data protection», Version: 2.2, (2017), διαθέσιμο σε https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf .

Ευθύνη για τις ζημίες που προκαλούνται από τις εφαρμογές της τεχνητής νοημοσύνης.

Μείζον ζήτημα για τη νομική θεωρία αποτελεί η απόδοση ευθύνης για τις ζημίες που προκαλούνται μέσω της τεχνολογίας της τεχνητής νοημοσύνης, κυρίως ως προς τη δυνατότητα εφαρμογής των σχετικών διατάξεων του αστικού και του ποινικού δικαίου[186]. Ως προς τις διατάξεις του ποινικού δικαίου και την απόδοση ποινικής ευθύνης, προκύπτει ο προβληματισμός, στην περίπτωση που αυτές τύχουν εφαρμογής, ποιον θα αφορούν, ενώ ως προς τις διατάξεις με βάση το αστικό δίκαιο, οι προβληματισμοί αφορούν κυρίως το κατά πόσο μία εφαρμογή τεχνητής νοημοσύνης αποτελεί προϊόν που υπάγεται στις διατάξεις περί προϊόντων ή υπηρεσία, στην οποία εφαρμόζονται οι διατάξεις περί αδικοπραξιών[187]. Εξετάζεται επίσης η πιθανότητα να φέρει η ίδια η οντότητα της τεχνητής νοημοσύνης ευθύνη, ανεξάρτητα από τις αντίστοιχες ποινικές και αστικές ευθύνες του κατασκευαστή, του χρήστη ή του κατόχου[188].

Λογοδοσία λόγω ζημίας.

Η έννοια της λογοδοσίας ορίζεται ως «η ανάγκη εξήγησης κι αιτιολόγησης των αποφάσεων και των πράξεων κάποιου απέναντι στους συνεργάτες του, τους χρήστες και αυτούς με τους οποίους το σύστημα αλληλεπιδρά. Για να διασφαλιστεί η λογοδοσία, οι αποφάσεις πρέπει να προέρχονται και να εξηγούνται από τους

186 Gabriel Hallevy, «The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control», *Akron Intellectual Property Journal*, Vol. 4/ 2, Article 1, (2010), διαθέσιμο σε http://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1 .

187 John Kingston, «Artificial Intelligence and Legal Liability» σε Max Brame και Miltiadis Petridis, «Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV», *Springer-Verlag*, (2016): 269-279.

188 Gabriel Hallevy, «AI v. IP - Criminal Liability for Intellectual Property IP Offenses of Artificial Intelligence AI Entities», (2015), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2691923 . Επίσης, Yavar Bathaee, The artificial intelligence black box and the failure of intent and causation, Harvard Journal of Law & Technology, Vol. 31/ 2, (2018): 889- 937.

αλγόριθμους που χρησιμοποιήθηκαν προς τούτο»[189]. Ειδικά στην τεχνολογία της τεχνητής νοημοσύνης, η λογοδοσία απαιτεί τόσο τη λειτουργία της καθοδηγητικής δράσης (σχηματισμός πεποιθήσεων και λήψη αποφάσεων), όσο και αυτή της εξήγησης (αναγωγή των αποφάσεων σε ένα ευρύτερο πλαίσιο και ταξινόμησή τους σύμφωνα με τις ισχύουσες ηθικές αξίες). Οι πολιτικές που εφαρμόζονται στην Αμερική και την Ευρωπαϊκή Ένωση εμφανίζονται να αποκλίνουν στον τρόπο κάλυψης του χάσματος της λογοδοσίας στην τεχνητή νοημοσύνη[190]. Οι μηχανισμοί της νομικής λογοδοσίας για τις ζημίες από την τεχνητή νοημοσύνη μπορούν να λάβουν τη μορφή του δικαιώματος επεξήγησης[191], της προστασίας των δεδομένων και της πληροφορίας, της διασφάλισης της διαφάνειας, του ελέγχου ή άλλων υποχρεώσεων αναφοράς[192].

5.3 **Ειδικά ζητήματα για τις εφαρμογές της ρομποτικής.**

Καθώς οι τεχνολογίες της τεχνητής νοημοσύνης και της ρομποτικής συνεργάζονται στενά και χρησιμοποιούν τεράστιες ποσότητες δεδομένων, συχνά θα επικαλύπτονται

189 Virginia Dignum, «The ART of AI — Accountability, Responsibility, Transparency», (2018), διαθέσιμο σε https://medium.com/@virginiadignum/the-art-of-ai-accountability-responsibility-transparency-48666ec92ea5 .

190 Sandra Wachter, Brent Mittelstadt και Luciano Floridi, «Transparent, explainable, and accountable AI for robotics», *Science Robotics*, Vol. 2/ 6 (2017).

191 Στον τομέα των αλγορίθμων, κυρίως σε σχέση με την τεχνολογία της τεχνητής νοημοσύνης και τα υποπεδία της, όπως η μηχανική μάθηση, το δικαίωμα στην επεξήγηση (ή το δικαίωμα σε μία εξήγηση) είναι το δικαίωμα του να αξιώσει κάποιος μία εξήγηση για το αποτέλεσμα μίας ενέργειας αλγορίθμου που τον αφορά σημαντικά, σε νομικό ή οικονομικό επίπεδο. Βλ. σχετικά Lilian Edwards και Michael Veale, «Enslaving the algorithm: from a 'right to an explanation' to a 'right to better decisions'?», *IEEE Security and Privacy Magazine* (2018). Βλ. επίσης Lilian Edwards και Michael Veale, «Slave to the Algorithm? Why a Right to an Explanation is Probably Not the Remedy You Are Looking For», *Duke Law and Technology Review,* Vol. 16/ 18 (2017).
Αντιλαμβανόμενοι την ανάγκη των ατόμων ώστε το δικαίωμα εξήγησης των αυτοματοποιημένων αποφάσεων που έχουν ληφθεί και τα αφορούν, να έχει δεσμευτικότητα, οι ερευνητές του ιδρύματος Alan Turing παρέχουν οδηγίες ως προς την εφαρμογή των νέων ευρωπαϊκών διατάξεων για την προστασία των δικαιωμάτων προστασίας των δεδομένων. Βλ. σχετικά https://www.turing.ac.uk/research/impact-stories/a-right-to-explanation .

192 Finale Doshi-Velez, Mason Kortz, Ryan Budish, Chris Bavitz, Sam Gershman, David O'Brien, Stuart Schieber, James Waldo, David Weinberger, and Alexandra Wood, »Accountability of AI Under the Law: The Role of Explanation», διαθέσιμο σε https://arxiv.org/pdf/1711.01134.pdf .

και θα έχουν πολλαπλασιαστικά αποτελέσματα, τα οποία θα οξύνουν τα νομικά κενά και τα ζητήματα που άπτονται των ανθρωπίνων δικαιωμάτων και σχετίζονται με τις τεχνολογίες αυτές. Τέτοιου είδους θέματα ενδέχεται και να πολλαπλασιαστούν, εάν η βιομηχανία της τεχνητής νοημοσύνης και της ρομποτικής αναπτύξει εφαρμογές και συστήματα χωρίς να δώσει έγκαιρα βάση στη διαδικασία σχεδιασμού και ανάπτυξης των επιπτώσεων των τεχνολογιών αυτών πάνω στα ανθρώπινα δικαιώματα και τις κοινωνικές αξίες.

Εξαπάτηση από Ρομπότ.

Η εξαπάτηση των ατόμων από τα ρομπότ[193], κυρίως των ευάλωτων ομάδων[194], αποτελεί αντικείμενο έρευνας, με τους ερευνητές να εστιάζουν κυρίως στην τεχνική που εφαρμόζεται από τα ρομπότ και τους προσδίδει τους ικανότητα εξαπάτησης, τεχνική η οποία χρησιμοποιείται ευρέως από τους ανθρώπους και τα ζώα κι έχει ως στόχο την επίτευξη συγκεκριμένων στόχων[195]. Ειδικά για τα διαφημιστικά ρομπότ, οι ευκαιρίες εξαπάτησης είναι πολλαπλές, καθώς οι καταναλωτές είναι συνήθως ευκολόπιστοι[196]. Μολαταύτα, δεν είναι όλες ενέργειες εξαπάτησης αξιόποινες ή παράνομες. Σύμφωνα με τις Αρχές του μάρκετινγκ, ένα μικρό ποσοστό «ανακρίβειας» είναι συχνά επιτρεπτό. Πολλά ρομπότ τα οποία είναι προγραμματισμένα προς παραπλάνηση των καταναλωτών, μπορεί απλά να παρέχουν εμπορικές υπηρεσίες ή να ασχολούνται με την κοινή ανάλυση δεδομένων, κατά τον

193 Jaeeun Shim, και Ronald C. Arkin, «A taxonomy of robot deception and its benefits in HRI», 2013 IEEE International Conference on Systems, Man, and Cybernetics. IEEE, 2013.

194 Τα ρομπότ μπορούν να εμπεριέχουν στο λογισμικό τους ικανότητες εξαπάτησης και διακρίσεων, οι οποίες ενδεχομένως να επηρεάζουν την ανθρώπινη αξιοπρέπεια. Βλ. σχετικά Amanda Sharkey και Natalie Wood, «The Paro seal robot: demeaning or enabling?», διαθέσιμο σε http://doc.gold.ac.uk/aisb50/AISB50-S17/AISB50-S17-Sharkey-Paper.pdf .

195 Karolina Zawieska, «Deception and manipulation in social robotics», Workshop on The Emerging Policy and Ethic of Human-Robot Interaction at the 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI2015), διαθέσιμο σε http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Zawieska.pdf .

196 Woodrow Hartzog, «Unfair and deceptive robots», *Maryland Law Review*, Vol. 74 (2014): 785, διαθέσιμο σε https://heinonline.org/HOL/LandingPage?handle=hein.journals/mllr74&div=41&id=&page= .

ίδιο τρόπο που ένας πωλητής ακολουθεί τη στρατηγική που θα τον οδηγήσει στην καλύτερη δυνατή συμφωνία[197].

Ικανότητα δικαίου.

Παρότι το ερώτημα εάν μπορούν τα ρομπότ να θεωρηθούν πρόσωπα δεν είναι καινούριο[198], το ενδιαφέρον για το θέμα αυτό δεν είχε ανανεωθεί μέχρι πρόσφατα που επικεντρώθηκε σε αυτό η Ευρωπαϊκή Ένωση. Το Ευρωπαϊκό Κοινοβούλιο, σε έκθεσή του σχετικά με τις ρυθμίσεις του αστικού δικαίου στον τομέα της ρομποτικής, παρέχει συστάσεις προς την Επιτροπή, στις περιπτώσεις που αυτή διενεργεί εκτίμηση επιπτώσεων για τα μελλοντικά νομοθετικά της μέσα, να ερευνά, να αναλύει και να εξετάζει τις επιπτώσεις όλων των πιθανών νομικών λύσεων, συμπεριλαμβανομένης και της δημιουργίας μακροπρόθεσμα, ενός ειδικού νομικού καθεστώτος για τα ρομπότ. Υπό το καθεστώς αυτό θα μπορεί να καθοριστεί ότι τα πιο εξελιγμένα τεχνολογικά αυτόνομα μηχανήματα θα υπάγονται στην ειδική κατηγορία των ηλεκτρονικών ατόμων που ενέχουν ευθύνη για την αποκατάσταση οποιασδήποτε ζημίας προκληθεί από αυτά και πιθανότατα να αποδοθεί ηλεκτρονική προσωπικότητα στις περιπτώσεις των ρομπότ που λαμβάνουν αυτόνομες αποφάσεις ή αλληλεπιδρούν με τρίτα μέρη ανεξάρτητα από την ανθρώπινη βούληση[199]. Στον αντίποδα, σε ανοιχτή επιστολή τους προς την Ευρωπαϊκή Επιτροπή, οι ειδικοί της τεχνητής νοημοσύνης και της ρομποτικής, εκπρόσωποι της βιομηχανίας και οι ειδικοί σε νομικά και ιατρικά ζητήματα, καθώς και σε ζητήματα ηθικής και δεοντολογίας ισχυρίζονται με έμφαση ότι τόσο από ηθικής, όσο και από νομικής άποψης, η

197 Ό.π. υποσημείωση 219.

198 Lawrence B Solum, «Legal personhood for artificial intelligences», *North Carolina Law Review*, Vol. 70/ 4 (1992): 1231- 1287.

199 Ευρωπαϊκό Κοινοβούλιο, Έκθεση με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής, (2015/2103(INL)), Επιτροπή Νομικών Θεμάτων, διαθέσιμο σε 27.1.2017.http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN .

απόδοση νομικής προσωπικότητας στα ρομπότ πρέπει να απορριφθεί, ανεξάρτητα από το μοντέλο του νομικού καθεστώτος που θα ακολουθηθεί[200].

Τέλος και σε μία ρηξικέλευθη οπτική, το 2009 εκφράστηκε η άποψη σχετικά με την εξομοίωση των ρομπότ με οικόσιτα ζώα, κυρίως ως προς το θέμα της υπαιτιότητας[201].

Χρήση αυτόνομων όπλων.

Η πρόκληση ζημίας από τα ρομπότ επιτυγχάνεται κυρίως με τη μορφή των αυτόνομων όπλων[202], των οπλισμένων μη επανδρωμένων αεροσκαφών (armed drones[203]), των πολεμικών μη επανδρωμένων αεροσκαφών ή των ρομπότ – δολοφόνων (killer robots[204]). Το Ευρωπαϊκό Κοινοβούλιο το 2018, σε ψήφισμά του σχετικά με τα οπλικά συστήματα, επεσήμανε ότι σε διάφορα κράτη, δημόσιες και ιδιωτικές επιχειρήσεις πραγματοποιούν έρευνες και αναπτύσσουν θανατηφόρα αυτόνομα οπλικά συστήματα, με στόχο τη μετατροπή του τρόπου διεξαγωγής του

200 «Open Letter to the European Commission Artificial Intelligence and Robotics», (2018), διαθέσιμο σε http://www.robotics-openletter.eu/ .

201 Enrique Schaerer, Richard Kelley και Monica Nicolescu, «Robots as Animals: A Framework for Liability and Responsibility in Human-Robot Interactions», RO-MAN 2009 - The 18th IEEE International Symposium on Robot and Human Interactive Communication, (2009), διαθέσιμο σε https://ieeexplore.ieee.org/document/5326244. Επίσης, Richard Kelley, Enrique Schaerer, Micaela Gomez και Monica Nicolescu, «Liability in robotics: an international perspective on robots as animals», *Advanced Robotics*, Vol. 24/ 13, (2010): 1861-1871, διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1163/016918610X527194 .

202 Mark Gubrud, «Why Should We Ban Autonomous Weapons?», (2016), διαθέσιμο σε https://spectrum.ieee.org/automaton/robotics/military-robots/why-should-we-ban-autonomous-weapons-to-survive .

203 Bruno Oliveira Martins, «The European Union and armed drones: framing the debate», *Global Affairs*, Vol. 1/3 (2015): 247-250, διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080930 . Βλ. επίσης, Jessica Dorsey και Christophe Paulussen, «A common European position on armed drones? Charting EU member states' views on questions of counterterrorism uses of force», *Global Affairs*, Vol. 1/ 3 (2015): 277–283, διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080037 , Anthony Dworkin, «Drones and targeted killing: Defining a European position, European Council on Foreign Relations», (2013), διαθέσιμο σε https://ecfr.eu/publication/drones_and_targeted_killing_defining_a_european_position211/ και Anthony Dworkin, «The EU and armed drones – epilogue», *Global Affairs*, Vol. 1/ 3 (2015): 293–297, διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080901 .

204 Armin Krishnan, «Killer robots: Legality and ethicality of autonomous weapons», Ashgate Publishing, Ltd., 2009. Βλ. επίσης Vincent C. Muller και Thomas W. Simpson, «Killer robots: Regulate, don't ban», University of Oxford, Blavatnik School of Government Policy Memo, (2014): 1-4.

πολέμου, μέσω της δημιουργίας ανεξέλεγκτων ανταγωνιστικών εξοπλισμών[205]. Κατ' επέκταση, προκύπτουν ουσιώδη ηθικά και νομικά ερωτήματα σχετικά με τον ανθρώπινο έλεγχο επί των εξοπλισμών, κυρίως στις περιπτώσεις που οι μηχανές και τα ρομπότ δεν μπορούν να λάβουν αποφάσεις όμοιες με τις ανθρώπινες, που να εμπεριέχουν τις βασικές νομικές Αρχές του στρατιωτικού δικαίου, της διάκρισης, της αναλογικότητας και της προφύλαξης[206]. Επίσης, εκφράζονται ανησυχίες σχετικά με τους ανταγωνιστικούς εξοπλισμούς σε αυτόνομα όπλα και τις ζημίες που μπορεί να προκαλέσουν λόγω δυσλειτουργίας τους ή έπειτα από κυβερνοεπίθεση[207].

Ασφάλεια και ζητήματα ελέγχου των ρομπότ.

Η ανθρώπινη ζωή και η ευημερία μπορεί να επηρεαστούν αρνητικά εξαιτίας ζητημάτων ασφαλείας κι ελέγχου που θα προκύψουν από τη χρήση των ρομπότ[208]. Για παράδειγμα, τα ιατρικά ρομπότ μπορεί να διακινδυνεύσουν την φροντίδα των ασθενών και να προκαλέσουν βλάβες ή και θάνατο, λόγω δυσλειτουργιών των συσκευών ή των εργαλείων[209]. Επίσης η ρομποτική προσθετική μπορεί να γίνει επισφαλής κι επικίνδυνη. Στις περιπτώσεις των ρομπότ φροντίδας απαιτούνται πρόσθετες διαφυλάξεις ασφαλείας, όπως επίσης και ακόμα υψηλότερο επίπεδο

205 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Σεπτεμβρίου 2018 σχετικά με τα αυτόνομα οπλικά συστήματα (2018/2752), διαθέσιμο σε http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0341+0+DOC+XML+V0//EN&language=EN .

206 Jean-Marie Henckaerts, «Μελέτη για το Εθιμικό Διεθνές Ανθρωπιστικό Δίκαιο. Μια Συνεισφορά στην κατανόηση και το σεβασμό των κανόνων Δικαίου των Ενόπλων Συρράξεων», Ευρωπαϊκό Κέντρο Έρευνας και Κατάρτισης Δικαιωμάτων του Ανθρωπου και Ανθρωπιστικής Δράσης Παντείου Πανεπιστημίου , Αθήνα 2007.

207 Ευρωπαϊκό Κοινοβούλιο, Κοινή Πρόταση Ψηφίσματος σύμφωνα με το άρθρο 110, παράγραφοι 2 και 4, του Κανονισμού σχετικά με τη χρήση οπλισμένων τηλεκατευθυνόμενων αεροσκαφών (2014/2567(RSP)), διαθέσιμο σε http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P7-RC-2014-0201+0+DOC+XML+V0//EN .

208 Milos Vasic και Aude Billard, «Safety issues in human-robot interactions», 2013 IEEE International Conference on Robotics and Automation, IEEE, (2013), διαθέσιμο σε https://ieeexplore.ieee.org/abstract/document/6630576 .

209 Homa Alemzadeh, Jaishankar Raman, Nancy Leveson, Zbigniew Kalbarczyk και Ravishankar K. Iyer, «Adverse events in robotic surgery: a retrospective study of 14 years of FDA data», *PloS One*, Vol. 11/ 4, (2016), διαθέσιμο σε http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0151470

αξιοπιστίας σε σχέση με τα βιομηχανικά ρομπότ[210]. Το Ευρωπαϊκό Κοινοβούλιο, σε έκθεσή του, υπογραμμίζει ότι πρέπει να ληφθούν πρόσθετα εχέγγυα προς διασφάλιση της ασφαλούς χρήσης των ρομπότ και της αποφυγής της παραβίασης του δικαιώματος στη σωματική ακεραιότητα των χρηστών[211].

Αναγνώριση ευθύνης από τη χρήση των ρομπότ.

Η αναγνώριση της ευθύνης, κακόβουλης[212] ή μη[213], από τη χρήση των ρομπότ, όπως στις περιπτώσεις των αυτόνομων οχημάτων ή των αυτόνομων οπλικών συστημάτων, έχει απασχολήσει ιδιαίτερα τη νομική θεωρία. Τόσο σε επίπεδο Ευρωπαϊκής Ένωσης[214], όσο και σε εθνικό, η αστική ευθύνη από τα αυτοκινούμενα οχήματα προβλέπεται σε αντίστοιχες διατάξεις. Η συζήτηση αφορά κυρίως την ποινική ευθύνη που προκύπτει, σε συνάρτηση με την ευθύνη των χειριστών στις περιπτώσεις που παραβλέπουν να λάβουν τα κατάλληλα μέτρα για τον έλεγχο των κινδύνων που προέρχονται από τα ρομπότ[215]. Προτείνεται ένα μόρφωμα ως μηχανισμός διαμοιρασμού της ευθύνης ανάμεσα στα ρομπότ, τον κατασκευαστή και τον κάτοχό τους, ο οποίος διαμοιρασμός θα εξαρτάται από τα δεδομένα που έχουν καταχωρηθεί από τον κατασκευαστή και από τη γνώση που παράγεται από το ίδιο το ρομπότ (μέσω της ικανότητας μάθησής του και τις προσαρμογές που έχουν γίνει από τον

210 Marion Hersh, «Overcoming Barriers and Increasing Independence – Service Robots for Elderly and Disabled People», *International Journal of Advanced Robotic Systems*, Vol. 12/ 8, (2015), διαθέσιμο σε http://eprints.gla.ac.uk/101946/1/101946.pdf .

211 European Parliamentary Research Service Scientific Foresight Unit (STOA), Scientific Foresight study, «Ethical Aspects of Cyber-Physical Systems», (2016), διαθέσιμο σε http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU(2016)563501_EN.pdf .

212 Για παράδειγμα, κυβερνοεπιθέσεις από εισβολείς (hackers) σε βιομηχανικά ή εμπορικά ή οικιακά ρομπότ, με στόχο την κατασκοπία ή την πρόκληση άλλης ζημίας. Βλ. σχετικά «Industrial and domestic robots highly vulnerable to malicious cyber-attacks», (2017), διαθέσιμο σε https://teiss.co.uk/special-reports/industrial-domestic-robots-vulnerable-cyber-attacks/ .

213 Για παράδειγμα, η ζημία που προκλήθηκε από αμέλεια ή προς αποφυγή άλλης βαρύτερης ζημίας.

214 European Parliament, «A common EU approach to liability rules and insurance for connected and autonomous vehicles: European Added Value Assessment», (2018), διαθέσιμο σε http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf .

215 Sabine Gless, Emily Silverman και Thomas Weigend, «If Robots cause harm, Who is to blame? Self-driving Cars and Criminal Liability», *New Criminal Law Review: In International and Interdisciplinary Journal*, Vol. 19/ 3 (2016): 412-436.

κάτοχο)[216]. Εξετάζεται, επίσης, η επίπτωση της τεχνολογίας της ρομποτικής στα νομικά συστήματα και το κατά πόσο μία νέα γενιά εμπόρων – ρομπότ, οδηγών τεχνητής νοημοσύνης, τεχνητών τραγουδιστών και αυτόνομων θανατηφόρων όπλων επηρεάζουν τη γνώση των ατόμων, το περιβάλλον και τις αντιλήψεις για τον κόσμο και προτείνεται στον τομέα του αστικού δικαίου η ευθύνη των ρομπότ να είναι αποκλειστική[217].

Ζητήματα παραβίασης της ιδιωτικότητας.

Οι αυτόνομες μηχανές, όπως είναι τα ρομπότ, δεδομένου ότι «πηγαίνουν σε μέρη όπου οι άνθρωποι δεν μπορούν να πάνε και βλέπουν πράγματα που οι άνθρωποι δεν μπορούν να δουν»[218], μπορεί να εντείνουν τις παραβιάσεις της ιδιωτικότητας, όπως για παράδειγμα, μέσω του λογισμικού αναγνώρισης προσώπου, το οποίο εντοπίζει κι αναγνωρίζει τα πρόσωπα, δημιουργώντας το προφίλ τους[219]. Τα ρομπότ διευκολύνουν ενεργά την επιβολή άμεσης επιτήρησης από τους έχοντες συμφέρον προς τούτο, λόγω των εξειδικευμένων αισθητήρων κι επεξεργαστών τους, οι οποίοι μεγεθύνουν εξαιρετικά την ανθρώπινη ικανότητα παρατήρησης. Επίσης, τα ρομπότ απειλούν την ιδιωτικότητα με την εισαγωγή νέων μέσων πρόσβασης σε ιστορικά προστατευμένα μέρη, όπως το οικιακό ρομπότ στην οικία. Η εισαγωγή των κοινωνικών ρομπότ στην καθημερινότητα και σε μέρη που ιστορικά είναι συνδεδεμένα με τη «μοναξιά», μπορεί να μειώσει τις ήδη μειωμένες ευκαιρίες για εσωτερικότητα και

216 Alejandro Zornoza, José C. Moreno, José L. Guzmán, Francisco Rodríguez και Julián Sánchez-Hermosilla, «Robots Liability: A Use Case and a Potential Solution, Robotics-Legal, Ethical and Socioeconomic Impacts», InTech, (2017), διαθέσιμο σε https://www.intechopen.com/books/robotics-legal-ethical-andsocioeconomic-impacts/robots-liability-a-use-case-and-a-potential-solution .

217 Ugo Pagallo, «What Robots Want: Autonomous Machines, Codes and New Frontiers of Legal Responsibility», σε Mireille Hildebrandt και Jeanne Gaakeer, «Human Law and Computer Law: Comparative Perspectives», Ius Gentium: Comparative Perspectives on Law and Justice, Vol 25, *Springer*, Dordrecht, διαθέσιμο σε https://link.springer.com/chapter/10.1007/978-94-007-6314-%202_3#citeas .

218 Ryan M. Calo, «Robots and privacy», σε Patrick Lin, Keith Abney και George A. Bekey, «Robot Ethics: The Ethical and Social Implications of Robotics», (2012):187-202.

219 Marcus Woo, «Robots: can we trust them with our privacy», (2014), διαθέσιμο σε http://www.bbc.com/future/story/20140605-the-greatest-threat-of-robots .

αυτοστοχασμό, τα οποία η ιδιωτικότητα έχει ως στόχο να προστατεύσει. Περαιτέρω, τα κοινωνικά ρομπότ μπορεί να βρίσκονται στη μοναδική θέση να εξάγουν πληροφορίες από τα άτομα και να αξιοποιήσουν τις περισσότερες από τα ανθρώπινες ιδιότητες, όπως το φόβο ή τον έπαινο, όπως επίσης μπορούν να έχουν τέλειες αναμνήσεις, να είναι ακούραστα, ενώ δεν μπορούν να έλθουν σε αμηχανία, πλεονεκτήματα που τους δίνουν προβάδισμα σε σχέση με τους ανθρώπους. Τέλος, η κοινωνική φύση των ρομπότ μπορεί να οδηγήσει στη δημιουργία νέων μορφών ιδιαίτερα ευαίσθητων προσωπικών στοιχείων[220].

Αντικατάσταση ανθρώπινου δυναμικού και απώλεια θέσεων εργασίας.

Μία βασική ανησυχία της τεχνολογίας της ρομποτικής σχετίζεται με τη χρήση των ρομπότ κατά την εργασία και την αντικατάσταση του ανθρωπίνου δυναμικού, κάτι που μαθηματικά οδηγεί στην απώλεια θέσεων εργασίας[221] (αν και αυτό δεν συμβαίνει σε κάθε περίπτωση[222], σε κάθε πλαίσιο ή αυτόματα και μπορεί να έχει και θετικά αποτελέσματα). Ο κίνδυνος αυτός σχετίζεται κυρίως με θέσεις εργασίας χαμηλότερης ειδίκευσης και με εργασιακούς τομείς που είναι πιο ευάλωτοι στην αυτοματοποίηση[223]. Προκύπτουν, λοιπόν, τα ερωτήματα κατά πόσο μπορεί η νομοθεσία να προστατεύσει αυτές τις πληθυσμιακές κατηγορίες που είναι ευάλωτες στην απώλεια της εργασιακής τους θέσης, εάν υπάρχει νομοθετικό και πολιτικό πλαίσιο που θα μπορούσε να επενδύσει στην εκπαίδευση και τις μεταρρυθμίσεις, με

220 Ό. π. υποσημείωση 242.

221 Larry Elliott, «Millions of UK workers at risk of being replaced by robots, study says», (2017), διαθέσιμο σε https://www.theguardian.com/technology/2017/mar/24/. Βλ. επίσης Rebecca J. Rosen, «In Praise of Short-Term Thinking», (2015), διαθέσιμο σε https://www.theatlantic.com/business/archive/2015/09/jobs-automation-technologicalunemployment-history/403576/ και Sam Earle, «Bullshit Jobs: Robots Are Replacing Human Workers, So Why Are Americans Still Working So Hard?», (2018) διαθέσιμο σε http://www.newsweek.com/bullshit-jobs-age-automation-why-areamericans-still-working-so-hard-983753 .

222 Gavin Jackson, «Job loss fears from automation overblown, says OECD», (2018), διαθέσιμο σε https://www.ft.com/content/732c3b78-329f-11e8-b5bf-23cb17fd1498 .

223 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)), διαθέσιμο σε https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EL.html .

στόχο τη βελτίωση της εργασιακής ανακατανομής, την ανάπτυξη νέων ικανοτήτων ή τη δια βίου εκπαίδευση για τους ανθρώπους που αντικαταστάθηκαν από τα ρομπότ ή τη συνύπαρξή τους με αυτά. Εάν αυτά δεν επιτευχθούν, τότε το ανθρώπινο δυναμικό θα στερείται εφοδίων και θα υπολείπεται ως προς τις δυνατότητες αυτοεκπλήρωσης και τη συμβολή του στην οικονομία και την κοινωνία[224].

Προστασία καταναλωτών.

Στις περιπτώσεις των ρομπότ που χρησιμεύουν ως οικιακοί ή ψηφιακοί προσωπικοί βοηθοί ή έχουν τη μορφή αυτόνομων οχημάτων και προσωπικών μη επανδρωμένων αεροσκαφών, προκύπτουν κοινά ζητήματα προστασίας καταναλωτών, όπως ο κίνδυνος απάτης, η παραβίαση της ιδιωτικότητας και της ασφάλειας των δεδομένων, κίνδυνοι προς την υγεία και τη σωματική ακεραιότητα, αλλά και ευπάθειες οικονομικής φύσης[225]. Η τεχνολογία των ρομπότ εγείρει νέα ζητήματα προστασίας των καταναλωτών, δεδομένου ότι τα ήδη υπάρχοντα αμφισβητούνται ως προς την εφαρμογή τους σε τέτοιου είδους ανερχόμενες τεχνολογίες.

Πνευματική ιδιοκτησία.

Τα ζητήματα που προκύπτουν από την εφαρμογή των διατάξεων του δικαίου πνευματικής ιδιοκτησίας στην τεχνολογία των ρομπότ, μέσω της τεχνητής νοημοσύνης, αφορούν κυρίως θέματα όπως απόδοση της ιδιότητας του δημιουργού, του συνδημιουργού ή του εφευρέτη σε ένα ρομπότ. Από τη στιγμή που δεν υπάρχει σχετική σύμπνοια στις απόψεις των θεωρητικών[226], κυριαρχεί η τάση ότι στην

224 World Economic Forum (In collaboration with The Boston Consulting Group), «Towards a Reskilling Revolution: A Future of Jobs for All», (2018), διαθέσιμο σε http://www3.weforum.org/docs/WEF_FOW_Reskilling_Revolution.pdf .

225 Woodrow Hartzog, «Unfair and Deceptive Robots», *Maryland Law Review*, Vol. 74/ 4 (2015): 785-829, διαθέσιμο σε http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3675&context=mlr .

226 Tiffany Li και Charles Roslof, «Robots vs. Monkeys: Intellectual Property Rights of Non-Human Creators», [Poster Session], (2016), διαθέσιμο σε https://ssrn.com/abstract=2756245 .

περίπτωση που δοθεί από το νομοθέτη ικανότητα δικαίου και νομική προσωπικότητα στα ρομπότ, αυτό να μπορεί να οδηγήσει και στην απονομή πνευματικών δικαιωμάτων σε αυτά[227]. Καθώς αυξάνει η ικανότητα των ρομπότ να δημιουργούν και να εφεύρουν, αυτή σταδιακά θα μετατραπεί σε πρόκληση που θα απαιτεί άμεσες απαντήσεις ή θα οδηγήσει σε συγκρούσεις μεταξύ ανθρώπων και ρομπότ ή ρομπότ μεταξύ τους.

6 Κενά και προκλήσεις

Στο ελληνικό δίκαιο οι νομοθετικές ρυθμίσεις που ισχύουν για τους τομείς της τεχνητής νοημοσύνης και της ρομποτικής, υπό το πρίσμα της προστασίας των δεδομένων, φαίνεται ότι δεν είναι επαρκείς, παρά τον Ευρωπαϊκό Κανονισμό και τη νομοθεσία που ακολούθησε εφαρμοστικά. Τα θέματα σχετικά με τα μη επανδρωμένα αεροσκάφη έχουν μεν ρυθμιστεί λεπτομερώς, αλλά όχι υπό το πρίσμα των αδικοπραξιών σε βάρος τρίτων (άρ. 914επ. ΑΚ). Το ίδιο κενό υφίσταται και στον τομέα των αυτοκινούμενων οχημάτων, όπου η υφιστάμενη νομοθεσία δεν επαρκεί να αντιμετωπίσει ζητήματα αστικής και ασφαλιστικής ευθύνης, τα οποία θα προκύψουν στο μέλλον με την εφαρμογή της τεχνολογίας αυτής, όπως για παράδειγμα η απόλυτη αυτονομία της σύναψης σύμβασης από έναν ηλεκτρονικό πράκτορα προς ένα άτομο ή κάποιον άλλο ηλεκτρονικό πράκτορα. Περαιτέρω, το ελληνικό δίκαιο δεν είναι έτοιμο ακόμα να αντιμετωπίσει για την επιδίκαση αποζημίωσης, τα θέματα ηθικής βλάβης που απορρέουν από τη φθορά ενός ρομπότ που φέρει την ιδιότητα του φροντιστή ενός ατόμου. Μία πιθανή μεταβολή στο νομικό καθεστώς των ρομπότ, όπως στην προκειμένη περίπτωση το ρομπότ φροντιστής, με το οποίο το πρόσωπο μπορεί να αναπτύξει στενή συναισθηματική σχέση εξάρτησης, θα μπορούσε να προσφέρει σημαντική πρόοδο στην αντιμετώπιση τέτοιου είδους περιπτώσεων. Εάν η

227 Paresh Kathrani, «Could intelligent machines of the future own the rights to their own creations?», (2017), διαθέσιμο σε https://theconversation.com/could-intelligent-machines-of-the-future-own-therights-to-their-own-creations-86005 .

χρήση των ρομπότ επεκταθεί στον τομέα της υγείας ή της φροντίδας των ηλικιωμένων, το δίκαιο πρέπει να αντιμετωπίσει και ζητήματα κοινωνικής ασφάλισης, σχετικά με την κάλυψη του κόστους τους, κάτι που θα έχει αντίκτυπο και στο εθνικό σύστημα υγείας. Σε κάθε περίπτωση πάντως, το ελληνικό δίκαιο και η νομική θεωρία πρέπει να αναθεωρήσουν ως προς το νομικό καθεστώς των αυτοματοποιημένων συστημάτων και να συμβαδίσουν με τις άλλες ευρωπαϊκές χώρες και τις σημαντικές εξελίξεις που έχουν επιφέρει σε αυτούς τους τομείς.

Μελετώντας περαιτέρω την τεχνολογία της τεχνητής νοημοσύνης, οι θεωρητικοί της νομικής επιστήμης έρχονται αντιμέτωποι με ζητήματα, όπως το θέμα των προκαταλήψεων και των διακρίσεων που προκύπτουν από την εξαγωγή των συμπερασμάτων μέσω αλγορίθμων ή την απόδοση των πνευματικών δικαιωμάτων επί των έργων που προκύπτουν μέσω της τεχνολογίας της τεχνητής νοημοσύνης.

Στα άρθρα 4, παρ. 1 και 2 και 25 του Ελληνικού Συντάγματος γίνεται σαφές, πέρα από την καθιέρωση της ισότητας μεταξύ των Ελλήνων πολιτών, ότι τα ανθρώπινα δικαιώματα που προστατεύονται από το Σύνταγμα αφορούν τόσο τις σχέσεις των πολιτών μεταξύ τους, όσο και με το Κράτος. Νομοθετικές πράξεις προστατεύουν την ισότητα υπό διαφορετικά πρίσματα, όπως ο νόμος 3769/2009 περί της αρχής της ίσης μεταχείρισης ανδρών και γυναικών και της ίσης πρόσβασης σε αγαθά και υπηρεσίες, όπου απαγορεύεται η διάκριση λόγω φύλου κατά την πρόσβαση αυτή. Αν και ο εν λόγω νόμος δεν κάνει αναφορά σε αλγορίθμους, δεδομένου ότι και η αλγοριθμική διάκριση προκαλεί άνιση μεταχείριση λόγω φύλου, και αυτού του είδους η διάκριση είναι απαγορευμένη.

Αναφορικά με τα ζητήματα που προκύπτουν από την τεχνολογία της τεχνητής νοημοσύνης σε σχέση με την πνευματική ιδιοκτησία, η σχετική ελληνική νομοθεσία δεν παρέχει προστασία στα έργα όταν δεν προκύπτει η φυσική ύπαρξη δημιουργού. Συγκεκριμένα, στο άρθρο 1 του νόμου 2121/1993[228] αποδίδονται δικαιώματα στα

228 Πνευματική ιδιοκτησία. 1. Οι πνευματικοί δημιουργοί με τη δημιουργία του έργου, αποκτούν πάνω σ` αυτό Πνευματική ιδιοκτησία, που περιλαμβάνει, ως αποκλειστικά και απόλυτα δικαιώματα, το δικαίωμα

έργα που έχουν δημιουργό και δεν προέρχονται από κάποιο τεχνητό μέσο, όπως ο υπολογιστής. Η θεωρία περί έργων που παρήχθησαν από υπολογιστή δεν έχει τύχει επεξεργασίας από την ακαδημαϊκή κοινότητα, πλην εξαιρέσεων. Κατά τους Μπάλλα και Κωνσταντακόπουλο, «σύμφωνα με το ελληνικό δίκαιο, η τεχνολογία που χρησιμοποιείται για τη δημιουργία ενός έργου θεωρείται ως «εργαλείο» καθοδηγούμενο κι ελεγχόμενο από ανθρώπινο χέρι, για παράδειγμα του δημιουργού του έργου. Μολαταύτα, είναι αμφίβολο το κατά πόσο αυτή η προσέγγιση παρέχει ικανοποιητικά συμπεράσματα, από νομικής και κοινωνικής πλευράς, στην περίπτωση των έργων που έχουν δημιουργηθεί, για παράδειγμα, από αυτόνομα ρομπότ, όπου η ανθρώπινη συνεισφορά είναι ελάχιστη ή ανύπαρκτη. Σε τέτοιες περιπτώσεις, ο νομικός προσδιορισμός του «δημιουργού» είναι σύνθετος και προς συζήτηση»[229]. Επίσης, σε άλλα σχετικά άρθρα, τονίζεται η άποψη ότι σύντομα ο νόμος περί πνευματικής ιδιοκτησίας θα κληθεί να αποδώσει δικαιώματα σε δημιουργούς – μη ανθρώπους[230]. Παρά τους ανωτέρω προβληματισμούς, δεν διαφαίνεται ο Οργανισμός Πνευματικής ιδιοκτησίας (ΟΠΙ[231]) να έχει την πρόθεση να εξερευνήσει το συγκεκριμένο ζήτημα στο άμεσο μέλλον. Εξάλλου, καμία πατέντα δεν μπορεί να κατοχυρωθεί και κανένα δίπλωμα ευρεσιτεχνίας δεν μπορεί να αποδοθεί σε εφεύρεση που έχει προκύψει από υπολογιστή[232]. Επίσης, μόνο ο δημιουργός του σχεδίου μπορεί να απαιτήσει πνευματικά δικαιώματα πάνω στο σχέδιο, σύμφωνα με το ελληνικό

της εκμετάλλευσης του έργου (περιουσιακό δικαίωμα) και το δικαίωμα της προστασίας του προσωπικού τους δεσμού προς αυτό (Ηθικό δικαίωμα).

229 Γεώργιος Μπάλλας και Θεόδωρος Κωνσταντακόπουλος σε Bruno Bonnell και Mady Delvaux-Stehres, «Comparative Handbook: Robotic Technologies law», (2016):133-166.

230 Θεόδωρος Χίου, «Νέα υποκείμενα στην Πνευματική Ιδιοκτησία; Από την «NARUTO» στον «BOT Dylan» και τις δημιουργίες των ρομπότ», (2017), διαθέσιμο σε http://www.iprights.gr/gnomes/198-nea-ypokeimena-stin-pneymatiki-idioktisia-apo-tin-naruto-ston-bot-dylan-kai-tis-dimiourgies-ton-robot. βλ. επίσης Μαρία Κανελλοπούλου - .Μπότη, «Το Δίκαιο της Πληροφορίας», Νομική Βιβλιοθήκη (2004) και Γιώργος Μπουχάγιαρ, «Το μονοπώλιο της ανθρώπινης νοημοσύνης. (Πρωτότυπα έργα αναζητούν δημιουργό)», *ΔiΜΕΕ,* 4/2016, (2016): 533-542.

231 Ο ΟΠΙ είναι νομικό πρόσωπο ιδιωτικού δικαίου που εποπτεύεται από το Υπουργείο Πολιτισμού και Αθλητισμού.

232 Σύμφωνα με το άρθρο 6 παρ. 1 του ν. 1733/1987 1. Δικαίωμα για την απόκτηση διπλώματος ευρεσιτεχνίας έχουν ο εφευρέτης ή ο δικαιούχος σύμφωνα με τις παραγράφους 4, 5 και 6 και οι καθολικοί ή ειδικοί διάδοχοί του. Αυτός που ζητεί τη χορήγηση διπλώματος ευρεσιτεχνίας θεωρείται εφευρέτης, από το οποίο καθίσταται σαφές ότι ο εφευρέτης είναι φυσική ή νομική οντότητα και όχι υπολογιστής.

δίκαιο[233] και κατ' επέκταση, δεν είναι εφικτή ούτε η προστασία του σήματος με δικαιούχο εφαρμογή της τεχνητής νοημοσύνης, καθώς στο ελληνικό δίκαιο κανενός είδους σύστημα τεχνητής νοημοσύνης δεν μπορεί να αποκτήσει οποιασδήποτε μορφής κυριότητα.

Τέλος, ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ[234]) περιέχει, έστω και έμμεσα, δικλείδες ασφαλείας κατά της αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένων και αυτών που στηρίζονται στην ανάλυση του προφίλ (κάτι που θα μπορούσε να αποτελέσει τη βάση για διακρίσεις), οι οποίες έχουν νομικές ή άλλες εξίσου σημαντικές επιδράσεις στα πρόσωπα. Συγκεκριμένα, στο άρθρο 22 του Γενικού Κανονισμού[235], περί αυτοματοποιημένης ατομικής λήψης αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ, ορίζεται ότι: «1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο».

Αναφορικά με τα ρομπότ, στο ελληνικό δίκαιο δεν υπάρχει κάποια ρύθμιση που να προβλέπει την προστασία τους. Σύμφωνα με το ισχύον Αστικό δίκαιο θεωρούνται «πράγματα»[236], δεν μπορούν να αποκτήσουν νομική προσωπικότητα, ούτε μπορούν να είναι υποκείμενα δικαιωμάτων και υποχρεώσεων[237]. Τα ρομπότ επίσης μπορούν να θεωρηθούν «προϊόντα», αποδίδοντας την αντίστοιχη ευθύνη στον κατασκευαστή τους[238]. Σχετικά με την πιθανότητα να είναι αντισυμβαλλόμενο μέρος σε μία

233 Νόμος 2417/1996 Διακανονισμός Χάγης για την κατάθεση βιομηχανικών σχεδίων.

234 Ο εφαρμοστικός του ΓΚΠΔ στην ελληνική επικράτεια νόμος 4624/2019 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις δημοσιεύθηκε στο ΦΕΚ στις 29-08-2019.

235 Το άρθρο αυτό μεταφέρθηκε και στον ελληνικό εφαρμοστικό νόμο ως άρθρο 52.

236 Άρθρο 947 ΑΚ

237 Γι' αυτό απαιτείται κάποιος να είναι φυσικό ή νομικό πρόσωπο. βλ. σχετικά Γενικές Αρχές Αστικού Δικαίου.

238 Βλ. σχετικά άρθρο 6 του ν. 2251/1994 περί Ευθύνης του παραγωγού για ελαττωματικά προϊόντα.

σύμβαση ένα ρομπότ, η νομική θεωρία είναι περιορισμένη και διχασμένη[239] και εν τέλει δεν υπάρχει κάποια σημαντική πρόοδος στις συζητήσεις για την απόδοση ενός συγκεκριμένου νομικού καθεστώτος στα ρομπότ[240]. Επίσης, υπάρχουν ειδικές ρυθμίσεις στο ελληνικό νομικό σύστημα για τα μη επανδρωμένα αεροσκάφη (drones) και τα αυτόνομα οχήματα[241], οι οποίες όμως δεν καλύπτουν την αποζημίωση από αδικοπραξία, αλλά προβλέπουν το σεβασμό στα προσωπικά δεδομένα[242]. Η σχετική γνωμοδότηση (3/2020) της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ακολουθεί τις απόψεις της ομάδας εργασίας του άρθρου 29 του ΓΚΠΔ[243] και πραγματεύεται αποκλειστικά τα ζητήματα της ιδιωτικής ζωής και της προστασίας των δεδομένων, συνιστώντας στο μελλοντικό νομοθέτη να σεβαστεί τις γνωστές Αρχές προστασίας των δεδομένων, μεταξύ άλλων τη νόμιμη επεξεργασία και τον περιορισμό του σκοπού[244]. Η ζημία που θα υποστεί ο τρίτος από ένα μη επανδρωμένο

239 Γεώργιος - Αλέξανδρος Γεωργιάδης, «Η σύναψη συμβάσεως μέσω του Διαδικτύου», Αντ. Ν. Σάκκουλα, Αθήνα- Κομοτηνή, (2003), ο οποίος δεν αναγνωρίζει τη δυνατότητα αυτή. βλ. αντίθετα Σταύρος Κιτσάκης, «Τεχνητή Νοημοσύνη και συμβατική διαδικασία – Εισαγωγή στα βασικά προβλήματα», *Εφαρμογές Αστικού Δικαίου και Πολιτικής Δικονομίας,* 6/2018, (2018): 605.

240 «Τα ρομπότ θα μπορούσαν ενδεχομένως να αναγνωρίζονται υπό την ίδια διπλή συνθήκη (ως εταιρίες, ως ιδιοκτησία και ως νομικά πρόσωπα), ικανοποιώντας και εξισορροπώντας διαφορετικές νομικές ανάγκες [...] Σημειώνεται ότι η κτήση ενός δικαιώματος δεν απαιτεί τη σωματική φυσική ικανότητα προς άσκησή του [...] Εάν δοθεί νομική προσωπικότητα στα ρομπότ, ο χρήστης τους θα μπορούσε να έχει την ιδιότητα του εκπροσώπου, του νομικού συμπαραστάτη, μεταφέροντας τις απαιτήσεις τους ενώπιον της δικαιοσύνης [...] Η συνείδηση και η αυτογνωσία δεν αποτελούν προϋπόθεση εκ των ων ουκ άνευ για την νομική προσωπικότητα». Γεώργιος Μπάλλας και Θεόδωρος Κωνσταντακόπουλος σε Bruno Bonnell και Mady Delvaux-Stehres, «Comparative Handbook: Robotic Technologies law», (2016):133-166.

241 Βλ. σχετικά υπ' αριθμ. Δ/ΥΠΑ/21860/1422/2016 (ΦΕΚ 3152/Β/30-09-2016) Κανονισμός – γενικό πλαίσιο πτήσεων Συστημάτων μη Επανδρωμένων Αεροσκαφών – ΣμηΕΑ (Unmanned Aircraft Systems -UAS) της Υπηρεσίας Πολιτικής Προστασίας και την Ευρωπαϊκή Οδηγία 2010/40/ΕΕ της 7ης Ιουλίου 2010 περί πλαισίου ανάπτυξης των Συστημάτων Ευφυών Μεταφορών στον τομέα των οδικών μεταφορών και των διεπαφών με άλλους τρόπους μεταφοράς, η οποία εισήχθη στο ελληνικό δίκαιο με το ΠΔ 50/2012.

242 Άρθρο 15, Προστασία Προσωπικών δεδομένων: 1. Στην περίπτωση που κατά την εκτέλεση των δραστηριοτήτων (αεροπορικών εργασιών ή άλλων χρήσεων) του(των) ΣμηΕΑ πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα, πρέπει αυτή να είναι σύμφωνη με την ισχύουσα σχετική νομοθεσία. 2. Η ΥΠΑ, εφόσον ενημερωθεί σχετικά, γνωστοποιεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ζητήματα που ανακύπτουν σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα από την χρήση των ΣμηΕΑ. 3. Κυρώσεις επιβάλλονται στους παραβάτες σύμφωνα με τις διατάξεις του Ν. 2472/1997 περί προστασίας δεδομένων προσωπικού χαρακτήρα.

243 Γνωμοδότηση 01/2015 αναφορικά με ζητήματα προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής που σχετίζονται με τη χρήση drones στην Ευρωπαϊκή Ένωση, διαθέσιμο σε https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/06/wp231_en.pdf .

244 Ό.π. υποσημείωση 102 σχετικά με τη Γνωμοδότηση 3/2020 Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, διαθέσιμη σε

αεροσκάφος αποτελεί αντικείμενο ευθύνης του ιδιοκτήτη – χειριστή του αεροσκάφους, σύμφωνα με τις διατάξεις περί αδικοπραξιών του ελληνικού Αστικού Κώδικα (άρθρο 914επ.). Τέλος, σημειώνεται ότι πρέπει να προκύψουν νέες νομοθετικές ρυθμίσεις που θα συμπεριλαμβάνουν και τα νέα επιχειρηματικά μοντέλα, την ευθύνη και τα ζητήματα απορρήτου των δεδομένων[245].

Ένα άλλο θέμα το οποίο πρέπει να ρυθμιστεί σχετικά, είναι το ζήτημα των αυτοκινούμενων οχημάτων. Ο ελληνικός Κώδικας Οδικής Κυκλοφορίας, στο άρθρο 13 παρ. 1, επιβάλλει σε όλα τα οχήματα την ύπαρξη οδηγού[246]. Περαιτέρω, στο άρθρο 48 του ν. 4313/2014 που ρυθμίζει θέματα οδικής κυκλοφορίας, προβλέπεται ότι «Λεωφορείο Αστικού Τύπου επιτρέπεται να κυκλοφορεί επί της οδού χωρίς την παρουσία οδηγού επ' αυτού, κατ' εξαίρεση της παρ. 1 του άρθρου 13 του νόμου 2696/1999 (Α` 57), όπως ισχύει, μόνο για ερευνητικούς σκοπούς στο πλαίσιο πιλοτικής εφαρμογής. Η κυκλοφορία του επιτρέπεται, μετά από απόφαση του οικείου Δημοτικού Συμβουλίου με τη σύμφωνη γνώμη των κατά τόπους αρμοδίων υπηρεσιών Τροχαίας ή των Αστυνομικών Υπηρεσιών που ασκούν καθήκοντα Τροχαίας, για καθορισμένη χρονική περίοδο και συγκεκριμένη αστική διαδρομή, η οποία καθορίζεται μετά από κυκλοφοριακή μελέτη, σύμφωνα με τις διατάξεις του άρθρου 52 του νόμου 2696/1999 (Α` 57), όπως ισχύει». Με την υπ' αριθμ. 50308/7695/2015 υπουργική απόφαση «Όροι και προϋποθέσεις για κυκλοφορία Λεωφορείου Αστικού Τύπου χωρίς Οδηγό» έχουν ρυθμιστεί τα ειδικότερα θέματα[247].

https://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=135,127,231,131,72,198,37,128 . Βλ. επίσης σχετικά Γρηγόρης Τσόλιας, «Διακινδύνευση των δεδομένων προσωπικού χαρακτήρα από τη χρήση μη επανδρωμένων αεροσκαφών», σε Λεωνίδας Κοτσαλής, «Προσωπικά Δεδομένα. Ανάλυση – Σχόλια – Εφαρμογή», Νομική Βιβλιοθήκη, Αθήνα (2016): 353.

245 Γεώργιος Μπάλλας και Θεόδωρος Κωνσταντακόπουλος, ο.π. υποσημ. 150.

246 ΚΟΚ, άρθρο 13, παρ. 1. Κάθε κινούμενο όχημα ή συνδυασμός οχημάτων επιβάλλεται να έχει οδηγό.

247 Άρθρο 48 παρ. 5-7 ν. 4313/2014: 5. Το Λεωφορείο Αστικού Τύπου χωρίς οδηγό επιβάλλεται να διαθέτει κατάλληλους μηχανισμούς και αυτόματα συστήματα, τα οποία εξασφαλίζουν συμπεριφορά κίνησης, πέδησης και ακινητοποίησης, αντίστοιχη με όχημα, το οποίο χειρίζεται οδηγός. 6. Για τη διασφάλιση της απρόσκοπτης κίνησης του Λεωφορείου Αστικού Τύπου χωρίς οδηγό, την ασφάλεια των επιβατών και των λοιπών χρηστών της οδού επιβάλλεται η παρακολούθηση του Λεωφορείου και της οδού στην οποία κινείται, καθ' όλη τη διάρκεια κίνησής του, από Κέντρο Ελέγχου μέσω ηλεκτρονικών συσκευών λήψης και καταγραφής εικόνας (κάμερες). Οι παραπάνω συσκευές τοποθετούνται επί του οχήματος και σε προκαθορισμένα σημεία της διαδρομής, προκειμένου να υπάρχει πλήρης έλεγχος της κίνησης του

Στην πόλη των Τρικάλων έχει τεθεί ήδη σε κυκλοφορία από το έτος 2016 αστικό λεωφορείο χωρίς οδηγό, υπό τις προϋποθέσεις και τους όρους του πιλοτικού προγράμματος CityMobil2[248].

Λεωφορείου και της λοιπής κυκλοφορίας της οδού, ώστε να παρέχεται η δυνατότητα ακινητοποίησής του από το Κέντρο Ελέγχου σε περίπτωση που το επιβάλλουν οι συνθήκες κυκλοφορίας ή λόγοι έκτακτης ανάγκης. 7. Ο υπεύθυνος για την παρακολούθηση της κίνησης του Λεωφορείου στο Κέντρο Ελέγχου, οφείλει να είναι κάτοχος αντίστοιχης ισχύουσας κατηγορίας άδειας οδήγησης και ευθύνεται κατά τις διατάξεις του ν. 2696/1999 (Α` 57), όπως ισχύει, ως οδηγός του οχήματος, για την ακινητοποίησή του, σε περίπτωση που το επιβάλλουν οι συνθήκες κυκλοφορίας ή λόγοι έκτακτης ανάγκης.

248 Αλεξάνδρα Κασσίμη, «Στα Τρίκαλα η πιο επιτυχημένη στον κόσμο πιλοτική χρήση λεωφορείων χωρίς οδηγό», (2016), διαθέσιμο σε https://www.kathimerini.gr/society/853069/sta-trikala-i-pio-epitychimeni-ston-kosmo-pilotiki-chrisi-leoforeion-choris-odigo .

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη διάρκεια της προηγούμενης δεκαετίας αναπτύχθηκαν παράλληλα οι έννοιες της ιδιωτικότητας και της αυτονομίας, έννοιες διακριτές μεταξύ τους, οι οποίες στηρίζονται μεν σε διαφορετικό κανονιστικό πλαίσιο, αλλά αποδίδουν και οι δύο την αξία τους στην ψηφιακή εποχή. Κατά τη διάρκεια αυτής της ανάπτυξης, έγινε αισθητό ότι οι νέες τεχνολογίες συχνά υπονομεύουν την ανθρώπινη αυτονομία, ενώ το δικαίωμα στην ιδιωτικότητα απαιτεί την προστασία των σχέσεων με τα άλλα πρόσωπα και τους οργανισμούς. Καθώς τα τεχνολογικά επιτεύγματα συρρικνώνουν τον κόσμο κι εκμηδενίζουν τις αποστάσεις, τίθεται υπό αμφισβήτηση η αξιοπιστία των εθνών ως προς τη μεταξύ τους συνεργασία, όσον αφορά στην αντιμετώπιση των διαδικτυακών παραβάσεων και των εμπορικών ζητημάτων που προκύπτουν. Ερευνάται εάν η ανάγκη διάδρασης των διεθνών νομικών συστημάτων και των κυβερνήσεων θα μεταβάλει τις αντιλήψεις σε σχέση με το ρόλο ενός έθνους – κράτους. Χρησιμοποιώντας τα λόγια του Μπαράκ Ομπάμα ότι «μπορούμε να θεωρούμε τους εαυτούς μας πολίτες του κόσμου»[1], η σύγχρονη κοινωνία διερωτάται εάν αυτή η οπτική θα έδινε έμφαση στην παγκόσμια αλλαγή και θα αποκέντρωνε τις δυνάμεις και τους ρόλους των εθνικών κυβερνήσεων, αλλά και πώς θα μπορούσαν να εξελιχθούν οι κυβερνητικοί θεσμοί μπροστά στην ανάγκη αντιμετώπισης των παγκοσμίων ζητημάτων που προκύπτουν σχεδόν καθολικά με αφορμή τις επαναστατικές τεχνολογίες. Νομοθέτες και νομικοί πρέπει να ορίσουν τη διαχωριστική γραμμή ανάμεσα στους νόμους που απαιτούνται για τη διαφύλαξη της εθνικής ασφάλειας, χωρίς να προκαλούν υπέρμετρους περιορισμούς στους πολίτες και αυτούς που είναι απαραίτητοι για την ανάπτυξη της εκάστοτε κυβερνητικής πολιτικής, όπως για παράδειγμα την προαγωγή της οικονομίας με τη φορολόγηση των προϊόντων που πωλούνται στο διαδίκτυο και το ρυθμιστικό ρόλο του νομίσματος, ως παράγοντα στις εξισώσεις αυτές. Μετά τη γένεση του σύγχρονου

1 «Obama's Speech in Berlin», (2008), διαθέσιμο σε https://www.nytimes.com/2008/07/24/us/politics/24text-obama.html?pagewanted=all&_r=0 .

έθνους – κράτους με τη Συνθήκη της Βεστφαλίας, προέκυψε σταδιακά το ερώτημα εάν θα μπορούσε η αναμόρφωση του κόσμου, μέσω της τεχνολογικής αλληλεξάρτησης, να σηματοδοτήσει μια αλλαγή στη σύγχρονη γεωπολιτική δυναμική που μειώνει τον ρόλο των εθνών – κρατών, αλλά κι εάν θα μπορούσαν οι εκτεταμένες τεχνολογικές εξελίξεις να οδηγήσουν σε μια σύγχρονη εκδοχή του Πύργου της Βαβέλ, καθώς άνθρωποι από όλο τον κόσμο έχουν τη δυνατότητα να ενωθούν μέσω μίας πλατφόρμας που στηρίζεται σε ευρείες υποδομές, μόνο για να προκαλέσουν καταστροφή λόγω της απουσίας ενωμένου μετώπου. Αυτός ο κίνδυνος δείχνει πλέον να απομακρύνεται, έπειτα και από την υπογραφή συνθήκης μεταξύ των Ευρωπαϊκών χωρών για συνεργασία κατά των σφαλμάτων ασφαλείας και της κυβερνοτρομοκρατίας[2].

Είναι αναμφίβολο ότι καινοτομίες, όπως για παράδειγμα η τρισδιάστατη εκτύπωση, θα μεταβάλουν τη μορφή του κόσμου όπως είναι σήμερα γνωστή[3]. Όταν ο πρώτος Πρόεδρος της Λαϊκής Δημοκρατίας της Κίνας, Zhou Enlai, ερωτήθηκε για τις επιπτώσεις της Γαλλικής Επανάστασης, περίπου δύο αιώνες πριν, απάντησε ότι ήταν «πολύ νωρίς για να πει κάποιος»[4]. Με τον ίδιο τρόπο μπορούν οι άνθρωποι μόνο να αρχίσουν να φαντάζονται τις νομικές επιπτώσεις ενός τεχνολογικά εξελισσόμενου κόσμου. Οι τεχνολογικές καινοτομίες αποτελούν εργαλεία και μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, ακόμα και αντιφατικούς μεταξύ τους, ανάλογα με τον τρόπο αξιοποίησής τους. Είναι πολύ απλοϊκό να αναρωτηθεί κάποιος κατά πόσο τέτοιου είδους καινοτομίες είναι ή πρόκειται να είναι ευεργετικές ή επιζήμιες για την κοινωνία. Περισσότερο πρέπει να θεωρηθούν ως αρωγοί αλλαγής και να διοχετεύονται για την καλύτερη προστασία της κοινωνίας. Αποτελεί καθήκον για τους δικαστές και τους νομικούς να διαμορφώσουν το νομικό σύστημα σε τέτοιο

2 Βλ. σχετικά Internet Governance Forum.

3 Neal K. Katyal, «Disruptive Technologies and the Law», *Georgetown Law Faculty Publications and Other Works* (2014):1878.

4 «Dean Nichols: Zhou Enlai's Famous Saying Debunked», (2011), διαθέσιμο σε https://historynewsnetwork.org/article/140010 .

επίπεδο, ώστε να είναι σε θέση να ανταποκριθεί στις προκλήσεις των εξελίξεων γύρω από το τεχνολογικό φάσμα.

Οι νέες τεχνολογίες διαφαίνεται ότι θα γίνουν αναπόσπαστα τμήματα της σύγχρονης ζωής, καθώς εξυπηρετούν σημαντικές κοινωνικές ανάγκες, όπως για παράδειγμα η τρισδιάστατη εκτύπωση καλύπτει την ανάγκη των ατόμων για καινοτομία. Παράλληλα, όμως, δεν πρέπει να παραβλεφθούν οι πιθανές βλάβες που μπορούν να επιφέρουν, όπως η εισβολή στην ιδιωτικότητα, η παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας και τα ζητήματα ευθύνης. Το δίκαιο πρέπει να καλύψει το κενό, κάτι που αποτελεί σε κάθε περίπτωση στόχος του, αλλά και να αναπτύξει παράλληλα τις ανθρώπινες αξίες, σε μία εποχή όπου η τεχνολογία προκαλεί βαθιά έκπληξη και αναστάτωση[5].

Σε Ευρωπαϊκό επίπεδο, η νομοθεσία που αφορά στις νέες τεχνολογίες διαρκώς εξελίσσεται. Μέσα σε ένα πολυετές ευρωπαϊκό δημοσιονομικό πλαίσιο (Multiannual Financial Framework), το πρόγραμμα Ψηφιακή Ευρώπη εστιάζει στο σχεδιασμό στρατηγικών ψηφιακών ευκαιριών και τη διάδοση των ψηφιακών τεχνολογιών στους πολίτες και τις επιχειρήσεις, με στόχο την ψηφιακή αναμόρφωση της ευρωπαϊκής κοινωνίας και οικονομίας[6]. Το πρόγραμμα αυτό περιλαμβάνει την προώθηση επενδύσεων που αφορούν στους υπερ – υπολογιστές, την τεχνητή νοημοσύνη, την κυβερνοασφάλεια, τις προηγμένες ψηφιακές δεξιότητες και τη διασφάλιση της ευρείας χρήσης των ψηφιακών τεχνολογιών στην οικονομία και την κοινωνία.

Διαδίκτυο των πραγμάτων

Το διαδίκτυο των πραγμάτων και οι «έξυπνες» συσκευές θέτουν, μεταξύ άλλων, το ακανθώδες ζήτημα της κυριότητας των δεδομένων που παράγονται από αυτές. Στην

5 Deborah Beth Medows, «3D Printing, Net Neutrality, and the Internet: Symposium Introduction», (2015), διαθέσιμο σε https://jolt.law.harvard.edu/digest/legal-issues-in-computer-and-internet-law-and-the-quagmire-of-appropriate-legal-frameworks-in-the-modern-era .

6 Βλ. σχετικά «Digital Europe for a more competitive, autonomous and sustainable Europe – Brochure», (2021), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/digital-europe-more-competitive-autonomous-and-sustainable-europe-brochure .

περίπτωση, για παράδειγμα, των δεδομένων που παράγονται από ένα «έξυπνο» αυτοκίνητο[7], κατά την ισχύουσα θεωρία, τα δεδομένα αυτά ανήκουν στην εταιρία που παρήγαγε το αυτοκίνητο. Παρόλο που ο καταναλωτής έχει την κυριότητα του αυτοκινήτου, τα δεδομένα που συγκεντρώνονται μέσω του οχήματος, δεν του αποδίδονται απευθείας, σε αντίθεση με τα δικαιώματα στην πρόσβαση, στη χρήση και την καταστροφή των δεδομένων. Στον κατασκευαστή της «έξυπνης» συσκευής συνήθως ανήκουν τα δικαιώματα από το λογισμικό, το οποίο αναπτύσσει τα δεδομένα και οι διατάξεις του δικαίου πνευματικής ιδιοκτησίας προστατεύουν το λογισμικό από μη εξουσιοδοτημένες χρήσεις. Ακόμα και στην περίπτωση που οι καταναλωτές θα είχαν τη δυνατότητα, μέσω μίας κανονιστικής εξαίρεσης, να παρακάμψουν το ιδιοκτησιακό καθεστώς του λογισμικού και την πρόσβαση στα δεδομένα, δεν θα αποκτούσαν το περιουσιακό δικαίωμα της εκμετάλλευσης των δεδομένων μέσω της εξαίρεσης αυτής. Κατά την ισχύουσα νομική θεωρία, δεν υπάρχουν ειδικές ρυθμίσεις για τη βιομηχανία που να καλύπτουν την κυριότητα των δεδομένων που προέρχονται από τις «έξυπνες» συσκευές, με αποτέλεσμα οι πολιτικές απορρήτου και οι όροι χρήσης να καθίστανται προς όφελος της κατασκευάστριας εταιρίας, η οποία διατηρεί την αποκλειστικότητα στην πρόσβαση και τη χρήση των δεδομένων των συσκευών. Κατ' αυτόν τον τρόπο, όλα τα συλλεγέντα δεδομένα που αφορούν στον καταναλωτή και την τοποθεσία του ανήκουν ουσιαστικά στην εταιρία που παρήγαγε τη συσκευή, κάτι που από την πλευρά του δικαίου, πρέπει να αλλάξει στο προσεχές μέλλον. Τα σοβαρά ζητήματα που προέκυψαν κατά καιρούς από τη χρήση δεδομένων[8] τείνουν να

7 «Το έτος 2022 πρόκειται να βγουν στους δρόμους τα πρώτα αυτόνομα ΙΧ, που θα μπορούν να κάνουν μόνα τους κάποιες επιλεγμένες διαδρομές, χωρίς την ανάγκη οδηγού. Το 2030 δε, οι γνωστές αυτοκινητοβιομηχανίες φιλοδοξούν να έχουν έτοιμα τα πλήρως αυτόνομα, ηλεκτρικά αυτοκίνητα, που θα διαθέτουν όλη την απαραίτητη τεχνολογία (ραντάρ, αισθητήρες κλπ) όχι μόνο για να οδηγούν μόνα τους, αλλά και για να αντιλαμβάνονται και να αντιδρούν ανάλογα, σε κάθε έκτακτο περιστατικό». Βλ. σχετικά «Έξυπνα» αυτοκίνητα στους δρόμους μέχρι το 2030», (2017), διαθέσιμο σε https://energypress.gr/news/exypna-aytokinita-stoys-dromoys-mehri-2030 .

8 Όπως αυτό της εταιρίας Cambridge Analytica, η οποία έχοντας ως αντικείμενο την ανάλυση εκλογικών δεδομένων, προσελήφθη από τον Πρόεδρο Trump κατά τη διάρκεια της προεκλογικής του εκστρατείας το 2016 και απέκτησε πρόσβαση σε πληροφορίες πενήντα περίπου εκατομμυρίων χρηστών του Facebook, με στόχο την ανάλυση της προσωπικότητας των Αμερικανών ψηφοφόρων και την επιρροή

ευαισθητοποιήσουν το κοινό και τους νομικούς, σχετικά με το πώς τυγχάνουν εκμετάλλευσης τα δεδομένα των καταναλωτών και ποιος έχει οικονομικά οφέλη από την εκμετάλλευση αυτή. Από την άλλη πλευρά, καθώς η τεχνολογία εμβαθύνει στην καθημερινή ζωή, οι καταναλωτές πρέπει να συνηθίσουν στην ιδέα της διαρκούς συγκέντρωσης δεδομένων που αφορούν στις πράξεις τους ή να πάψουν να ενοχλούνται από αυτή[9]. Οι ανησυχίες για την προστασία των δεδομένων τείνουν να διαμορφώσουν το νομικό τοπίο, αλλά αυτό δεν πρέπει να επισκιάσει τη σημασία της κυριότητας των δεδομένων. Στην περίπτωση που οι βιομηχανίες συνεχίσουν να έχουν την αποκλειστική πρόσβαση στα ευαίσθητα δεδομένα των «έξυπνων» συσκευών, οι καταναλωτές, οι κυβερνητικοί φορείς και οι επιχειρήσεις που επιθυμούν να τα χρησιμοποιήσουν, πρέπει να διαπραγματευθούν με αυτές. Είναι σημαντικό να γίνει αντιληπτό ότι η δημιουργία δεδομένων από τις «έξυπνες» συσκευές θα αυξήσει την «οικονομική πίτα». Όποιος θα κατέχει τα δεδομένα αυτά, αυτός και θα απολαύσει το πρώτο και μεγαλύτερο κομμάτι αυτής της πίτας[10].

Σε ευρωπαϊκό επίπεδο και μέσω του προγράμματος Horizon 2020[11] σχετικά με τις νέες τεχνολογίες, στον τομέα του Διαδικτύου των πραγμάτων τίθεται ο στόχος της ενίσχυσης των ευρωπαϊκών βιομηχανιών. Υπό το πρίσμα του τομέα της

στην εκλογική συμπεριφορά τους. Βλ. σχετικά Kevin Granville, «Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens», (2018), διαθέσιμο σε https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html .

9 Σε έρευνα που πραγματοποιήθηκε παρατηρήθηκε ότι το 46% των ατόμων δεν θα αφιέρωνε ούτε πέντε λεπτά από το χρόνο του για να εξαιρεθεί της αναγνώρισης από τους αισθητήρες των αυτόνομων αυτοκινήτων σε δημόσιους χώρους. Βλ. σχετικά Cara Bloom, Joshua Tan, Javed Ramjohn και Lujo Bauer, «Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles», Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017) (2017): 357-375, διαθέσιμο σε https://www.usenix.org/system/files/conference/soups2017/soups2017-bloom.pdf . Βλ. επίσης John Fleming και Amy Adkins, «Data Security: Not a Big Concern for Millennials», (2016), διαθέσιμο σε https://news.gallup.com/businessjournal/192401/data-security-not-big-concernmillennials.aspx .

10 Sylvia Zhang, «Who owns the data generated by your smart car?», *Harvard Journal of Law & Technology,* Vol. 32/ 1, (2018): 299-320.

11 Βλ. σχετικά έργα AdMiRe 952027, ATLANTIS 951900, BRIDGES 952043, eTryOn 951908, HoviTron 951989, xR4DRAMA 952133, PrismArch 952002 και SOCRATES 951930. «Fostering the European Interactive Technologies ecosystem –new H2020 projects on Augmented Reality / Virtual Reality», (2020), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/fostering-european-interactive-technologies-ecosystem-new-h2020-projects-augmented .

Ψηφιοποίησης της Ευρωπαϊκής Βιομηχανίας, ενισχύεται η ανάπτυξη των τομέων που αφορούν στις «έξυπνες πόλεις», τον «έξυπνο» αγροτικό τομέα, τις κατοικίες και την ενέργεια, τον τομέα της υγείας και των αυτόνομων οχημάτων στην Ευρώπη. Παράλληλα, τονίζεται η ανάγκη διασφάλισης του ανοικτού διαμοιρασμού και της ανοιχτής διαλειτουργικότητας των δεδομένων μέσω της τεχνολογίας του Διαδικτύου των Πραγμάτων, της ασφάλειας και ιδιωτικότητας «στο σχεδιασμό» (by design) και της τροφοδότησης μοντέλων ανοιχτής πλατφόρμας. Οι λύσεις που προκρίνονται οδηγούν σε ένα «διαλειτουργικό, ευέλικτο, έμπιστο, προσβάσιμο και εύχρηστο» Διαδίκτυο των πραγμάτων[12].

Παράλληλα, στο Γενικό Κανονισμό Προστασίας Δεδομένων (και κατ' επέκταση το νόμο 4624/2019 με τον οποίο ο Κανονισμός ενσωματώθηκε στην ελληνική πραγματικότητα), ως προς το Διαδίκτυο των πραγμάτων γίνεται αναφορά μόνο στη διασφάλιση της φορητότητας των δεδομένων και τη συγκατάθεση. Όπως αναφέρθηκε και στο σχετικό κεφάλαιο, σύμφωνα με τον ENISA, οι σχετικές ρυθμίσεις δεν είχαν υπόψη τους το Διαδίκτυο των πραγμάτων, καθώς «δεν υπήρξαν νομικές κατευθυντήριες γραμμές για τις συσκευές του Διαδικτύου των πραγμάτων και των υπηρεσιών εμπιστοσύνης (service trust), αλλά ούτε ένα «επίπεδο μηδέν» προσδιορισμένο για την ασφάλεια και την ιδιωτικότητα των διασυνδεδεμένων και «έξυπνων» συσκευών».

Κρυπτονομίσματα

Στον τομέα των ψηφιακών νομισμάτων η Ευρωπαϊκή Επιτροπή έχει προτείνει ένα πιλοτικό νομικό καθεστώς για τις αγορές που συναλλάσσονται σε κρυπτονομίσματα[13]. Το καθεστώς αυτό θα επιτρέπει παρεκκλίσεις από τους

12 Βλ. σχετικά «Internet of Things - brochure», (2019), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/internet-things-brochure .

13 Βλ. σχετικά Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις αγορές κρυπτοστοιχείων και για την τροποποίηση της οδηγίας (ΕΕ) 2019/1937.

υπάρχοντες κανόνες και θα δώσει τη δυνατότητα στο νομοθέτη να παρατηρήσει στην πράξη τη χρήση της τεχνολογίας του διαμοιρασμένου καθολικού. Στόχος της Επιτροπής είναι να δημιουργηθεί ένα πλαίσιο ασφάλειας δικαίου ως προς τη νομοθετική αντιμετώπιση όλων των κρυπτονομισμάτων, είτε υπάγονται στις υπάρχουσες νομοθεσίες είτε είναι προς το παρόν αρρύθμιστα. Περαιτέρω, τον Ιανουάριο του 2021, η Ευρωπαϊκή Επιτροπή προχώρησε σε κοινή ανακοίνωση με την Ευρωπαϊκή Κεντρική Τράπεζα σχετικά με τη συνεργασία τους ως προς την παρουσίαση του ψηφιακού ευρώ[14]. Παράλληλα, όπως έχει ήδη αναφερθεί στην παρούσα, πέρα από την Τράπεζα της Ελλάδος που το έτος 2018 παρέπεμψε για τη χρήση των κρυπτονομισμάτων στην Ελλάδα στη σχετική κοινή ανακοίνωση της Ευρωπαϊκής Αρχής Τραπεζών (EBA), της Ευρωπαϊκής Αρχής Ασφαλίσεων και Επαγγελματικών Συντάξεων (EIOPA) και της Ευρωπαϊκής Αρχής Κινητών Αξιών και Αγορών (ESMA), η Ανεξάρτητη Αρχή Δημοσίων Εσόδων με το επιχειρησιακό της σχέδιο, το 2019, πρότεινε τη θεσμοθέτηση της φορολόγησης των κρυπτονομισμάτων και ως «επένδυση χαρτοφυλακίου», με φόρο 15%.

Εικονική κι επαυξημένη πραγματικότητα.

Είναι κοινός τόπος πλέον ότι οι εφαρμογές της τεχνολογίας της εικονικής πραγματικότητας αποκτούν δημοφιλία και για το λόγο αυτό οι δημιουργοί τους δεν πρέπει να παραβλέπουν τα πολυάριθμα νομικά ζητήματα που τίθενται, όπως η προστασία της πνευματικής ιδιοκτησίας στην εικονική πραγματικότητα ή η υπεύθυνη διαχείριση των μεγάλων ποσοτήτων δεδομένων των χρηστών, τα οποία συγκεντρώνουν οι συσκευές. Δεδομένου ότι η τεχνολογία αυτή είναι η πιο σημαντική δύναμη στον τομέα των παιχνιδιών, το δίκαιο πνευματικής ιδιοκτησίας δείχνει να

14 Λαμβάνοντας υπόψη τους τις ταχείες εξελίξεις στο πεδίο των μεθόδων πληρωμών και την διάδοση των κρυπτονομισμάτων, οι δύο φορείς εξετάζουν την πιθανότητα δημιουργίας ενός ψηφιακού νομίσματος - ευρώ, συμπληρωματικά προς τις πληρωμές στον ιδιωτικό τομέα. Βλ. σχετικά «Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro», (2021), διαθέσιμο σε https://ec.europa.eu/info/files/210119-ec-ecb-joint-statement-digital-euro_en .

αποτελεί τη βάση της αντιμετώπισης της εικονικής πραγματικότητας στο άμεσο μέλλον. Μολαταύτα, η τεχνολογία αυτή χρησιμοποιείται και σε άλλους τομείς, πέραν αυτού των παιχνιδιών και κατά συνέπεια, με την πάροδο του χρόνου, η χρήση του τομέα αυτού του δικαίου τείνει να περιορίζεται. Ως προς την ευθύνη από βλάβες που προκύπτουν από συσκευές ή εφαρμογές που σχετίζονται με την τεχνολογία της εικονικής πραγματικότητας, όπως οι σωματικές βλάβες και η παραβίαση του απορρήτου, οι ισχύουσες νομικές κατευθύνσεις είναι επίσης πολύ περιορισμένες. Προς το παρόν, η πιο αποτελεσματική στρατηγική για την προστασία και την υποστήριξη των χρηστών της εικονικής πραγματικότητας είναι να προσαρμοστούν οι επικρατούσες νομοθετικές ρυθμίσεις στη νέα πραγματικότητα, καθώς, όσο ταχεία υπήρξε η ανάπτυξη της τεχνολογίας αυτής, σε ακόμα λιγότερο χρόνο απ' ό,τι μπορεί κάποιος να φανταστεί, θα υπάρξουν νέες μορφές δικαίου που θα εστιάζουν σε αυτή[15].

Στον αντίποδα της εικονικής πραγματικότητας, όπου η θεωρία ισχυρίζεται ότι κυβερνάται από διαφορετικούς κανόνες και διατάξεις απ΄ ό,τι ο πραγματικός κόσμος, η επαυξημένη πραγματικότητα δεν περιλαμβάνει τέτοιου είδους διαχωρισμούς. Για παράδειγμα, το δίκαιο πνευματικής ιδιοκτησίας και οι συμβάσεις ηλεκτρονικού εμπορίου πρέπει να εφαρμοστούν στο λογισμικό των συσκευών, αν και το πρόβλημα προκύπτει όταν αυτοί οι τομείς του δικαίου αρχίζουν να ρυθμίζουν τον πραγματικό κόσμο. Το εμπράγματο δίκαιο και οι διατάξεις περί αδικοπραξιών θα συνεχίσουν να έχουν σημαντικό ρόλο στον πραγματικό κόσμο και στην καθημερινή ζωή των ατόμων. Χωρίς μία ανεπτυγμένη θεωρία για την επαυξημένη πραγματικότητα, το δίκαιο της πνευματικής ιδιοκτησίας και οι συμβάσεις ηλεκτρονικού εμπορίου θα υπερκεράσουν το εμπράγματο δίκαιο και τις διατάξεις περί αδικοπραξιών. Και τότε πρέπει να αντιμετωπίσουμε τον κίνδυνο το δίκαιο πνευματικής ιδιοκτησίας που ρυθμίζει τις διαδικτυακές αλληλεπιδράσεις, να ρυθμίζει επίσης και τις ενέργειες των χρηστών της επαυξημένης πραγματικότητας στον πραγματικό κόσμο. Οι νόμοι που

15 Crystal Nwaneri, «Ready lawyer one: legal issues in the innovation of Virtual Reality», *Harvard Journal of Law & Technology,* Vol. 30/ 2 (2017): 601-627.

ρυθμίζουν τα άυλα περιουσιακά στοιχεία δεν έχουν σχεδιαστεί να εφαρμόζονται και στον πραγματικό κόσμο και εάν αυτό συμβεί, τα αποτελέσματα θα είναι περίπλοκα και θα προξενούν σύγχυση.

Η σύνδεση των ανθρώπων με τα δεδομένα, η νέα δυνατότητα που οι άνθρωποι γεύονται το περιβάλλον τους μέσω των «έξυπνων» τηλεφώνων και άλλων παρόμοιων συσκευών, εγείρουν ενστάσεις σχετιζόμενες με την προστασία της φήμης (law of reputation[16]). Είναι πλέον πολύ πιο εύκολο για κάποιον να δημοσιεύσει πληροφορίες, χωρίς να ελέγξει την ορθότητά τους και ακόμη χειρότερα, οι πληροφορίες αυτές είναι προσβάσιμες σε οποιονδήποτε έχει κάποια συσκευή νέας τεχνολογίας. Δεν θα εξεταστούν οι προθέσεις αυτού που δημοσιεύει, εάν δηλαδή ο στόχος του ήταν να πλήξει τη φήμη του άλλου προσώπου. Και από τη στιγμή που το διαδίκτυο έχει καταστεί το κύριο μέσο συλλογής πληροφοριών (προσωπικών, οικογενειακών ή επαγγελματικών) για άλλους ανθρώπους, ο κίνδυνος να διαπράξει κάποιος οποιαδήποτε αδικοπραξία έχει μεγεθυνθεί[17].

Σχετικά με το εμπράγματο δίκαιο, οι τεχνολογίες της επαυξημένης πραγματικότητας αναπτύσσουν νέου είδους διαφορές, όπως αυτές που σχετίζονται με τα «υψηλού επιπέδου» ονόματα χώρου (top-level domain names[18]), με τα προβλήματα του κυβερνοσφετερισμού[19] (cybersqautting), με το twitterjacking[20] ή με τους κόσμους –

16 Η απειλή που προκύπτει από τις νέες μεθόδους επικοινωνίας αφορά στην πιθανή βλάβη στη φήμη των ατόμων, των εταιριών ή των σημάτων και είναι ταχεία και παγκόσμια. Βλ. σχετικά «Reputation law: an international approach to protecting brands», (2010), διαθέσιμο σε https://www.inhouselawyer.co.uk/legal-briefing/reputation-law-an-international-approach-to-protecting-brands/ .

17 Joshua A.T. Fairfield, «Mixed Reality: How the Laws of virtual worlds govern everyday life», *Berkeley Technology Law Journal*, Vol. 27 (2012):55.

18 Ένα υψηλού επιπέδου όνομα χώρου είναι η κατάληξη του ονόματος χώρου. Για παράδειγμα, για τα ελληνικά ονόματα χώρου είναι η κατάληξη .gr, για τα Νορβηγικά η κατάληξη .no, για τα Σουηδικά .se κοκ. Πέρα από τον κωδικό της χώρας, υπάρχουν και γενικά ονόματα – καταλήξεις, όπως τα .com, .org και .google. Σε γενικές γραμμές, η κατάληξη μπορεί να είναι .ο,τιδήποτε. Βλ. σχετικά Ιωάννης Ιγγλεζάκης, «Οδηγός σχετικά με τα Ονόματα Χώρου (Domain Names)», Θεσσαλονίκη, (2016).

19 Πρόκειται για την «κακόπιστη καταχώρηση ως domain name ή/ και η χρήση ενός τέτοιου, το οποίο αποτελεί εμπορικό σήμα, σήμα φήμης ή διακριτικό γνώρισμα εμπορικής επιχείρησης τρίτου (διακριτικό τίτλο, επωνυμία επιχείρησης, έτερο domain name κλπ.), προς το σκοπό του προσπορισμού παράνομου οφέλους». Βλ. σχετικά Νικόλαος Α. Ιωάννου, «Κυβερνοσφετερισμός (cybersquatting): Σύγκρουση σήματος και domain name», (2020), διαθέσιμο σε https://ilf.gr/

20 Πρόκειται για την ενέργεια του να αποστέλλει κάποιος μηνύματα μέσω Twitter, χρησιμοποιώντας το όνομα κάποιου άλλου, συνήθως δημοφιλούς προσώπου. Βλ. σχετικά

καθρέφτες (mirror worlds[21]). Σε αυτούς τους τομείς εφαρμόζεται κατά κύριο λόγο το δίκαιο πνευματικής ιδιοκτησίας. Εάν, για παράδειγμα, κάποιος αποφασίσει να προβάλει μία προσβλητική λέξη επάνω σε ένα σπίτι, η οποία θα είναι ορατή μόνο μέσω μία κατάλληλης συσκευής, όπως είναι τα γυαλιά της Google, το ερώτημα που προκύπτει είναι εάν πρέπει και αυτή η παράβαση να αντιμετωπιστεί με τις διατάξεις του δικαίου πνευματικής ιδιοκτησίας. Η απάντηση είναι αρνητική, καθώς ειδικά για τέτοιου είδους παραβάσεις, πρέπει να εφαρμοστούν οι διατάξεις του ουσιαστικού δικαίου, δεδομένου ότι πρόκειται για προσβολή της προσωπικότητας ή της ιδιοκτησίας και όχι για περίπτωση ψηφιακής «γης», όπως στον κυβερνοσφετερισμό[22]. Παρόλο που ο νόμος εμφανίζεται να παρέχει περισσότερα δικαιώματα στους κατόχους πνευματικών δικαιωμάτων σε σχέση με άλλα δικαιώματα, όπως η προσωπικότητα ή η πραγματική ιδιοκτησία, η μείωση της εφαρμογής των διατάξεων του δικαίου πνευματικής ιδιοκτησίας και η αύξηση της εφαρμογής των παραδοσιακών αρχών του συμβατικού δικαίου τείνουν να αποκαταστήσουν την ισορροπία.

Αναφορικά με τα ζητήματα παραβίασης της ιδιωτικότητας εντός των εφαρμογών της εικονικής και της επαυξημένης πραγματικότητας, η λύση είναι η απλή, αλλά θεμελιώδης εξισορρόπηση του συμβατικού δικαίου κατά τη διαδικτυακή εφαρμογή του, δεδομένου ότι όπως εφαρμόζεται το συμβατικό δίκαιο σήμερα στο διαδίκτυο, έχει αφαιρέσει από τους καταναλωτές τη δυνατότητα να συντάσσουν συμβάσεις. Οι

https://www.ldoceonline.com/dictionary/twitterjacking .

21 Πρόκειται για ένα σύστημα υπολογιστή που επιτρέπει στους χρήστες του να δουν, να μελετήσουν, να διερευνήσουν και να αντιληφθούν κάποιο ουσιαστικό σκηνικό στον πραγματικό κόσμο, όπως ένα σχολείο, ένα νοσοκομείο, μία πόλη ή ολόκληρο τον κόσμο. Οι χρήστες μπορούν να μετακινούνται στους καθρέφτες: γεωγραφικά, από δωμάτιο σε δωμάτιο ή από δρόμο σε δρόμο, τοπικά, από την προβολή της ακαδημαϊκής δομής έως την προβολή της οικονομικής δομής, μέσω επιπέδων αφαίρεσης, από επισκόπηση υψηλού επιπέδου έως λεπτομέρεια χαμηλού επιπέδου ή χρονικά, στην κατάσταση της ρύθμισης πριν από μια εβδομάδα ή ένα χρόνο. Σε κάθε σημείο, ο κόσμος του καθρέφτη παρέχει τις πληροφορίες του σε μια εικόνα, λεπτομερή αλλά εύκολα κατανοητή. Βλ. σχετικά David Gelernter, «Mirror Worlds: or The Day Software Puts the Universe in a Shoebox... How It Will Happen and What It Will Mean», Oxford University Press, Νέα Υόρκη (1991): 237.

22 Το σπίτι βρίσκεται στον πραγματικό κόσμο, εμπλέκονται πραγματικοί άνθρωποι και όχι ψηφιακές απεικονίσεις τους (avatars) και το γεγονός ότι ο ιδιοκτήτης τους σπιτιού δεν μπορεί να δει την προσβολή, παρά μόνο μέσω ειδικής συσκευής, δεν σημαίνει ότι η προσβολή αυτή δεν υφίσταται. Joshua A.T. Fairfield, ό.π. υποσημείωση 6.

συμβάσεις συντάσσονται από τις εταιρίες και περιλαμβάνουν νομικούς όρους σε τέτοιο όγκο πληροφοριών, τους οποίους ο χρήστης τελικά δεν διαβάζει. Το δικαίωμα διαπραγμάτευσης πρέπει να παρέχεται και στα δύο μέρη της σύμβασης. Οι καταναλωτές έχουν στον ίδιο βαθμό με τις εταιρίες δικαίωμα να προσθέσουν δεσμευτικούς όρους στη σύμβαση. Εάν ένας καταναλωτής τοποθετήσει επιλογή μη εντοπισμού (a «do not track» flag[23]) στο φυλλομετρητή του, αυτό πρέπει να αντιμετωπίζεται ως συμβατικός όρος, όπως επίσης πρέπει να ερμηνεύεται ως συμφωνία (agree) στις διαδικτυακές συμβάσεις το γεγονός ότι οι καταναλωτές εξακολουθούν να χρησιμοποιούν μία ιστοσελίδα ή μία διαδικτυακή υπηρεσία. Το ίδιο πρέπει να ισχύσει και για τις εταιρίες και πρέπει να δεσμεύονται από την επιλογή του μη εντοπισμού (a «do not track» flag), για όσο διάστημα παρέχουν υπηρεσίες σε καταναλωτές που έχουν επιλέξει τον όρο αυτό. Η έλευση της τεχνολογίας της επαυξημένης πραγματικότητας καθιστά εξαιρετικά σημαντική την επιστροφή στον καταναλωτή της εξουσίας πάνω στα προσωπικά του δεδομένα.

Συμπερασματικά, στις εφαρμογές της επαυξημένης πραγματικότητας μπορούν να ανακύψουν ζητήματα που άπτονται της προστασίας της ιδιωτικότητας, των προσωπικών δεδομένων, της ιδιοκτησίας, της ελευθερίας έκφρασης, του εμπορικού σήματος και των καταναλωτών. Μολονότι υπάρχουν διεθνή νομοθετήματα που αναφέρονται στα ανωτέρω δικαιώματα[24], απουσιάζουν οι ειδικοί κανόνες δικαίου που

23 Πρόκειται για ρύθμιση του φυλλομετρητή που σε συνδυασμό με μία εφαρμογή, απενεργοποιεί τη δυνατότητα εντοπισμού του χρήστη. Ο φυλλομετρητής αποστέλλει ένα ειδικό σήμα στις ιστοσελίδες, στις εταιρίες ανάλυσης, στα δίκτυα διαφημίσεων, στους παρόχους σύνδεσης και τις άλλες υπηρεσίες του διαδικτύου που συναντά ο χρήστης κατά την περιήγησή του, για την παύση εντοπισμού της δραστηριότητάς του. Βλ. σχετικά https://allaboutdnt.com/ .

24 Οικουμενική διακήρυξη για τα ανθρώπινα δικαιώματα (άρθρα 12, 17 και 19), Σύμφωνο για τα αστικά και πολιτικά δικαιώματα (άρθρα 17 και 19), Ευρωπαϊκή Σύμβαση για τα ανθρώπινα δικαιώματα (άρθρα 1, 8 και 10), Χάρτης των θεμελιωδών δικαιωμάτων της ΕΕ (άρθρα 7, 8, 11, 17 και 21), ΓΚΠΔ (άρθρο 6), Οδηγία 2000/78/ΕΚ του Συμβουλίου της 27ης Νοεμβρίου 2000 για τη διαμόρφωση γενικού πλαισίου για την ίση μεταχείριση στην απασχόληση και την εργασία (άρθρο 2), Οδηγία 2011/83/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2011 σχετικά με τα δικαιώματα των καταναλωτών, την τροποποίηση της οδηγίας 93/13/ΕΟΚ του Συμβουλίου και της οδηγίας 1999/44/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση της οδηγίας 85/577/ΕΟΚ του Συμβουλίου και της οδηγίας 97/7/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και Κανονισμός (ΕΕ) 2017/1001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Ιουνίου 2017 για το σήμα της Ευρωπαϊκής Ένωσης.

θα ρυθμίζουν τους τομείς των αναδυομένων τεχνολογιών. Επιπλέον, είναι ελάχιστες οι περιπτώσεις όπου οι ήδη υπάρχοντες κανόνες κλήθηκαν να επιλύσουν νομικά ζητήματα στις εφαρμογές της επαυξημένης πραγματικότητας, ώστε να εκτιμηθεί εάν τα αποτελέσματα είναι ικανοποιητικά.

Τεχνητή Νοημοσύνη

Στον τομέα της τεχνητής νοημοσύνης, στον οποίο οφείλεται μεγάλος αριθμός ανακαλύψεων των νέων τεχνολογιών, η ευρεία χρήση της τεχνολογίας αυτής στη λήψη αποφάσεων σχεδόν σε όλους τους τομείς της καθημερινότητας έχει δικαιολογημένα πυροδοτήσει αντιπαραθέσεις σχετικά με τους πολλούς κινδύνους και τα όριά της. Οι επιπτώσεις της στο απόρρητο των ψηφιακών δεδομένων είναι ιδιαίτερα ανησυχητικές, καθώς η τεχνητή νοημοσύνη έχει οδηγήσει στη συνεχή συλλογή δεδομένων και την απουσία αλγοριθμικής ευθύνης. Ταυτόχρονα, όμως, η τεχνολογία αυτή μπορεί να βοηθήσει και στην ελάφρυνση των προκλήσεων που σχετίζονται με το ψηφιακό απόρρητο, απεκδυόμενη έτσι το μανδύα της ψηφιακής απειλής. Οι νέες τεχνικές ελαχιστοποιούν τον όγκο των δεδομένων που συγκεντρώνονται, αποθηκεύονται και διαμοιράζονται, όσο επιτρέπουν παράλληλα στις εταιρίες να συνεχίσουν να λαμβάνουν πολύτιμες πληροφορίες από τις δραστηριότητες των χρηστών τους. Οι ελεγκτές και οι πρωτοπόροι της τεχνολογίας της τεχνητής νοημοσύνης μπορούν να αναπαραστήσουν τα ενδιαφέροντα των καταναλωτών μέσω της «κολεκτιβοποίησης» και να καταγράφουν τα συμπεράσματα σε άλλα συστήματα. Με αυτόν το τρόπο, η τεχνητή νοημοσύνη έχει τη δυνατότητα να βοηθήσει στον προσδιορισμό του ίδιου του απορρήτου. Η επιτυχημένη εφαρμογή των τεχνικών αυτών θα εξαρτηθεί από το συντονισμό της νομοθεσίας και της ιδιωτικής δράσης και με τη σωστή καθοδήγηση, η τεχνητή νοημοσύνη θα μεταβάλει την καθημερινότητα προς το καλύτερο[25].

25 Andrea Scripa, «Artificial intelligence as a digital privacy protector», *Harvard Journal of Law & Technology,* Vol. 31/ 1, (2017): 217-235.

Ειδικά ως προς τη ρύθμιση των εφαρμογών της τεχνητής νοημοσύνης, η καθιέρωση διατάξεων που θα απαγόρευαν την παραγωγή μη πιστοποιημένων συστημάτων τεχνητής νοημοσύνης θα παρείχε ένα ισχυρό κίνητρο στους προγραμματιστές της τεχνολογίας αυτής να ενσωματώνουν χαρακτηριστικά ασφαλείας. Η απόδοση συλλογικής ευθύνης στις περιπτώσεις μη πιστοποιημένου συστήματος τεχνητής νοημοσύνης θα ενθάρρυνε τους διανομείς, τους πωλητές και τους χειριστές να εξετάσουν προσεκτικά τα χαρακτηριστικά ασφαλείας του, ενώ η πιθανότητα απώλειας της αρχής του αποκλεισμού από την ευθύνη, θα αποθάρρυνε την τροποποίηση ενός πιστοποιημένου συστήματος, εκτός εάν παρέχονταν τα εχέγγυα ότι η τροποποίηση αυτή δεν θα προκαλούσε σημαντικούς κινδύνους. Ένα πιο αυστηρό από τις διατάξεις περί αδικοπραξιών, ρυθμιστικό καθεστώς, θα ομοίαζε με το πρόγραμμα έγκρισης φαρμάκων της Υπηρεσίας Τροφίμων και Φαρμάκων[26], όπου τα προϊόντα δεν μπορούν να πωληθούν χωρίς επίσημη άδεια, αλλά και η ίδια η διαδικασία αδειοδότησης περιλαμβάνει πολλαπλές φάσεις αυστηρών δοκιμών ασφαλείας[27]. Μία τέτοιου είδους αυστηρή προσέγγιση θα ήταν αναπόφευκτη, στην περίπτωση που η τεχνητή νοημοσύνη παρουσίαζε σοβαρούς κινδύνους, ενώ μία προσέγγιση πιο φιλική προς την αγορά θα απαιτούσε από τους κατασκευαστές και τους χειριστές των συστημάτων, να συμβληθούν με εγκεκριμένες ασφαλιστικές εταιρίες, επιτρέποντας με αυτόν τον τρόπο την ελεύθερη αγορά να καθορίσει πιο άμεσα τους κινδύνους που προκαλούν τα συστήματα αυτά, μέσω της διατύπωσης των ασφαλιστικών όρων. Μία πρόταση θα μπορούσε να είναι η δημιουργία ενός νομικού καθεστώτος παρόμοιου με την προσωπικότητα των νομικών προσώπων, ώστε τα συστήματα της τεχνητής νοημοσύνης να έχουν νομικά τη δυνατότητα, ως

26 Η Υπηρεσία Τροφίμων και Φαρμάκων (FDA) είναι υπεύθυνη για την προστασία της δημόσιας υγείας με τη διασφάλιση της ασφάλειας και της αποτελεσματικότητας των ανθρωπίνων και κτηνιατρικών φαρμάκων, των βιολογικών προϊόντων και των ιατρικών συσκευών, όπως επίσης και με την εξασφάλιση της απουσίας ραδιενεργών ουσιών σε τρόφιμα και καλλυντικά. Βλ. σχετικά https://www.fda.gov/about-fda/what-we-do .

27 Βλ. σχετική διαδικασία σε http://www.fda.gov/Drugs/DevelopmentApprovalProcess/HowDrugsareDevelopedandApproved/default.htm .

ανεξάρτητες νομικές οντότητες, τόσο της απόκτησης περιουσίας, όσο και της ιδιότητας του εναγομένου[28]. Τέλος, θα μπορούσαν να εφαρμοστούν και στις εφαρμογές της τεχνητής νοημοσύνης οι σχετικές διατάξεις του ΓΚΠΔ περί διαφάνειας[29], απαιτώντας από τους σχεδιαστές και τους χειριστές των σχετικών συστημάτων να αποκαλύψουν δημόσια τον κώδικα και τις προδιαγραφές των συστημάτων αυτών, ώστε να παρέχεται η δυνατότητα στο κοινό να υποδείξει και να επισημάνει τις εφαρμογές που ενδέχεται να υποκρύπτουν κινδύνους. Η απήχηση καθεμίας από τις ανωτέρω προσεγγίσεις θα εξαρτηθεί από την περαιτέρω ανάπτυξη της τεχνητής νοημοσύνης και τους κινδύνους και τα οφέλη που θα γίνουν αντιληπτά. Όσοι πιστεύουν, όπως ο Elon Musk, ότι η τεχνητή νοημοσύνη θα μπορούσε να δημιουργήσει υπαρξιακούς κινδύνους, μπορεί να ευνοήσουν την αύξηση της κυβερνητικής εποπτείας στην ανάπτυξή της[30]. Όσοι, όμως, πιστεύουν ότι οι κίνδυνοι που σχετίζονται με την τεχνητή νοημοσύνη είναι διαχειρίσιμοι και οι υπαρξιακοί κίνδυνοι ανύπαρκτοι, πιθανότατα θα αντιταχθούν σε οποιαδήποτε κυβερνητική παρέμβαση και θα ενθαρρύνουν μόνο περιορισμένες κανονιστικές πράξεις της λειτουργίας της τεχνολογίας αυτής. Σε κάθε περίπτωση, η ανθρωπότητα εισέρχεται σε μία εποχή όπου οι αυτόνομες μηχανές και οι μηχανές μάθησης θα εκτελούν έναν ακόμα μεγαλύτερο αριθμό εργασιών. Τα νομικά συστήματα καλούνται να

28 Θα ήταν, επίσης, ενδιαφέρον να μπορέσουν οι εταιρίες που παράγουν και χρησιμοποιούν «έξυπνες» μηχανές να προωθήσουν την απόδοση ενός είδους ανεξάρτητης νομικής προσωπικότητας (ως αντιπρόσωποι), όπως αυτή των εταιριών, ως μέσο μείωσης των οικονομικών και νομικών υποχρεώσεων όσων τις δημιουργούν και τις χρησιμοποιούν. Βλ. σχετικά Wendell Wallach και Colin Allen, «Moral Machines: Teaching Robots Right from Wrong», 1st Edition, Oxford University Press, 2009.
Μία προσέγγιση αναφορικά με την ευθύνη από σωματική βλάβη που προέρχεται από αυτόνομα οχήματα θα ήταν να είναι το ίδιο το όχημα υπεύθυνο, με την προϋπόθεση ότι το δίκαιο θα απέδιδε νομική προσωπικότητα στο όχημα και θα απαιτούσε να έχει κατάλληλη ασφάλεια. Βλ. σχετικά David C. Vladeck, «Machines Without Principals: Liability Rules and Artificial Intelligence», *Washington Law Review,* Vol. 89/ 1, (2014): 117- 150.

29 Βλ. σχετικά άρθρα 12-14 ΓΚΠΔ.

30 Aileen Graef, «Elon Musk: We Are "Summoning a Demon" with Artificial Intelligence», (2014), διαθέσιμο σε http://www.upi.com/Business_News/2014/10/27/ElonMusk-We-are-summoning-a-demon-with-artificial-intelligence/4191414407652/ .

αποφασίσουν πώς θα αντιδράσουν στις περιπτώσεις που οι μηχανές αυτές θα προκαλέσουν ζημίες[31].

Στην Ευρώπη, η τεχνητή νοημοσύνη και η εξελιγμένη ρομποτική ανοίγουν νέους ορίζοντες σε όλους τους τομείς της βιομηχανίας, με τη μορφή της ανάπτυξης καινοτόμων τεχνικών παραγωγής, εστιάζοντας παράλληλα στη αλληλεπίδραση του ανθρώπινου δυναμικού με τα αυτοματοποιημένα εργαλεία. Παρόλο που η Ευρώπη κατέχει ηγετικό ρόλο στην ανάπτυξη της τεχνητής νοημοσύνης, χρειάζεται να διανυθεί ακόμα αρκετός δρόμος. Η Ευρωπαϊκή Επιτροπή προωθεί στρατηγικές σχετικά με τις εφαρμογές της τεχνητής νοημοσύνης, σε συνεργασία με τα Κράτη – μέλη, οι οποίες συμπεριλαμβάνονται σε σχετική Έκθεσή της προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβουλιο και την Ευρωπαϊκη Οικονομικη και Κοινωνικη Επιτροπη[32].

Στον τομέα της ασφάλειας και της ευθύνης, το νομικό πλαίσιο που θα διαμορφωθεί πρέπει να διασφαλίσει ότι οι αναδυόμενες τεχνολογίες, όπως είναι μεταξύ άλλων, η τεχνητή νοημοσύνη, το διαδίκτυο των πραγμάτων και τα ρομπότ, θα παρέχουν στους πολίτες ασφάλεια και αξιοπιστία και την πεποίθηση ότι σε περίπτωση ζημίας, αυτή αφενός μεν θα μπορεί αποκατασταθεί, αφετέρου δε ότι θα αποδοθεί η ευθύνη στο ζημιώσαντα. Παρόλο που η Ευρωπαϊκή Ένωση έχει ήδη διαμορφώσει το κατάλληλο κανονιστικό πλαίσιο για την ασφάλεια και την ευθύνη από ελαττωματικά προϊόντα, οι νέες τεχνολογίες μεταβάλλουν τα δεδομένα, καθώς έννοιες όπως συνδεσιμότητα, αυτονομία, εξάρτηση από τα δεδομένα και ο σύνθετος χαρακτήρας των τεχνολογιών τροποποιούν τα χαρακτηριστικά των προϊόντων. Όπως έχει ήδη σημειωθεί από την Ευρωπαϊκή Επιτροπή[33], «τα συστήματα Τεχνητής Νοημοσύνης θα πρέπει να

31 Matthew U. Scherer, «Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies», *Harvard Journal of Law & Technology,* Vol. 29/ 2 (2016): 354-400.

32 Βλ. σχετικά «Communication Artificial Intelligence for Europe», (2018), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe .

33 Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών - Οικοδόμηση εμπιστοσύνης στην ανθρωποκεντρική τεχνητή νοημοσύνη.

περιλαμβάνουν ενσωματωμένους μηχανισμούς προστασίας και ασφάλειας ήδη από το στάδιο του σχεδιασμού, προκειμένου να βεβαιώνεται ότι είναι αποδεδειγμένα ασφαλή σε κάθε βήμα, θέτοντας ως προτεραιότητα τη σωματική και πνευματική ασφάλεια όλων των εμπλεκομένων». Η διαρκής συνδεσιμότητα των προϊόντων που στηρίζονται στις νέες τεχνολογίες και η αυτονομία κάποιων από αυτά, θέτουν νέους κανόνες στα θέματα ασφαλείας, συμπεριλαμβανομένης και της κυβερνοασφάλειας. Δεδομένου ότι ο παραγωγός / κατασκευαστής των προϊόντων οφείλει, βάσει των κειμένων κανόνων, να προβαίνει σε εκτίμηση επικινδυνότητας της χρήσης τους, στο ίδιο πλαίσιο και ο κατασκευαστής του προϊόντος που στηρίζεται σε αναδυόμενη τεχνολογία, όπως η τεχνητή νοημοσύνη, δύναται να προχωρήσει στην ίδια εκτίμηση.

Περαιτέρω, από τη στιγμή που τα συστήματα της τεχνητής νοημοσύνης διαθέτουν ως βασικό χαρακτηριστικό την αυτοδιδασκαλία, υπάρχει η πιθανότητα να λάβουν αποφάσεις που παρεκκλίνουν από το σχεδιασμό τους, με αποτέλεσμα να προκύπτουν ζητήματα σε σχέση με την ύπαρξη ή μη ανθρωπίνου ελέγχου και σε ποιο βαθμό. Στο επίπεδο αυτό δεν υφίστανται ακόμα νομοθετικές ρυθμίσεις, κάτι που κρίνεται αναγκαίο να διευθετηθεί κατ' αρχάς σε Ευρωπαϊκό επίπεδο και στη συνέχεια σε επίπεδο Κρατών – μελών. Επίσης, πρέπει να διασφαλίζεται ότι τα δεδομένα με τα οποία είναι συνδεδεμένα οι συσκευές αυτές οδηγούν στη λήψη σύμφωνων με την πρόθεση του κατασκευαστή, αποφάσεων, διαφορετικά οι κίνδυνοι που ενδέχεται να προκύψουν από τα εσφαλμένα δεδομένα δεν καλύπτονται νομοθετικά επί του παρόντος. Παράλληλα, ζητήματα ως προς την ασφάλεια των συσκευών της τεχνητής νοημοσύνης δύναται να προκαλέσει και ο σύνθετος χαρακτήρας τους, καθώς κατασκευαστικά εμπεριέχουν στοιχεία που μπορούν κατά τη λειτουργία τους να επηρεάσουν το ένα το άλλο. Το δεδομένο αυτό πρέπει να λαμβάνεται υπόψη από τον κατασκευαστή κατά την εκτίμηση επικινδυνότητας, ειδικά για τις ενημερώσεις του λογισμικού, οι οποίες «θα μπορούσαν να εξομοιωθούν με τις εργασίες συντήρησης, υπό τον όρο ότι δεν τροποποιούν προϊόν που ήδη διατίθεται στην αγορά κατά τρόπο

που να επηρεάζει τη συμμόρφωση του τελευταίου με τις ισχύουσες απαιτήσεις»[34]. Επιπλέον, όπως έχει ήδη επισημανθεί στην παρούσα, τα χαρακτηριστικά των αναδυομένων τεχνολογιών καθιστούν δυσχερή την απόδοση ευθύνης από ζημία λόγω πλημμελούς ανθρώπινης συμπεριφοράς, ώστε να προκύψουν αξιώσεις σύμφωνα με την πταισματική ευθύνη, όπως αυτή προβλέπεται στο εσωτερικό δίκαιο των Κρατών – μελών. Σύμφωνα με την Έκθεση της σύνθεσης για τις νέες τεχνολογίες της ομάδας εμπειρογνωμόνων για την ευθύνη και τις νέες τεχνολογίες, το εσωτερικό δίκαιο των μελών της ΕΕ πρέπει να διαμορφωθεί κατάλληλα ως προς το βάρος απόδειξης των ζημιωθέντων από τις συσκευές της τεχνητής νοημοσύνης[35]. Ο κατασκευαστής έχει την υποχρέωση να διασφαλίσει ότι το προϊόν του είναι ασφαλές για όλη τη διάρκεια του κύκλου ζωής του, αλλά και ως προς την αναμενόμενη χρήση του. Προκύπτει επίσης και ο παράγοντας του συντρέχοντος πταίσματος, για την περίπτωση που το άτομο που υφίσταται τη ζημία δεν πραγματοποιεί τις απαραίτητες, για την ασφάλεια, ενημερώσεις. Τέλος, η ίδια ομάδα εμπειρογνωμόνων επεσήμανε ότι μπορεί να αποδοθεί συγκεκριμένο προφίλ κινδύνου στις συσκευές που λειτουργούν με αυτονομία, καθώς μπορεί να προσβάλουν δημόσια αγαθά, όπως η ζωή, η υγεία και η περιουσία. Ζήτημα τίθεται ως προς το εάν μπορεί να υιοθετηθεί και για τις συσκευές αυτές η αντικειμενική ευθύνη που υπάρχει στο εσωτερικό δίκαιο των Κρατών – μελών σε σχέση με τους κινδύνους στους οποίους εκτίθενται τα άτομα σε δημόσιους χώρους, όπως από οχήματα ή αεροσκάφη[36]. Στην Ελλάδα, το σχέδιο για τη δημιουργία Ερευνητικού Ινστιτούτου για την Τεχνητή Νοημοσύνη[37] αναμένεται να

34 Βλ. σχετικά Ανακοίνωση της Επιτροπής Ο «Γαλάζιος Οδηγός» του 2016 σχετικά με την εφαρμογή των κανόνων της ΕΕ για τα προϊόντα.

35 Βλ. σχετικά «Liability for Artificial Intelligence and other emerging technologies Report», (2019), διαθέσιμο σε https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199 .

36 Πρόταση της Ευρωπαϊκής Επιτροπής είναι ο συνδυασμός της αντικειμενικής ευθύνης με την υποχρέωση σύναψης ασφάλισης, κατά το πρότυπο της ασφάλισης των αυτοκινήτων. Βλ. σχετικά Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή, Έκθεση σχετικά με τις επιπτώσεις της τεχνητής νοημοσύνης, του διαδικτύου των πραγμάτων και της ρομποτικής στην ασφάλεια και την ευθύνη.

37 Ανακοινώθηκε από την Επιτροπή «Ελλάδα 2021» και αποτελεί «μια πρωτοβουλία που θα βάλει την Ελλάδα στην αιχμή του δόρατος της παγκόσμιας τεχνολογικής πρωτοπορίας». Βλ. σχετικά https://www.greece2021.gr/arthro/4669-to-ergo-kai-oi-protaseis-ths-epitropis-ellada2021/.

θέσει τις βάσεις για τις οποιεσδήποτε νομοθετικές ρυθμίσεις οι οποίες θα ακολουθήσουν στο μέλλον.

Όπως γίνεται κατανοητό, η ευρεία εξάπλωση των νέων τεχνολογιών σε κάθε πτυχή της καθημερινότητας καθιστά άμεση την ανάγκη για ρύθμισή τους, τόσο σε παγκόσμιο, αλλά ακόμα περισσότερο σε ενωσιακό και τοπικό επίπεδο. Σύντομα θα κάνουν την εμφάνισή τους και στην ελληνική πραγματικότητα εφαρμογές των τεχνολογιών της επαυξημένης πραγματικότητας και της τεχνητής νοημοσύνης, οι οποίες θα καλύπτουν ευαίσθητους τομείς, όπως η υγεία και η εκπαίδευση, και η ανάγκη για οριοθέτησή τους θα μεγεθυνθεί. Η εφαρμογή των κανόνων του συμβατικού δικαίου στις τεχνολογίες αυτές, όπου αυτό είναι εφικτό, πρέπει να αποτελέσει τον κανόνα, ενώ το δίκαιο πνευματικής ιδιοκτησίας που εφαρμόζεται σήμερα σχεδόν αποκλειστικά, πρέπει να αποτελέσει την εξαίρεση. Διότι, όπως σημείωσε πολύ εύστοχα ο Μάρσαλ Μακ Λούαν «Όταν μια παλιότερη τεχνολογία δίνει τη θέση της σε μια καινούργια, η παλιότερη επιστρέφει σαν τέχνη».

Παράρτημα Α΄

Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή

INT/846
Εμπιστοσύνη, ιδιωτικότητα και ασφάλεια / Διαδίκτυο των πραγμάτων

ΓΝΩΜΟΔΟΤΗΣΗ
Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή
Εμπιστοσύνη, ιδιωτικότητα και ασφάλεια των καταναλωτών και των επιχειρήσεων στο Διαδίκτυο των πραγμάτων
[γνωμοδότηση πρωτοβουλίας]

Εισηγητής: **Carlos TRIAS PINTÓ**
Συνεισηγητής: **Δημήτρης ΔΗΜΗΤΡΙΑΔΗΣ**

Απόφαση της συνόδου ολομέλειας	15/02/2018
Νομική βάση	Άρθρο 29 παράγραφος 2 του Εσωτερικού Κανονισμού Γνωμοδότηση πρωτοβουλίας
Αρμόδιο τμήμα	«Ενιαία αγορά, παραγωγή και κατανάλωση»
Υιοθέτηση από το τμήμα	04/09/2018
Υιοθέτηση από την Ολομέλεια	19/09/2018
Σύνοδος ολομέλειας αριθ.	537
Αποτέλεσμα της ψηφοφορίας (υπέρ/κατά/αποχές)	182/3/2

Συμπεράσματα και συστάσεις

Το Διαδίκτυο των πραγμάτων (εφεξής ΔτΠ), χάρη στη διασυνδεσιμότητα ατόμων και αντικειμένων, προσφέρει τεράστιο εύρος ευκαιριών στους πολίτες και τις επιχειρήσεις. Ωστόσο, θα πρέπει να υπάρξουν πλείστες διασφαλίσεις και έλεγχοι ώστε να λειτουργεί ικανοποιητικά.

Λαμβάνοντας υπόψη ότι ένας από τους πυλώνες του ΔτΠ βασίζεται στην αυτόματη λήψη αποφάσεων χωρίς ανθρώπινη παρέμβαση, πρέπει να εξασφαλίζεται ότι οι αποφάσεις αυτές δεν υπονομεύουν τα δικαιώματα των καταναλωτών, δεν εγκυμονούν κινδύνους ηθικής φύσεως και δεν αντιβαίνουν προς τις θεμελιώδεις αρχές και τα ανθρώπινα δικαιώματα

Η ΕΟΚΕ ζητεί από τα ευρωπαϊκά όργανα και τα κράτη μέλη της ΕΕ:

1. να διασφαλίσουν την προστασία της ασφάλειας και της ιδιωτικότητας, μέσω της ανάπτυξης κατάλληλων κανονιστικών πλαισίων που θα περιλαμβάνουν αυστηρά μέτρα παρακολούθησης και ελέγχου·

2. να προσδιορίσουν με σαφήνεια την ευθύνη όλων των επαγγελματιών στην αλυσίδα εφοδιασμού του προϊόντος και στη ροή πληροφοριών που συνδέονται με αυτήν, αποφεύγοντας τα κανονιστικά κενά όταν εμπλέκονται πολλοί παραγωγοί και διανομείς.

3. να προβλέψουν κατάλληλους πόρους και αποτελεσματικούς μηχανισμούς για τον συντονισμό μεταξύ της Ευρωπαϊκής Επιτροπής και των κρατών μελών, προκειμένου να εξασφαλιστεί η συνεκτική και εναρμονισμένη εφαρμογή τόσο της νομοθεσίας που θα αναθεωρηθεί όσο και της νέας νομοθεσίας, αντιμετωπίζοντας παράλληλα τις προκλήσεις του διεθνούς περιβάλλοντος·

4. να παρακολουθούν την ανάπτυξη των αναδυόμενων τεχνολογιών που σχετίζονται με το ΔτΠ, ώστε να εξασφαλίζεται υψηλό επίπεδο ασφάλειας, πλήρης διαφάνεια και θεμιτή προσβασιμότητα·

5. να προωθήσουν τις ευρωπαϊκές και διεθνείς πρωτοβουλίες τυποποίησης για την εξασφάλιση της αξιοπιστίας, της διαθεσιμότητας, της ανθεκτικότητας και της συντήρησης των προϊόντων·

6. να παρακολουθούν τις αγορές και να διατηρούν ισότιμους τους όρους ανταγωνισμού στην εφαρμογή του ΔτΠ, προκειμένου να αποφεύγεται η συγκέντρωση της διακρατικής οικονομικής ισχύος στους νέους παράγοντες της τεχνολογίας·

7. να αναλάβουν τη δέσμευση να προωθούν δράσεις ευαισθητοποίησης και αναβάθμισης των ψηφιακών δεξιοτήτων, εκ παραλλήλου με τη βασική έρευνα και την καινοτομία στον εν λόγω τομέα·

8. να εγγυηθούν την πλήρη εφαρμογή και αποτελεσματική χρήση των συστημάτων εναλλακτικής επίλυσης διαφορών εντός και εκτός διαδικτύου (ΗΕΚΔ και ΕΕΚΔ)·

9. να διασφαλίσουν την ύπαρξη, την υλοποίηση και την αποτελεσματική λειτουργία ενός συστήματος συλλογικής δράσης που θα επιτρέπει την διακοπή και την αποζημίωση όταν η χρήση του ΔτΠ προκαλεί ζημίες ή βλάβες συλλογικού χαρακτήρα, όπως προβλέπεται δυνάμει της «Νέας Συμφωνίας για τους Καταναλωτές».

Για να δείχνουν εμπιστοσύνη οι καταναλωτές πρέπει αφενός να τηρείται αυστηρά η σχετική νομοθεσία και αφετέρου να κοινοποιείται ότι ακολουθούνται βέλτιστες επιχειρηματικές πρακτικές όσον αφορά την ιδιωτικότητα και την ασφάλεια, ενώ είναι καθήκον των θεσμικών οργάνων η σύνδεσή τους με τις στρατηγικές εταιρικής κοινωνικής ευθύνης και τις κοινωνικά υπεύθυνες επενδύσεις.

Ο κοινωνικός και οικονομικός αντίκτυπος του ΔτΠ θα είναι περισσότερο θετικός εφόσον συνδεθεί κατάλληλα με την ανάπτυξη κοινωνικών και περιβαλλοντικών πολιτικών στο πλαίσιο της συνεργατικής οικονομίας, της κυκλικής οικονομίας και της λειτουργικής οικονομίας.

Ιστορικό και ευρύτερο πλαίσιο

Κατά τα τελευταία δεκαπέντε έτη, η εμφάνιση του διαδικτύου έχει επιφέρει αλλαγές σε όλους τους τομείς της καθημερινής ζωής, επηρεάζοντας τις διάφορες καταναλωτικές συνήθειες. Επίσης, προβλέπεται ότι εντός της επόμενης δεκαετίας η επανάσταση του διαδικτύου των πραγμάτων (ΔτΠ) θα επηρεάσει τους τομείς της ενέργειας, της γεωργίας και των μεταφορών, όπως επίσης και τους πιο παραδοσιακούς τομείς της οικονομίας και της κοινωνίας. Το γεγονός αυτό οδηγεί στη χάραξη ολοκληρωμένων πολιτικών που θα αντιμετωπίζουν "έξυπνα" αυτήν την τεχνολογική ανατροπή.

Η έννοια του ΔτΠ γεννήθηκε στο Massachusetts Institute of Technology (MIT) και ουσιαστικά βασίζεται σε έναν κόσμο γεμάτο από πλήρως διασυνδεδεμένες συσκευές, ώστε να είναι δυνατή η αυτοματοποίηση όλων των διαφορετικών διαλειτουργικών διαδικασιών. Από την πλευρά της, η Ευρωπαϊκή Ένωση προετοιμάζεται για να αντιμετωπίσει την ψηφιακή σύγκλιση και τις νέες προκλήσεις του ΔτΠ, ξεκινώντας από τη δρομολόγηση του σχεδίου «Η στρατηγική i2010 – Ευρωπαϊκή κοινωνία της πληροφορίας για την ανάπτυξη και την απασχόληση»[1], μέχρι και το πρόσφατο Σχέδιο Δράσης ΔτΠ (Βλ. έγγραφο «Η πρόοδος στο Διαδίκτυο των Πραγμάτων στην Ευρώπη», που αποτέλεσε μέρος της ανακοίνωσης του 2016 «Ψηφιοποίηση της ευρωπαϊκής βιομηχανίας. Τα πλήρη οφέλη από την ψηφιακή ενιαία αγορά»)[2].

1 COM(2005) 229 final.
2 COM(2016) 180 final.

Η ΕΟΚΕ έχει επανειλημμένως αποφανθεί για την τέταρτη βιομηχανική επανάσταση, η οποία χαρακτηρίζεται από τη σύγκλιση των ψηφιακών, φυσικών και βιολογικών τεχνολογιών, με σημαντικότερη τη γνωμοδότηση του 2017[3]. Πράγματι, το ΔτΠ αποτελεί το προτιμώμενο πεδίο εφαρμογής για τις πιο προηγμένες μορφές τεχνητής νοημοσύνης και το πεδίο όπου δοκιμάζονται οι αρχές που αναφέρει η ΕΟΚΕ, ιδίως η αρχή του ανθρωπίνου ελέγχου (human in control).

Οι συσκευές του ΔτΠ συχνά δεν διαθέτουν τις προδιαγραφές επαλήθευσης ταυτότητας που απαιτούνται για την ασφάλεια των δεδομένων του χρήστη. Αυτό οδηγεί στην εμφάνιση προβλημάτων, καθότι οι συσκευές, τα δεδομένα και οι εταίροι της αλυσίδας εφοδιασμού είναι εκτεθειμένοι σε παραβιάσεις ασφαλείας.

Οι αναδυόμενες τεχνολογίες, όπως η blockchain (αλυσίδα συστοιχιών), μπορούν να δίνουν λύση σε ζητήματα ασφαλείας και εμπιστοσύνης: μπορούν να χρησιμοποιηθούν για την ιχνηλάτηση των μετρήσεων δεδομένων από αισθητήρες και, όχι μόνο να αποτρέψουν την αλληλεπικάλυψη με κακόβουλα δεδομένα, αλλά και να διατηρήσουν την ακεραιότητα και την ιχνηλασιμότητα των τροποποιήσεων· ένα κατανεμημένο καθολικό (distributed ledger) μπορεί να παρέχει στις συσκευές του ΔτΠ ταυτοποίηση, εξακρίβωση και απρόσκοπτη ασφαλή μεταφορά δεδομένων· οι αισθητήρες του ΔτΠ μπορούν να χρησιμοποιηθούν για την ανταλλαγή δεδομένων μέσω αλυσίδας συστοιχιών αντί της ανταλλαγής μέσω τρίτου· η χρήση της τεχνολογίας blockchain και των "έξυπνων" συμβάσεων επιτρέπει την αυτονομία των συσκευών, καθώς και την ατομική ταυτότητα και την ακεραιότητα των δεδομένων· τα έξοδα δημιουργίας και λειτουργίας μειώνονται καθώς δεν υπάρχουν μεσάζοντες· τέλος, οι συσκευές του ΔτΠ στην αλυσίδα συστοιχιών παρέχουν το ιστορικό των διασυνδεδεμένων συσκευών που είναι πολύ χρήσιμο αν τυχόν χρειαστεί να αντιμετωπιστούν προβλήματα[4].

Επιπλέον, αναπτύσσονται τεχνολογίες κατανεμημένου καθολικού, ανοιχτού κώδικα, για την ανταλλαγή πληροφοριών και τιμών μεταξύ συσκευών του ΔτΠ. Δεν επιτρέπουν την άντληση δεδομένων, αλλά χρησιμοποιούν μια αρχιτεκτονική που βασίζεται σε μια μαθηματική έννοια που ονομάζεται κατευθυνόμενο άκυκλο γράφημα (DAG), με την οποία αποφεύγονται οι προμήθειες και δίνεται η δυνατότητα αύξησης της δυναμικότητας του δικτύου ανάλογα με την αύξηση του αριθμού των χρηστών.

Βρισκόμαστε μπροστά σε ένα φαινόμενο με μεγάλο οικονομικό[5] και κοινωνικό δυναμικό που παρουσιάζει μεγάλες ευκαιρίες, αλλά παράλληλα και σημαντικές προκλήσεις συνδεδεμένες με

3 Η τεχνητή νοημοσύνη — Η επίδραση της τεχνητής νοημοσύνης στην (ψηφιακή) ενιαία αγορά, στην παραγωγή, στην κατανάλωση, στην απασχόληση και στην κοινωνία, ΕΕ C 288 της 31.8.2017, σ. 1.

4 Βλ. Khwaja Shaik, Why blockchain and IoT are best friends, https://www.ibm.com· όσον αφορά τις καινοτομίες στον ευρωπαϊκό χρηματοοικονομικό τομέα Βλ. ΕΕ C 246 της 28.7.2017, σ. 8.

5 Η Digital McKinsey εκτιμά ότι το ΔτΠ έχει πιθανό οικονομικό αντίκτυπο που κυμαίνεται από 3,9 τρις USD μέχρι $ 11,1 τρις USD ετησίως έως το 2025.

άδηλους κινδύνους, πολυδιάστατου και οριζόντιου χαρακτήρα, που επηρεάζουν εξίσου επιχειρήσεις και καταναλωτές, διοικήσεις και πολίτες. Για τον λόγο αυτό, η αντιμετώπιση αυτού του θέματος απαιτεί κοινή προσέγγιση η οποία να επικεντρώνεται, παράλληλα, σε όσα στοιχεία είναι μοναδικά σε κάθε περίπτωση. Από αυτήν την άποψη, αρκεί να αναφερθεί ότι τα Ηνωμένα Έθνη έχουν εκτιμήσει πως το 2020 θα υπάρχουν 50 τρισεκατομμύρια διασυνδεδεμένες συσκευές, με εφαρμογές για τους καταναλωτές μέσω τηλεοράσεων, ψυγείων, καμερών ασφαλείας, οχημάτων κ.λπ.

Οι εφαρμογές του ΔτΠ προσφέρουν ήδη οικονομικά και κοινωνικά οφέλη στο πλαίσιο της παγκοσμιοποίησης, παρέχοντας, μεταξύ άλλων, περισσότερες υπηρεσίες με κοινωνικοοικονομική ευαισθησία, μικρότερους κύκλους ανάδρασης, επισκευές από απόσταση, στήριξη των διαδικασιών λήψης αποφάσεων, καλύτερη κατανομή πόρων ή εξ αποστάσεως έλεγχο των υπηρεσιών. Ωστόσο, υπάρχουν πολύ ευαίσθητα συνεπακόλουθα ζητήματα, όπως είναι η ιδιωτικότητα και η ασφάλεια, η ασύμμετρη πληροφόρηση και η διαφάνεια των συναλλαγών, οι σύνθετες αρμοδιότητες, ο αποκλεισμός προϊόντων και συστημάτων ή, επίσης, η αύξηση των υβριδικών προϊόντων που μπορεί να έχει προεκτάσεις όσον αφορά θέματα ιδιοκτησίας και να εκθέσει τους καταναλωτές στην πραγματοποίηση εξ αποστάσεως συμβάσεων, με επακόλουθο μειωμένες εγγυήσεις.

Οι τεράστιες νομικές προκλήσεις που αντιμετωπίζουν η ΕΕ και τα κράτη μέλη της μπορούν να εξηγηθούν από το γεγονός ότι πολλά από τα ειδικά χαρακτηριστικά του ΔτΠ (υψηλά επίπεδα πολυπλοκότητας και ισχυρή αλληλεξάρτηση, το στοιχείο της αυτονομίας, οι συνιστώσες της δημιουργίας και/ή επεξεργασίας δεδομένων και μια ανοιχτή διάσταση) διακρίνουν και άλλες αναδυόμενες ψηφιακές τεχνολογίες, όπως η blockchain, η εκτύπωση σε 3D και το υπολογιστικό νέφος. Κατά την άποψη της ΕΟΚΕ, το έγγραφο εργασίας της Ευρωπαϊκής Επιτροπής[6] σχετικά με την ευθύνη των αναδυόμενων ψηφιακών τεχνολογιών αποτελεί ένα ακόμη βήμα προς τη σωστή κατεύθυνση.

Εν ολίγοις, η μεγιστοποίηση του οφέλους και η ελαχιστοποίηση των κινδύνων που συνδέονται με το ΔτΠ συνεπάγεται την παροχή πληροφοριών προσιτών, σαφών, συνοπτικών και αξιόπιστων, ιδίως με την προώθηση της ένταξης και της ψηφιακής συνδεσιμότητας των πλέον ευάλωτων καταναλωτών, μέσω του σχεδιασμού προϊόντων και υπηρεσιών απολύτως ανιχνεύσιμων που θα ενσωματώνουν ολοκληρωμένα πρότυπα εμπιστοσύνης, ιδιωτικότητας και ασφάλειας.

Εμπιστοσύνη των καταναλωτών και των επιχειρηματιών στο ΔτΠ

Το ΔτΠ αποτελεί ένα πολυσύνθετο οικοσύστημα που επιτρέπει τη διασύνδεση συσκευών διαφορετικών κατασκευαστών, διανομέων ή παραγωγών λογισμικού. Αυτό δημιουργεί δυσκολίες στην απόδοση ευθυνών σε περιπτώσεις μη συμμόρφωσης με τη νομοθεσία ή σε περίπτωση υλικών ζημιών ή άλλων ζημιών που προκαλούνται σε τρίτους ή σε συστήματα λόγω ελαττωματικών

6 SWD(2018) 137.

προϊόντων ή λόγω της στρεβλής χρήσης των προϊόντων από τρίτους μέσω του διαδικτύου. Υπάρχει επίσης το ενδεχόμενο πολλοί από τους επαγγελματίες που συμμετέχουν στην παγκόσμια αλυσίδα αξίας του προϊόντος να μην διαθέτουν επαρκείς γνώσεις και εμπειρία σε θέματα ασφάλειας ή προστασίας δεδομένων όσον αφορά τις δικτυωμένες συσκευές.

Για τον λόγο αυτόν απαιτείται μια νέα προσέγγιση όσον αφορά τις ευθύνες, με στόχο να διασφαλιστεί ότι τόσο οι καταναλωτές όσο και οι επιχειρήσεις που υιοθετούν εφαρμογές του ΔτΠ προστατεύονται σε περιπτώσεις που προϊόντα με ενδεδειγμένες ρυθμίσεις μπορεί να αποδειχθούν ελαττωματικά ή μη ασφαλή λόγω συμβάντων ψηφιακής ασφάλειας ή λόγω μη εξουσιοδοτημένης αθέμιτης χρήσης (π.χ. από hackers). Το περιβάλλον αυτό πρέπει να δίνει τη δυνατότητα για πρόβλεψη, πρόληψη και προστασία από εκείνες τις αυτοματοποιημένες αποφάσεις που μπορεί παραβιάζουν τις ηθικές αξίες και τα παγκοσμίως αναγνωρισμένα ανθρώπινα δικαιώματα.

Η ΕΟΚΕ χαιρετίζει τόσο την επανεξέταση της εφαρμογής της οδηγίας του 1985 σχετικά με την ευθύνη λόγω ελαττωματικών προϊόντων[7] όσο και την πρόσφατη δημιουργία της πολυσυμμετοχικής ομάδας εμπειρογνωμόνων σχετικά με την ευθύνη και τις νέες τεχνολογίες, για να επιτευχθεί η κατάλληλη ισορροπία ανάμεσα στα συμφέροντα των παραγωγών και των καταναλωτών. Το νέο πλαίσιο ευθύνης πρέπει να προβλέπει με σαφή τρόπο την ιχνηλασιμότητα της ευθύνης και της ασφάλειας, τόσο κατά μήκος της αλυσίδας αξίας του προϊόντος όσο και κατά τη διάρκεια του κύκλου ζωής του, περιλαμβάνοντας τη βιωσιμότητα ως νέο στοιχείο βάσει του οποίου θα προβλέπεται η επικαιροποίηση, η βελτίωση, η φορητότητα, η συμβατότητα, η επαναχρησιμοποίηση, η επισκευή ή η αποκατάσταση του προϊόντος.

Θα πρέπει επίσης να αποτελέσει αντικείμενο ειδικής εξέτασης για το ΔτΠ ο προσδιορισμός της ευθύνης όλων των επαγγελματιών στην αλυσίδα εφοδιασμού του προϊόντος, καθώς και η αποφυγή κανονιστικών κενών όταν εμπλέκονται πολλοί παραγωγοί και διανομείς. Η ΕΟΚΕ θεωρεί ότι είναι σημαντικό να καθοριστούν σαφώς οι διαδικασίες που θα πρέπει να ακολουθούν οι καταναλωτές σε κάθε περίπτωση, με την προώθηση μηχανισμών εναλλακτικής επίλυσης διαφορών (ADR).

Η ΕΟΚΕ τονίζει τη σημασία των προσυμβατικών πληροφοριών και της διαφάνειας των καθοριζόμενων ρητρών, καθώς και των οδηγιών χρήσης των συσκευών, με ρητή προειδοποίηση όσον αφορά τους πιθανούς συναφείς κινδύνους και την κάλυψή τους.

Η διαλειτουργικότητα και η συμβατότητα των συναφών συσκευών, καθώς και του σχετικού λογισμικού, πρέπει να εξασφαλίζεται προκειμένου να αποφεύγονται οι αποκλεισμοί και να μπορεί ο καταναλωτής να συγκρίνει τους προμηθευτές. Η ΕΟΚΕ υπογραμμίζει ότι ο παράγοντας αυτός είναι επίσης καίριας σημασίας για τη δημιουργία ισότιμων όρων ανταγωνισμού μεταξύ μεγάλων εταιρειών και ΜΜΕ.

7 COM(2018) 246 final.

Τέλος, η ΕΟΚΕ συνιστά να τηρείται η ουδετερότητα του δικτύου και παροτρύνει την Επιτροπή να ασκεί αυστηρή εποπτεία της συμπεριφοράς στην αγορά.

Ιδιωτικότητα των καταναλωτών στο ΔτΠ

Οι καταναλωτές έχουν ενισχύσει την ικανότητά τους να ασκούν έλεγχο επί των προσωπικών τους δεδομένων και των ιδιωτικών τους προτιμήσεων βάσει του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ)[8]. Ο χρήστης μιας συσκευής πρέπει να ελέγχει τον τρόπο με τον οποίο γίνεται χρήση των δεδομένων που παράγει και το ποιος έχει τη δυνατότητα πρόσβασης σε αυτά, λαμβανομένου υπόψη ότι η ποικιλία των δεδομένων, καθώς και η συγκέντρωση και η σύνδεσή τους με άλλα δεδομένα, συνεπάγονται σοβαρό κίνδυνο για την ιδιωτικότητα στο οικοσύστημα του ΔτΠ.

Πρέπει να ληφθούν υπόψη οι επιπτώσεις που μπορεί να έχει το πλήθος των προϊόντων, των υπηρεσιών ή των φορέων στην ιδιωτικότητα και στην προστασία των δεδομένων, όταν αυτά μεταφέρονται με τρόπο αυτόνομο λόγω της διασυνδεσιμότητάς τους. Κατά τον ίδιο τρόπο, στις περιπτώσεις επεξεργασίας ή επανεπεξεργασίας πληροφοριών με βάση αρχικώς ασφαλή δεδομένα, υπάρχει το ενδεχόμενο να γίνουν γνωστές με ακρίβεια οι συνήθειες, τα μέρη όπου συχνάζουν, τα ενδιαφέροντα και οι προτιμήσεις των ατόμων. Αυτό αυξάνει την προσβασιμότητα και τη δυνατότητα εντοπισμού του προφίλ του χρήστη.

Οι νομικές εγγυήσεις θα πρέπει να διασφαλίζουν την απόλυτη δυνατότητα των χρηστών να ασκούν τα δικαιώματα της ιδιωτικότητάς τους και της προστασίας των δεδομένων τους προσωπικού χαρακτήρα χωρίς περιορισμό, ώστε να αποφεύγονται ενδεχόμενες επιβλαβείς συνέπειες όπως οι διακρίσεις, οι επιθετικές πωλήσεις, η συρρίκνωση της ιδιωτικής σφαίρας ή οι παραβιάσεις της ασφάλειας. Από την άλλη πλευρά, οι καταναλωτές θα πρέπει να έχουν ενημέρωση σχετικά με την οικονομική αξία των δεδομένων τους και να διατηρούν το δικαίωμα να τα κοινοποιούν.

Όπως προβλέπει ο ΓΚΠΔ, οι εταιρείες και οι ρυθμιστικές αρχές θα πρέπει να επανεξετάζουν τακτικά το πεδίο εφαρμογής της συλλογής δεδομένων και να αξιολογούν τον βαθμό στον οποίον τα δεδομένα που υποβάλλονται σε επεξεργασία είναι κατάλληλα και αναγκαία για την παροχή της υπηρεσίας. Οι πτυχές και οι επιπτώσεις της ιδιωτικότητας πρέπει να αξιολογούνται σε όλη τη διάρκεια της σύλληψης, του κύκλου σχεδιασμού και της ανάπτυξης ενός συνδεδεμένου προϊόντος, αλλά και του διαδικτυωμένου οικοσυστήματος, όπου αυτό λειτουργεί (ιδιωτικότητα εκ σχεδιασμού). Ως εκ τούτου, οι αρχές της προστασίας της ιδιωτικότητας εκ σχεδιασμού και της ιδιωτικότητας εξ ορισμού πρέπει να εφαρμόζονται με συνέπεια όσον αφορά το ΔτΠ.

8 Σε ισχύ από τις 25 Μαΐου 2018.

Επίσης, η διαμόρφωση κάθε συνδεδεμένου προϊόντος πρέπει, από προεπιλογή, να διασφαλίζει το υψηλότερο επίπεδο προστασίας της ιδιωτικότητας (εκ σχεδιασμού και εξ ορισμού) ώστε να αποφεύγεται η ανεπιθύμητη παρακολούθηση της συμπεριφοράς των χρηστών και των δραστηριοτήτων τους.

Σε κάθε περίπτωση, οι καταναλωτές πρέπει να γνωρίζουν επακριβώς ποια δεδομένα συλλέγονται, ποιοι έχουν πρόσβαση σε αυτά και πώς πρόκειται να χρησιμοποιηθούν ενόσω γίνεται χρήση του προϊόντος ή της υπηρεσίας, καθώς και ποια είναι η εφαρμοζόμενη πολιτική προστασίας της ιδιωτικότητας, όπως και αν οι χρησιμοποιούμενοι αλγόριθμοι επηρεάζουν την ποιότητα, την τιμή ή την προσβασιμότητα της υπηρεσίας.

Ασφάλεια των καταναλωτών και των επιχειρηματιών στο ΔτΠ

Η διασυνδεσιμότητα των συσκευών που χαρακτηρίζει το οικοσύστημα του ΔτΠ μπορεί να ενθαρρύνει τη διαμόρφωση παράνομων ή ανεπιθύμητων τεχνολογικών πρακτικών και να το μετατρέψει σε ένα περιβάλλον με δεδομένα εύκολα προσπελάσιμα και ταχύτατα διαδιδόμενα. Για τον λόγο αυτόν απαιτείται να εδραιωθεί με ολοκληρωμένο τρόπο η ασφάλεια, σε καθένα ξεχωριστά και σε όλα μαζί τα στοιχεία του συστήματος.

Η προσφορά προϊόντων και επικαιροποιήσεων που συνδέονται με την ασφάλεια στον κυβερνοχώρο πρέπει να αιτιολογείται και να καλύπτει όχι μόνο τις μεμονωμένες συσκευές, αλλά να παρέχει και κάλυψη έναντι των κινδύνων για την ασφάλεια που ενέχει η διασυνδεσιμότητα με άλλες συσκευές στο ΔτΠ, ενώ ο αριθμός των συσκευών δεν πρέπει να οδηγεί σε έκπτωση των προτύπων ποιότητας της ασφάλειας αυτής.

Στο πλαίσιο αυτό, η πρόταση κανονισμού σχετικά με τον Οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο[9] περιλαμβάνει ένα πλαίσιο για την πιστοποίηση των τεχνολογιών πληροφοριών και επικοινωνιών που θα επιτρέψει τον καθορισμό εθελούσιων συστημάτων πιστοποίησης ασφάλειας και επισήμανσης για διάφορες κατηγορίες προϊόντων, μεταξύ των οποίων και το ΔτΠ. Παρότι η ΕΟΚΕ επικροτεί το μέτρο αυτό, εκφράζει επίσης την ανησυχία της διότι δεν έχει υποχρεωτικό χαρακτήρα.

Τα μέτρα ασφάλειας στον κυβερνοχώρο θα πρέπει να καλύπτουν από κινδύνους λόγω προσβλητότητας, ιδίως από την υποκλοπή (hacking), τη μη επιτρεπόμενη πρόσβαση ή την αθέμιτη χρήση, καθώς και από κινδύνους σχετικούς με τον τρόπο πληρωμής και τις οικονομικές απάτες. Στο πλαίσιο αυτό, η ΕΟΚΕ στηρίζει τις αρμοδιότητες της πολυσυμμετοχικής ομάδας εμπειρογνωμόνων σχετικά με την ευθύνη και τις νέες τεχνολογίες.

9 Βλ. COM(2017) 477 final.

Επιπλέον, πρέπει να καλύπτουν την προσωπική ασφάλεια των καταναλωτών σε σχέση με κινδύνους, όπως η χρήση της γεωγραφικής εγγύτητας, οι κοινές ζώνες συχνοτήτων, η έκθεση σε ηλεκτρομαγνητικά πεδία ή οι πιθανές παρεμβολές με συνδεδεμένο εξοπλισμό ζωτικής σημασίας. Η ΕΟΚΕ ζητεί να εφαρμοστούν μέτρα επιτήρησης και προληπτικής απόσυρσης όταν υπάρχουν κίνδυνοι για την υγεία και την ασφάλεια των καταναλωτών ή των προσωπικών και οικονομικών συμφερόντων τους.

Οι επιχειρήσεις πρέπει να υιοθετούν πρότυπα ορθών πρακτικών, όπως η ασφάλεια εκ σχεδιασμού και εξ ορισμού, και να υπόκεινται σε αξιολογήσεις από ανεξάρτητους εξωτερικούς φορείς. Σε περιπτώσεις παραβίασης της ασφάλειας ή των δεδομένων, οι επιχειρήσεις οφείλουν να κοινοποιούν τα περιστατικά αυτά, παρέχοντας ενημέρωση σχετικά με την ευθύνη για ζημίες και μη συμμόρφωση προς τη νομοθεσία.

Οι επιχειρήσεις πρέπει να παρέχουν στους καταναλωτές απλές και προσβάσιμες πληροφορίες που θα τους επιτρέπουν να παίρνουν τις κατάλληλες αποφάσεις και να εφαρμόζουν ασφαλείς πρακτικές, παρέχοντας στους καταναλωτές τις επικαιροποιήσεις ασφαλείας που είναι ουσιαστικής σημασίας καθ' όλη τη διάρκεια του κύκλου ζωής του προϊόντος.

Η έλλειψη συνεκτικών προτύπων όσον αφορά τα δίκτυα ΔτΠ πρέπει να αντιμετωπιστεί. Είναι αναγκαίο να διαμορφωθούν προηγμένες ευρυζωνικές τεχνολογίες νέας γενιάς που να βελτιώνουν τις υφιστάμενες υποδομές.

Προτάσεις για ανάληψη δράσης στο πλαίσιο των δημόσιων πολιτικών[10]

Οι δημόσιες αρχές, κατά την άσκηση των αρμοδιοτήτων τους στις διάφορες περιοχές της Ευρωπαϊκής Ένωσης, πρέπει να συμμετέχουν ενεργά στη χάραξη πολιτικής και σχεδίων δράσης για το ΔτΠ, με στόχο την επίτευξη ισορροπίας μεταξύ των διαφόρων ενδιαφερόμενων μερών, προλαμβάνοντας τα προβλήματα και αμβλύνοντας προληπτικά τις πιθανές αρνητικές επιπτώσεις. Η ΕΟΚΕ προτείνει:

1. να δημιουργηθούν περιβάλλοντα δοκιμών (sand boxes), δηλαδή φυσικοί χώροι, συνεργατικοί σχηματισμοί κ.λπ., για τα πιλοτικά έργα και τις αποδείξεις αρχών. Αυτά θα αποσκοπούν όχι μόνο στην απλή δοκιμή τεχνολογιών, αλλά και στη δοκιμή κανονιστικών προτύπων[11];

2. να χρηματοδοτηθούν τεχνολογικές υποδομές που θα επιτρέπουν την ανάπτυξη καινοτόμων έργων ΔτΠ στο πλαίσιο του νέου προγράμματος «Ορίζων Ευρώπη».

10 Βλ. Όμιλος Παγκόσμιας Τράπεζας, *Internet of things. The New Government to Business Platform* (Το Διαδίκτυο των Πραγμάτων. Η νέα πλατφόρμα κυβέρνησης-επιχειρήσεων).

11 Βλ. https://ec.europa.eu/digital-single-market/en/news/eu-and-eea-member-states-sign-cross-border-experiments-cooperative-connected-and-automated.

3. να οριστούν ιδρύματα και ανεξάρτητες αρχές ως παράγοντες διευκόλυνσης και εποπτείας των έργων του ΔτΠ. Η ΕΟΚΕ χαιρετίζει τα σχετικά μέτρα που προβλέπονται από τον κανονισμό του 2017 για την ασφάλεια στον κυβερνοχώρο και ζητεί από την Επιτροπή να προωθήσει αποτελεσματικά και με τους κατάλληλους δημοσιονομικούς πόρους τις διαδικασίες τυποποίησης για την ψηφιακή βιομηχανία[12]·

4. να προωθηθούν συμπράξεις και πλατφόρμες συνεργασίας δημόσιου και ιδιωτικού τομέα, με τη συμμετοχή της επιστημονικής κοινότητας, της βιομηχανίας και των καταναλωτών·

5. να ενθαρρυνθούν οι επενδύσεις στην ανάπτυξη τοπικών επιχειρηματικών μοντέλων που θα αξιοποιούν τα οφέλη του ΔτΠ και θα διευκολύνουν την προσέγγιση τόσο περίπλοκων θεμάτων όπως η προστασία και η κυριότητα των δεδομένων·

6. να υλοποιηθούν δράσεις ανάπτυξης δεξιοτήτων στον χώρο των επιχειρήσεων υπό το πρίσμα της συνυπευθυνότητας. Είναι σκόπιμο να εξασφαλιστεί ότι η ασφάλεια και η προστασία της ιδιωτικής ζωής εκ σχεδιασμού και εξ ορισμού θα ενσωματώνονται στα προϊόντα και τις υπηρεσίες των ΤΠΕ, σύμφωνα με την αρχή της «υποχρέωσης φροντίδας» που υποστηρίζει ο νέος Κανονισμός για την ασφάλεια στον κυβερνοχώρο. Ως προς αυτό, η ΕΟΚΕ εκφράζει την ικανοποίησή της για την προβλεπόμενη κατάρτιση κωδίκων δεοντολογίας, συμπληρωματικά προς τα κανονιστικά μέτρα·

7. να ενθαρρυνθούν οι ευρωπαϊκές και διεθνείς πρωτοβουλίες τυποποίησης, ώστε να εξασφαλιστεί ότι τα συστήματα του ΔτΠ θα διαθέτουν τα βασικά χαρακτηριστικά, δηλαδή αξιοπιστία, ασφάλεια, διαθεσιμότητα, ανθεκτικότητα, συντηρησιμότητα και λειτουργία. Ειδικότερα, η τυποποίηση είναι ουσιαστικής σημασίας για την ταχεία υλοποίηση βιομηχανικών μεταποιητικών διεργασιών με υψηλό βαθμό ψηφιοποίησης.

8. να εξασφαλιστεί η οικονομικά προσιτή και υψηλής ποιότητας πρόσβαση στους χρήστες του ΔτΠ, ιδίως στις πλέον ευάλωτες ομάδες ή σε αυτές που ζουν στις πιο αραιοκατοικημένες περιοχές·

9. να προωθηθούν εκστρατείες ευαισθητοποίησης και εκπαιδευτικά προγράμματα για την ευκολότερη υιοθέτηση του ΔτΠ από τις επιχειρήσεις και τους καταναλωτές που να δίνουν τη δυνατότητα απόκτησης συγκεκριμένων δεξιοτήτων και ικανοτήτων[13], με ιδιαίτερη προσοχή στις ευάλωτες ομάδες και στην πολυμορφία·

10. να αναληφθούν πρωτοβουλίες στον χώρο της εκπαίδευσης ώστε να υπάρξει αποτελεσματική πρόληψη, δεδομένης της πρόωρης ένταξης των παιδιών στα ψηφιακά περιβάλλοντα·

12 ΕΕ C 197 της 8.6.2018, σ. 1.
13 ΕΕ C 434 της 15.12.2017, σ. 36.

11. να καταρτιστούν αναλύσεις και διαγνωστικές μελέτες σχετικά με τον αντίκτυπο του ΔτΠ στα νέα μοντέλα βιώσιμης παραγωγής και κατανάλωσης·

12. να εγγυηθούν την πλήρη εφαρμογή και αποτελεσματική χρήση των συστημάτων εναλλακτικής επίλυσης διαφορών εντός και εκτός διαδικτύου (ΗΕΚΔ και ΕΕΚΔ)·

13. να διασφαλίσουν την ύπαρξη, την υλοποίηση και την αποτελεσματική λειτουργία ενός συστήματος συλλογικής δράσης που θα επιτρέπει την διακοπή και την αποζημίωση όταν η χρήση του ΔτΠ προκαλεί ζημίες ή βλάβες συλλογικού χαρακτήρα, όπως προβλέπεται δυνάμει της «Νέας Συμφωνίας για τους Καταναλωτές».

Επιπλέον, η ΕΟΚΕ καλεί την Επιτροπή να αξιολογήσει τη νομοθεσία που συνδέεται άμεσα ή έμμεσα με το ΔτΠ και, όπου είναι απαραίτητο, να βελτιώσει τις ισχύουσες νομοθετικές πράξεις. Στο πλαίσιο αυτό, η New Deal for Consumers θα πρέπει, επίσης, να μελετήσει εκ του σύνεγγυς τόσο τις διασυνδεόμενες συσκευές όσο και τα δίκτυα και την ασφάλειά τους, καθώς και τα δεδομένα που συνδέονται με τις συσκευές.

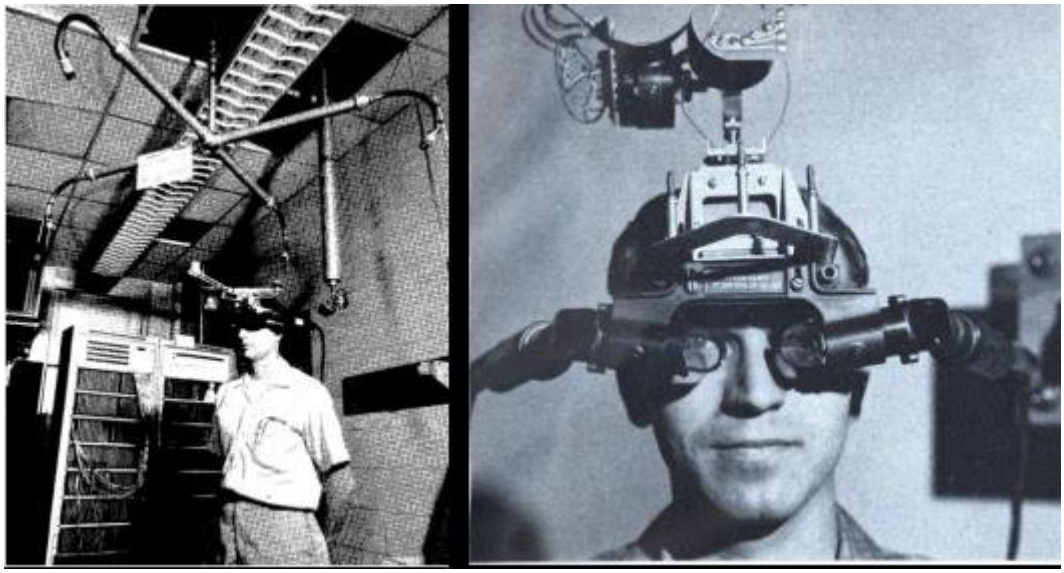
Τέλος, η ΕΟΚΕ τονίζει τη σημασία της ύπαρξης μηχανισμών συνεργασίας και συντονισμού μεταξύ των κρατών μελών για την αποτελεσματική και ομοιόμορφη εφαρμογή των προβλεπόμενων ρυθμίσεων, καθώς και για τις συμβάσεις που πρέπει να συνάψει η Ευρωπαϊκή Ένωση εκτός του εδάφους της, λόγω του τόπου όπου εδρεύουν οι επιχειρήσεις και οι πάροχοι, με ιδιαίτερη έμφαση στην ανταλλαγή βέλτιστων πρακτικών. Απαιτείται συντονισμός της διεθνούς πολιτικής για τις διασυνοριακές ροές δεδομένων, ώστε οι ενδιαφερόμενες χώρες να είναι σε θέση να θεσπίσουν και να εισαγάγουν εξίσου αυστηρούς κανόνες προστασίας στο εθνικό τους δίκαιο, τόσο το ουσιαστικό όσο και το δικονομικό.

Βρυξέλλες, 19 Σεπτεμβρίου 2018

Luca JAHIER

Πρόεδρος της Ευρωπαϊκής Οικονομικής και Κοινωνικής Επιτροπής

Παράρτημα Β΄



Η πρώτη συσκευή επαυξημένης πραγματικότητας - “Sword of Damocles” (Δαμόκλειος Σπάθη).

Βιβλιογραφία – Αρθρογραφία

Ακτύπης Σπυρίδων - Ηρακλής, Philippe Jougleux και Τατιάνα - Ελένη Συνοδινού, *«Ελευθερία έκφρασης δημοσιογράφων και σκιτσογράφων»*, Σάκκουλας, 2016.

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, *«Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679»*, ΔΙΤΕ (π. ΔΙΜΕΕ), *τ.* 1, 2018.

Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία, *«Προσωπικα Δεδομενα»*, Νομική Βιβλιοθήκη, 2016

Βεργής Νικόλαος, *«Μέτρηση της αποτελεσματικότητας και του κινδύνου των ομολόγων και των ομολογιακών δανείων ως μεθόδου κρατικής κι εταιρικής χρηματοδότησης. Η σύγχρονη διεθνής κι ελληνική πραγματικότητα»*, Πανεπιστήμιο Μακεδονίας, Τμήμα Λογιστικής και Χρηματοοικονομικής, 2010.

Βογιατζής Παναγιώτης, *«Η Ελευθερία της Έκφρασης στο Διαδίκτυο: ένας θαυμαστός, καινούριος κόσμος στη νομολογία του ΕΔΔΑ»*, ΔiΜΕΕ, τ. 3, 2016.

Γεωργιάδης Γεώργιος - Αλέξανδρος, *«Η σύναψη συμβάσεως μέσω του Διαδικτύου»*, Αντ. Ν. Σάκκουλα, Αθήνα- Κομοτηνή, 2003.

Γιαννόπουλος Γιώργος, *«Εισαγωγή στη Νομική Πληροφορική. Μια πρώτη προσέγγιση της σχέσης δικαίου & νέων τεχνολογιών»*, Νομική Βιβλιοθήκη, Αθήνα, 2018.

Γιαννόπουλος Γιώργος, *«Η ευθύνη των παρόχων υπηρεσιών στο Internet»*, Νομική Βιβλιοθήκη, Αθήνα, 2013.

Γιαννόπουλος Γεώργιος κλπ, *«Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR). Νομική Διάσταση και Πρακτική Εφαρμογή»*, επιμ. Λεωνίδας Κοτσαλής - Κωνσταντίνος Μενουδάκος, έκδοση 2η, Νομική Βιβλιοθήκη, 2021.

Δόνος Πελοπίδας, Φίλιππος Βασιλόγιαννης, Τάκης Βιδάλης, Βασίλης Βουτσάκης, Ηλίας Καστανάς, Γιάννης Κτιστάκις, Ευάγγελος Κ. Μάλλιος, Χαράλαμπος Σαββάκης, Ανδρέας Τάκης, Κωνσταντίνος Τσιτσελίκης και Δημήτρης Χριστόπουλος, *«Νέες τεχνολογίες και συνταγματικά δικαιώματα»*, Σάκκουλας, 2004.

Δουγαλής Ζήσης, *«Ενημέρωση και συναίνεση του ασθενούς: Πότε δεν απαιτείται – Δικαίωμα μη γνώσης»*, σε πρακτικά συνεδρίου «Τα νέα φάρμακα στην τεχνολογία», Άγιος Σάββας (υπό έκδοση).

Δρίτσας Σταμάτης, Γεώργιος Σωτηρόπουλος, Ευάγγελος Περάκης και Χριστίνα Λειβαδά, *«Το Δίκαιο της Λογιστικής»*, Νομική Βιβλιοθήκη, 2017.

Θεοδωράκης Νικόλαος και Γεώργιος Καλογεράκης, *«Blockchain: εφαρμογές, προοπτικές και προκλήσεις για το ελληνικό νομικό σύστημα. Ιδίως, οι εφαρμογές του στις έννομες σχέσεις ιδιωτικού δικαίου»*, ΔiΜΕΕ, τ.1, έτος 16ο, 2019.

Ιγγλεζάκης Ιωάννης, *«Δίκαιο πληροφορικής»*, 3η έκδοση, Σάκκουλας, Αθήνα, 2018.

Ιγγλεζάκης Ιωάννης, *«Δίκαιο πληροφορικής»*, 4η έκδοση, Σάκκουλας, Αθήνα, 2021.

Ιγγλεζάκης Ιωάννης (επιμ), *«Δίκαιο πληροφορικής & διαδικτύου»*, 2η έκδ., Σάκκουλας, Αθήνα, 2020.

Ιγγλεζάκης Ιωάννης, *«Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019)»*, Interactive Books, 2020.

Ιγγλεζάκης Ιωάννης, «Οδηγός σχετικά με τα Ονόματα Χώρου (Domain Names)», Θεσσαλονίκη, (2016).

Κάλλας Γιάννης, *«Η Κοινωνία της Πληροφορίας και ο νέος ρόλος των Κοινωνικών Επιστημών»*, εκδόσεις Νεφέλη, 2006.

Καλλιμόπουλος Γεώργιος, *«Το δίκαιο του χρήματος»*, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα, 1993.

Κανελλοπούλου-Μπότη Μαρία, *«Ιατρική ευθύνη για μη ενημέρωση ή πλημμελή ενημέρωση του ασθενούς κατά το ελληνικό και το αγγλοσαξωνικό δίκαιο»*, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα, 1999.

Κανελλοπούλου - Μπότη Μαρία, *«Το Δίκαιο της Πληροφορίας»*, Νομική Βιβλιοθήκη, Αθήνα, 2004.

Κανέλλος Λεωνίδας, *«Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο και στη δικαστική πρακτική»*, Νομική Βιβλιοθήκη, Αθήνα, 2021.

Κανέλλος Λεωνίδας, *«The GDPR Handbook»*, Νομική Βιβλιοθήκη, 2020.

Καράκωστας Ιωάννης Κ., *«Δίκαιο και Ίντερνετ»*, Π.Ν. Σάκκουλας, Αθήνα, 2009.

Καρύδα Μαρία, Σπύρος Κοκολάκης, Λίλιαν Μήτρου, Άννα-Μαρία Πισκοπάνη και Σπύρος Τάσσης, *«Facebook, Blogs και δικαιώματα»*, Σάκκουλας, Αθήνα, 2013.

Κιτσάκης Σταύρος, *«Τεχνητή Νοημοσύνη και συμβατική διαδικασία – Εισαγωγή στα βασικά προβλήματα»*, Εφαρμογές Αστικού Δικαίου και Πολιτικής Δικονομίας, 6/2018.

Κοτσαλής Λεωνίδας, *«Προσωπικά Δεδομένα. Ανάλυση – Σχόλια – Εφαρμογή»*, Νομική Βιβλιοθήκη, Αθήνα, 2016.

Μανιτάκης Αντώνης, *«Η επίδραση του Συντάγματος στις ιδιωτικές έννομες σχέσεις»*, Χαριστήρια Ι. Δεληγιάννη, Επιστημονική Επετηρίδα Τμήματος Νομικής, Θεσσαλονίκη, 1992.

Μήτρου Λίλιαν, *«Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων. Νέο δίκαιο - νέες υποχρεώσεις - νέα δικαιώματα»*, Σάκκουλας, Αθήνα, 2017.

Μήτρου Λίλιαν, *«Το δίκαιο στην κοινωνία της πληροφορίας»*, εκδόσεις Σάκκουλα, Αθήνα – Θεσσαλονίκη, 2002.

Μητσόπουλος Γεώργιος Γ., *«Το πρόβλημα της εννοίας του δικαιικού πλάσματος»*, Εκδόσεις Αντ.Ν. Σάκκουλα, 1998.

Μιχαηλάκη Αναστασία, *«Επαυξημένη ή Ενισχυμένη Πραγματικότητα (mixed or augmented reality). Εφαρμογές της και αντιμετώπισή της απο την πλευρά του δικαίου»*, 2014.

Μπουχάγιαρ Γιώργος, *«Το μονοπώλιο της ανθρώπινης νοημοσύνης. (Πρωτότυπα έργα αναζητούν δημιουργό)»*, ΔιΜΕΕ, *τ.* 4, 2016.

Παναγοπούλου – Κουτνατζή Φερενίκη, *«Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: Σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)»*, ΔιΜΕΕ, τ. 4, 2013.

Παναγοπούλου – Κουτνατζή Φερενίκη, *«Διαδίκτυο των πραγμάτων και προστασία της ιδιωτικότητας»*, ΔιΜΕΕ, τ. 3, 2014.

Παναγοπούλου – Κουτνατζή Φερενίκη, *«Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ. Εισαγωγή και Προστασία Δικαιωμάτων»*, Σάκκουλας, Αθήνα, 2018.

Παναγοπούλου-Κουτνατζή Φερενίκη, *«Οι ιστότοποι Κοινωνικής Δικτυώσεως»*, Σάκκουλας, 2010.

Παντελίδου Καλλιρρόη Δ., *«Γενικό Ενοχικό Δίκαιο»*, Νομική Βιβλιοθήκη, Αθήνα, 2019.

Παπαστάμου Στάμος, Γεράσιμος Προδρομίτης, Βασίλης Γ. Παυλόπουλος, *«Κοινωνική Σκέψη, Νόηση και Συμπεριφορά. 29 Έλληνες Κοινωνικοί Ψυχολόγοι ανα-κρίνουν την επιστήμη τους»*, Πεδίο, 2010.

Ρόκας Ιωάννης, *«Εισαγωγή στο δίκαιο των εταιριών του εμπορικού δικαίου»*, 6η έκδοση, Νομική Βιβλιοθήκη, Αθήνα, 2019.

Σαμαράς Αθανάσιος Ν., Εμμανουήλ Τάκας και Βάλια Καϊμάκη, *«Από την Κυβερνοασφάλεια στα Fake News. Μέσα, Μηνύματα, Στρατηγικές. Βιβλίο Συνόψεων 7ου Επιστημονικού Συνεδρίου»*, Εργαστήριο Στρατηγικής Επικοινωνίας και Μέσων Ενημέρωσης, 2018.

Σταματούδη Ειρήνη (επιστημονική επιμέλεια), *«Δημοσιογράφοι και Εκδότες, Ζητήματα πνευματικής ιδιοκτησίας»*, Σάκκουλας, Αθήνα, 2009.

Σταμέλος Χ., *«Το δικαίωμα της δημοσιότητας (right of publicity) του επαγγελματία αθλητή στις ΗΠΑ»*, Δίκαιο Μέσων Ενημέρωσης & Επικοινωνίας, Τεύχος 1, Ιανουάριος - Φεβρουάριος – Μάρτιος, 2009.

Συνδουκάς Δημήτριος, *«Συστήματα Πολυμέσων, Ενότητα 10: Εικονική πραγματικότητα»*, Τμήμα Διοίκησης Επιχειρήσεων (Γρεβενά), 2013.

Λύρας-Χατζής Κωνσταντίνος, *«Η παράνομη δημοσιογραφική έρευνα στη νεότερη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου»*, ΠΜΣ στην «Επικοινωνία και τα Μέσα Μαζικής Ενημέρωσης», Σχολή Οικονομικών και Πολιτικών Επιστημών, Τμήμα Επικοινωνίας και Μέσων Μαζικής Ενημέρωσης, 2019.

Χριστοδούλου Κων/νος, *«Ηλεκτρονικά έγγραφα και ηλεκτρονική δικαιοπραξία. Μετά τις νέες κοινοτικές ρυθμίσεις»*, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2001.

Χρυσανθάκης Χαράλαμπος, *«Εισηγήσεις Συνταγματικού Δικαίου»*, Νομική Βιβλιοθήκη, Αθήνα 2007.

Χρυσόγονος Κώστας και Σπύρος Βλαχόπουλος, *«Ατομικά και Κοινωνικά Δικαιώματα»*, 4η έκδοση, Νομική Βιβλιοθήκη, Αθήνα, 2017.

Hess Burkhard, Σπυρίδων Β. Βλαχόπουλος, Λίλιαν Μήτρου, Βιργινία Τζώρτζη, Χρίστος Γεραρής, Κωνσταντίνος Μενουδάκος και Βασίλειος Σκουρής, *«Προστασία των δεδομένων προσωπικού χαρακτήρα. Εξελίξεις ενόψει της θέσης σε εφαρμογή του νέου Γενικού Κανονισμού ΕΕ 2016/679»*, Σάκκουλας, Αθήνα, 2018.

«Augmented Reality: Hearing Before the US Senate Committee on Commerce, Science, and Transportation», 114th Cong, 2016.

«Mirror Worlds: The Universe in a Box?», (IN)VISIBLE, Springer, Vienna, 2008.

«The Future of the Securities and Exchange Commission in a Changing World», The Center for Strategic and International Studies, CreateSpace Independent Publishing Platform, Washington DC, 2015.

«The Rule of Law in the Technological Age Challenges and opportunities for the EU», ACELG's Annual Conference 2016.

Adhami Saman, Giancarlo Giudici και Stefano Martinazzi, *«Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings»*, Journal of Economics and Business, 2018.

Aldridge Judith και David Décary-Hétu, *«Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation»*, Ohio State Public Law Working Paper No. 314, 2014.

Anscombe G.E.M., *«Modern moral philosophy»*, Philosophy Vol. 33/124, Cambridge University Press, 1958.

Antonikova Nika, *«Real Taxes on Virtual Currencies: What Does the IRS Say?»*, Virginia Tax Review, Vol. 34/ 3, 2014.

Arun Chinmayi, *«AI and the Global South: Designing for Other Worlds»*, (2019), σε Markus D. Dubber, Frank Pasquale και Sunit Das (eds.), The Oxford Handbook of Ethics of AI, Oxford University Press.

Arena Fox, D. και J.N. Bailenson, *«Virtual Reality: A survival guide for the social scientist»*, Journal of Media Psychology Theories Methods and Applications, Vol. 21/ 3, 2009.

Atsalakis George , Ioanna Atsalaki, Fotis Pasiouras και Konstantinos D. Zopounidis, *«Bitcoin prices forecasting with neuro-fuzzy techniques»*, European Journal of Operational Research, Vol. 276/ 2, 2019.

Baeza-Yates Ricardo, *«Data and algorithmic bias in the web»*, Proceedings of the 8th ACM Conference on Web Science, 2016.

Bagheri Roya, *«Virtual Reality: The Real Life Consequences»*, 17 UC Davis Business Law Journal, Vol. 17/1, 2016.

Baldwin J., *«In Digital We Trust: Bitcoin Discourse, Digital Currencies, and Decentralized Network Fetishism»,* Palgrave Communications, Vol. 4/ 1, 2018.

Bathaee Yavar, *«The artificial intelligence black box and the failure of intent and causation»*, Harvard Journal of Law & Technology, Vol. 31/ 2 2018.

Bayamlioglu Emre, Irina Baraliuc, Liisa Albertha Wilhelmina Janssens και Mireille Hildebrandt, *«Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen»*, Amsterdam, Amsterdam University Press, 2018.

Beer και B. Weber, *«Bitcoin – The Promise and Limits of Private Innovation in Monetary and Payment Systems»*, Monetary Policy and the Economy, Q4/2014, 2015.

Bell Marc W., *«Toward a Definition of Virtual Worlds»,* Journal of Virtual Worlds Research, Vol. 1 / 1, 2008.

Bennett Moses Lyria, *«Why Have a Theory of Law and Technological Change?»*, Minnesota Journal of Law, Science & Technology, Vol. 8/ 2, 2007.

Bicchieri Cristina, *«The Grammar of Society: The Nature and Dynamics of Social Norms»*, Cambridge University Press, Cambridge, UK, 2006.

Blitz Marc Jonathan, *«The Freedom Of 3d Thought: The First Amendment In Virtual Reality»*, Cardozo Law Review, Vol. 30/ 3, 2008.

Boddington David, *«Radio-controlled Model Aircraft»*, The Crowood Press Ltd, 2004.

Bodo B., N Helberger, K Irion, K Zuiderveen Borgesius, J Moller, B van de Velde, N Bol, B van Es και C de Vreese, *«Tackling the Algorithmic Control Crisis-the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents»*, Yale Journal of Law and Technology, Vol. 19/ 1, 2018.

Bogosian Rob και Charlene Rousseau, *«How and Why Millennials are Shaking Up Organizational Cultures»*, Rutgers Business Review, Vol. 2/ 3, 2017.

Bonnell Bruno και Mady Delvaux-Stehres, *«Comparative Handbook: Robotic Technologies law»*, Editions Larcier, 2016.

Bouchagiar George, *«Collective Management Organizations as Fiduciaries and Blockchains's Potential for Copyright Management»*, Journal of the Copyright Society of the USA, Vol.66/ 2, 2019.

Brame Max και Miltiadis Petridis, *«Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV»*, Springer-Verlag, 2016.

Bratspies Rebecca M., *«Cryptocurrency and the Myth of the Trustless Transaction»*, 25 Mich. Telecomm. & Tech. L. Rev. 1 (2018).

Bresett Marc, *«Bitcoin: What You Need To Know About The Cryptocurrency»*, independently published, 2017.

Brill Hillary και Scott Jones, *«Little Things And Big Challenges: Information Privacy And The Internet Of Things»*, American University Law Review, Vol. 66, 2017.

Brożek Bartosz και Marek Jakubiec, *«On the legal responsibility of autonomous machines»*, Artificial Intelligence and Law, Vol. 25/ 3, 2017.

Bryson Joanna, Mihailis Diamantis και Thomas D, *«Grant, of, for, and by the People: The Legal Lacuna of Synthetic Persons»*, Artificial Intelligence & Law, University of Cambridge Faculty of Law Research Paper No. 25/ 5, 2018.

Calo Ryan, *«Robotics and the Lessons of Cyberlaw»*, California Law Review, Vol. 103/ 3, 2015.

Camp Bryan, *«The Play's The Thing: A Theory of Taxing Virtual Worlds»*, Hastings Law Journal, Vol. 59/ 1, 2007.

Caporale Guglielmo Maria και Alex Plastun, *«Price Overreactions in the Cryptocurrency Market»*, CESifo Working Paper Series No. 6861, 2018.

Castro Daniel και Alan McQuinn, *«The Privacy Panic Cycle: A Guide to Public Fears about New Technologies»*, Information Technology and Innovation Foundation, Washington, DC, 2015.

Čerka Paulius, Jurgita Grigienė και Gintarė Sirbikytė, *«Is it possible to grant legal personality to artificial intelligence software systems?»*, Computer Law & Security Review, Vol. 33/5, 2017.

Chen Matthew και Anton Badev, *«Bitcoin: Technical Background and Data Analysis»*, FEDS Working Paper No. 2014-104, 2014.

Christopher M., *«Why on Earth Do People Use Bitcoin?»*, Business & Bankruptcy L.J., Forthcoming, 2014.

Coglianese Cary και David Lehr, *«Transparency and algorithmic governance»*, Administrative Law Review, Vol. 71/ 1, 2019.

Conway Meredith R., *«Money, Money, Money; It's a Rich Man's World: Making the Corporate Tax Fair»*, 17 J. Bus. L., 2015.

Crotty Shane, *«The Aerial Dragnet: A Drone-ing Need for Fourth Amendment Change»*, Valparaiso University Law Review, Vol. 49/ 1, 2014.

Cummings James J. και Jeremy N. Bailenson, *«How Immersive Is Enough? A Meta-Analysis of the Effect of Immersive Technology on User Presence»*, Media Psychology, Vol. 19/ 2, 2015.

Curri Granit, *«Intellectual Property Law – Age of Internet»*, Academic Journal of Interdisciplinary Studies, Vol 5/ 3, MCSER Publishing, Rome-Italy, 2016.

Davenport Nikole, *«Smart Washers May Clean Your Clothes, but Hacks Can Clean out Your Privacy, and Underdeveloped Regulations Could Leave You Hanging on a Line»*, 32 J. Marshall J. Info. Tech. & Privacy L. 259, 2016.

Davies Glyn και Duncan Connors, *«A History of Money»*, University of Wales Press; 4th Edition, 2016.

Demitriadou Eleni, Kalliopi - Evangelia Stavroulia και Andreas Lanitis, *«Comparative evaluation of virtual and augmented reality for teaching mathematics in primary education»*, Education and Information Technologies, Vol. 25, 2020.

Diamantis Mihailis, *«Algorithms Acting Badly: A Solution from Corporate Law»*, 89 George Washington Law Review, (forthcoming 2020), U Iowa Legal Studies Research Paper No. 2020-12.

Diamantis Mihailis, *«The Extended Corporate Mind: When Corporations Use AI to Break the Law»*, 97 North Carolina Law Review, 2020.

Lilian Edwards και Michael Veale, *«Enslaving the algorithm: from a «right to an explanation» to a «right to better decisions»?»*, IEEE Security and Privacy Magazine, 2018.

Edwards Lilian και Michael Veale, *«Slave to the algorithm? Why a «right to an explanation» is probably not the remedy you are looking for»*, Duke Law and Technology Review, 16/1, 2017.

Emord Jonathan W., *«Freedom, Technology, and the First Amendment»*, Harvard Journal of Law & Technology, Vol. 5, 1992.

Fairfield Joshua, *«Mixed Reality: How the Laws of virtual worlds govern everyday life»*, Berkeley Technology Law Journal, Vol. 27/ 55, 2012.

Farringer Deborah R., *«Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals»*, Seattle University Law Review, Vol. 40, Belmont University College of Law Research Paper No. 2017-35, 2017.

Finck Michèle, *«Blockchains and Data Protection in the European Union»*, Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 2017.

Fotios Fitsilis, *«Imposing Regulation on Advanced Algorithms»*, Springer, 2019.

Floridi Luciano, *«Translating principles into practices of digital ethics: Five risks of being unethical»*, Philosophy & Technology, Vol. 32, 2019.

Fogg Brian Jeffrey, *«Persuasive Technology: Using Computers To Change What We Think And Do, Ubiquity»,* Vol. 2002 December, Association for Computing Machinery New York, NY, United States, 2002.

Franks Mary Anne, *«The Desert of the Unreal: Inequality in Virtual and Augmented Reality»*, UC Davis Law Review, Vol. 51, University of Miami Legal Studies Research Paper No. 17-24, 2017.

Gershowitz Adam M., *«Google Glass While Driving»*, William & Mary Law School Research Paper No. 09-280, 2014.

Gikay Asress Adimi, *«Regulating Decentralized Cryptocurrencies Under Payment Services Law: Lessons from European Union Law»*, 9 Case W. Res. J.L. Tech. & Internet 1, 2018.

Girvan Carina, *«What is a virtual world? Definition and classification»*, Educational Technology Research and Development, Vol. 66, 2018.

Gless Sabine, Emily Silverman και Thomas Weigend, *«If Robots cause harm, Who is to blame? Self-driving Cars and Criminal Liability»*, New Criminal Law Review: In International and Interdisciplinary Journal, Vol. 19/ 3, 2016.

Gold Sara, *«When Pokémon GO(es) Too Far: Augmented Reality and Tort Law»*, Whittier Law Review, Vol. 38, 2018.

Greene Daniel, Anna Lauren Hoffmann και Luke Stark, *«Better, nicer, clearer, fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning»*, σε Proceedings of the 52nd Hawaii international conference on system sciences, Maui, Hawaii, 2019.

Grinberg Reuben, *«Bitcoin: An Innovative Alternative Digital Currency»*, Hastings Science & Technology Law Journal, Vol. 4, 2011.

Hacker Philipp, *«Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law»*, Common Market Law Review, Vol. 55/ 4, 2018.

Hagendorff Thilo, *«The ethics of AI ethics. An evaluation of guidelines»*, Minds and Machines, Vol. 30, 2020.

Hajian Sara, Francesco Bonchi και Carlos Castillo, *«Algorithmic bias: From discrimination discovery to fairness-aware data mining»*, KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, California, 2016.

Hegadekatti Kartik και S. G. Yatish, *«Examining Taxation of Fiat Money and Bitcoins vis-a-vis Regulated Cryptocurrencies»*, International Finance eJournal, Vol. 8/ 117, 2016.

Henckaerts Jean-Marie, *«Μελέτη για το Εθιμικό Διεθνές Ανθρωπιστικό Δίκαιο. Μια Συνεισφορά στην κατανόηση και το σεβασμό των κανόνων Δικαίου των Ενόπλων Συρράξεων»*, Ευρωπαϊκό Κέντρο Έρευνας και Κατάρτισης Δικαιωμάτων του Ανθρωπου και Ανθρωπιστικής Δράσης Παντείου Πανεπιστημίου , Αθήνα 2007.

Hildebrandt Mireille και Jeanne Gaakeer, *«Human Law and Computer Law: Comparative Perspectives»*, Ius Gentium: Comparative Perspectives on Law and Justice, Vol 25, Springer, Dordrecht.

Hobson Anne, *«Reality Check: The Regulatory Landscape for Virtual and Augmented Reality»*, Policy Study 69, R Street Institute, Washington, DC, 2016.

Hunter Dan και Jake Goldenfein, *«Blockchains, Orphan Works, and the Public Domain»*, Columbia Journal of Law & the Arts, Vol. 41, No. 1, 2017.

Ioannides Isabelle και Simona Guagliardo, *«EU-US Trade and Investment Relations: Effects on Tax Evasion, Money Laundering and Tax Transparency In-Depth Analysis»*, Reference No: PE 598.602. Brussels: European Parliamentary Research Service, 2017.

International Bar Association, Global Employment Institute, *«Artificial Intelligence and Robotics and Their Impact on the Workplace»*, Απρίλιος 2017.

Iwamura Mitsuru, Yukinobu Kitamura, Tsutomu Matsumoto και Kenji Saito, *«Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money»*, Hitotsubashi Journal of Economics, vol 60/1, 2019.

Jansen Philip, Stearns Broadhead, Rowena Rodrigues, David Wright, Philip Brey, Alice Fox, Ning Wang, Owen King, Raja Chatila και Virginia Romano, SIENNA D4.1: State-of-the-art Review: AI and robotics, (2018).

Janssens Liisa, *«The Art of Ethics in the Information Society»*, Amsterdam University Press, 2016.

Jobin Anna, Marcello Ienca και Effy Vayena, *«The global landscape of AI ethics guidelines»*, Nature Machine Intelligence, Vol. 1/9, 2019.

Jones Brian Christopher, *«The Online/Offline Cognitive Divide: Implications for Law»*, SCRIPT-ed, Vol. 13/ 1, 2016.

Jones Meg Leta, *«Does Technology Drive Law? The Dilemma Of Technological Exceptionalism In Cyberlaw»*, Journal Of Law, Technology & Policy, No. 2, Technological Exceptionalism In Cyberlaw, 2018.

Kanellopoulou- Bottis Maria, *«Disclosing Software Vulnerabilities, Internet Security: Hacking, Counterhacking and Society»*, Jones and Bartlett Publishers, 2006.

Kang Jerry και Dana Cuff, *«Pervasive Computing: Embedding the Public Sphere»*, 62 Wash. & Lee L. Rev. 93, 2005.

Kelemen Bence Kis, *«Targeted Killings and Human Rights Law»*, Hungarian Yearbook of International Law and European Law, 2018.

Kelly Kevin, *«The Inevitable: Understanding the 12 Technological Forces That Will Shape our future»*, Penguin Books, N.Y., 2016.

Kerawalla Lucinda, Rosemary Luckin, Simon Seljeflot και Adrian Woolard, *«Making it real: exploring the potential of augmented reality for teaching primary school science»*, Virtual-Reality, Vol. 10, 2006.

Kesan Jay P. και Carol M. Hayes, *«Self Defense in Cyberspace: Law and Policy»*, TPRC 2011, Illinois Public Law Research Paper No. 11-16, Illinois Program in Law, Behavior and Social Science Paper No. LBSS12-08 (2011).

Keum Do Hee, Su-Kyoung Kim, Jahyun Koo, Geon-Hui Lee1, Cheonhoo Jeon, Jee Won Mok, Beom Ho Mun, Keon Jae Lee, Ehsan Kamrani, Choun-Ki Joo, Sangbaie Shin, Jae-Yoon Sim, David Myung, Seok Hyun Yun, Zhenan Bao και Sei Kwang Hahn, *«Wireless smart contact lens for diabetic diagnosis and therapy»*, Science Advances, Vol. 6/ 17 (2020) .

Kondo Kazuhiro, *«Multimedia Information Hiding Technologies and Methodologies for Controlling data»*, IGI Global, 2012.

Kotsios Andreas, *«Privacy in an Augmented Reality»*, International Journal of Law and Information Technology, Vol. 23/ 2, 2015.

Kretzmer David, *«Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Self-Defence»*, European Journal of International Law, 2005.

Kreuser Jérôme και Didier Sornette, *«Bitcoin Bubble Trouble»,* Forthcoming in Wilmott Magazine, Swiss Finance Institute Research Paper No. 18-24, 2018.

Krishnan Armin, *«Killer robots: Legality and ethicality of autonomous weapons»*, Ashgate Publishing, Ltd., 2009.

Langenderfer Jeff, *«End-User License Agreements: A New Era of Intellectual Property Control»*, Journal of Public Policy & Marketing, Vol. 28/ 2, Sage Publications, Inc (2009): 202-211.

Lastowka F. Gregory και Dan Hunter, *«The Laws of the Virtual Worlds»*, California Law Review*,* Vol. 92/ 1, 2004.

Lederman Leandra, *«Stranger Than Fiction: Taxing Virtual Worlds»*, New York University Law Review, Vol. 82, 2007.

Lee David Kuo Chuen, Guo Li Και Wang Yu, *«Cryptocurrency: A new investment opportunity?»*, Journal of Alternative Investments*,* Vol. 20/3, 2018.

Lee Larissa, *«New Kids on the blockchain: How Bitcoin's Technology Could Reinvent the Stock Market»*, Hastings Business Law Journal, Vol. 12/ 2, University of Utah College of Law Research Paper No. 138, 2016.

Lee Newton, *«Encyclopedia of Computer Graphics and Games»*, Springer, 2015.

Lemley Mark και Eugene Volokh, *«The Real Law of Virtual Reality»*, University of California, Davis, Vol. 51, 2017.

Lepri Bruno, Nuria Oliver, Emmanuel Letouzé, Alex Pentland και Patrick Vinck, *«Fair, transparent, and accountable algorithmic decision-making processes»*, Philosophy & Technology, Vol. 31/ 4, 2018.

Levitin Adam J., *«Pandora's Digital Box: The Promise and Perils of Digital Wallets»*, University of Pennsylvania Law Review, Vol. 166, 2017.

Li Tiffany, *«Pokémon Go and the Law: Privacy, Intellectual Property, and Other Legal Concerns»*, Yale Law School - Information Society Project, 2016.

Lin Patrick, Keith Abney και George A. Bekey, *«Robot Ethics: The Ethical and Social Implications of Robotics»*, 2012.

Low Kelvin F.K. και Ernie G. S. Teo, *«Legal Risks of Owning Cryptocurrencies»*, Reed Elsevier, Handbook of blockchain, Digital Finance, and Inclusion, Vol. 1, 1st Edition, Singapore Management University School of Law Research Paper No. 23/2016, 2018.

Lu Lerong, *«Bitcoin: Speculative Bubble, Financial Risk and Regulatory Response»*, Butterworths Journal of International Banking and Financial Law, Vol. 33/3, 2018.

Mallick Samuel, Note, *«Augmenting Property Law: Applying the Right to Exclude in the Augmented Reality Universe»*, Vanderbilt Journal of Entertainment and Technology Law, Vol. 19/ 4, Vanderbilt University, School of Law, 2017.

Maloney Michael, *«Guide To Investing in Gold & Silver: Protect Your Financial Future»*, WealthCycle Press ,2015.

Magkos Emmanouil, Panayiotis Kotzanikolaou, *«Enhancing Privacy-Preserving Access Control for Pervasive Computing Environments»*, σε «The Second International ICST Conference on Security and Privacy in Mobile Information and Communication Systems - MOBISEC 2010», Catania, Sicily. LNICST, Springer, 2010.

Martin Felix, *«Money: The Unauthorized Biography--From Coinage to Cryptocurrencies»*, Vintage, Reprint Edition, 2015.

McGinnis John O. και Kyle Roche, *«Bitcoin: Order without Law in the Digital Age»*, Northwestern Public Law Research Paper No. 17-06, 2017.

Melzer Nils, *«Human Rights Implications of the Usage of Drone and Unmanned Robots in Warfare»*, European Parliament, Directorate-General for External Policies of the Union, Directorate B, Policy Department, Study, 2013.

Mishra, S., P., Jacob, V., Radhakrishnan, S., *«Bitcoin Mining and Its Cost»*, 2017.

Mittelstadt Brent, *«Principles alone cannot guarantee ethical AI»*, Nature Machine Intelligence, Vol. 1, 2019.

Moses Lyria Bennett, *«Agents of Change: How the Law Copes with Technological Change»*, Griffith Law Revew, Vol. 20/ 4, 2011.

Muller Vincent C. και Thomas W. Simpson, *«Killer robots: Regulate, don't ban»*, University of Oxford, Blavatnik School of Government Policy Memo, 2014.

Nakar Sharon και Dove Greenbaum, *«Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy»*, 23 B.U School of Law, Journal of Science & Technology Law 88, 2017.

Nelson Bill, *«Children's Connected Toys: Data Security & Privacy Concerns»*, Committee On Commerce, Science & Transportation, Office of Oversight and Investigations, Minority Staff Report, 2016.

Neumann John von και Oskar Morgenstern, *«Theory of Games and Economic Behaviour»*, Princeton University, 1953.

Nica Octavian, Karolina Piotrowska και Klaus Reiner Schenk-Hoppé, *«Cryptocurrencies: Economic Benefits and Risks»*, University of Manchester, FinTech working paper no. 2, 2017.

Nwaneri Crystal, *«Ready Lawyer One: Legal Issues in the Innovation of Virtual Reality»*, Harvard Journal of Law & Technology, Vol. 30/ 2, (2017): 601-627.

O'Dorisio Roderick, *«Torts in the Virtual World»*, 94 Denver Law Revew Online 1, 1 2017.

Olleros F. Xavier και Majlinda Zhegu, *«Blockchain Technology: Principles and Applications»*, Research Handbook on Digital Transformations, Edward Elgar, 2016.

Ostbye Peder, *«The Case for a 21 Million Bitcoin Conspiracy»*, Journal of Financial Transformation, Capco Institute, Vol. 48, 2018.

Peppet Scott R., *«Regulating the Internet of Things: First Steps toward Managing Discrimination»*, Privacy, Security, and Consent, Texas Law Review, Vol. 93/ 1, 2014.

Pevey Madison, *«Cover Your Ash: Upholding the Physical Entry Requirement for Trespass in the Age of Pokémon Go»*, 44 Vermont Law Review (fall issue), 2019.

Pfeifer Rolf και Christian Scheier, *«Understanding Intelligence»*, https://mitpress.mit.edu/books/understanding-intelligence, 1999.

Phillips Whitney, *«This Is Why We Can't Have Nice Things: Mapping the Relationship between Online Trolling and Mainstream Culture»*, Cambridge, MA: MIT Press, 2015.

Pieters Gina C., *«The Potential Impact of Decentralized Virtual Currency on Monetary Policy»*, Federal Reserve Bank of Dallas, Globalization and Monetary Policy Institute Annual Report, 2016.

Raji Inioluwa Deborah, Timnit Gebru, Margaret Mitchell, Joy Buolamwini, Joonseok Lee και Emily Denton, *«Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing»*, AIES '20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 2020.

Ramirez Edith, *«The Privacy Challenges of Big Data: A View from the Lifeguard's Chair»*, Technology Policy Institute Aspen Forum, Aspen, CO, 2013.

Rogers Jacob, *«Note, A Passive Approach to Regulation of Virtual Worlds»*, 76 George Washington Law Review, 2008.

Rohr Jonathan and Aaron Wright, *«Blockchain-Based Token Sales, Initial Coin Offerings and the Democratization of Public Capital Markets»*, Cardozo Legal Studies Research Paper No. 527, University of Tennessee Legal Studies Research Paper No. 338, 2017.

Rudesill Dakota, James Caverlee και Daniel Sui, *«The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box»*, Woodrow Wilson International Center for Scholars, STIP 03, 2015.

Saifedean Ammous, *«Can Cryptocurrencies Fulfil the Functions of Money?»*, Columbia University, Center on Capitalism and Society, Working Paper No. 92, 2016.

Savelyev Alexander Ivanovitch, *«Copyright in the blockchain era: promises and challenges»*, Computer Law & Security Review, Vol. 34/3, 2018.

Schlosser Ann E., *«Learning Through Virtual Product Experience: The Role of Imagery on True Versus False Memories»*, Journal of Consumer Research, Vol. 33/ 3, 2006.

Shackelford Scott J., *«Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations»*, Seton Hall Journal of Diplomacy and International Relations, in press, 2019.

Shackelford Scott και Scott O. Bradner, *«Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything»*, Hastings Law Journal, Kelley School of Business Research Paper No. 18-60, 2021.

Shakow David J., *«The Tax Treatment of Tokens: What Does it Betoken?»*, Tax Notes, Vol. 156, U of Penn, Inst for Law & Econ Research Paper No. 17-45, 2017.

Shekhar Shashi, Hui Xiong και Xun Zhou, *«Encyclopedia of GIS»*, Springer, Boston, MA, 2008.

Shim Jaeeun και Ronald C. Arkin, *«A taxonomy of robot deception and its benefits in HRI»*, 2013 IEEE International Conference on Systems, Man, and Cybernetics. IEEE, 2013.

Skorup Brent και Connor Haaland, *«How Drones Can Help Fight the Coronavirus»*, Mercatus Center Research Paper Series, Special Edition Policy Brief, 2020.

Smith Michael L., *«Regulating Law Enforcement's Use of Drones: The Need for State Legislation»*, Harvard Journal on Legislation, Vol. 52, 2015.

Solum Lawrence B, *«Legal personhood for artificial intelligences»*, North Carolina Law Review, Vol. 70/ 4 (1992): 1231- 1287.

Steuer Jonathan, *«Defining Virtual Reality: Dimensions Determining Telepresence»*, Social Responses to Communication Technologies Paper 104, Stanford University Department of Communication, Stanford, CA, 1993.

Stevenson Andrea, *«Two Virtual Reality Pilot Studies for the Treatment of Pediatric CRPS Pain»*, Medicine, Vol. 16/ 8, 2015.

Stonehem Bill, *«Satoshi Nakamoto: The Bitcoin Founder»*, First Rank Publishing 2016.

Sunstein Cass R., *«Social Norms and Social Roles»*, Columbia Law Review 96, 1996.

Surden Harry, *«Machine Learning and Law»*, Washington Law Review, Vol. 89/ 1, 2014.

Tabusca Alexandru, *«Augmented Reality – A Possible Game-Changer in Education»*, National Strategies Observer No.2/Vol.1, 2015.

Terry Nicolas P, Chad S. Priest και Paul Szotek, *«Google Glass and Health Care: Initial Legal and Ethical Questions»*, Indiana University Robert H. McKinney School of Law Research Paper, 2015.

Terry Nicolas P., *«Physicians and Patients Who Friend or Tweet: Constructing a Legal Framework for Social Networking in a Highly Regulated Domain»*, 43 Induiana Law Review 285, 2010.

Thacker Scott και Marc D. Griffiths, *«An Exploratory Study of Trolling in Online Video Gaming»* International Journal of Cyber Behavior, Psychology and Learning 2, no. 4, 2012.

Thierer Adam, Camp, J., *«Permissionless Innovation and Immersive Technology: Public Policy for Virtual and Augmented Reality»*, Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, 2017.

Thierer Adam D., *«Privacy Law's Precautionary Principle Problem»*, Maine Law Review 66, no. 2, 2014.

Thierer Adam D., *«The Pursuit of Privacy in a World Where Information Control Is Failing»*, Harvard Journal of Law and Public Policy 36, no. 2, 2013.

Tsohou Aggeliki, Manos Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni και Beatriz Gallego-Nicasio Crespo, *«Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform»*, Information & Computer Security, Emerald Insight (υπό έκδοση), 2020.

Tran Cuong , Karlin Bark και Victor Ng-Thow-Hing, *«A Left-Turn Driving Aid Using Projected Oncoming Vehicle Paths with Augmented Reality»*, σε Proceedings of the 5th International Conference on Automotive User Interfaces and Interactive Vehicular Applications, New York, Association for Computed Machinery, 2015.

Trautman Lawrence J., *«Cybersecurity: What About U.S. Policy?»*, Journal of Law, Technology and Policy, Vol. 2015, 341 (2015).

Trautman Lawrence J., *«Is Disruptive blockchain Technology the Future of Financial Services?»*, 69 The Consumer Finance Law Quarterly Report 232, 2016.

Trautman Lawrence J., *«Virtual Currencies; Bitcoin & What Now after Liberty Reserve»*, Silk Road, and Mt. Gox? Richmond Journal of Law and Technology, Vol. 20/ 4, 2014.

Wachter Sandra, Brent Mittelstadt και Luciano Floridi, *«Transparent, explainable, and accountable AI for robotics»*, Science Robotics, Vol. 2/ 6, 2017.

Wagner Gerhard, *«Robot Liability»*, Humboldt University School of Law; University of Chicago Law School, 2018.

Wagner Michael S., *«Google Glass: A Preemptive Look at Privacy Concerns»*, S. 11 Journal on Telecommunications & High Technology Law, 2013.

Wang Kelvin, *«Bitcoin: Everything You Need To Know: (blockchain and Cryptocurrency technologies, Internet Money Guide on Trading, Making and Mining, Digital Gold Rush)»*, CreateSpace Independent Publishing Platform, 2017.

Warren Samuel D. και Louis D. Brandeis, *«The Right to Privacy»*, Harvard Law Review 4, 1890.

Wheatley Spencer, Didier Sornette, Tobias Huber, Max Reppen, και Robert N. Gantner, *«Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model»*, Swiss Finance Institute Research Paper No. 18-22, 2018.

White Lawrence H., *«The Market for Cryptocurrencies»*, GMU Working Paper in Economics No. 14-45, 2014.

Witten Ian H., *«Data Mining: Practical Machine Learning Tools And Techniques»*, Morgan Kaufmann; 3rd Edition, 2011.

Yadin Gilad, *«Virtual Reality Intrusion»*, Willamette Law Review, Vol. 53/ 1, 2016.

Yadin Gilad, *«Virtual Reality Surveillance»*, Cardozo Arts & Entertainment Law Journal, Vol. 35/ 3, 2017.

Yannopoulos Georgios N., *«Real Rights in Virtual Worlds and Virtual Rights in a Real World»*, στο Συνέδριο: 5th International Conference on Information Law "Equity, integrity and beauty in information law and ethics", Ιόνιο Πανεπιστήμιο, Κέρκυρα, 2012.

Zhou Michael, Mark A.A.M. Leenders και Ling Mei Cong, *«Ownership in the virtual world and the implications for long-term user innovation success»*, Technovation, Vol. 78, 2018.

Ηλεκτρονική Αρθρογραφία

«Αντονι Γκίντενς: Επαναστατικό φαινόμενο η παγκοσμιοποίηση», (2007), διαθέσιμο σε https://m.naftemporiki.gr/story/155396 .

«Bitcoin: η αυταπάτη που θα μπορούσε να κατακτήσει τον κόσμο», (2017), διαθέσιμο σε https://tvxs.gr/news/kosmos/bitcoin-i-aytapati-poy-tha-mporoyse-na-kataktisei-ton-kosmo .

«Bitcoin: φλερτάρει τα 20.000$ το αόρατο κρυπτο-νόμισμα», (2017), διαθέσιμο σε https://indicator.gr/bitcoin-

«Crowdfunding σε απλά ελληνικά», (2014), διαθέσιμο σε http://www.itech4u.gr.

«Google Glass, εκπληκτική εφαρμογή που σας δείχνει trailers ταινιών κοιτώντας απλά τις αφίσες», (2014), διαθέσιμο σε https://www.techgear.gr/google-glass-preview-21812 .

«Από το Διαδίκτυο των Πραγμάτων στο Διαδίκτυο των Σκέψεων», (2019), διαθέσιμο σε https://www.kathimerini.gr/1036966/article/epikairothta/episthmh/apo-to-diadiktyo-twn-pragmatwn-sto-diadiktyo-twn-skeyewn .

«Αυτό είναι το έξυπνο σουτιέν της Microsoft!», (2013), διαθέσιμο σε https://www.inewsgr.com/61/afto-einai-to-exypno-soutien-tis-Microsoft.htm

«Αυτοκόλλητα μετατρέπουν σε οθόνη οποιοδήποτε παράθυρο και βιτρίνα», (2014), διαθέσιμο σε https://www.kathimerini.gr/life/technology/553161/aytokollita-metatrepoyn-se-othoni-opoiodipote-parathyro-kai-vitrina/

«Γερμανία: Θρίλερ στον κυβερνοχώρο με έναν νεκρό», (2020), διαθέσιμο σε https://www.kathimerini.gr/world/561084721/germania-thriler-ston-kyvernochoro-me-enan-nekro .

«Γυναίκα δέχεται κλήση για οδήγηση με τα Google Glasses», (2013), διαθέσιμο σε https://www.techgear.gr/woman-gets-ticket-for-driving-with-google-glass-21910 .

«Διαδίκτυο των Σκέψεων: Η νέα τάση στο Internet;», (2019) διαθέσιμο σε https://www.efsyn.gr/epistimi/epistimonika-nea/206150_diadiktyo-ton-skepseon-i-nea-tasi-sto-internet .

«Δικαστής με τεχνητή νοημοσύνη αποφασίζει για τον κατηγορούμενο», (2018), διαθέσιμο σε https://www.ethnos.gr/kosmos/1691_dikastis-me-tehniti-noimosyni-apofasizei-gia-ton-katigoroymeno .

ΕΔΔΑ, Ahmet Yildirm κατά Τουρκίας, 18-12-2012, παρ. 48, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Ashby Donald και λοιποί κατά Ηνωμένου Βασιλείου, 10-01-2013, παρ. 34, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Editorial Board of Pravoye Delo και Shtekel κατά Ουκρανίας, 05-05-2011, παρ. 63, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Jersild κατά Δανίας (τμήμα ευρείας σύνθεσης), 22-09-1994, παρ. 31. https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Masley κατά Ηνωμένου Βασιλείου, 10-05-2011, παρ. 129, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Niskasaari and Otavamedia Oy, κατά Φινλανδίας, 23-06-2015, παρ. 9 και 54-59, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Stoll κατά Ελβετίας, (Τμήμα ευρείας σύνθεσης), 10-12-2007, παρ. 104, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Sürek κατά Τουρκίας (No 1), (τμήμα ευρείας σύνθεσης), 08-07-1999, παρ. 62, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Times Newspapers Ltd, (nos 1 et 2) κατά Ηνωμένου Βασιλείου, 10-03-2009, παρ. 27, https://www.echr.coe.int/Pages/home.aspx?p=caselaw/HUDOC&c=.

ΕΔΔΑ, Times Newspapers Ltd, (nos 1 et 2).

«Εικονική αναπαράσταση της «Ναυμαχίας της Σαλαμίνας» από το Ίδρυμα Μείζονος Ελληνισμού», (2020), διαθέσιμο σε https://www.in.gr/2020/05/21/culture/texni/eikoniki-anaparastasi-tis-naymaxias-tis-salaminas-apo-idryma-meizonos-ellinismou/.

«Εμβόλιο κορονοϊού: Η τεχνητή νοημοσύνη έλυσε βιολογικό μυστήριο δεκαετιών», (2020), διαθέσιμο σε https://www.news247.gr/good-news/emvolio-koronoioy-i-techniti-noimosyni-elyse-viologiko-mystirio-dekaetion.9067074.html .

«Έρευνα: Η τεχνητή νοημοσύνη και το «Διαδίκτυο των Πραγμάτων» υιοθετείται όλο και περισσότερο οι επιχειρήσεις παγκοσμίως», (2020), διαθέσιμο σε https://www.fortunegreece.com/article/erevna-i-techniti-noimosini-ke-to-diadiktio-ton-pragmaton-iiothetite-olo-ke-perissotero-i-epichirisis-pagkosmios/ .

«Ευρωπαϊκό Δικαστήριο: Παραβίαση της ιδιωτικής ζωής η παρακολούθηση των emails εργαζομένου», (2017), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/eyropaiko-dikastirio-paraviasi-tis-idiotikis-zois-i-parakoloythisi-ton-emails-ergazomenoy .

Ευρωπαϊκό Κοινοβούλιο, Έκθεση με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής, (2015/2103(INL)), Επιτροπή Νομικών Θεμάτων, διαθέσιμο σε 27.1.2017.http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN .

Ευρωπαϊκό Κοινοβούλιο, Κοινή Πρόταση Ψηφίσματος σύμφωνα με το άρθρο 110, παράγραφοι 2 και 4, του Κανονισμού σχετικά με τη χρήση οπλισμένων τηλεκατευθυνόμενων αεροσκαφών (2014/2567(RSP)), διαθέσιμο σε http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+P7-RC-2014-0201+0+DOC+XML+V0//EN .

«Η Google επιστρέφει στα «έξυπνα» γυαλιά, χρόνια μετά το Google Glass, |εξαγοράζοντας τη North», (2020), διαθέσιμο σε https://www.naftemporiki.gr/story/1615173/h-google-epistrefei-sta-eksupna-gualia-xronia-meta-to-google-glass-eksagorazontas-ti-north.

«ΗΠΑ: Κήρυξη διαθήκης γραμμένης σε ταμπλέτα ως έγκυρης», (2013), διαθέσιμο σε https://lawnet.gr/law-news/dikeo-technologia/hpa-kiruxi-dia8ikis-grammenis-se-tampleta-os-egkuris/ .

«Η προκατάληψη και οι διακρίσεις μέσα από την κοινωνική ψυχολογία», (2016), διαθέσιμο σε https://socialpolicy.gr/2016/10/%CE%B7-%CF%80%CF%81%CE%BF%CE%BA%CE%B1%CF%84%CE%AC%CE%BB%CE%B7%CF%88%CE%B7-%CE%BA%CE%B1%CE%B9-%CE%BF%CE%B9-%CE%B4%CE%B9%CE%B1%CE%BA%CF%81%CE%AF%CF%83%CE%B5%CE%B9%CF%82-%CE%BC%CE%AD%CF%83%CE%B1-%CE%B1.html .

«Η Samsonite λανσάρει μία έξυπνη τσάντα ώμου που συνδέεται με το smartphone», (2020), διαθέσιμο σε https://m.naftemporiki.gr/story/1650134/h-samsonite-lansarei-mia-eksupni-tsanta-omou-pou-sundeetai-me-to-smartphone .

«Ιατρική εξέταση με το Google Glass», (2014), διαθέσιμο σε https://www.naftemporiki.gr/story/779540/iatriki-eksetasi-me-to-google-glass .

«Ισχυρό πλήγμα στην αξιοπιστία του Bitcoin - Έκλεισε το ανταλλακτήριο Mt Gox μετά την κλοπή 365 εκατ. ευρώ από hackers - «Ψάχνει λύση» ο CEO», (2014), διαθέσιμο σε www.bankingnews.gr.

«Μαγικά γυαλιά» από την Google», 2012, διαθέσιμο σε https://www.naftemporiki.gr/video/406415/magika-gualia-apo-tin-google .

«Με απλά λόγια: Τι είναι το 5G και πώς πρόκειται να αλλάξει τη ζωή μας;», (2018), διαθέσιμο σε https://www.epixeiro.gr/article/83575 .

«Ο δείκτης ευφυΐας των «έξυπνων» συσκευών», (2012), διαθέσιμο σε https://www.kathimerini.gr/economy/international/457788/o-deiktis-eyfy-as-ton-

«Ο επιχειρηματίας Κ. Ράιτ είναι ο δημιουργός του Bitcoin», διαθέσιμο σε https://www.naftemporiki.gr/finance/story/1099156/o-epixeirimatias-k-rait-einai-o-dimiourgos-tou-bitcoin .

«Ο θαυμαστός κόσμος του παιχνιδιού εικονικής πραγματικότητας», (2018), διαθέσιμο σε http://gadgetblog.gr/vr-in-gaming-o-thaymastos-kosmos-toy-paichnidioy-eikonikis-pragmatikotitas.

«Οι τεχνολογικές προβλέψεις του Eric Schmidt», (2014), διαθέσιμο σε https://www.fortunegreece.com/article/technologikes-provlepsis-tou-eric-schmidt.

«Παρουσίαση της νέας επένδυσης της Microsoft στην Ελλάδα από τον Πρωθυπουργό Κυριάκο Μητσοτάκη και τον Πρόεδρο της εταιρείας», Brad Smith, (2020), διαθέσιμο σε https://primeminister.gr/2020/10/05/24950 .

«Πώς μπορούμε να προβλέψουμε την κίνηση του bitcoin», (2019), https://www.brief.com.cy/blockchaincrypto/pos-mporoyme-na-problepsoyme-tin-kinisi-toy-bitcoin .

«Σύμβαση που αφορά στην προμήθεια Συστημάτων για Έξυπνη Αστυνόμευση (Smart Policing)», (2019), διαθέσιμο σε http://www.astynomia.gr/images/stories/2019/prokirikseis19/14122019anakoinosismartpolicing.pdf

«Τα κρυπτονομίσματα «επελαύνουν» και στην ελληνική πραγματικότητα», (2017), διαθέσιμο σε http://www.dealnews.gr/roi/item/219451#.XoTbgIgzZPY.

«Τεχνητή νοημοσύνη, β) Συμπεράσματα σχετικά με το συντονισμένο σχέδιο για την τεχνητή νοημοσύνη», (2019), διαθέσιμο σε https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/el/pdf .

«Τίτλοι τέλους για τα έξυπνα γυαλιά της Google», (2015), διαθέσιμο σε https://www.news247.gr/technologia/titloi-teloys-gia-ta-exypna-gyalia-tis-google.6319959.html.

«Το 2019 φεύγει, τα νανορομπότ έρχονται», (2019), διαθέσιμο σε https://www.liberal.gr/technology/to-2019-feugei-ta-nanorompot-erchontai/279784 .

«Το αυτοκόλλητο φιλμ της LG που μετατρέπει οποιαδήποτε γυάλινη επιφάνεια σε… οθόνη προβολής», (2019), διαθέσιμο σε https://www.fortunegreece.com/article/to-aftokollito-film-tis-lg-pou-metatrepi-opiadipote-gialini-epifania-se-othoni-provolis/ .

«Το bitcoin έκανε πρεμιέρα στο Χρηματιστήριο του Σικάγου», (2017), διαθέσιμο σε https://www.kathimerini.gr/economy/international/938841/to-bitcoin-ekane-premiera-sto-chrimatistirio-toy-sikagoy/

«Το γαλλικό ΣτΕ απαγόρευσε τη χρήση drones για την επιτήρηση των πολιτών», (2020), διαθέσιμο σε https://www.kathimerini.gr/1078711/article/epikairothta/kosmos/to-galliko-ste-apagoreyse-th-xrhsh-drones-gia-thn-epithrhsh-twn-politwn.

«Υιοθετώντας τα νέα εργαλεία της επαυξημένης πραγματικότητας», (2018), διαθέσιμο σε https://www.kathimerini.gr/986719/article/politismos/eikastika/yio8etwntas-ta-nea-ergaleia-ths-epay3hmenhs-pragmatikothtas.

«Φορολογία κρυπτονομισμάτων στο εξωτερικό και την Ελλάδα», (2020), διαθέσιμο σε https://horizonlawfirm.gr/forologia-kryptonomismaton-sto-exoteriko-ke-stin-ellada/.

«Ψυγείο…χάκερ συμμετείχε σε κυβερνοεπίθεση», (2014), διαθέσιμο σε https://www.inewsgr.com/257/psygeiochaker-symmeteiche-se-kyvernoepithesi.htm .

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 12ης Σεπτεμβρίου 2018 σχετικά με τα αυτόνομα οπλικά συστήματα (2018/2752), διαθέσιμο σε http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0341+0+DOC+XML+V0//EN&language=EN .

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017 με συστάσεις προς την Επιτροπή σχετικά με ρυθμίσεις αστικού δικαίου στον τομέα της ρομποτικής (2015/2103(INL)), διαθέσιμο σε https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EL.html .

Αγγελέτου Βάσω, *«Οι Έλληνες αγοράζουν Bitcoin παρά τα capital controls»*, (2017), διαθέσιμο σε https://www.insider.gr/hristika/ependyseis/68904/oi-ellines-agorazoyn-bitcoin-para-ta-capital-controls .

Ατσαλάκη Ιωάννα, Γιώργος Σ. Ατσαλάκης, Κωνσταντίνος Ζοπουνίδης και Φώτης Πασιούρας, *«Bitcoin και Τεχνητή Νοημοσύνη»*, (2019), διαθέσιμο σε https://m.naftemporiki.gr/story/1526339/bitcoin-kai-texniti-noimosuni.

Βελεσιώτη Αγγελική, *«Στον «πυρετό» του Bitcoin: Πόσα ATMs λειτουργούν στην Ελλάδα»*, (2020), διαθέσιμο σε https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/ston-pireto-tou-bitcoin-posa-atms-litourgoun-stin-ellada/ .

Δούκας Χ., Π. Ξυδώνας, *«Άποψη: Κρυπτονομίσματα και ενεργειακή παραδοξότητα»*, (2018), διαθέσιμο σε https://www.kathimerini.gr/943122/article/oikonomia/ellhnikh-oikonomia/apoyh-kryptonomismata-kai-energeiakh-parado3othta.

Κανέλλος Γεώργιος Π., *«AI: Δέσμη δικαιωμάτων για την προστασία των καταναλωτών στα πλαίσια της τεχνητής νοημοσύνης ζητάει το Ευρωκοινοβούλιο»*, (2020), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/ai-desmi-dikaiomaton-gia-tin-prostasia-ton-katanaloton-sta-plaisia-tis-tehnitis .

Κανέλλος Λεωνίδας, *«Η Τεχνητή Νοημοσύνη στην υπηρεσία μιας Έξυπνης Δικαιοσύνης»*, (2020), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/i-tehniti-noimosyni-stin-ypiresia-mias-exypnis-dikaiosynis#footnote10_c75t8oh .

Κασσίμη Αλεξάνδρα, *«Στα Τρίκαλα η πιο επιτυχημένη στον κόσμο πιλοτική χρήση λεωφορείων χωρίς οδηγό»*, (2016), διαθέσιμο σε https://www.kathimerini.gr/society/853069/sta-trikala-i-pio-epitychimeni-ston-kosmo-pilotiki-chrisi-leoforeion-choris-odigo/ .

Κασσωτάκη Αλίκη, *«Στρατηγικές Ανάπτυξης Σημασιολογικών Δομών του Λόγου»*, διαθέσιμο σε https://upbility.gr/blogs/blog/79662083 .

Κολλιδάς Γιώργος, *«Σκοτεινό Διαδίκτυο» και κυβερνοέγκλημα»*, (2020) διαθέσιμο σε https://www.kathimerini.gr/economy/561084904/apopsi-skoteino-diadiktyo-kai-kyvernoegklima/ .

Κορνηλάκη Ευδοκία, *«Η προστασία του εμπορικού απορρήτου»*, (2019), διαθέσιμο σε https://koumentakislaw.gr/arthra/prostasia-emporikoy-aporrhtoy/ .

Λογαράς Κων/νος, *«Η Τεχνολογία blockchain, οι εφαρμογές και οι νομικές πτυχές της Τι είναι η τεχνολογία blockchain, ποιες είναι οι κυριότερες εφαρμογές της και οι κυριότερες νομικές πτυχές της»*, (2018), διαθέσιμο σε https://www.lawspot.gr/nomika-nea/h-tehnologia-blockchain-oi-efarmoges-kai-oi-nomikes-ptyhes-tis.

Ματσανιώτης Νικόλαος, *«Βιοηθικά διλήμματα: πρόσφατα και μελλοντικά»*, (2005), διαθέσιμο σε https://www.iatrikionline.gr/Deltio_52d/07.htm .

Μιχαηλίδου Χρυσούλα, *«Κυβερνοέγκλημα και ηλεκτρονική απόδειξη - ένας τρόπος εξακρίβωσης του ψηφιακού αποτυπώματός του. Ευρώπη με μια ματιά»*, (2018), διαθέσιμο σε https://theartofcrime.gr

Μπρούμας Αντώνης, *«Η Προστασία των Προσωπικών Δεδομένων Παιδιού»*, (2019), διαθέσιμο σε https://lawandtech.eu/2019/10/09/children-data/

Νανόπουλος Κων/νος, *«Ποια είναι η φορολογία υπεραξίας από Bitcoins»*, (2017), διαθέσιμο σε https://www.newsbeast.gr/financial/arthro/2718492/pia-ine-i-forologia-iperaxias-apo-bitcoins.

Ομάδα Εργασίας ΤΕΕ, *«Μελέτη των πνευματικών δικαιωμάτων του έργου που παράγεται και διακινείται στο ΤΕΕ»*, (2009), διαθέσιμο σε http://library.tee.gr/digital/m2386.pdf .

Παζόπουλος Βασίλης, *«Δόθηκε η πρώτη άδεια τράπεζας κρυπτονομισμάτων»*, (2020), διαθέσιμο σε https://www.euro2day.gr/investments/crypto/article/2042288/dothhke-h-proth-adeia-trapezas-kryptonomismaton-.html .

Παλαιτσάκης Γιώργος, *«Οι αλλαγές στη φορολογία το 2019»*, (2019), διαθέσιμο σε https://www.naftemporiki.gr/finance/story/1461604/aade-oi-allages-sti-forologia-to-2019.

Παναγοπούλου – Κουτνατζή Φερενίκη, *«Η προστασία προσωπικών δεδομένων σε περίοδο πανδημίας»*, (2020), διαθέσιμο σε https://www.constitutionalism.gr/2020-03-28_panagopoulou-privacy-koronavirus/ .

Παπαδόπουλος Γιάννης, *«Το «ξέπλυμα» ψηφιακών λύτρων και η σύλληψη Ρώσου στη Χαλκιδική»*, (2017), διαθέσιμο σε https://www.kathimerini.gr/920181/article/epikairothta/ellada/to-3eplyma-yhfiakwn-lytrwn-kai-h-syllhyh-rwsoy-sth-xalkidikh.

Πασαμιχάλη Ελένη Θ., *«Η αλληλέγγυα ευθύνη διοικούντων νομικά πρόσωπα και νομικές οντότητες»*, (2019), διαθέσιμο σε http://www.nsk.gr/documents/15678/84519/%CE%95%CE%99%CE%A3%CE%97%CE%93%CE%97%CE%A3%CE%95%CE%99%CE%A3_18-12-2019.pdf/3388c219-a316-49cb-a836-d7f0c2986e74 .

Πικραμένος Μιχάλης Ν., *«Τι σημαίνει ότι μπορώ να αναπτύξω ελεύθερα την προσωπικότητά μου;»*, (2019), διαθέσιμο σε https://www.syntagmawatch.gr/my-constitution/ti-simainei-oti-boro-na-anaptyxo-elefthera-tin-prosopikotita-mou/ .

Πλάντζος Κωστής, *«Φόρο στα κέρδη από το bitcoin σχεδιάζει η εφορία»*, (2019), διαθέσιμο σε https://www.newmoney.gr/roh/palmos-oikonomias/oikonomia/foro-sta-kerdi-apo-to-bitcoin-sxediazei-i-eforia/.

Πρωτοπαπαδάκης Ιωάννης, *«Ποιοι είναι οι Millennials; Πώς μπορείτε να τους προσεγγίσετε;»*, (2017), διαθέσιμο σε https://www.epixeiro.gr/article/2641.

Σκόνδρα Μαγδαληνή, *«Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα»*, (2020), διαθέσιμο σε https://www.ddikastes.gr/node/5271 .

Σουλιώτης Γιάννης, *«Σε τελική ευθεία το σχέδιο για τις κάμερες στις διμοιρίες των ΜΑΤ»*, (2020), διαθέσιμο σε https://www.kathimerini.gr/society/561085486/se-teliki-eytheia-to-schedio-gia-tis-kameres-stis-dimoiries-ton-mat/ .

Σουφλέρη Ιωάννα Α., *«Το ελληνικό Κέντρο Γονιδιωματικής»*, (2016), διαθέσιμο σε https://www.tovima.gr/2016/05/20/science/to-elliniko-kentro-gonidiwmatikis/ .

Χατζηνικολάου Προκόπης, *«Με τεχνητή νοημοσύνη η εφορία στη μάχη κατά της φοροδιαφυγής»*, (2020), διαθέσιμο σε https://www.kathimerini.gr/economy/561186367/me-techniti-noimosyni-i-eforia-sti-machi-kata-tis-forodiafygis/ .

Χίου Θεόδωρος, *«Νέα υποκείμενα στην Πνευματική Ιδιοκτησία; Από την «NARUTO» στον «BOT Dylan»* και τις δημιουργίες των ρομπότ», (2017), διαθέσιμο σε http://www.iprights.gr/gnomes/198-nea-ypokeimena-stin-pneymatiki-idioktisia-apo-tin-naruto-ston-bot-dylan-kai-tis-dimiourgies-ton-robot .

«3 reasons why millennials need to diversify investments in cryptocurrencies», (2021), διαθέσιμο σε https://economictimes.indiatimes.com/markets/stocks/news/3-reasons-why-millennials-need-to-diversify-investments-in-cryptocurrencies/articleshow/80840141.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst .

«19 Corporations Working On blockchain And Distributed Ledgers», (2018), διαθέσιμο σε https://www.cbinsights.com.

«A Brief History of Drones», (2018), Imperial War Museum διαθέσιμο σε https://www.iwm.org.uk/history/a-brief-history-of-drones.

«A Cyber Security Framework For Europe», European Commission, (2014). διαθέσιμο σε http://cordis.europa.eu/news/rcn/121360_en.html.

«A Federal Judge Just Ordered Coinbase to Report More Than 10,000 Users to the IRS», (2017), διαθέσιμο σε https://futurism.com.

«AI tools threaten right to privacy and freedom of expression — report», (2018), διαθέσιμο σε https://medium.com/@privacyint/ai-tools-threaten-right-to-privacy-and-freedom-of-expression-report-443be95f3b75 .

«A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe, Directorate Gen. Internal Policies Union», (2009), διαθέσιμο σε http://www.statewatch.org/news/2009/apr/ep-study-norris-cctv-video-surveillance.pdf.

«Augmented Reality Technology Policy Primer», (2015), διαθέσιμο σε http://techpolicylab.uw.edu/wp-content/uploads/2017/08/Augmented_Reality_Primer-TechPolicyLab.pdf .

«Augmented reality: the future of surgery», (2019), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/blogposts/augmented-reality-future-surgery .

«Beijing Internet court launches AI judge», (2019), διαθέσιμο σε http://www.chinadaily.com.cn/a/201906/28/WS5d156cada3103dbf1432ac74.html .

«Benefits of Reminiscence Therapy», (2017), διαθέσιμο σε https://eldercarealliance.org/blog/benefits-reminiscence-therapy.

«Bigbelly Smart Waste & Recycling Systems Captured over 112 Million Gallons of Public Space Waste Last Year», (2017), διαθέσιμο σε http://bigbelly.com/bigbelly-smart-waste-recycling-systems-captured-over-112-million-gallons-of-publicspace-waste-last-year .

«Buy Bitcoin Overtakes Buy Gold as Private Gold Trading Declines in October», (2017), διαθέσιμο σε https://www.ccn.com.

«Can you duplicate Bitcoins and Cryptocurrency?», (2017), διαθέσιμο σε https://blockogy.com.

«CCBE Considerations on the Legal Aspects of Artificial Intelligence», (2020), διαθέσιμο σε https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf .

«Chinese Film Director Jia Zhangke to Experiment with Virtual Reality Film—a Romance», (2016), διαθέσιμο σε https://www.scmp.com/culture/film-tv/article/1977929/chinese-film-director-jia-zhangke-experiment-virtual-reality-film.

«Complaint & Request for Investigation, Injunction, & Other Relief», (2016), διαθέσιμο σε https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf.

«Communication Artificial Intelligence for Europe», (2018), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe .

«Criminal justice system should be cautious when approaching risk assessment», (2019), διαθέσιμο σε https://phys.org/news/2019-04-criminal-justice-cautious-approaching.html .

«Cryptocurrency News: Ripple jubilant as major international bank adopts their platform», (2018), διαθέσιμο σε https://www.express.co.uk/finance/city/914301/cryptocurrency-news-national-bank-abu-dhabi-ripple-transactions.

«Data Breach on VTech Learning Lodge», (2015), διαθέσιμο σε https://www.vtech.com/en/press_release/2015/data-breach-on-vtech-learning-lodge-update/.

«Data Mining. What it is & why it matters», διαθέσιμο σε https://www.sas.com/en_us/insights/analytics/data-mining.html#:~:text=Data%20mining%20is%20the%20process,relationships%2C%20reduce%20risks%20and%20more .

«Dealing with the Law Lag», (2018), διαθέσιμο σε https://legalvision.com.au/dealing-with-the-law-lag/ .

«Digital Europe for a more competitive, autonomous and sustainable Europe – Brochure», (2021), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/digital-europe-more-competitive-autonomous-and-sustainable-europe-brochure .

«Drones», διαθέσιμο σε https://ico.org.uk/for-the-public/drones

«Easing Pain for Burns Victims Using Virtual Reality», (2011), διαθέσιμο σε https://www.bbc.com/news/health-12297569.

«Echelon, Shining A Light On Energy Savings», (2017), διαθέσιμο σε http://www.echelon.com/assets/blt1f1c055db1151a7c/Outdoor-Lighting-WiredSolution-Brochure.pdf.

«Executive Summary Artificial Intelligence and Childrens Rights», (2019), διαθέσιμο σε https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf .

European Parliament, *«A common EU approach to liability rules and insurance for connected and autonomous vehicles: European Added Value Assessment»*, (2018), διαθέσιμο σε http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf .

European Parliamentary Research Service Scientific Foresight Unit (STOA), Scientific Foresight study, *«Ethical Aspects of Cyber-Physical Systems»*, (2016), διαθέσιμο σε http://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU(2016)563501_EN.pdf .

«Facts about GPS tracking using QR codes, RFID/NFC, Bluetooth & GSM/SMS», διαθέσιμο σε https://gocodes.com/facts-about-gps-tracking-using-qr-codes-rfid-bluetooth-sms/ .

«Family Hub Refrigerator» σε http://www.samsung.com/us/explore/family-hub-refrigerator .

«Fostering the European Interactive Technologies ecosystem –new H2020 projects on Augmented Reality / Virtual Reality», (2020), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/fostering-european-interactive-technologies-ecosystem-new-h2020-projects-augmented .

«FAQ About Cyber Attack on VTech Learning Lodge», (2018), διαθέσιμο σε https://www.vtech.com/en/press_release/2018/faq-about-cyber-attack-on-vtech-learning-lodge/.

«Four blockchain Use Cases for Banks, FinTech Network», διαθέσιμο σε https://blockchainapac.fintecnet.com.

«Future Of Privacy Forum, Family Online Safety Inst. Kids & The Connected Home: Privacy In The Age Of Connected Dolls, Talking Dinosaurs, And Battling Robots», (2016), διαθέσιμο σε https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf

«Germany: A Surprising Bitcoin Tax Haven», (2018), διαθέσιμο σε http://www.nomoretax.eu.

«Google Glass puts the focus on Parkinson's», (2014), διαθέσιμο σε https://www.ncl.ac.uk/press/articles/archive/2014/04/googleglassputsthefocusonparkinsons.html.

«How do bone conduction headphones work?», (2018), διαθέσιμο σε https://www.salusuhealth.com/Pennsylvania-Ear-Institute/Events/News-Stories/How-Do-Bone-Conduction-Headphones-Work.aspx .

«How Trolls Are Ruining the Internet», (2016), διαθέσιμο σε https://time.com/4457110/internet-trolls/.

«How Virtual Reality Works, The Economist Explains», (2015), διαθέσιμο σε https://www.economist.com/the-economist-explains/2015/09/01/how-virtual-reality-works .

«iiMote», SMARTV, σε http://smartv.hk/iiMote.html.

«In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information», (2017), διαθέσιμο σε https://ico.org.uk/media/1542/cctv-code-of-practice.pdf.

«Industrial and domestic robots highly vulnerable to malicious cyber-attacks», (2017), διαθέσιμο σε https://teiss.co.uk/special-reports/industrial-domestic-robots-vulnerable-cyber-attacks/ .

«Inside the infamous Mirai IoT Botnet: A Retrospective Analysis», (2017), διαθέσιμο σε https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis

«Internet of Things - brochure», (2019), διαθέσιμο σε https://ec.europa.eu/digital-single-market/en/news/internet-things-brochure .

«Internet of Things: Privacy & Security in a Connected World», (2015), διαθέσιμο σε https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

«Internet of Things, Oxford Dictionaries», διαθέσιμο σε. https://en.oxforddictionaries.com/definition/Internet_of_things .

«Introduction to Remotely Piloted Aircraft Systems (RPAS)», (2020), διαθέσιμο σε https://www.skybrary.aero/index.php/Introduction_to_Remotely_Piloted_Aircraft_Systems_(RPAS)

«Legal Status of Cryptocurrency», διαθέσιμο σε https://lawstrust.com.

«Joint statement by the European Commission and the European Central Bank on their cooperation on a digital euro», (2021), διαθέσιμο σε https://ec.europa.eu/info/files/210119-ec-ecb-joint-statement-digital-euro_en .

«LGD Coin - Legends Room - Voted #1 PICK for 2018», (2018), διαθέσιμο σε https://steemit.com.

«Liability for Artificial Intelligence and other emerging technologies Report», (2019), διαθέσιμο σε https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199 .

«Liberty Victoria calls on the Federal government to make 5 promises about the Tracing App», (2020), διαθέσιμο σε https://libertyvictoria.org.au/content/liberty-victoria-calls-federal-government-make-5-promises-about-tracing-app .

«Maduro bids to revive Venezuela's 'petro' cryptocurrency», (2020), διαθέσιμο σε https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency .

«Mixed Reality Education», διαθέσιμο σε https://govrpro.com/services/mixed-reality-education#:~:text=Mixed%20Reality%20Education&text=Mixed%20reality%20offers%20students%20a,concepts%20being%20taught%20to%20them.&text=Mixed%20reality%20helps%20students%20to%20grasp%20complicated%20concepts%20and%20topics%20with%20ease .

«Mixed reality – how real and virtual worlds are merging», (2020), διαθέσιμο σε https://job-wizards.com/en/mixed-reality-how-real-and-virtual-worlds-are-merging/ .

«Mixed Reality in Education: boosting students' learning experience», (2017), διαθέσιμο σε https://acerforeducation.acer.com/innovative-technologies/mixed-reality-in-education-boosting-students-learning-experience/,

«Moor Insights & Strategy, Echelon's Efficient Connected Lighting Solutions», (2015), διαθέσιμο σε http://www.moorinsightsstrategy.com/wp-content/uploads/2015/06/Echelons-Efficient-Connected-Lighting-Solutions-by-Moor-Insights-Strategy.pdf.

«Pokemon Go Privacy Concerns», διαθέσιμο σε https://www.privacytrust.com/blog/pokemon-go-privacy-concerns.html .

«Pokemon Go shines new attention on trespass laws», (2016) διαθέσιμο σε https://constitutioncenter.org/blog/pokemon-go-shines-new-attention-on-trespass-laws.

«Protecting, Monitoring & Researching the Wildlife of Kuku», διαθέσιμο σε http://maasaiwilderness.org/programs/species-research.

«Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System», διαθέσιμο σε https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/ .

«Researchers Discover a Not-so-Smart Flaw in Smart Toy Bear», (2016), διαθέσιμο σε https://www.trendmicro.com/vinfo/us/security/news/Internet-of-things/researchers-discover-flaw-in-smart-toy-bear.

«Robot Maker Escapes Liability In Fatal Auto Factory Accident», (2019), διαθέσιμο σε https://www.law360.com/articles/1192734/robot-maker-escapes-liability-in-fatal-auto-factory-accident .

«Supervision pursuant to the General Data Protection Regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students», (2019), διαθέσιμο σε https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf .

«'Smart bra' to detect early-stage breast cancer», (2020), διαθέσιμο σε https://healthcare-in-europe.com/en/news/smart-bra-to-detect-early-stage-breast-cancer.html .

«Smarter Coffee», σε https://www.firebox.com/Smarter-Coffee/p6991

«Switzerland now a Cryptocurrency Tax Haven», (2018), διαθέσιμο σε https://bit-media.org.

«Tax Treatment of Cryptocurrencies in Slovenia», (2018), διαθέσιμο σε http://www.nomoretax.eu.

«Technology Quarterly, Taking Flight», (2017), Economist. διαθέσιμο σε https://www.economist.com/technology-quarterly/2017-06-08/civilian-drones.

«The blockchain is the new Google», (2016), διαθέσιμο σε https://techcrunch.com.

«The threat of fully autonomous weapons», (2020), διαθέσιμο σε https://www.stopkillerrobots.org/learn/ .

«Top Ten Operational Impacts of the GDPR», (2018), διαθέσιμο σε https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/.

«Trust, privacy and consumer security in the Internet of Things (IoT)», (2018), διαθέσιμο σε https://www.eesc.europa.eu/el/node/59507?fbclid=IwAR28bSm9c9gZzskz_Q_F11CTKsXXhDsSeHOEWnBcZ_6wJNWHis6A8lnqdRM.

«Twitter and LinkedIn ban cryptocurrency adverts – leaving regulators behind», (2018), διαθέσιμο σε https://www.independent.co.uk/news/business/analysis-and-features/twitter-ban-cryptocurrency-adverts-regulators-bitcoin-facebook-social-media-a8277176.html.

«U.S. airstrikes in Pakistan called 'very effective", CNN Politics», (2009), διαθέσιμο σε http://edition.cnn.com/2009/POLITICS/05/18/cia.pakistan.airstrikes/.

«US v. Faiella and Shrem – Ruling on Bitcoin as Money or Funds», (2014), διαθέσιμο σε https://internetlawcommentary.com.

«Using the Name or Likeness of Another», (2020), διαθέσιμο σε http://www.dmlp.org/legal-guide/using-name-or-likeness-another.

«Virtual Reality in the Military», (2016), διαθέσιμο σε https://www.vrs.org.uk/virtual-reality-military.

«What Does Free Speech Mean?», διαθέσιμο σε https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does .

«What is Personal Data?», διαθέσιμο σε https://eugdprcompliant.com/personal-data.

«What is Ripple? A step-by-step guide to XRP», (2018), διαθέσιμο σε https://www.finder.com.

«What makes a virtual world more than a game?», (2019), διαθέσιμο σε https://decentraland.org/blog/technology/virtual-worlds/ .

«Why VR/AR May NOT Be the Next Big Thing», (2016), διαθέσιμο σε https://www.arovia.com.

«World Economic Forum Announces 100 New Technology Pioneers In 2020 Cohort», (2020), διαθέσιμο σε https://www.weforum.org/press/2020/06/world-economic-forum-announces-100-new-technology-pioneers-in-2020-cohort/ .

Addady Michal, *«Oculus Teams Up with 20th Century Fox to Bring Virtual Reality to Movies»*, (2015), διαθέσιμο σε https://fortune.com/2015/09/27/oculus-movies-virtual-reality.

Agarwal Vikas, *«10 Real Life Examples of Internet of Things»*, (2017) διαθέσιμο σε http://circuitdigest.com/ten-examples-of-internet-of-things-iot.

Aizenberg Evgeni και Jeroen van den Hoven, *«Designing for human rights in AI»*, (2020), διαθέσιμο σε https://bigdatasoc.blogspot.com/2020/09/evgeni-aizenberg-and-jeroen-van-*den.html* .

Allen Jason G, *«What's Offered in an ICO? Digital Coins as Things»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3140499 .

Alliance for Internet of Things Innovation, Working Group 3 Report, IoT LSP Standard Framework Concepts, Release 2.0, AIOTI WG03 – loT Standardisation (2015), διαθέσιμο σε https://aioti.eu/aioti-wg03-reports-on-iot-standards/analysis.

Alsop Thomas, *«Virtual Reality (VR) - statistics & facts»*, (2020), διαθέσιμο σε https://www.statista.com/topics/2532/virtual-reality-vr/ .

Amsden Ryan και Denis Schweizer, *«Are blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3163849

Ananny Mike και Kate Crawford, *«Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability»*, (2016), διαθέσιμο σε https://journals.sagepub.com/doi/abs/10.1177/1461444816676645 .

Anderson Janna και Lee Rainie, *«The Internet of Things Will Thrive by 2025»*, (2014), Pew Reserch Center, Internet and Technology, διαθέσιμο σε www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

Anderson Janna, Lee Rainie και Alex Luchsinger, *«Artificial Intelligence and the Future of Humans»*, (2018), διαθέσιμο σε https://www.elon.edu/docs/e-web/imagining/surveys/2018_survey/AI_and_the_Future_of_Humans_12_10_18.pdf .

Anjum Zafar, *«How Internet Devices Are Working to Save the Rainforest»*, (2013), διαθέσιμο σε http://www.pcworld.com/article/2042086/how-internet-devices-are-working-to-save-the-rainforest.html.

Arthur Charles, *«Google 'Bans' Facial Recognition on Google Glass—But Developers Persist»*, (2013), διαθέσιμο σε https://www.theguardian.com/technology/2013/jun/03/google-glass-facial-recognition-ban.

Article 19, *«Governance with teeth: How human rights can strengthen fat and ethics initiatives on artificial intelligence»*, (2019), διαθέσιμο σε https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

Atkinson R., *«Lessons Learned in Data Privacy Compliance from Pokemon Go»*, (2016), διαθέσιμο σε https://www.driven-inc.com/lessons-learned-in-data-privacy-compliance-from-pokemon-go/ .

Atzori Marcella, *«Blockchain Technology and Decentralized Governance: Is the State Still Necessary?»*, (2015), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709713 .

Bachman Rachel και Sarah E. Needleman, *«Want to Exercise More? Try Screen Time»*, (2016), διαθέσιμο σε https://www.wsj.com/articles/want-to-exercise-more-try-screen-time-1481976002.

Balkam Stephen, *«The New Realities: Virtual, Augmented and Mixed»*, (2017), διαθέσιμο σε https://www.fosi.org/good-digital-parenting/new-realities-virtual-augmented-and-mixed/.

Bedwell Helena, Vanessa Dezem, Stephen Stapczynski και Jonathan Tirone, *«The Cost of Crypto Is Turning Miners Towards Green Power»*, (2018), διαθέσιμο σε https://www.bloomberg.com/news/articles/2018-02-04/power-hungry-crypto-mines-clean-up-as-cost-of-electricity-grows.

Bennett Richard, *«The Year of Augmented Reality»*, (2016), διαθέσιμο σε https://hightechforum.org/the-year-of-augmented-reality.

Bennett Richard, *«Augmented Reality Drama»*, (2016), διαθέσιμο σε https://hightechforum.org/augmented-reality-content-and-communication.

Berg Chris, Jason Potts και Sinclair Davidson, *«KodakOne could be the start of a new kind of intellectual property»*, (2018), διαθέσιμο σε https://theconversation.com/kodakone-could-be-the-start-of-a-new-kind-of-intellectual-property-89966.

Bergman Adam, *«What You Should Know About Taxation Of Cryptocurrencies»*, (2018), διαθέσιμο σε https://www.forbes.com.

Berk Richard, *«Accuracy and fairness for juvenile justice risk assessments»*, (2017), διαθέσιμο σε https://crim.sas.upenn.edu/sites/default/files/Berk_FairJuvy_1.2.2018.pdf .

Bernard Zoë, *«Maybe you shouldn't catch 'em all — A new study links 'Pokémon Go' to traffic deaths, injuries, and vehicle damage»*, (2017), διαθέσιμο σε https://www.businessinsider.com/pokemon-go-linked-to-traffic-deaths-accidents-and-hundreds-of-thousands-of-dollars-in-vehicular-damage-2017-11 .

Blythe Bruce, *«How Are Gains or Losses on Cryptocurrencies Taxed?»*, (2018), διαθέσιμο σε https://tickertape.tdameritrade.com.

Bours Ben, *«How a Dorm Room Minecraft Sam Brought Down the Internet»*, (2017), διαθέσιμο σε https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

Bracy Jedidiah, *«Pokémon GO, augmented reality, and privacy»*, (2016), διαθέσιμο σε https://iapp.org/news/a/pokemon-go-augmented-reality-and-privacy.

Brodkin John, *«Google Forbids Facial Recognition Apps on Glass in the Name of Privacy»*, (2013), διαθέσιμο σε https://arstechnica.com/information-technology/2013/06/google-forbids-facial-recognition-apps-on-glass-in-the-name-of-privacy/.

Bromwich Jonah Engel, *«Where Pokémon Should Not Go»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/13/technology/where-pokemon-should-not-go.html?searchResultPosition=1.

Brown, *«Governor of California, Et Al. V. Entertainment Merchants Association Et Al. 564 U.S. 08–1448»*, (2011), διαθέσιμο σε https://www.supremecourt.gov/opinions/10pdf/08-1448.pdf.

Brownlee Jason, *«A Gentle Introduction to Computer Vision»*, (2019), διαθέσιμο σε https://machinelearningmastery.com/what-is-computer-vision/ .

Brush Jason, *«Why Virtual Reality Matters»*, (2016), διαθέσιμο σε https://www.vox.com/2016/6/28/12046730/virtual-reality-vr-creative-content-industry-investment.

Bruveris Martins, *«Have you heard of NCRFRILS?»*, (2020), διαθέσιμο σε https://martinsbruveris.com/2020/11/have-you-heard-of-ncrfrils/#more-659 .

Buck Jon, *«Former Bitcoin Exchange BTC-e Reopens as WEX.nz»*, (2017), διαθέσιμο σε https://cointelegraph.com/news/former-bitcoin-exchange-btc-e-reopens-as-wexnz.

Burgess Matt, *«What Is the Internet of Things?»*, (2017) διαθέσιμο σε http://www.wired.co.uk/article/internet-of-things-what-is-explained-iot.

Burgess Matt, *«UK police are using AI to inform custodial decisions – but it could be discriminating against the poor»*, (2018), διαθέσιμο σε https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit .

Burks Robin, *«How Drones and Virtual Reality Will Change Tourism»*, (2015), διαθέσιμο σε https://www.techtimes.com/articles/57076/20150601/how-drones-and-virtual-reality-will-change-tourism.htm.

Burrus Daniel, *«The Internet of Things is Far Bigger than Anyone Realizes»*, (2014), διαθέσιμο σε http://www.wired.com/2014/11/the-internet-of-things-bigger.

Bye Kent, *«Using VR to Treat Lazy Eye with 'Vivid Vision»*, (2016), διαθέσιμο σε https://www.roadtovr.com/using-vr-treat-lazy-eye-vivid-vision.

Cachin Christian, Angelo De Caro, Pedro Moreno-Sanchez, Björn Tackmann και Marko Vukolic, *«The Transaction Graph for Modeling blockchain Semantics»*, (2017), διαθέσιμο σε https://assets.pubpub.org/oh4wbdb0/71581340107043.pdf .

Calo Ryan, Tamara Denning, Batya Friedman, Tadayoshi Kohno, Lassana Magassa, Emily McReynolds, Bryce C. Newell & Jesse Woo, *«Augmented Reality: A Technology and Policy Primer»,* (2016), διαθέσιμο σε https://digitalcommons.law.uw.edu/techlab/1 .

Calvano Emilio, Giacomo Calzolari, Vincenzo Denicolò, Sergio Pastorello, *«Artificial intelligence, algorithmic pricing, and collusion»*, (2019), διαθέσιμο σε https://voxeu.org/article/artificial-intelligence-algorithmic-pricing-and-collusion .

Cameron Euan, *«How will automation impact jobs?»,* διαθέσιμο σε https://www.pwc.co.uk/services/economics/insights/the-impact-of-automation-on-jobs.html .

Carey Matthew, *«Why Disney Might Want to 'Escape from Tomorrow»*, (2013), διαθέσιμο σε https://edition.cnn.com/2013/01/24/showbiz/movies/escape-tomorrow-sundance-disney/index.html.

Carlson Jill, *«Cryptocurrency and Capital Controls»*, (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046954.

Carson Eric, *«How Virtual Reality Gets Industrial Training Simulators Closer to Real Life than Ever Before»*, (2016), διαθέσιμο σε https://www.techrepublic.com/article/how-virtual-reality-gets-industrial-training-simulators-closer-to-real-life-than-ever-before.

Carson Erin, *«NASA Shows the World Its 20-Year Virtual Reality Experiment to Train Astronauts: The Inside Story»*, (2015), διαθέσιμο σε https://www.techrepublic.com/article/nasa-shows-the-world-its-20-year-vr-experiment-to-train-astronauts.

Catalini Christian και Joshua S. Gans, *«Initial Coin Offerings and the Value of Crypto Tokens»*, (2018), διαθέσιμο σε http://ide.mit.edu/sites/default/files/publications/SSRN-id3137213.pdf.

Catalini Christian και Joshua S. Gans, *«Some Simple Economics of the blockchain»*, (2017), διαθέσιμο σε https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf .

Cath Corinne, *«Governing artificial intelligence: ethical, legal and technical opportunities and challenges»*, (2018), διαθέσιμο σε https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080 .

Cawley Conor, *«In Virtual Reality, Trolls Will Be Worse than Ever»*, (2017), διαθέσιμο σε https://virtualrealityinsider.com/index.php/2017/02/08/in-virtual-reality-trolls-will-be-worse-than-ever/.

CEIPI, *«Artificial Intelligence and Intellectual Property»*, διαθέσιμο σε http://www.ceipi.edu/en/training-seminars/artificialintelligence-and-intellectual-property/ .

Cervantes Edgar, *«Google Cardboard Helps Doctor Save Baby's Life»*, (2015), διαθέσιμο σε https://www.androidauthority.com/google-cardboard-helps-doctor-save-babys-life-664885.

Cheng Evelyn, *«Cyberattack temporarily hits bitcoin exchange Bitfinex»*, (2017), διαθέσιμο σε https://www.cnbc.com.

Chohan Usman W., *«A History of Dogecoin»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091219 .

Chohan Usman W., *«Cryptocurrencies as Asset-Backed Instruments: The Venezuelan Petro»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3119606 .

Chohan Usman W., *«The Cryptocurrency Tumblers: Risks, Legality and Oversight»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080361 .

Chohan Usman W., *«The Decentralized Autonomous Organization and Governance Issues»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082055 .

Chris Berg, Sinclair Davidson και Jason Potts, *«Beyond Money: Cryptocurrencies, Machine-Mediated Transactions and High Frequency Bartering»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3158047 .

Christakis Nicholas A., *«How AI Will Rewire Us»*, (2019), διαθέσιμο σε https://www.theatlantic.com/magazine/archive/2019/04/robots-human-relationships/583204/ .

Clark Peter, *«'Pokemon Go' Creator on Augmented Reality's Massive Potential»*, (2019), διαθέσιμο σε https://variety.com/2019/gaming/features/pokemon-go-creator-on-augmented-realitys-massive-potential-1203169992/ .

Clayton Jay και J. Christopher Giancarlo, *«Regulators Are Looking at Cryptocurrency»*, (2018), διαθέσιμο σε https://www.wsj.com.

Clor-Proell Shana, Ryan Guggenmos, και Kristina M. Rennekamp, *«Mobile Devices and Investment Apps: The Effects of Push Notification, Information Release, and the Fear of Missing Out»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2991262 .

CMA, *«The commercial use of consumer data Report on the CMA's call for information»*, (2015), διαθέσιμο σε https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf .

Coates Charlotte, *«Virtual Reality is a big trend in museums, but what are the best examples of museums using VR?»*, (2020), διαθέσιμο σε https://www.museumnext.com/article/how-museums-are-using-virtual-reality/ .

Corbet Shaen, Charles James Larkin, Brian M. Lucey και Larisa Yarovaya, *«Kodakcoin: A blockchain Revolution or Exploiting a Potential Cryptocurrency Bubble?»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3073727 .

Corpuz John, *«Best Augmented Reality Apps»*, (2019), διαθέσιμο σε https://www.tomsguide.com/us/pictures-story/657-best-augmented-reality-apps.html

Couch Christina, *«Healing Minds with Virtual Reality»*, (2015), διαθέσιμο σε https://www.pbs.org/wgbh/nova/article/vr-therapy.

Courtland Rachel, *«Bias detectives: the researchers striving to make algorithms fair»*, (2018), διαθέσιμο σε https://www.nature.com/articles/d41586-018-05469-3 .

Cox David, *«Virtual Reality Can Help People Conquer Their Phobias»*, (2014), διαθέσιμο σε https://www.theguardian.com/science/blog/2014/oct/16/virtual-reality-phobias-public-speaking-flying.

Crichton Danny, *«South Korea passes one of the world's first comprehensive cryptocurrency laws»*, (2020), διαθέσιμο σε https://techcrunch.com/2020/03/05/south-korea-passes-one-of-the-worlds-first-comprehensive-cryptocurrency-laws.

Crist Ry, *«Amazon Alexa: Device Compatibility, How-tos and Much More»*, (2016), διαθέσιμο σε https://www.cnet.com/how-to/amazon-alexa-devicecompatibility-how-tos-and-much-more.

Dalton, *«Re-live the First Surgery Recorded via Snapchat Spectacles»*, (2016), διαθέσιμο σε https://www.engadget.com/2016-12-15-first-snapchat-spectacles-surgery.html .

Danko JP., *«Blockchain Copyright Protection – A Viable Solution To Prove Ownership of Creative Works?»*, (2018), διαθέσιμο σε https://www.diyphotography.net/blockchain-copyright-protection-a-viable-solution-to-prove-ownership-of-creative-works/ .

Danks David και Alex John London, *«Algorithmic bias in autonomous systems»*, Proceedings of the 26th International Joint Conference on Artificial Intelligence, AAAI Press, (2017), διαθέσιμο σε https://www.cmu.edu/dietrich/philosophy/docs/london/IJCAI17-AlgorithmicBias-Distrib.pdf .

Das Samburaj, *«Israel Tax Authority Deems Bitcoin a Taxable Asset»*, (2017), διαθέσιμο σε https://fintechranking.com/2017/01/16/israel-tax-authority-deems-bitcoin-a-taxable-asset/ .

Davidson Jacob, *«No, Big Companies Aren't Really Accepting Bitcoin»*, (2015), διαθέσιμο σε https://money.com/money/3658361/dell-microsoft-expedia-Bitcoin.

Davidson Sinclair, Primavera De Filippi και Jason Potts, *«Economics of blockchain»*, (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751.

Davis Charlotte, *«Bitcoin price: Analyst reveals what Wall Street investment Will mean for the price of BTC»*, (2018), https://www.express.co.uk/finance.

Davison John, *«WTF Is 'Pokémon Go,' Explained, Rolling Stone»*, (2016), διαθέσιμο σε https://www.rollingstone.com/culture/features/wtf-is-pokemon-go-explained-20160711.

Deane Michael, *«AI and the Future of Privacy»*, (2018), διαθέσιμο σε https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4 .

Delcker Janosch, *«Top German court deems spying on foreigners' internet traffic is unconstitutional»*, διαθέσιμο σε https://www.politico.eu/article/top-german-court-deems-spying-on-foreigners-internet-traffic-is-unconstitutional/.

Dell' Antonia Kj., *«Pokémon Has Kids on the Move - and on their Phones»*, (2016), διαθέσιμο σε https://well.blogs.nytimes.com/2016/07/12/pokemon-has-children-on-the-move/?mtrref=www.google.com&gwh=33F88D0A1D440BBA2F5216E19A7A00FC&gwt=pay&assetType=REGIWALL.

Denham Hannah, *«IBM's decision to abandon facial recognition technology fueled by years of debate»*, (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/ .

Desatoff Sam, *«Niantic settles 2016 Pokemon Go class action trespassing lawsuit»*, (2016), διαθέσιμο σε https://finance.yahoo.com/news/niantic-settles-2016-pokemon-class-194800175.html.

Diamantis Mihailis E., *«Who Pays for AI Injury?»*, (2020), διαθέσιμο σε https://www.law.ox.ac.uk/business-law-blog/blog/2020/05/who-pays-ai-injury .

Diane Tsai, *«This Virtual Reality Game Could Help Treat Lazy Eye»*, (2016), διαθέσιμο σε https://time.com/4154830/virtual-reality-lazy-eye.

Dignum Virginia, *«The ART of AI — Accountability, Responsibility, Transparency»*, *(*2018), διαθέσιμο σε https://medium.com/@virginiadignum/the-art-of-ai-accountability-responsibility-transparency-48666ec92ea5 .

Doctorow Cory, *«More on 'Escape from Tomorrow,' the Guerrilla Art-House Movie Shot at Walt Disney World and Disneyland»*, (2013), διαθέσιμο σε https://boingboing.net/2013/01/21/more-on-escape-from-tomorrow.html.

Dorsey Jessica και Christophe Paulussen, *«A common European position on armed drones? Charting EU member states' views on questions of counterterrorism uses of force»*, Global Affairs, Vol. 1/ 3, (2015), διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080037 .

Doshi-Velez Finale, Mason Kortz, Ryan Budish, Chris Bavitz, Sam Gershman, David O'Brien, Stuart Schieber, James Waldo, David Weinberger, and Alexandra Wood, *«Accountability of AI Under the Law: The Role of Explanation»*, διαθέσιμο σε https://arxiv.org/pdf/1711.01134.pdf .

DuPont Sam, *«Facial Recognition Is Here But We Have No Laws. Without legal safeguards, this technology will undermine democratic values and fundamental rights»*, (2020), διαθέσιμο σε https://www.nextgov.com/ideas/2020/07/facial-recognition-here-we-have-no-laws/166711/ .

Dworkin Anthony, *«Drones and targeted killing: Defining a European position, European Council on Foreign Relations»*, (2013), διαθέσιμο σε https://ecfr.eu/publication/drones_and_targeted_killing_defining_a_european_position211/ .

Dworkin Anthony, *«The EU and armed drones – epilogue»*, Global Affairs, Vol. 1/ 3, (2015), διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080901 .

Dwoskin Elizabeth, Michael Alison Chandler και Brian Fung, *«Auschwitz, Sex Assault and Police Shootings: Where Virtual Reality Is Going Next»*, (2016), διαθέσιμο σε https://www.washingtonpost.com/news/the-switch/wp/2016/11/11/auschwitz-sex-assault-and-police-shootings-where-virtual-reality-is-going-next.

Earle Sam, *«Bullshit Jobs: Robots Are Replacing Human Workers, So Why Are Americans Still Working So Hard?»*, (2018) διαθέσιμο σε http://www.newsweek.com/bullshit-jobs-age-automation-why-areamericans-still-working-so-hard-983753 .

Earnest Josh, *«How to See the White House on a Dollar Bill»*, (2016), διαθέσιμο σε https://obamawhitehouse.archives.gov/blog/2016/11/30/how-see-white-house-dollar-bill.

EDPS, *«Artificial Intelligence, Robotics, Privacy and Data Protection Background document for the 38th International Conference of Data Protection and Privacy Commissioners»*, 2016, διαθέσιμο σε https://edps.europa.eu/data-protection/our-work/publications/other-documents/artificial-intelligence-robotics-privacy-and_en .

Elliott Larry, *«Millions of UK workers at risk of being replaced by robots, study says»*, (2017), διαθέσιμο σε https://www.theguardian.com/technology/2017/mar/24/millions-uk-workers-risk-replaced-robots-study-warns#:~:text=3%20years%20old-,Millions%20of%20UK%20workers%20at%20risk,replaced20by%20robots%2C%20study%20says&text=The%20report%20predicted%20that%20automation,used%20for%20low%2Dskill%20tasks .

Erlank Wian, *«Property in Virtual Worlds»*, (2013), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2216481 .

EU Agency for Fundamental Rights (FRA), *«BigData: Discrimination in data-supported decision making»*, (2018), διαθέσιμο σε http://fra.europa.eu/en/publication/2018/big-data-discrimination .

European Commission, *«Digital Single Market – Bringing down barriers to unlock online opportunities»*, (2017), διαθέσιμο σε https://www.europeansources.info/record/digital-single-market-bringing-down-barriers-to-unlock-online-opportunities/.

European Data Protection Board, *«Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak»,* διαθέσιμο σε https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en .

Evangelista Benny, *«Narrative Wearable Camera: Valuable Tool or Little Brother?»*, (2016), διαθέσιμο σε https://www.sfchronicle.com/business/article/Narrative-wearable-camera-valuable-tool-or-7294627.php.

Evans Dave, *«The Future of Wearable Technology: Smaller, Cheaper, Faster, and Truly Personal Computing»*, διαθέσιμο σε https://blogs.cisco.com/digital/the-future-of-wearable-technology-smaller-cheaper-faster-and-truly-personal-computing.

Fabian Benjamin, Tatiana Ermakova, Jonas Krah, Ephan Lando και Nima Ahrary, *«Adoption of Security and Privacy Measures in Bitcoin – Stated and Actual Behavior»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3184130 .

Fairfield Joshua A.T., *«The Magic Circle»*, 14 Vand. J. Ent. & Tech. L. 545, (2012), διαθέσιμο σε https://opensource.org/licenses.

Fairfield Joshua A.T., *«Escape into the Panopticon: Virtual Worlds and the Surveillance Society»*, 118 Yale L.J. Pocket Part 131 (2009), διαθέσιμο σε http://thepocketpart.org/2009/01/19/fairfield.html.

Feldstein Steven, *«The Global Expansion of AI Surveillance»*, (2019), διαθέσιμο σε https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 .

Finnegan Daniel Joseph, *«How to solve virtual reality's human perception problem»*, (2018), διαθέσιμο σε http://theconversation.com/how-to-solve-virtual-realitys-human-perception-problem-92128.

Fogel Stephanie, *«Pokemon Go creator Niantic will allow 130 foot buffer zones to protect private property from trespassing players»*, (2019), διαθέσιμο σε https://www.businessinsider.com/pokemon-go-new-rules-private-property-legal-settlement-2019-2.

Foley Sean, Jonathan R. Karlsen και Tālis J. Putniņš, *«Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?, Review of Financial Studies»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645 .

Fox Douglas, *«What sparked the Cambrian explosion?»*, (2016), διαθέσιμο σε https://www.nature.com/news/what-sparked-the-cambrian-explosion-1.19379 .

Forrest Conner, *«Robot kills worker on assembly line, raising concerns about human-robot collaboration»*, (2017), διαθέσιμο σε https://www.techrepublic.com/article/robot-kills-worker-on-assembly-line-raising-concerns-about-human-robot-collaboration/ .

Fossi Connie και Phil Prazan, *«Miami Police Used Facial Recognition Technology in Protester's Arrest»*, (2020), διαθέσιμο σε https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ .

Fowler Geoffrey A., *«Texting while Walking Isn't Funny Anymore»*, (2016), διαθέσιμο σε https://www.wsj.com/articles/texting-while-walking-isnt-funny-anymore-1455734501.

Frankenfield Jake, *«Block (Bitcoin Block)»*, διαθέσιμο σε https://www.investopedia.com/terms/b/block-bitcoin-block.asp#:~:text=What%20Is%20a%20Block%20(Bitcoin,a%20ledger%20or%20record%20book.

Frankenfield Jake, *«HODL»*, (2020), διαθέσιμο σε https://www.investopedia.com/terms/h/hodl.asp .

Franklin Jonathan, *«Escape from Tomorrow' a Disney's Lawyers Nightmares»*, (2013), διαθέσιμο σε http://lawofficesofjonathanfranklin.blogspot.com/2013/01/escape-from-tomorrow-disneys-lawyers.html.

Freed Richard, *«Wired Child: Reclaiming Childhood in a Digital Age»*, (2018), διαθέσιμο σε http://richardfreed.com/ .

Fruhlinger Josh, *«The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet»*, (2018), διαθέσιμο σε https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

Fung Brian, *«Facebook is banning ads for bitcoin and other cryptocurrencies»*, (2018), διαθέσιμο σε https://www.washingtonpost.com/news/the-switch/wp/2018/01/30/facebook-bans-misleading-advertisements-for-cryptocurrencies-including-bitcoin

Gamerman Ellen, *«A Look at the Museum of the Future»*, (2015), διαθέσιμο σε https://www.wsj.com/articles/a-look-at-the-museum-of-the-future-1444940447.

Gandal Neil, JT Hamrick, Tyler Moore και Tali Oberman, *«Price Manipulation in the Bitcoin Ecosystem»*, CEPR Discussion Paper No. DP12061, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2977479 .

Garbade Michael J., *«A Simple Introduction to Natural Language Processing»*, (2018), διαθέσιμο σε https://becominghuman.ai/a-simple-introduction-to-natural-language-processing-ea66a1747b32 .

Gartland Claire, *«Biometrics Are a Grave Threat to Privacy»*, (2016), διαθέσιμο σε https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy.

Gaudiosi John, *«Now You Can Shop for Luxury Homes in Virtual Reality»*, (2015), διαθέσιμο σε https://fortune.com.

Gaudiosi John, *«This Company Is Redesigning How It Works with Virtual Reality»*, (2015), διαθέσιμο σε https://fortune.com/2015/09/02/virtual-reality-interior-design.

Gebhart Andrew, *«Google Home vs. Amazon Echo»*, (2017), διαθέσιμο σε https://www.cnet.com/news/google-home-vs-amazon-echo.

Gerlach J-C, Guilherme Demos και Didier Sornette, *«Dissection of Bitcoin's Multiscale Bubble History»*, Swiss Finance Institute Research Paper No. 18-30, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3164246 .

Gipp Bela, Norman Meuschke και André Gernandt, *«Decentralized Trusted Timestamping using the Crypto Currency Bitcoin»*, (2015), διαθέσιμο σε https://arxiv.org/abs/1502.04015 .

Glon Ronan, *«Distracted behind the Wheel? Try One of These Aftermarket Heads-Up Displays»*, (2017), διαθέσιμο σε https://finance.yahoo.com/news/distracted-behind-wheel-try-one-161533448.html.

Goldin Ian, *«Will AI kill developing world growth?»*, (2019), διαθέσιμο σε https://www.bbc.com/news/business-47852589 .

Goodin Dan, *«Internet-Connected Hello Barbie Doll Gets Bitten by Nasty Poodle Crypto Bug»*, (2015), διαθέσιμο σε https://arstechnica.com/security/2015/12/internet-connected-hello-barbie-doll-gets-bitten-by-nasty-poodle-crypto-bug .

Gordon Scott, *«Will we Get a GDPR for the IOT?»*, (2018), διαθέσιμο σε https://www.scmagazineuk.com/will-we-get-a-gdpr-for-the-iot/article/758037/.

Graff Garrett M., *«How a Dorm Room Minecraft Scam Brought Down the Internet»*, (2017), διαθέσιμο σε https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet.

Greene Jay, *«Amazon bans police use of its facial-recognition technology for a year»*, (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/10/amazon-rekognition-police/ .

Greene Jay, *«Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM»*, (2020), διαθέσιμο σε https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ .

Griffin John M. και Amin Shams, *«Is Bitcoin Really Un-Tethered?»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3195066 .

Griffith Erin, *«Can Virtual Reality Save Journalism?»*, (2016). διαθέσιμο σε https://fortune.com/2016/05/02/virtual-reality-nyt-newfronts/.

Grossman Dave, *«Videogames as Murder Simulators»*, (2013), διαθέσιμο σε https://variety.com/2013/voices/opinion/grossman-2640/.

Grubb Jeff, *«Immersv Enables Virtual Reality Developers to Advertise Their Games in Other VR Apps»*, (2016), διαθέσιμο σε https://venturebeat.com/2016/03/10/immersv-enables-virtual-reality-developers-to-advertise-their-games-in-other-vr-apps.

Grubb Jeff, *«What Oculus Rift and Virtual Reality Mean for Sex, Death, Violence, and Identity»*, (2014), διαθέσιμο σε https://venturebeat.com/2014/06/05/what-oculus-rift-and-virtual-reality-mean-for-sex-death-violence-and-identity.

Gubrud Mark, *«Why Should We Ban Autonomous Weapons?»*, (2016), διαθέσιμο σε https://spectrum.ieee.org/automaton/robotics/military-robots/why-should-we-ban-autonomous-weapons-to-survive .

Gup Benton E., *«What Is Money? From Commodities to Virtual Currencies/Bitcoin»*, (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409172 .

Halamka John, *«Order Interrupted by Text: Multitasking Mishap, AHRQ Morbidity & Mortality Rounds on the Web»*, (2011), διαθέσιμο σε https://aornjournal.onlinelibrary.wiley.com/doi/full/10.1016/j.aorn.2013.05.013.

Hallevy Gabriel, *«AI v. IP - Criminal Liability for Intellectual Property IP Offenses of Artificial Intelligence AI Entities»*, (2015), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2691923 .

Hallevy Gabriel, *«The Criminal Liability of Artificial Intelligence Entities - from Science Fiction to Legal Social Control»*, Akron Intellectual Property Journal, Vol. 4/ 2, Article 1, (2010), διαθέσιμο σε http://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1 .

Hardy Robert Augustus και Julia R Norgaard, *«Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web»*, (2015), διαθέσιμο σε https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/reputation-in-the-internet-black-market-an-empirical-and-theoretical-analysis-of-the-deep-web/560A8645D47BBDDC4E71101EC1C100CA.

Hartzog Woodrow, *«Unfair and deceptive robots»*, Maryland Law Review, Vol. 74/ 4, (2015), διαθέσιμο σε http://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3675&context=mlr .

Harvey Campbell R., *«Bitcoin Myths and Facts»*, (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479670 .

Harvey Campbell R., *«Cryptofinance»*, (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438299 .

Harwell Drew, *«Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use»*, (2019), διαθέσιμο σε https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/ .

Hautala Laura, *«Playtime Is Over: Can Smart Toys Ever Be Safe?»*, (2016), διαθέσιμο σε https://www.cnet.com/news/internet-of-things-connected-smart-toys-rsa-security-conference.

Hayes Adam, *«The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets»*, (2015), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579448 .

Heilweil Rebecca, *«How virtual reality is helping seniors breathe new life into old memories»*, (2019), διαθέσιμο σε https://www.nbcnews.com/mach/science/how-virtual-reality-helping-seniors-breathe-new-life-old-memories-ncna1069461.

Henning Peter J., «*Should Congress Create a Crypto-Cop?»*, (2018), διαθέσιμο σε https://nyti.ms.

Henry M. Kim και Marek Laskowski, *«Towards an Ontology-Driven blockchain Design for Supply Chain Provenance»*, (2016), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828369 .

Hern Alex, *«Pokémon Go Becomes Global Craze as Game Overtakes Twitter for US Users»*, (2016), διαθέσιμο σε https://www.theguardian.com/technology/2016/jul/12/pokemon-go-becomes-global-phenomenon-as-number-of-us-users-overtakes-twitter.

Hersh Marion, *«Overcoming Barriers and Increasing Independence – Service Robots for Elderly and Disabled People»*, International Journal of Advanced Robotic Systems, Vol. 12/ 8, (2015), διαθέσιμο σε http://eprints.gla.ac.uk/101946/1/101946.pdf .

Herzog Rudolph, *«Rise of the Drones»*, διαθέσιμο σε https://www.laphamsquarterly.org/spies/rise-drones.

Higgins Stan, *«Saudi Central Bank to Test Ripple Payments Tech»*, (2018), διαθέσιμο σε https://www.coindesk.com/saudi-central-bank-test-ripple-payments-tech.

Hill Beth, *«The important privacy lessons from Pokemon Go»*, (2016), διαθέσιμο σε https://iapp.org/news/a/beth-hill-the-important-privacy-lessons-from-pokemon-go/.

Hill Kashmir, *«This Tool Could Protect Your Photos From Facial Recognition»*, (2020), διαθέσιμο σε https://www.nytimes.com/2020/08/03/technology/fawkes-tool-protects-photos-from-facial-recognition.html.

Hill Kashmir, *«Facial Recognition Start-Up Mounts a First Amendment Defense»*, (2020), διαθέσιμο σε https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html .

Hobson Anne, *«Reality Check»*, (2016), διαθέσιμο σε https://www.rstreet.org/wp-content/uploads/2016/09/69.pdf.

Hody Peter, *«Crypto Currencies: Switzerland's New Banking Secrecy?»,* (2017), διαθέσιμο σε https://www.finews.com.

Holden Richard και Anup Malani, *«Why the I.R.S. fears Bitcoin»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/22/opinion/irs-bitcoin-fear.html.

Holmes Aaron, *«All it takes to fool facial recognition at airports and border crossings is a printed mask, researchers found»*, (2020), διαθέσιμο σε https://www.businessinsider.com/facial-recognition-fooled-with-mask-kneron-tests-2019-12 .

Holub Marc και Jackie Johnson, *«Bitcoin Price Anomalies on Localbitcoins: The AU$/BTC Market»*, (2018), διαθέσιμο σε https://cryptocoinsinfoclub.com/cryptocurrency/bitcoin-babe-localbitcoins .

Horizon 2020 Work Programme, European Commission (2015), διαθέσιμο http://ec.europa.eu/digitalagenda/sites/digital-agenda/files/discussions/h2020-wp1617-focus_en.pdf.

Houy Nicolas, *«It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency»*, (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393940 .

Hsieh Ying-Ying και Jean-Philippe Vergne, *«Bitcoin and the Rise of Decentralized Autonomous Organizations»*, Journal of Organization Design, Forthcoming, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082911 .

Huang Weihong, Renfa Li, Jianbo Xu, Yin Huang και Osama Hosam, *«Intellectual property protection for FPGA designs using the public key cryptography»*, (2019), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/1687814019836838 .

Hudson Laura, *«How to Protect Privacy While Using Pokémon Go and Other Apps»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/14/technology/personaltech/how-to-protect-privacy-while-using-pokemon-go-and-other-apps.html.

ICO, *«Big data, artificial intelligence, machine learning and data protection, Version: 2.2»*, (2017), διαθέσιμο σε https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf .

Iyidogan Engin, *«Incentive Mechanism and Economic Model of Blockchain Based Cryptocurrencies»*, (2018), διαθέσιμο σε https://www.competitionpolicyinternational.com/incentive-mechanism-and-economic-model-of-blockchain-based-cryptocurrencies/ .

Jackson Gavin, *«Job loss fears from automation overblown, says OECD»*, (2018), διαθέσιμο σε https://www.ft.com/content/732c3b78-329f-11e8-b5bf-23cb17fd1498 .

Jafari Saman, Tien Vo-Huu, Bahruz Jabiyev, Alejandro Mera και Reza Mirzazade Farkhani, *«Cryptocurrency: A Challenge to Legal System»*, (2018), διαθέσιμο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172489 .

Jansen P, Brey P, Fox A, Maas J, Hillas B, Wagner N, Smith P, Oluoch I, Lamers L, van Gein H, Resseguier A, Rodrigues R, Wright D, Douglas D, *«Ethical analysis of AI and robotics technologies»*, August, (2019), SIENNA D4.4, διαθέσιμο σε https://www.sienna-project.eu/digitalAssets/801/c_801912-l_1-k_d4.4_ethical-analysis .

Steven John, *«Does Nest work with Alexa?: How to connect Nest devices to Alexa for various at-home commands»*, (2020), διαθέσιμο σε https://www.businessinsider.com/does-nest-work-with-alexa .

Johnson Stephen, *«How designers are fighting the rise of facial recognition technology»*, (2019), διαθέσιμο σε https://bigthink.com/technology-innovation/facial-recognition?rebelltitem=2#rebelltitem2 .

Johnson Steven, *«Beyond the Bitcoin bubble»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/16/magazine/beyond-the-bitcoin-bubble.html.

Jouvenal Justin και Spencer S. Hsu, *«Facial recognition used to identify Lafayette Square protester accused of assault»*, (2020), διαθέσιμο σε https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html .

Kapur Neena, *«The Rise of IoT Botnets»*, (2017) διαθέσιμο σε https://www.americansecurityproject.org/the-rise-of-iot-botnets/.

Kathrani Paresh, *«Could intelligent machines of the future own the rights to their own creations?»*, (2017), διαθέσιμο σε https://theconversation.com/could-intelligent-machines-of-the-future-own-therights-to-their-own-creations-86005 .

Kavanaugh Jeff, *«How Mixed Reality and Machine Learning Are Driving Innovation in Farming»*, (2016), διαθέσιμο σε https://techcrunch.com/2016/11/17/how-mixed-reality-and-machine-learning-are-driving-innovation-in-farming .

Kelley Richard, Enrique Schaerer, Micaela Gomez και Monica Nicolescu, *«Liability in robotics: an international perspective on robots as animals»*, Advanced Robotics, Vol. 24/ 13, (2010), διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1163/016918610X527194 .

Khatwani Sudhir, *«Countries With 0% Tax On Bitcoin/Cryptos: Tax Free Life»*, (2019), διαθέσιμο σε https://coinsutra.com.

King Leo, Ford, *«Where Virtual Reality Is Already Manufacturing Reality»*, (2014), διαθέσιμο σε https://www.forbes.com/sites/leoking/2014/05/03/ford-where-virtual-reality-is-already-manufacturing-reality/#761025986e4d .

Klöver Chris και Alexander Fanta, *«No red lines: Industry defuses ethics guidelines for artificial intelligence»*, (2019) διαθέσιμο σε https://algorithmwatch.org/en/industry-defuses-ethics-guidelines-for-artificial-intelligence/.

Knapton Sarah, *«Care-bots' for the elderly are dangerous, warns artificial intelligence professor»*, (2016), διαθέσιμο σε https://www.telegraph.co.uk/science/2016/05/30/care-bots-for-the-elderly-are-dangerous-warns-artificial-intelli/ .

Knutson Ryan και Laura Stevens, *«Amazon and Google Consider Turning Smart Speakers into Home Phones»*, (2017), διαθέσιμο σε https://www.wsj.com/articles/amazon-google-dial-up-plans-to-turn-smart-speakers-into-home-phones-1487154781.

Kolo Kris, *«Mativision Launches World's First Virtual Medical Reality Training Facility»*, (2016), διαθέσιμο σε https://www.thevrara.com/blog2/2016/11/3/mativision-launches-worlds-first-virtual-medical-reality-training-facility .

Kottasová I., *«Jamie Dimon regrets calling bitcoin a 'fraud'»*, 2018, διαθέσιμο σε http://money.cnn.com.

Kovach Steve, *«It Sounds Like Google Glass Will Have Awful Battery Life»*, (2013), διαθέσιμο σε https://www.businessinsider.com/google-glass-poor-battery-life-2013-4 .

Kraakevik Jeff, *«Crafting a positive professional digital profile to augment your practice»*, (2016), διαθέσιμο σε https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5765898/#:~:text=A%20digital%20profile%20is%20the,profile%20is%20through%20social%20media .

Kreis Dylan, Daniel Magorrian και Gavin Moore, *«Current and Future Virtual Reality Applications and the Application of User Experience Design Principles»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3173934 .

Kuchera Ben, *«How Should Parents Treat Violence in Virtual Reality?»*, (2016) διαθέσιμο σε https://www.polygon.com/2016/2/26/11120792/how-should-parents-treat-violence-in-virtual-reality.

Kulkarni Nitish, *«Stanford Researchers Treat Autism with Google Glass»*, (2015), διαθέσιμο σε https://techcrunch.com/2015/10/19/stanford-researchers-treat-autism-with-google-glass .

Lancheres Eric, *«Virtual Reality Is Coming and It Will Change the World in 2016»*, (2015), διαθέσιμο σε https://www.engadget.com/2015-11-15-virtual-reality-is-coming-and-it-will-change-the-world-in-2016.html.

Langston Jennifer, *«Parents who play 'Pokémon GO' with kids: 'It wasn't really about the Pokémon»*, (2017), διαθέσιμο σε https://www.washington.edu/news/2017/03/28/parents-who-play-pokemon-go-with-kids-it-wasnt-really-about-the-pokemon/ .

Larson Jeff, Surya Mattu, Lauren Kirchner και Julia AngwinMay, *«How We Analyzed the COMPAS Recidivism Algorithm»*, (2016), διαθέσιμο σε https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm .

Latimer John, *«Pennsylvania Senator Launches Drone Moratorium Law»*, Gov't Tech, (2015), διαθέσιμο σε http://www.govtech.com/state/Pennsylvania-Senator-Launches-Drone-Moratorium-Law.html [https://perma.cc/GU6G-6U5K]

Leising Matthew, *«U.S. Regulators Subpoena Crypto Exchange Bitfinex»*, Tether, (2018), διαθέσιμο σε https://www.bloomberg.com/news/articles/2018-01-30/crypto-exchange-bitfinex-tether-said-to-get-subpoenaed-by-cftc .

Leinz Kailey, *«People Desperate to Buy Bitcoin Are Paying With Credit Cards»*, (2018), διαθέσιμο σε https://www.bloomberg.com/news/articles/2018-01-11/bitcoin-buyers-turn-to-credit-cards-as-fomo-breeds-risk-taking .

Leiva Ashley, *«How VR Experiments at Sundance Are Bringing Our Bodies into the Picture»*, (2016), διαθέσιμο σε https://www.wareable.com.

Leuz Christian, Steffen Meyer, Maximilian Muhn, Eugene Soltes και Andreas Hackethal, *«Who Falls Prey to the Wolf of Wall Street? Investor Participation in Market Manipulation»*, διαθέσιμο σε https://ideas.repec.org/p/nbr/nberwo/24083.html (2017).

Lewis Tanya, *«Virtual Reality Treatment Relieves Amputee's Phantom Pain»* (2014), διαθέσιμο σε https://www.scientificamerican.com/author/tanya-lewis.

Lewis Tanya, *«Virtual-Reality Tech Helps Treat PTSD in Soldiers»*, (2014), διαθέσιμο σε https://www.livescience.com/47258-virtual-reality-ptsd-treatment.html .

Li Angela, Zorash Montaño, Vincent J Chen και Jeffrey I Gold, *«Virtual reality and pain management: current trends and future directions»*, (2011), διαθέσιμο σε https://pubmed.ncbi.nlm.nih.gov/21779307/ .

Li Tiffany και Charles Roslof, *«Robots vs. Monkeys: Intellectual Property Rights of Non-Human Creators»*, [Poster Session], (2016), διαθέσιμο σε https://ssrn.com/abstract=2756245 .

Liew Jim Kyung - Soo, Richard Ziyuan Li, Tamás Budavári και Avinash Sharma, *«Cryptocurrency Investing Examined»*, (2019), διαθέσιμο σε https://jbba.scholasticahq.com/article/8720-cryptocurrency-investing-examined .

Liew Jim Kyung-Soo και Levar Hewlett, *«The Case for Bitcoin for Institutional Investors: Bubble Investing or Fundamentally Sound?»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3082808 .

Lince Tim, *«Virtual Reality Is Set to Emerge as a New Trademark Battleground, Brand Owners Are Warned»*, (2016), διαθέσιμο σε https://www.worldtrademarkreview.com/brand-management/virtual-reality-set-emerge-new-trademark-battleground-brand-owners-are-warned .

Liptak Andrew, *«Three major banks confirm that they won't allow cryptocurrency transactions with their credit cards»*, (2018), διαθέσιμο σε https://www.theverge.com/2018/2/4/16971666/cryptocurrency-bitcoin-jpmorgan-chase-bank-of-america-citigroup-credit-card .

Lomas Natasha, *«Pokemon Go T&Cs strip users of legal rights»*, (2016), διαθέσιμο σε https://techcrunch.com/2016/07/17/pokemon-go-tcs-strip-users-of-legal-rights/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEJiAr0pm33gSskRgQXoVzwZutNnIww-YCRfyuwdyJB2r7kbgYHL8xo7FnWtu3yiTAaSnnlHSGCRu8hXGI3OaPBdSC_PdhgQLikVE6mEmyqsHgOETRHQk9niJtsaPaJECanH92A9gMqWDzcVZErIAjiNf7M5g0Hy9oyy9_uCWNGE.

Lubell Sam, *«VR Is Totally Changing How Architects Dream Up Buildings»*, (2016), διαθέσιμο σε https://www.wired.com/2016/11/vr-totally-changing-architects-dream-buildings .

Machkovech Sam, *«Ars Tests The Nest, the HTC Vive's First VR Sniper Simulator»*, (2016), διαθέσιμο σε https://arstechnica.com/gaming/2016/06/ars-tests-the-nest-the-htc-vives-first-vr-sniper-simulator.

Malinova Katya και Andreas Park, «Market Design with blockchain Technology», (2017), διαθέσιμο σε https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/19_slides_park.pdf?la=en .

Malhotra Yogesh, *«Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System»*, (2013), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2911623 .

Manjoo Farhad, *«If You Like Immersion, You'll Love This Reality»*, (2014), διαθέσιμο σε https://www.nytimes.com.

Manoj Viswanathan, *«Tax Compliance in a Decentralizing Economy»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002213 .

Markovitz Leon, *«Venezuela's Petro Cryptocurrency Is a Gift to Future Generations»*, (2018), διαθέσιμο σε https://www.coindesk.com/venezuelas-petro-cryptocurrency-is-a-gift-to-future-generations .

Marr Bernard, *«What The Heck is… The Internet of Things?»* (2013), διαθέσιμο σε https://www.linkedin.com/pulse/20131023054859-64875646-what-the-heck-is-the-internet-of-things.

Marr Bernard, *«How Big Data Is Disrupting Law Firms And The Legal Profession»*, (2016), διαθέσιμο σε https://www.forbes.com/sites/bernardmarr/2016/01/20/how-big-data-is-disrupting-law-firms-and-the-legal-profession/?sh=157daecf7c23 .

Martindale Jon, *«What is augmented reality? Augmented reality brings VR to the real world in all sorts of exciting ways»*, (2019), διαθέσιμο σε https://www.digitaltrends.com/virtual-reality/what-is-augmented-reality.

Mart´ınez-Miranda Enrique και Peter McBurney and Matthew J. Howard, *«Learning Unfair Trading: a Market Manipulation Analysis From the Reinforcement Learning Perspective»*, (2015), διαθέσιμο σε https://arxiv.org/pdf/1511.00740.pdf .

Martins Bruno Oliveira, *«The European Union and armed drones: framing the debate»*, Global Affairs, Vol. 1/ 3, 2015, διαθέσιμο σε https://www.tandfonline.com/doi/abs/10.1080/23340460.2015.1080930 .

Martins Nuno R. B., Amara Angelica, Krishnan Chakravarthy, Yuriy Svidinenko, Frank J. Boehm, Ioan Opris, Mikhail A. Lebedev, Melanie Swan, Steven A. Garan, Jeffrey V. Rosenfeld,Tad Hogg και Robert A. Freitas Jr, *«Human Brain/Cloud Interface»*, (2019), διαθέσιμο σε https://www.frontiersin.org/articles/10.3389/fnins.2019.00112/full.

Mazur Michal, *«Six Ways Drones are Revolutionizing Agriculture»*, (2016), διαθέσιμο σε https://www.technologyreview.com/s/601935/six-ways-drones-are-revolutionizing-agriculture.

McArthur Steven, *«Right of Publicity in Video Games: How You Can Legally Include a Celebrity in Your Game»*, (2014), διαθέσιμο σε https://www.gamasutra.com/blogs/StephenMcArthur/20141117/230361/Right_of_Publicity_in_Video_Games__How_You_Can_Legally_Include_a_Celebrity_in_Your_Game.ph .

Mcquaid Darius, *«It's a revolution' Cryptocurrency investors flock to Swiss town Crypto Valley»*, (2018), διαθέσιμο σε https://www.express.co.uk.

Metz Rachel, *«Google Glass Is Dead; Long Live Smart Glasses»*, (2014), διαθέσιμο σε https://www.technologyreview.com/2014/11/26/169918/google-glass-is-dead-long-live-smart-glasses/ .

Michael Kimani, *«SALT Lending and Mauritius State Bank Partner on blockchain Backed Cash Loans»*, (2017), διαθέσιμο σε https://cryptovest.com.

Miller, *«The Moral Hazards and Legal Conundrums of our Robot-Filled Future»*, (2014), διαθέσιμο σε https://www.wired.com/2014/07/moral-legal-hazards-robot-future.

Mittelstadt Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter και Luciano Floridi, *«The ethics of algorithms: Mapping the debate»*, (2016), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/2053951716679679 .

Mnuchin Steven, *«Bitcoin shouldn't become the new 'Swiss bank account': Mnuchin»*, (2018), διαθέσιμο σε https://www.thelocal.ch/20180113/bitcoin-shouldnt-become-the-new-swiss-bank-account-mnuchin.

Moreau Elise, *«13 Major Retailers and Services That Accept Bitcoin»*, (2018), διαθέσιμο σε https://www.lifewire.com.

Morgan Jacob, *«A Simple Explanation of The Internet of Things»*, (2014), διαθέσιμο σε https://www.forbes.com/sites/jacobmorgan/2014/05/13/simpleexplanation-internet-things-that-anyone-can-understand.

Murphy Kate, *«Your New Home: Ready to See Now, via Virtual Reality»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/05/12/style/virtual-reality-interior-design.html.

Narula Neha, *«Digital Currency Initiative and Federal Reserve Bank of Boston Announce CBDC Design Collaboration»*, (2020), διαθέσιμο σε https://medium.com/mit-media-lab-digital-currency-initiative/digital-currency-initiative-and-federal-reserve-bank-of-boston-announce-cbdc-design-collaboration-39041d8fe2 .

Neghaiwi Brenna Hughes, *«Top Swiss cryptocurrency lawyer questions 'stupid' ICO structure»*, (2018), διαθέσιμο σε https://uk.reuters.com.

Newman Jared, *«Google's Schmidt Roasted for Privacy Comments»*, (2009), διαθέσιμο σε https://www.pcworld.com/article/184446/googles_schmidt_roasted_for_privacy_comments.html .

Nicholson Eric, *«Dallas Anesthesiologist Being Sued Over Deadly Surgery Admits to Texting, Reading iPad During Procedures»*, (2014) διαθέσιμο σε http://blogs.dallasobserver.com/unfairpark/2014/04/dallas_anesthesiologist_cops_t.php .

O' Kane S., *«The FAA's Drone Regulations Won't Be Ready Until at Least 2017»*, VERGE, (2014) διαθέσιμο σε https://www.theverge.com/2014/12/10/7370955/the-faas-drone-regulations-wont-be-ready-until-at-least-2017 .

Offenhartz Jake και George Joseph, *«De Blasio Will Reassess NYPD's Use Of Facial Recognition Tech After Protester Arrest»*, (2020), διαθέσιμο σε https://gothamist.com/news/de-blasio-will-reassess-nypds-use-facial-recognition-tech-after-protester-arrest .

Omri Marian Y., *«Are Cryptocurrencies 'Super' Tax Havens?»*, (2013), διαθέσιμο σε https://repository.law.umich.edu/mlr_fi/vol112/iss1/2.

Osoba Osonde A. και William Welser IV, *«The Risks of Artificial Intelligence to Security and the Future of Work»*, Santa Monica, CA: RAND Corporation, (2017), διαθέσιμο σε . https://www.rand.org/pubs/perspectives/PE237.html .

Ozelli Selva, *«Why Switzerland is Becoming a Crypto Nation with a Flourishing ICO Market: Expert Take»*, (2018), διαθέσιμο σε https://cointelegraph.com.

Özgür Gürerk και Alina Kasulke, *«Does Virtual Reality Increase Charitable Giving? An Experimental Study»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072002 .

Pascu Luana, *«France looks to establish legal framework to deploy biometric video surveillance»*, (2020), διαθέσιμο σε https://www.biometricupdate.com/202001/france-looks-to-establish-legal-framework-to-deploy-biometric-video-surveillance .

Pearce Matt, *«Johns Hopkins Gynecologist with Camera: Victims to Get $190 Million»*, (2014), διαθέσιμο σε www.latimes.com/nation/nationnow/la-na-nn-johns-hopkins-gynecologist-photos-settlement-20140721-story.html .

Peterson Andrea, *«Holocaust Museum to visitors: Please stop catching Pokémon here»*, (2016), διαθέσιμο σε https://www.washingtonpost.com/ .

Phalippou Ludovic, *«The Future of Private Markets»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3170928 .

Pham Lisa, *«This Company Added the Word 'Blockchain' to Its Name and Saw Its Shares Surge 394%»*, (2017), διαθέσιμο σε https://www.bloomberg.com/news/articles/2017-10-27/what-s-in-a-name-u-k-stock-surges-394-on-blockchain-rebrand .

Pierce David, *«I Watched the Debate in Virtual Reality. Things Got Weird»*, (2015), διαθέσιμο σε https://www.wired.com/2015/10/dnc-debate-virtual-reality-gear-vr/ .

Pollock Darryn, *«Ethereum Island Mauritius Craves To Become blockchain Paradise»*, (2017), διαθέσιμο σε https://cointelegraph.com.

Polonski Vyacheslav W., *«How artificial intelligence conquered democracy»*, (2017), διαθέσιμο σε https://www.independent.co.uk/news/long_reads/artificial-intelligence-democracy-elections-trump-brexit-clinton-a7883911.html .

Popper Ben, *«This is how Facebook will animate you in VR»*, (2016), διαθέσιμο σε https://www.theverge.com/2016/10/6/13176906/oculus-connect-3-facebook-social-vr-avatars

Popper Nathaniel, *«As Bitcoin bubble loses air, frauds and flaws rise to surface»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html.

Popper Nathaniel, *«Bitcoin exchange was a nexus of crime, indictment says»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html .

Popper Nathaniel, *«Bitcoin hasn't replaced cash, but investors don' t care»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/12/06/technology/bitcoin-payments-gold.html .

Popper Nathaniel, *«Bitcoin Sees Wall Street Warm to Trading Virtual Currency»*, (2018), διαθέσιμο σε https://www.nytimes.com.

Popper Nathaniel, *«Bitcoin's price has soared. What comes next?»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html.

Popper Nathaniel, *«Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/06/13/technology/bitcoin-price-manipulation.html.

Popper Nathaniel, *«Cryptocurrencies come to Campus»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/02/08/technology/cryptocurrencies-come-to-campus.html.

Popper Nathaniel, *«Move over Bitcoin. Ether is the digital currency of the moment»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html.

Popper Nathaniel, *«One Firm Is Way Ahead of Wall Street on Bitcoin»*, (2018), διαθέσιμο σε https://www.nytimes.com.

Popper Nathaniel, *«Rise of Bitcoin competitor Ripple creates wealth to rival Zuckerberg»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/04/technology/bitcoin-ripple.html.

Popper Nathaniel, *«There is nothing virtual about Bitcoin's energy appetite»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/21/technology/bitcoin-mining-energy-consumption.html.

Popper Nathaniel, *«What is Bitcoin? All about the mysterious digital currency»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/05/15/business/all-about-bitcoin-the-mysterious-digital-currency.html.

Post Kollen, *«US Congressman Introduces Crypto-Currency Act of 2020»*, (2020), διαθέσιμο σε https://cointelegraph.com/news/us-congressman-introduces-crypto-currency-act-of-2020.

Price Lloyd, *«7 ways Google Glass is revolutionising healthcare»*, (2020), διαθέσιμο σε https://www.healthcare.digital/single-post/2017/08/23/7-ways-Google-Glass-is-revolutionising-healthcare .

Pruthi Hitesh, Hardik Parvadiya,Varun Rawool και Joel Philip, *«Artificial Intelligence Dietician»*, (2017), διαθέσιμο σε https://www.ijrter.com/papers/volume-3/issue-2/artificial-intelligence-dietician.pdf .

Redman Jamie, *«Las Vegas Strip Club Aims to Use Cryptocurrency for Daily Operations»*, (2017), διαθέσιμο σε https://news.bitcoin.com/las-vegas-strip-club-cryptocurrency-daily-operations/ .

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997), διαθέσιμο σε https://supreme.justia.com/cases/federal/us/521/844/.

Rességuier Anaïs και Rowena Rodrigues, *«AI ethics should not remain toothless! A call to bring back the teeth of ethics»*, (2020), διαθέσιμο σε https://journals.sagepub.com/doi/full/10.1177/2053951720942541 .

Reuben Jackson *«Bitcoin mining uses as much energy as mining for gold, according to new research»* (2018), διαθέσιμο σε https://www.weforum.org/agenda/2018/11/study-reveals-that-bitcoin-mining-uses-as-much-energy-as-mining-for-gold/ .

Rivington J., *«Google Glass: what you need to know»*, (2013), διαθέσιμο σε https://www.techradar.com.

Rodrigues Rowena, *«AI and robotics adverse impacts – how resilient or vulnerable are we?»*, (2020), διαθέσιμο σε https://www.trilateralresearch.com/ai-and-robotics-adverse-impacts-how-resilient-or-vulnerable-are-we/ .

Rodrigues Rowena και Anaïs Rességuier, Trilateral Research, *«The underdog in the AI ethical and legal debate: human autonomy»*, (2019), διαθέσιμο σε https://www.ethicsdialogues.eu/2019/06/12/the-underdog-in-the-ai-ethical-and-legal-debate-human-autonomy/ .

Roettgers Janco, *«Sharks, Survival and Surfing: Discovery Goes Virtual Reality with New Apps»*, (2015), διαθέσιμο σε https://finance.yahoo.com/news/sharks-survival-surfing-discovery-goes-virtual-reality-apps-172530893.html .

Rogers James, *«Death by Pokemon? Public safety fears mount as 'Pokemon GO' craze continues»*, (2016), διαθέσιμο σε https://www.foxnews.com/tech/death-by-pokemon-public-safety-fears-mount-as-pokemon-go-craze-continues.

Rohrer Brandon, *«An Adaptive Learning Algorithm for the Internet of Things»*, (2016), διαθέσιμο σε https://brohrer.github.io/adaptive_reinforcement_learning_iot.html.

Roose Kevin, *«I was wrong about Bitcoin. Here is why»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/12/12/technology/bitcoin-predictions.html.

Roose Kevin, *«Kodak's dubious cryptocurrency gamble»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/01/30/technology/kodak-blockchain-bitcoin.html.

Rosen Rebecca J., *«In Praise of Short-Term Thinking»*, (2015), διαθέσιμο σε https://www.theatlantic.com/business/archive/2015/09/jobs-automation-technologicalunemployment-history/403576/ .

Rosenblatt Bill, *«Dot blockchain Media Makes blockchain Plus Watermarking a Reality»*, (2018), διαθέσιμο σε https://copyrightandtechnology.com.

Rosenblatt Bill, *«Get Ready for the blockchain Tsunami»*, (2018), διαθέσιμο σε https://copyrightandtechnology.com.

Rosenblatt Bill, *«Judge's Ruling in Redbox Case Raises Concerns for Physical/Digital Content Bundles»*, (2018), διαθέσιμο σε https://copyrightandtechnology.com.

Rosenblatt Bill, *«New White Paper: Watermarking Technology and blockchains in the Music Industry»*, (2017), διαθέσιμο σε https://copyrightandtechnology.com.

Rosic Ameer, *«What Is Hashing? Under The Hood Of blockchain»*, (2017), διαθέσιμο σε https://blockgeeks.com/guides/what-is-hashing/.

Rothman Joshua, *«Are We Already Living in Virtual Reality?»*, (2018). διαθέσιμο σε https://www.newyorker.com/magazine/2018/04/02/are-we-already-living-in-virtual-reality

Russell Stuart και Peter Norvig, *«Artificial Intelligence: A Modern Approach»*, (2010), διαθέσιμο σε https://www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf .

Sablich Justin, *«Let Pokémon Go Be Your Tour Guide»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/13/travel/pokemon-go-nyc-tourism.html.

Sahdev Navroop K., *«The Tokenization of the Economy: ICOs and the Implications for Entrepreneurship»*, (2017), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3057083 .

Salomatin Konstantin και Shura Burtin, *«Beyond Orwell's Worst Nightmares: How China Uses Artificial Intelligence to Commit Genocide»*, (2019), διαθέσιμο σε https://bylinetimes.com/2019/11/18/beyond-orwells-worst-nightmares-how-china-uses-artificial-intelligence-to-commit-genocide/ .

Sami Ahmed J.D., *«Cryptocurrency & Robots: How To Tax and Pay Tax on Them»*, (2017), διαθέσιμο σε https://www.kellogghansen.com/assets/htmldocumentsu/CryptocurrencydRobots-HowToTaxAndPayTaxOnThem69S.C.L.Rev.6972018.pdf .

Sample Ian, *«Watchdog criticises 'chaotic' police use of facial recognition»*, (2019), διαθέσιμο σε https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition .

Santos Maria, *«Singapore revenue authority recognizes and taxes Bitcoin»*, (2018), διαθέσιμο σε https://99bitcoins.com/singapore-revenue-authority-recognizes-and-taxes-bitcoin/

(Dos) Santos Renato, *«On the Philosophy of Bitcoin/blockchain Technology: Is It a Chaotic, Complex System?»*, (2017), διαθέσιμο σε https://onlinelibrary.wiley.com/doi/abs/10.1111/meta.12266 .

Schaerer Enrique, Richard Kelley και Monica Nicolescu, *«Robots as Animals: A Framework for Liability and Responsibility in Human-Robot Interactions»*, RO-MAN 2009 - The 18th IEEE

International Symposium on Robot and Human Interactive Communication, (2009), διαθέσιμο σε https://ieeexplore.ieee.org/document/5326244/citations#citations .

Schechter Sonia, *«Virtual Reality for Retail: Lowe's Holoroom Rolls Out to US Retail Locations»*, (2015), διαθέσιμο σε https://www.marxentlabs.com.

Schmitt Angie, *«Uber Got Off the Hook for Killing a Pedestrian with its Self-Driving Car»*, (2019), διαθέσιμο σε https://usa.streetsblog.org/2019/03/08/uber-got-off-the-hook-for-killing-a-pedestrian-with-its-self-driving-car/ .

Schwab Klaus, *«The Fourth Industrial Revolution»*, (2017), διαθέσιμο σε https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab .

Schwartzel Erich, *«Virtual-Reality Movies: Get Ready for the VR Revolution»*, (2016), διαθέσιμο σε https://www.wsj.com/articles/virtual-reality-movies-get-ready-for-the-vr-revolution-1457030357 .

Scimeca Dennis, *«Resident Evil 7 in Virtual Reality Is a Heart Attack Waiting to Happen»*, (2016), διαθέσιμο σε https://www.dailydot.com/parsec/resident-evil-7-teaser-demo-e3-2016.

Scott Marc και Natasha Singer, *«How Europe Protects your Online Data Differently than the US»*, (2016), διαθέσιμο σε https://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html.

Segal David, *«Hey, You Free on Friday for a Meeting and a Bank Heist?»*, (2020), διαθέσιμο σε https://www.nytimes.com/2020/07/31/business/video-game-meetings.html.

Segerdahl Pär, *«Ethical frameworks for research»*, (2020), διαθέσιμο σε https://ethicsblog.crb.uu.se/2020/08/19/ethical-frameworks-for-research/ .

Segerdahl Pär, *«Ethics as renewed clarity about new situations»*, (2020), διαθέσιμο σε https://ethicsblog.crb.uu.se/2020/08/26/ethics-as-renewed-clarity-about-new-situations/ .

Seidenberg Steven, *«Copyright in the Age of YouTube»*, (2009), διαθέσιμο σε https://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube.

Semple Kirk και Nathaniel Popper, *«Venezuela Launches Virtual Currency,Hoping to Resuscitate Economy»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/02/20/world/americas/venezuela-petro-currency.html.

Sharkey Amanda και Natalie Wood, *«The Paro seal robot: demeaning or enabling?»*, διαθέσιμο σε http://doc.gold.ac.uk/aisb50/AISB50-S17/AISB50-S17-Sharkey-Paper.pdf .

Shepherd Katie, *«An artist stopped posting protest photos online to shield activists from police. Then, he was arrested»*, (2020), διαθέσιμο σε https://www.washingtonpost.com/nation/2020/08/03/philadelphia-arrest-protest-photos/ .

Shin Laura, *«Ripple's Chris Larsen: Meet The Richest Person In Cryptocurrency»*, (2018), διαθέσιμο σε https://www.forbes.com/sites/laurashin/2018/02/07/ripple-chris-larsen-xrp-crypto-cryptocurrency/#6c3f9cd75e03.

SIENNA, D4.1: State-of-the-art Review, (2018), διαθέσιμο σε https://www.sienna-project.eu/digitalAssets/787/c_787382-l_1-k_sienna-d4.1-state-of-the-art-review--final-v.04-.pdf

Sigal Samuel, *«Activists want Congress to ban facial recognition. So they scanned lawmakers' faces»*, (2019), διαθέσιμο σε https://www.vox.com/future-perfect/2019/11/15/20965325/facial-recognition-ban-congress-activism .

Sintumuang Kevin, *«This Pocketable Camera Gear Will Change the Way You Take Travel Photos»*, (2016), διαθέσιμο σε https://www.wsj.com/articles/this-pocketable-camera-gear-will-change-the-way-you-take-travel-photos-1467311630.

Skenazy Lenore, *«Beware of Pokémon Go. Also, Rollerskates»*, (2016), διαθέσιμο σε https://www.wsj.com/articles/beware-of-pokemon-go-also-rollerskates-1468796256.

Slyter Kirsten, *«What Is Information Technology? A Beginner's Guide to the World of IT»*, (2019), διαθέσιμο σε https://www.rasmussen.edu/degrees/technology/blog/what-is-information-technology.

Smith Lauren, *«Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making»*, (2017), διαθέσιμο σε https://fpf.org/2017/12/11/unfairness-by-algorithm-distilling-the-harms-of-automateddecision-making/ .

Smith Rebecca, *«First Operation Streamed Live with Surgeon Wearing Google Glass»*, (2014), διαθέσιμο σε www.telegraph.co.uk/health/healthnews/10851116/First-operation-streamed-livewith-surgeon-wearing-Google-glass.html.

SnatchBot Team, *«How Legal Chatbots Will Automate Lawyer Services in the Future»*, (2020), διαθέσιμο σε https://snatchbot.me/amp/blog/130/legal-chatbots .

Soble Jonathan, *«Driver in Japan Playing Pokémon Go Kills Pedestrian»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/08/26/business/japan-driver-pokemon-go-kills-pedestrian.html.

Solmecke Wilde Beuger, *«Civilian Drones and the Legal Issues Surrounding Their Use»*, (2014), διαθέσιμο σε https://www.wbs-law.de/internetrecht/civilian-drones-legal-issues-surrounding-use-50459.

Solsman Joan E., *«Juiced for Olympics in VR? Better Grab a Samsung Headset»*, (2016), διαθέσιμο σε https://www.cnet.com/news/juiced-about-olympics-in-virtual-reality-better-grab-a-samsung-headset.

Spangler Todd, *«Netflix, Hulu to Launch Virtual-Reality Apps»*, (2015), διαθέσιμο σε https://variety.com/2015/digital/news/netflix-hulu-virtual-reality-apps-1201601645 .

Squires Peter, *«Evaluating CCTV: Lessons from a Surveillance Culture, Citizens, Cities, and Video Surveillance»*, (2010), διαθέσιμο σε http://efus.eu/files/2013/05/CCTV_ANGLAIS.pdf

Stanley Aaron, *«The rise — and fall — of the cryptocurrency millionaires»*, (2018), διαθέσιμο σε https://www.ft.com/content/d0df4322-1559-11e8-9c33-02f893d608c2.

Stassen Maarten, *«The EU Cybersecurity Act: Addressing the Risks of a Connected Europe»*, (2019), διαθέσιμο σε https://www.retailconsumerproductslaw.com/2019/08/the-eu-cybersecurity-act-addressing-the-risks-of-a-connected-europe/.

Stavroyiannis Stavros, *«Expected Shortfall via Filtered Historical Simulation for Bitcoin and Ethereum»*, (2018), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162537

Stegner Ben, *«8 Ridiculous EULA Clauses You May Have Already Agreed To»*, (2019), διαθέσιμο σε https://www.makeuseof.com/tag/10-ridiculous-eula-clauses-agreed/ .

Stibel Jeff, *«Google Is Already in Our Nests»*, (2014), διαθέσιμο σε http://www.breakpointbook.com/google-nests-privacy-jeff-stibel.

Streitfeld David, *«Chasing Pokémon, a Baby Step Toward Virtual Reality»*, (2016) διαθέσιμο σε https://www.nytimes.com/2016/07/22/technology/personaltech/chasing-pokemon-a-baby-step-toward-virtual-reality.html

Sutner Shaun, *«Blockchain payroll systems coming to HR tech»*, (2018), διαθέσιμο σε https://searchhrsoftware.techtarget.com/feature/Blockchain-payroll-systems-coming-to-HR-tech.

Swanson Brett, *«The 5G-Pokémon Moment»*, (2016), διαθέσιμο σε https://www.aei.org/technology-and-innovation/innovation/5g-pokemon-moment.

Tardi Carla, *«Near-Field Communication (NFC)»*, (2020), διαθέσιμο σε https://www.investopedia.com/terms/n/near-field-communication-nfc.asp .

Tashea Jason, *«Courts Are Using AI to Sentence Criminals. That Must Stop Now»*, (2017), διαθέσιμο σε https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now/ .

Thierer Adam, *«Muddling Through: How We Learn to Cope with Technological Change»*, (2014), διαθέσιμο σε https://techliberation.com.

Thompson Clive, *«Googling Yourself Takes On a Whole New Meaning»*, (2013), διαθέσιμο σε https://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html .

Thompson II Richard M., *«Domestic Drones and Privacy: A Primer»*, (2015), διαθέσιμο σε https://fas.org/sgp/crs/misc/R43965.pdf.

Torpey Kyle, *«The Republic of Mauritius's Regulatory Sandbox Could Attract blockchain Startups»*, (2017), διαθέσιμο σε https://bitcoinmagazine.com.

Ugelvig Jeppe, *«8 Artists Pushing the Limits of Digital Effects and VR»*, (2019), διαθέσιμο σε https://www.artsy.net/article/artsy-editorial-8-artists-pushing-limits-digital-effects-vr .

Vasic Milos και Aude Billard, *«Safety issues in human-robot interactions»*, 2013 IEEE International Conference on Robotics and Automation, IEEE, (2013), διαθέσιμο σε https://ieeexplore.ieee.org/abstract/document/6630576 .

Victor Daniel, *«Security Breach at Toy Maker VTech Includes Data on Children»*, (2015), διαθέσιμο σε https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html .

Villamena Vincenzo, *«Cryptocurrency and taxes: What you need to know»*, (2018), διαθέσιμο σε https://www.cnbc.com.

Wachter Sandra και Brent Mittelstadt, *«A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI»*, Columbia Business Law Review, 2019, διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829# .

Wakabayashi Daisuke, *«Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam»*, (2018), διαθέσιμο σε https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html .

Walton Joseph, *«Cryptocurrency Public Policy Analysis»*, (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2708302 .

Warso Zuzanna, *«Harnessing existing human rights jurisprudence to guide AI»*, (2019), διαθέσιμο σε https://digitalfreedomfund.org/harnessing-existing-human-rights-jurisprudence-to-guide-ai/ .

Wassom Brian D., *«How Pokémon GO Players Could Run Into Real-Life Legal Problems»*, (2016), διαθέσιμο σε https://www.hollywoodreporter.com/thr-esq/how-pok-mon-go-players-909869.

Watercutter Angela, *«This Ebola Documentary Shows VR Film's Radical Potential»*, (2015), διαθέσιμο σε https://www.wired.com/2015/09/vr-ebola-film.

Waynne Teddy, *«Grandpa had a pension. This generation has cryptocurrency»*, (2017), διαθέσιμο σε https://www.nytimes.com/2017/08/03/style/what-is-cryptocurrency.html.

Weber Beat, *«Can Bitcoin Compete with Money? Journal of Peer Production»*, Vol. 4, (2014), διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483867 .

Weber Tim, *«How Real Is Virtual Reality»*, (2016), διαθέσιμο σε https://techonomy.com/2016/12/real-virtual-reality/.

Weissmann Jordan, *«Amazon Created a Hiring Tool Using A.I. It Immediately Started Discriminating Against Women»*, (2018), διαθέσιμο σε https://slate.com/business/2018/10/amazon-artificial-intelligence-hiring-discrimination-women.html .

Weslow David E., *«Cybersquatting & Internet IP»*, διαθέσιμο σε https://www.wiley.law/practices-cybersquatting-and-internet-IP .

West Darrell M., *«The Ethical Dilemmas of Virtual Reality»*, (2016), διαθέσιμο σε https://www.brookings.edu/blog/techtank/2016/04/18/the-ethical-dilemmas-of-virtual-reality.

White & Case LLP, *«Algorithms and bias: What lenders need to know»*, (2017), διαθέσιμο σε https://www.lexology.com/library/detail.aspx?g=c806d996-45c5-4c87-9d8a-a5cce3f8b5ff .

Wiewiórowski Wojciech, *«Facial recognition: A solution in search of a problem?»*, (2019), διαθέσιμο σε https://edps.europa.eu/press-publications/press-news/blog/facial-recognition-solution-search-problem_en .

Wiles Paul, Annual Report 2018, Commissioner for the retention and use of biometric material, March 2019, διαθέσιμο σε https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf .

Williams Sean, *«5 Big Banks Currently Testing Ripple's blockchain Technology»*, (2017), διαθέσιμο σε https://www.fool.com/investing/2017/12/17/5-big-banks-currently-testing-ripples-blockchain-t.aspx.

Wingfield Nick και Mike Isaac, *«Pokémon Go Brings Augmented Reality to a Mass Audience»*, (2016), διαθέσιμο σε https://www.nytimes.com/2016/07/12/technology/pokemon-go-brings-augmented-reality-to-a-mass-audience.html .

Wingfield Nick και Vindu Goel, *«Facebook in $2 Billion Deal for Virtual Reality Company»*, (2014), διαθέσιμο σε https://www.nytimes.com.

Wong Wee Seng , Dennis Saerbeck, και Dante Delgado Silva, *«Cryptocurrency: A New Investment Opportunity? An Investigation of the Hedging Capability of Cryptocurrencies and Their Influence on Stock, Bond and Gold Portfolios»*, (2018) διαθέσιμο σε https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3125737.

Woo Marcus, *«Robots: can we trust them with our privacy»*, (2014), διαθέσιμο σε http://www.bbc.com/future/story/20140605-the-greatest-threat-of-robots .

World Economic Forum (In collaboration with The Boston Consulting Group), *«Towards a Reskilling Revolution: A Future of Jobs for All»*, (2018), διαθέσιμο σε http://www3.weforum.org/docs/WEF_FOW_Reskilling_Revolution.pdf .

Wu Tim, *«It's a Mad, Mad, Mad, Mad Disney World»*, (2013), διαθέσιμο σε https://www.newyorker.com/culture/culture-desk/its-a-mad-mad-mad-mad-disney-world.

Yang Junwei και Timothy Reuter, *«3 ways China is using drones to fight coronavirus»* (2020), διαθέσιμο σε https://www.weforum.org/agenda/2020/03/three-ways-china-is-using-drones-to-fight-coronavirus/ .

Yoon Clara, *«Assumptions that led to the failure of Google Glass»*, (2018), διαθέσιμο σε https://medium.com/nyc-design/the-assumptions-that-led-to-failures-of-google-glass-8b40a07cfa1e#:~:text=In%20an%20exploding%20digital%20market,on%20why%20this%20product%20exists.&text=This%20revolutionary%20product%20never%20succeeded,needed%20it%20in%20their%20lives.

Young J., *«South Korea More Than Doubled Ripple's Price in Single Week»*, (2018), διαθέσιμο σε https://cointelegraph.com.

Zawieska Karolina, *«Deception and manipulation in social robotics»*, Workshop on The Emerging Policy and Ethic of Human-Robot Interaction at the 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI2015), διαθέσιμο σε http://www.openroboethics.org/hri15/wp-content/uploads/2015/02/Mf-Zawieska.pdf .

Zornoza Alejandro, José C. Moreno, José L. Guzmán, Francisco Rodríguez και Julián Sánchez-Hermosilla, *«Robots Liability: A Use Case and a Potential Solution»*, Robotics-Legal, Ethical and Socioeconomic Impacts, InTech, (2017), διαθέσιμο σε https://www.intechopen.com/books/robotics-legal-ethical-andsocioeconomic-impacts/robots-liability-a-use-case-and-a-potential-solution .

Zurkus Kacy, *«FTC Says Data and Privacy Are Top Security Concerns»*, (2015), διαθέσιμο σε https://www.csoonline.com/article/2983853/ftc-says-data-and-privacy-are-top-security-concerns.html.

Ιστότοποι

http://informatics.teicm.gr

http://outerlimitsvirtualreality.com

http://nn.physics.auth.gr

http://www.goldmansachs.com

http://www.imf.org

http://www.inewsgr.com

http://www.nooz.gr

http://www.nytimes.com

http://www.realitytechnologies.com

http://www.secnews.gr

https://ada.com

https://blacklivesmatter.com

https://coinatmradar.com

https://coinmarketcap.com

https://dci.mit.edu

https://ec.europa.eu

https://en.bitcoin.it/wiki

https://en.wikipedia.org

https://eur-lex.europa.eu
https://greeklaw.wordpress.com
https://help.gnome.org
https://hpc.grnet.gr
https://ico.org.uk
https://internetofthingsagenda.techtarget.com
https://libertyvictoria.org.au
https://onchainfx.com
https://onlinelibrary.wiley.com
https://repository.kallipos.gr
https://searchnetworking.techtarget.com
https://solarcoin.org
https://techterms.com
https://unric.org
https://usa.visa.com
https://whatis.techtarget.com
https://wrohellas.gr
https://zarifopoulos.com
https://www.aade.gr
https://www.ama-assn.org
https://www.amnesty.gr
https://www.bankofgreece.gr
https://www.bitfinex.com
https://www.britannica.com
https://www.bynorth.com
https://www.chemist.gr
https://www.coinbase.com
https://www.coindesk.com
https://www.dpa.gr
https://www.defendproject.eu/
https://www.eetn.gr
https://www.eett.gr
https://www.europarl.europa.eu
https://www.fitbit.com
https://www.forbes.com
https://www.hfhr.pl/en
https://www.iatronet.gr
https://www.ibanet.org
https://www.iccs.gr
https://www.imf.org
https://www.investopedia.com
https://www.intgovforum.org
https://www.ired.gr
https://www.irs.gov
https://www.iti.gr
https://www.kathimerini.gr
https://www.law.cornell.edu
https://www.managementstudyguide.com
https://www.nature.com
https://www.news247.gr
https://www.nist.gov
https://www.ocf.berkeley.edu
https://www.oculus.com
https://www.ohchr.org
https://www.opi.gr
https://www.partnershiponai.org
https://www.paypal.com
https://www.possible.com
https://www.predpol.com
https://www.project-sherpa.eu
https://www.rand.org
https://www.realitytechnologies.com
https://www.refworld.org
http://www.robotics-openletter.eu

https://www.sas.com
https://www.sciencedirect.com
https://www.sienna-project.eu
https://www.snapchat.com
https://www.stellar.org
https://www.swissinfo.ch
https://www.techopedia.com
https://www.techopedia.com
https://www.tovima.gr
https://www.turing.ac.uk
https://www.weforum.org
https://www.westernunion.com
https://www.wikipedia.org
www.lawnet.gr
www.naftemporiki.gr
www.ncl.ac.uk
www.techgear.gr