ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ ΣΤΑ ΔΙΚΤΥΑ ΕΚΤΗΣ ΓΕΝΙΑΣ (6G) ΥΠΟΣΤΗΡΙΖΟΜΕΝΑ ΑΠΟ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ»

(LEGAL ISSUES ON 6G NETWORKS SUPPORTED BY ARTIFIACIAL INTELLIGENCE)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΦΟΙΤΗΤΡΙΑΣ ΜΑΡΙΑ ΛΑΛΑΚΟΥ Α.Μ. 321/2016085

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΛΙΛΙΑΝ ΜΗΤΡΟΥ

ΣΑΜΟΣ, ΟΚΤΩΒΡΙΟΣ, 2021

Ευχαριστίες

Με την ολοκλήρωση της διπλωματικής μου εργασίας, θα ήθελα αρχικά να εκφράσω την ευγνωμοσύνη μου και να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτρια της διπλωματικής μου εργασίας, κα Λίλιαν Μήτρου, για τη διαρκή βοήθεια, καθοδήγηση και εμπιστοσύνη καθ΄ όλο το διάστημα εκπόνησης της διπλωματικής μου εργασίας.

Επιπλέον, ιδιαίτερες ευχαριστίες θα ήθελα να απευθύνω στους γονείς μου Νικόλαο και Ευαγγελία αλλά και στα αδέρφια μου για τη συνεχή υποστήριξη καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι ο εντοπισμός, κατανόηση και ανάλυση των νομικών ζητημάτων που διέπουν τα δίκτυα έκτης γενιάς. Αναλυτικότερα πραγματοποιείται ανάλυση των εφαρμογών και τεχνολογιών που θα υποστηρίζουν και χρησιμοποιούν αντίστοιχα τα δίκτυα 6G ώστε να επιτευχθεί εξαγωγή των νομικών ζητημάτων που διέπουν τις εφαρμογές και τεχνολογίες των δικτυών έκτης γενιάς.

Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (Κανονισμό 2016/679 - ΓΚΠΔ), γνωστός και ως General Data Protection Regulation (GDPR), που έχει τεθεί σε ισχύ από τις 25 Μαΐου του 2018, έχει οδηγήσει σε θεμελιώδεις αλλαγές στον τομέα της συλλογής, επεξεργασίας, διαχείρισης και αποθήκευσης των προσωπικών δεδομένων από τις επιχειρήσεις και τους οργανισμούς που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση.

Για την αξιολόγηση των νομικών ζητημάτων που μπορεί να επιφέρει το 6G πραγματοποιείται εστίαση στις βασικές αρχές του ΓΚΠΔ, δηλαδή την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, την αρχή του περιορισμού του σκοπού, την αρχή της αναλογικότητας, την αρχή της ακρίβειας των δεδομένων, την αρχή του περιορισμού, την αρχή της ακεραιότητας και εμπιστευτικότητας και την αρχή της λογοδοσίας του υπευθύνου επεξεργασίας, όπως προβλέπεται από το άρθρο 5 του ΓΚΠΔ.

Όσο τα δίκτυα κινητών επικοινωνιών εξελίσσονται το απόρρητο των ανθρώπων κινδυνεύει, καθώς όλο και μεγαλύτερος όγκο από τα προσωπικά τους δεδομένα συλλέγεται, υπόκεινται σε επεξεργασία και αποθηκεύεται με ή χωρίς την συγκατάθεση τους για την παροχή και χρήση των υπηρεσιών που παρέχουν τα δίκτυα κινητών επικοινωνιών. Επομένως η κατανόηση των παραβιάσεων του δικτύου 6G στο απόρρητο και την ιδιωτική ζωή των ανθρώπων αποτελεί θέμα μείζονος σημασίας.

Λέξεις κλειδιά: 6G, Νομικά Ζητήματα, Τεχνητή Νοημοσύνη, ΓΚΠΔ, Απόρρητο, Ιδιωτική Ζωή.

Abstract

The purpose of this dissertation is to identify, understand and analyze the legal issues governing the sixth-generation networks. A more detailed analysis of the applications and technologies that will support and use the 6G networks is performed in order to identify the legal issues that relate to the applications and technologies of the sixth-generation networks.

The General Data Protection Regulation (Regulation 2016/679-GDPR), which entered into force on 25 May 2018, has led to fundamental changes in the sector of collection, processing, management and storage of personal data by companies and organizations operating in the European Union.

In order to assess the legal issues that 6G may poses, emphasis is put on the basic principles of the GPDR, namely the principle of legality, fairness and transparency, the principle of limitation of purpose, the principle of proportionality, the principle of data accuracy, the principle of restraint, the principle of integrity and confidentiality and the principle of accountability of the controller, as provided for in Article 5 of the GDPR.

As mobile networks evolve, people's privacy is at stake, as more and more of their personal data is collected, processed and stored with or without their consent to the provision and use of their services provide by mobile networks. Understanding 6G breaches of people's privacy is therefore a major issue.

Keywords: 6G, Legal Issues, Artificial Intelligence, GDPR, Privacy.

Πίνακας περιεχομένων

1. Εισαγωγή στα Δίκτυα 6ης Γενιάς

Τα Δίκτυα Πέμπτης Γενιάς (5G) έχουν ξεκινήσει να αναπτύσσονται παγκοσμίως από το 2020. Η αξιοπιστία, η μαζική συνδεσιμότητα και η χαμηλή καθυστέρηση του 5G δεν επαρκούν, ώστε να ικανοποιήσουν τις απαιτήσεις των νέων εφαρμογών του μέλλοντος. Σε αυτό το σημείο τα δίκτυα 6G με την αξιοποίηση της τεχνητής νοημοσύνης υπόσχονται να οδηγήσουν στην παροχή καινοτόμων εφαρμογών και υπηρεσιών και παράλληλα στη μείωση της καθυστέρησης, ώστε οι εφαρμογές και υπηρεσίες να παρέχονται σε πραγματικό χρόνο. Η παγκόσμια κάλυψη, η ασφάλεια, ο υψηλός ρυθμός δεδομένων και η εξαιρετικά χαμηλή καθυστέρηση αποτελούν τα θεμέλια των δικτύων έκτης γενιάς.

Η σημαντική αύξηση της κίνησης στα δίκτυα κινητής τηλεφωνίας που έχει παρατηρηθεί τα τελευταία χρόνια λόγω του αυξανόμενου αριθμού έξυπνων συσκευών αλλά και η ανάγκη για νέες υπηρεσίες δεν μπορεί να αντιμετωπιστεί από τα ήδη υπάρχοντα δίκτυα κινητής επικοινωνίας. Την λύση στο παραπάνω πρόβλημα υπόσχονται να φέρουν τα δίκτυα 6G. Παρά το γεγονός ότι οι προδιαγραφές για τα δίκτυα 5G εξακολουθούν να αναπτύσσονται, έχουν ήδη ξεκινήσει μελέτες για τα δίκτυα 6G. Τον Μάρτιο του 2019 πραγματοποιήθηκε στην Φιλανδία η πρώτη διάσκεψη κορυφής για το 6G στον κόσμο, με κορυφαίους επιστήμονες και συντάχθηκε η Λευκή Βίβλος του 6G [1].

Ως 6G ορίζονται τα δίκτυα ασύρματης επικοινωνίας έκτης γενιάς. Αποτελούν τον διάδοχό των δικτύων πέμπτης γενιάς και θα βασίζονται στην τεχνολογία κυψελοειδών δικτύων. Τα δίκτυα έκτης γενιάς αναμένεται να καλύψουν τις απαιτήσεις που δεν θα πληρούν τα δίκτυα 5G στο μέλλον από το 2030 και έπειτα καθώς θα χρησιμοποιούν υψηλότερες συχνότητες από το 5G και θα παρέχουν υψηλότερη χωρητικότητα και εξαιρετικά χαμηλή καθυστέρηση [2]. Το 6G θα αποτελέσει ένα άλμα της επιστήμης, μια επανάσταση και όταν τεθεί σε λειτουργία θα αλλάξει τον τρόπο που η ανθρωπότητα ζει. Τα δίκτυα έκτης γενιάς θα διαθέτουν ποικίλα πλεονεκτήματα και θα υποστηρίζουν ποικίλες νέες και καινοτόμες τεχνολογίες και υπηρεσίες. Στα κύρια πλεονεκτήματα που θα διαθέτουν ανήκουν η μαζική συνδεσιμότητα, η υψηλή ταχύτητα, η αξιοπιστία και η χαμηλή καθυστέρηση, στοιχεία τα όποια κρίνονται απαραίτητα για την σωστή λειτουργία των διαφόρων τεχνολογιών και εφαρμογών των δικτύων 6G.

Η υψηλή ταχύτητα και η χαμηλή καθυστέρηση αποτελούν τους δυο βασικούς πυλώνες των δικτύων 6G. Πιο συγκεκριμένα το 5G επιτρέπει την λήψη ταινίας σε λιγότερο από ένα λεπτό, ενώ το 6G θα έχει τη δυνατότητα λήψης περισσότερων από 140 ωρών ταινιών σε ένα λεπτό. Το 5G και 6G θα αξιοποιούν ασύρματο φάσμα υψηλότερου εύρους για να επιτυγχάνουν ταχύτερη μετάδοση δεδομένων. Ειδικότερα το φάσμα, το οποίο εμπίπτει στην περιοχή 95 GHz – 3 THz είναι διαθέσιμο για την πειραματική αξιοποίηση του από τα δίκτυα έκτης γενιάς. Το συγκεκριμένο φάσμα θα προσφέρει υψηλότερης ταχύτητας εφαρμογές και θα οδηγήσει στη βελτίωση των ήδη υπαρχουσών υποδομών και υπηρεσιών. Οι βασικές

διαφορές του 5G με το 6G είναι η χρήση διαφορετικού φάσματος, η αύξηση της ταχύτητας, η ακόμη χαμηλότερη καθυστέρηση και η ενσωμάτωση ακόμη περισσότερων συσκευών IoT στο δίκτυο. Παρατηρείται λοιπόν η ανάγκη για τη μετάβαση από τα δίκτυα πέμπτης γενιάς στα δίκτυα έκτης γενιάς, τα οποία θα διαθέτουν ισχυρότερα χαρακτηριστικά για την υποστήριξη εφαρμογών όπως η αυτόνομη οδήγηση, η ηλεκτρονική υγεία και τα έξυπνα περιβάλλοντα.

Για λόγους κατανόησης της διαφοροποίησης του 5G από το 6G παρατίθεται ο Πίνακα 1 στον οποίο γίνεται σύγκριση των βασικών χαρακτηριστικών των δυο αυτών δικτύων κινητών επικοινωνιών. Αρχικά είναι εμφανές ότι η αξιοπιστία (Reliability) του δικτύου γίνει $1\text{-}10^{-5}$ που είναι στο 5G αναμένεται να γίνει $1\text{-}10^{-9}$ στο 6G. Ο ρυθμό για την δημοσίευση δεδομένων (Uplink data rate) θα αυξηθεί από 10 Gbps στο 1 Tbps και ο ρυθμός λήψης δεδομένων (Downlink data rate) θα αυξηθεί από 20Gbps σε 1Tbps. Επιπλέον το 5G αξιοποιεί την μετάδοση terahertz σε περιορισμένη κλίμακα ενώ το 6G θα την αξιοποιεί ευρέως. Ακόμη η καθυστέρηση (Latency) θα μειωθεί από 1ms σε μικρότερη του 0,1ms. Η κινητικότητα (Mobility) από 500km/hr θα αυξηθεί σε 1000km/hr. Η συχνότητα (Operating frequency) από 3-30GHz θα αυξηθεί σε 1THz και η ακρίβεια εντοπισμού (Localization precision) από 10cm σε δισδιάστατο χώρο θα γίνει 1cm σε τρισδιάστατο χώρο. Τέλος γίνεται κατανοητό ότι η ενσωμάτωση τεχνητής νοημοσύνης (AI integration), εκτεταμένης πραγματικότητας (XR integration), αυτοματισμού (Automation integration), οπτικών επικοινωνιών (Haptic communication integration) και η δορυφορική ολοκλήρωση (Satellite integration) θα είναι πλήρης στο 6G σε αντίθεση με το 5G στο οποίο όλες οι παραπάνω λειτουργίες έχουν ενσωματωθεί εν μέρει.

Εικόνα 1. Τα δίκτυα έκτης γενιάς [3].

Η Τεχνητή Νοημοσύνη (Artificial Intelligence – AI), χρησιμοποιείται ήδη στα δίκτυα 5G σε περιορισμένη κλίμακα με σκοπό να παρέχει καλύτερη κατανομή πόρων, επεξεργασία δεδομένων, βελτιστοποίηση και χαμηλό λανθάνων χρόνο. Ο όρος τεχνητή νοημοσύνη αναφέρεται στην σχεδίαση και υλοποίηση μηχανών οι οποίες αναπαράγουν γνωστικές λειτουργίες του ανθρώπου, όπως η μάθηση, η προσαρμοστικότητα, η εξαγωγή συμπερασμάτων, η επίλυση προβλημάτων κλπ. [4]. Επομένως η χρήση της στα δίκτυα 6G αναμένεται να ανοίξει τον δρόμο για νέες και πρωτοποριακές δυνατότητες και εφαρμογές, όπως ολογραφική επικοινωνίας, αυτόνομα συστήματα κλπ. Επιπλέον η Μηχανική Μάθηση (Machine Learning) η οποία ορίζεται ως «το φαινόμενο κατά το οποίο ένα σύστημα βελτιώνει την απόδοση του κατά την εκτέλεση μιας συγκεκριμένης εργασίας, χωρίς να υπάρχει ανάγκη να προγραμματιστεί εκ νέου» [5], θα οδηγήσει σε αύξηση του αυτοματισμού του δικτύου όταν εφαρμοστεί μαζί με την τεχνητή νοημοσύνη. Ακόμη ο συνδυασμός τεχνητής νοημοσύνης και μηχανικής μάθησης θα ενισχύσει τις νέες αυτές τεχνολογίες και θα παρέχει μοναδικές εμπειρίες στον χρήστη. Όμως η στενή σύνδεση της τεχνητής νοημοσύνης και των δικτύων έκτης γενιάς δεν εγγυάται απαραίτητα την ασφάλεια και την προστασία της ιδιωτικής ζωής.

Το Διαδίκτυο των Πραγμάτων (Internet of Things) αποτελεί μια κορυφαία τεχνολογική εξέλιξη και αναφέρεται σε ένα δίκτυο επικοινωνίας ποικίλλων συσκευών που χρησιμοποιούν οι άνθρωποι με σκοπό την σύνδεση τους στο διαδίκτυο. Οι συσκευές αυτές διαθέτουν αισθητήρες, λογισμικά, ενεργοποιητές κλπ., ώστε να είναι δυνατή η πραγματοποίηση συλλογής και ανταλλαγής δεδομένων μεταξύ τους [6]. Στις συσκευές που αποτελούν το Διαδίκτυο των Πραγμάτων ανήκει μια μεγάλη ποικιλία συσκευών, όπως αυτοκίνητα, φώτα, κλιματιστικά, θερμοσίφωνες κλπ. Το βασικό πλεονέκτημα των παραπάνω συσκευών είναι τόσο ότι μπορούν να αλληλεπιδρούν μεταξύ τους όσο και ότι μπορούν να συνδέονται με τον υπολογιστή και το κινητό του χρήστη ώστε να μπορεί να πραγματοποιηθεί χειρισμός τους από απόσταση. Το Διαδίκτυο των Πραγμάτων θα βοηθήσει και ενισχύσει τις διάφορες εφαρμογές του 6G. Όμως ήδη αυτό και μόνο το πλήθος των συσκευών IoT στα δίκτυα 6G, καθώς θα αυξηθεί 10 φορές περισσότερο από την κλίμακα 10 δισεκατομμυρίων που αφορά τα δίκτυα 5G στην κλίμακα 100 δισεκατομμυρίων για το 6G αναμένεται να οδηγήσει στη δημιουργία σημαντικών κινδύνων για την ασφάλεια και το απόρρητο [7].

	5G	6G
Reliability	$1\text{-}10^{-5}$	$1\text{-}10^{-9}$
Uplink data rate	10Gbps	1Tbps
Downlink data rate	20Gbps	1Tbps
Latency	1ms	<0,1ms
Mobility	500km/hr	1000km/hr
Operating frequency	3-30GHz	1THz
Localization precision	10cm in 2D	1cm in 3D
THz communication	Very limited	Widely
AI integration	Partially	Fully
XR integration	Partially	Fully
Automation integration	Partially	Fully
Haptic communication integration	Partially	Fully
Satellite integration	Partially	Fully

Πίνακας 1. Σύγκριση του 5G με το 6G [8], [9], [10].

Όμως αυτές οι εξελίξεις στα δίκτυα κινητών επικοινωνιών θέτουν αρκετά νομικά ζητήματα. Οι ποικίλες εφαρμογές και τεχνολογίες του 6G θα διεισδύσουν στην ιδιωτική ζωή των ανθρώπων και η απαίτηση για ολοένα και περισσότερα προσωπικά δεδομένα για την παροχή και σωστή λειτουργία των εφαρμογών θα οδηγήσει στους περιορισμούς των ελευθεριών τους. Ο ΓΚΠΔ εν μέρει υπόσχεται την προστασία και τη νόμιμη συλλογή, επεξεργασία και αποθήκευση των προσωπικών δεδομένων των ανθρώπων. Όμως λόγω της εξέλιξης της τεχνολογίας ο ΓΚΠΔ ενδεχομένως δεν μπορεί να καλύψει το εύρος των νομικών ζητημάτων οδηγώντας στην παραβίαση των δικαιωμάτων των ανθρώπων.

Η παρούσα διπλωματική εργασία χωρίζεται σε πέντε κεφάλαια. Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στα δίκτυα 6G και αναλύονται τα βασικά χαρακτηριστικά και οι τεχνολογίες που θα αξιοποιήσουν. Επιπλέον παρατίθεται ένα πίνακας για τη σύγκριση των χαρακτηριστικών μεταξύ των δικτύων πέμπτης και έκτης γενιάς.

Στο δεύτερο κεφάλαιο αναλύονται οι βασικές εφαρμογές των δικτύων έκτης γενιάς. Στις εφαρμογές αυτές ανήκουν τα ψηφιακά δίδυμα, ο βιομηχανικός αυτοματισμός, οι ολογραφικές επικοινωνίες, τα συνδεδεμένα ρομποτικά και

αυτόνομα συστήματα, η ηλεκτρονική υγεία, η επαυξημένη και εικονική πραγματικότητα, η αυτόνομη οδήγηση και τέλος τα έξυπνα περιβάλλοντα.

Στο τρίτο κεφάλαιο πραγματοποιείται μια παράθεση των καίριων τεχνολογιών που θα ενσωματώσουν τα δίκτυα έκτης γενιάς. Ειδικότερα αναλύονται οι τεχνολογίες ενεργοποίησης: επικοινωνίες terahertz (THz), τεχνητή νοημοσύνη, μη επίγειες τεχνολογίες, οπτικές ασύρματες επικοινωνίες, edge intelligent, διαδίκτυο των πάντων (IoE) και multi – access edge computing (MEC). Για κάθε μια από τις παραπάνω τεχνολογίες παρατίθεται ορισμός της και γίνεται μια ανάλυση του τρόπου με τον οποίο θα συνδράμει στην ικανοποίηση των απαιτήσεων των δικτύων 6G.

Στο τέταρτο κεφάλαιο προκειμένου ο αναγνώστης να κατανοήσει καλύτερα τον Γενικό Κανονισμό Προστασίας Δεδομένων (εφεξής ΓΚΠΔ) παρατίθεται τα βασικά χαρακτηριστικά του. Αρχικά γίνεται μια σύντομη εισαγωγή και περιγραφή του ΓΚΠΔ και των βασικών εννοιών του Κανονισμού σύμφωνα με το άρθρο 4. Κατόπιν αναλύονται οι βασικές αρχές επεξεργασίας και το πεδίο εφαρμογής του Κανονισμού. Έπειτα αναφέρονται οι τρόποι για την νόμιμη επεξεργασία των δεδομένων. Η κατανόηση των νόμιμων τρόπων επεξεργασίας δεδομένων καθώς και της έγκυρης συγκατάθεσης είναι σημαντική ώστε να γίνουν πλήρως αντιληπτά τα νομικά ζητήματα που διέπουν τις εφαρμογές και τεχνολογίες του 6G. Στο τέλος του τρίτου κεφαλαίου περιγράφεται η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ σύμφωνα με το άρθρο 22 του ΓΚΠΔ.

Στο πέμπτο κεφάλαιο πραγματοποιείται ο εντοπισμός και η ανάλυση των νομικών ζητημάτων των δικτύων έκτης γενιάς. Πιο συγκεκριμένα αρχικά περιγράφεται η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ στα δίκτυα 6G και αναλύονται οι παραβιάσεις που θα προκαλέσει στην ιδιωτική ζωή των ανθρώπων. Στη συνέχεια εντοπίζονται κατά σειρά τα νομικά ζητήματα για την τεχνητή νοημοσύνη, την αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ, τα αυτόνομα οχήματα, τα ψηφιακά δίδυμα, τα έξυπνα περιβάλλοντα, την ηλεκτρονική υγεία, το διαδίκτυο των πραγμάτων και τέλος για την επαυξημένη, μικτή και εικονική πραγματικότητα.

Στο τέλος της διπλωματικής παρουσιάζονται τα συμπεράσματα που εξήχθησαν σχετικά με τα νομικά ζητήματα και την θυσία των προσωπικών δεδομένων στον βωμό του 6G για την παροχή των καινοτόμων εφαρμογών.

2. Εφαρμογές των Δικτύων 6ης Γενιάς

Ο χαμηλός λανθάνων χρόνος, ο υψηλός ρυθμός δεδομένων, η πανταχού παρούσα κάλυψη και η αξιοπιστία αποτελούν τους στυλοβάτες των δικτυών έκτης γενιάς, ώστε στο νέο ψηφιακό κόσμο που θα οδηγηθούμε να δημιουργηθούν νέες και βιώσιμες εφαρμογές. Η τεχνητή νοημοσύνη και η μηχανική μάθηση θα ενσωματώνονται στις νέες εφαρμογές με σκοπό τη μείωση της καθυστέρησης και την αύξηση της αξιοπιστίας των μελλοντικών αυτών εφαρμογών. Η συνεισφορά των εφαρμογών στο μετασχηματισμό της κοινωνίας θα είναι υψηλού βαθμού και θα οδηγήσουν σε βελτίωση της ποιότητας ζωής του ανθρώπου, αύξηση του βιοτικού επιπέδου και διευκόλυνση του στις καθημερινές δραστηριότητες του και υποχρεώσεις.

Πιο συγκεκριμένα έχοντας ως βάση τα κυψελοειδή δίκτυα πέμπτης γενιάς, τα δίκτυα έκτης γενιάς θα συνεχίσουν να βελτιώνουν σημαντικά την απόδοση της ασύρματης επικοινωνίας και θα επεκτείνουν τις υπηρεσίες από τον φυσικό κόσμο στον ψηφιακό. Εφαρμογές όπως το ψηφιακό δίδυμο, ο βιομηχανικός αυτοματισμός, οι ολογραφικές επικοινωνίες, τα συνδεδεμένα συστήματα ρομποτικής και αυτοματισμού, η ηλεκτρονική υγεία, η επαυξημένη και εικονική πραγματικότητα, η αυτόνομη οδήγηση και τα έξυπνα περιβάλλοντα θα γνωρίσουν αλματώδη εξέλιξη λόγω του 6G. Οι παραπάνω νέες περιπτώσεις χρήσης θα οδηγήσουν σε αύξηση του όγκου της κίνησης του δικτύου με αποτέλεσμα την ανάγκη για την μετάβαση από τα δίκτυα πέμπτης γενιάς στα δίκτυα έκτης γενιάς. Τα δίκτυα έκτης γενιάς θα διαθέτουν μεγαλύτερη χωρητικότητα με σκοπό την ανακούφιση του δικτύου και την ταχεία εξυπηρέτηση των συνεχώς αυξανόμενων αιτημάτων.

2.1. Ψηφιακό Δίδυμο - Digital twin body area network

Εικόνα 2. Το ψηφιακό δίδυμο [11].

Η έλευση των δικτυών 6G και η πλήρης ανάπτυξη διεπιστημονικών θεμάτων θα οδηγήσουν στη δημιουργία ενός ψηφιακού δίδυμου του ανθρώπινου σώματος. Ο όρος ψηφιακό δίδυμο αναφέρεται στη δημιουργία ενός ψηφιακού αντίγραφου ενός φυσικού αντικείμενου, οντότητας, συστήματος ή διαδικασίας του φυσικού κόσμου με σκοπό την κατανόηση και την πρόβλεψη των χαρακτηριστικών απόδοσης του πραγματικού δίδυμου [12]. Παρατηρείται ότι το ψηφιακό δίδυμο μπορεί να αντιπροσωπεύει είτε υλικές οντότητες, όπως πόλη, άνθρωπο, ζώα είτε άυλες οντότητες, όπως υπηρεσίες ή διαδικασίες. Πιο συγκεκριμένα στις άυλες οντότητες εντάσσεται το ψηφιακό δίδυμο μιας διαδικασίας παραγωγής το οποίο βοηθάει στην προσομοίωση και την επιβεβαίωση της σωστής λειτουργίας της διαδικασίας παραγωγής πριν ξεκινήσει η παραγωγή στην πραγματικότητα. Το πλεονέκτημα των ψηφιακών διδύμων είναι ότι χρησιμοποιεί δεδομένα σε πραγματικό χρόνο από διάφορες πηγές, όπως αισθητήρες που τοποθετούνται στο φυσικό δίδυμο. Για να αναπαράγει πραγματικές καταστάσεις και να εξάγει αποτελέσματα ο ψηφιακός δίδυμο χρησιμοποιεί τα δεδομένα που λαμβάνει από τους αισθητήρες και εφαρμόζει μηχανική μάθηση και τεχνητή νοημοσύνη. Το σύνολο δεδομένων που περιέχει το ψηφιακό δίδυμο σε αρκετές περιπτώσεις είναι μεγαλύτερο από αυτό που περιέχει το αντίστοιχο φυσικό δίδυμο.

Μέχρι σήμερα οι εφαρμογές του ψηφιακού δίδυμου πραγματοποιούνται σε μικρή κλίμακα, όμως η πρόοδος της επιστήμης και των δικτύων θα συνεισφέρει στην ανάπτυξη τους σε μεγαλύτερη κλίμακα. Η εφαρμογή του ήδη στο σχεδιασμό, κατασκευή, λειτουργία, προσομοίωση και πρόβλεψη έχει οδηγήσει σε μοναδικά συμπεράσματα. Αρχικά τα σύνολα δεδομένων που διαθέτουν οι ψηφιακοί δίδυμοι και στα οποία πραγματοποιούν αναλύσεις και προσομοιώσεις σε πραγματικό χρόνο, μπορούν να χρησιμοποιηθούν για την εξαγωγή μοτίβων σχετικά με την παράταση της διάρκειας ζωής των ανθρώπων μέσω φαρμάκων κατά της γήρανσης,

[13]. Επιπλέον μπορεί να χρησιμοποιηθεί για την άντληση πληροφοριών από άλλα ψηφιακά δίδυμα και να ανιχνεύσει δυσλειτουργίες, όπως προσδιορισμός των παρενεργειών ενός φαρμάκου ή δυσλειτουργία ενός μηχανήματος πριν ακόμη αρχίσει η παραγωγή του. Τα δεδομένα προτύπων και οι στατιστικές πληροφορίες χρησιμοποιούνται από τον ψηφιακό δίδυμο για την παρακολούθηση των αλλαγών σε μια συγκεκριμένη δραστηριότητα, δηλαδή αλλαγές στον καρδιακό παλμό, στην πίεση στα επίπεδα οξυγόνου στο αίμα, κλπ.

Η εφαρμογή του ψηφιακού δίδυμου στην υγεία αναμένεται να ανοίξει το δρόμο σε μια νέα εποχή. Σύμφωνα με τον Bill Ruh, Διευθύνοντα Σύμβουλο της GE Digital, " I believe we will end up with health care being the ultimate digital twin" [13]. Ειδικότερα η τοποθέτηση αισθητήρων στο ανθρώπινο σώμα (περισσότεροι από 100 αισθητήρες ανά άτομο) θα συμβάλλει στην απεικόνιση σε πραγματικό χρόνο του ανθρώπινου σώματος με ακρίβεια ώστε να πραγματοποιείται ανάλυση δεδομένων και κατανόηση της λειτουργία των οργάνων, του νευρικού, αναπνευστικού, ουροποιητικού συστήματος κλπ.[14]. Πιο συγκεκριμένα έχουν ήδη δημιουργηθεί ασύρματοι αισθητήρες, οι οποίοι παρακολουθούν τον καρδιακό παλμό, την αρτηριακή πίεση και πολλές άλλες παραμέτρους. Οι ασύρματοι αισθητήρες κρίνονται αναγκαίοι, καθώς ο ασθενείς δεν θα χρειάζεται πλέον να είναι συνδεδεμένος σε ιατρικές συσκευές με πλήθος καλωδίων. Μέσα σε λίγα χρόνια η τεχνολογία θα επιτρέψει την παρακολούθηση του ασθενή μέσω ενός ασύρματου δικτύου και οι γιατροί θα μπορούν να μάθουν οτιδήποτε συμβαίνει στον ασθενή από οποιαδήποτε συνδεδεμένη συσκευή. Ακόμη ο γιατρός θα μπορεί να παρακολουθεί 24ώρες το 24ώρο τον ασθενή και θα έχει συνεχή ροή των δεδομένων υγείας του [15].

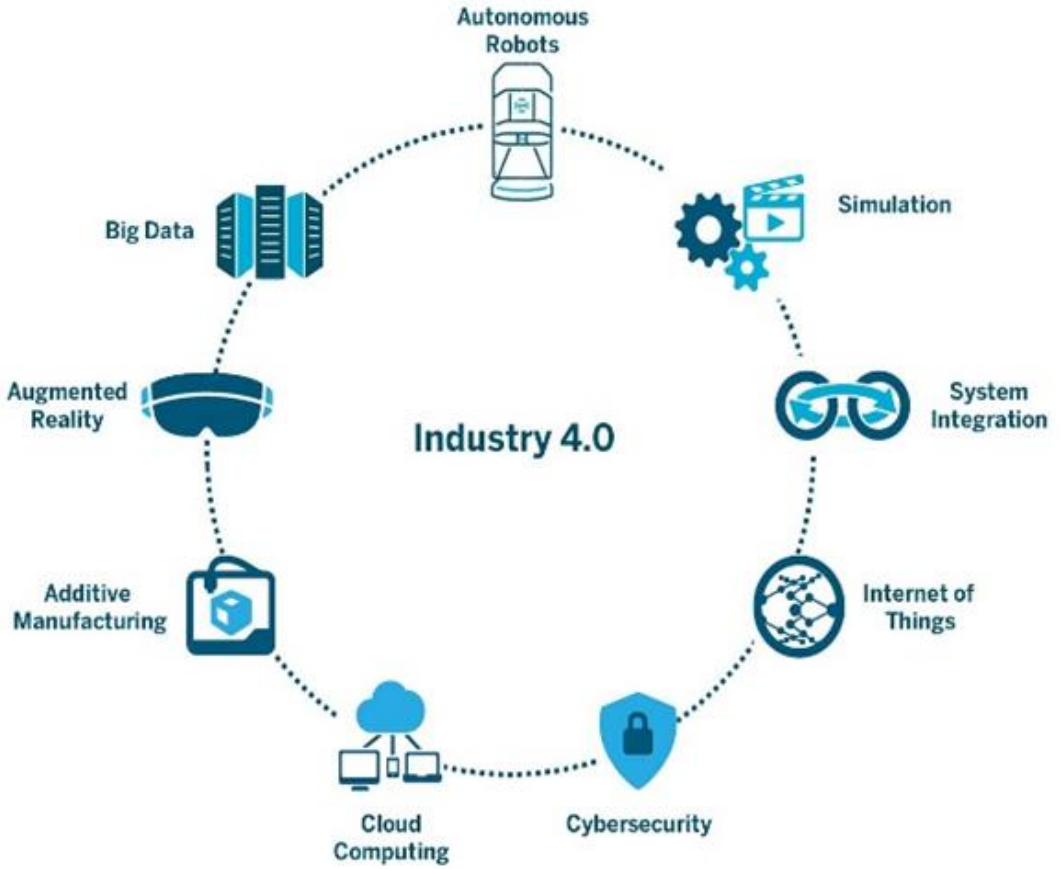
Η χαρτογράφηση σε πραγματικό χρόνο δημιουργεί ένα ακριβές αντίγραφο του ανθρώπινου σώματος και στη συνέχεια παρακολουθεί σε πραγματικό χρόνο τα δεδομένα υγείας του ανθρώπου. Επίσης ο συνδυασμός απεικονίσεων και βιοχημικών εξετάσεων, όπως των αποτελεσμάτων της μαγνητικής, των εξετάσεων αίματος και ούρων με αλγορίθμους μηχανικής μάθηση, όπως εποπτευόμενη μάθηση (supervised learning), μάθηση χωρίς επίβλεψη (unsupervised learning) και βαθιά μάθηση (deep learning) μπορεί να οδηγήσει στην έγκαιρη και ακριβή διάγνωση και παρέμβαση για την αντιμετώπιση ενός προβλήματος υγείας [14]. Η προσφορά του ψηφιακού δίδυμου στον τομέα της υγείας θα ασκήσει μεγάλη επιρροή, καθώς:

- θα μπορεί να προσομοιώσει την λειτουργία του σώματος όταν λαμβάνει μια φαρμακευτική αγωγή και να προβλέψει την επίδραση που θα έχει,
- θα μπορεί να παρακολουθεί καθημερινά την κατάσταση της υγείας ενός ατόμου και τις ζωτικές του λειτουργίες,
- θα μπορεί να βοηθήσει στην πρόληψη αλλά και διάγνωση μιας ασθένειας,

- θα συμβάλλει στην στοχευμένη θεραπεία ασθενειών.

Από όλα τα παραπάνω συμπεραίνουμε ότι καθώς οδηγούμαστε σε έναν ψηφιακό κόσμο οι ποικίλες εφαρμογές, όπως το ψηφιακό δίδυμο, θα οδηγήσουν στη βελτίωση της ποιότητας της ανθρώπινης ζωής.

2.2. Βιομηχανικός Αυτοματισμός 4.0. - Industry Automation 4.0.



Εικόνα 3. Βιομηχανικός Αυτοματισμός 4.0 στα δίκτυα έκτης γενιάς. [16].

Η Τρίτη Βιομηχανική Επανάσταση ή αλλιώς Ψηφιακή Επανάσταση βασίστηκε στις τεχνολογίες πληροφορικής και επικοινωνιών, στους υπολογιστές, το διαδίκτυο και την ηλεκτρονική. Η Βιομηχανία 4.0, η οποία βρίσκεται προ των πυλών στην εποχή που διανύουμε, αναφέρεται στη νέα φάση της Βιομηχανικής Επανάστασης η οποία έχει ως βασικά συστατικά στοιχεία της τη διασυνδεσιμότητα, την αυτοματοποίηση, τη μηχανική μάθηση και τα δεδομένα σε πραγματικό χρόνο [17]. Το 6G θα πραγματοποιήσει πλήρως την επανάσταση του Industry 4.0 που ξεκίνησε με το 5G. Ειδικότερα η Βιομηχανία 4.0 είναι ο ψηφιακός μετασχηματισμός της παραγωγής μέσω κυβερνο-φυσικών συστημάτων και υπηρεσιών IoT. Βασικός στόχος της νέας αυτής Βιομηχανικής Επανάστασης είναι η ψηφιοποίηση της βιομηχανίας. Ακόμη με τη σύνδεση του φυσικού και ψηφιακού κόσμου η

Βιομηχανία 4.0 επιτυγχάνει καλύτερη συνεργασία και συνεννόηση μεταξύ των διάφορων τμημάτων, προμηθευτών και εργαζομένων.

Οι κύριες τεχνολογίες, τις οποίες περιλαμβάνει η Βιομηχανία 4.0 για την επίτευξη των στόχων της είναι τα κυβερνο-φυσικά συστήματα (Cyber-Physical Systems), το διαδίκτυο των πραγμάτων (Internet of Things), η μηχανική μάθηση (machine learning), η τεχνητή νοημοσύνη (artificial intelligence), οι τεχνολογίες ρομποτικής (robotics), το υπολογιστικό νέφος (cloud computing), τα Big Data και Data Analytics, την ασφάλεια των δεδομένων (data security) και την 3D εκτύπωση (3D printing) [18]. Στη νέα αυτή βιομηχανία η παρέμβαση του ανθρώπου στη διαδικασία κατασκευής θα μειωθεί σημαντικά, καθώς τη θέση αυτή θα αναλάβουν αυτοματοποιημένα συστήματα [19]. Η βιομηχανία 4.0 αποτελεί τη βάση του όρου “έξυπνο εργοστάσιο”. Το “έξυπνο εργοστάσιο” περιλαμβάνει τα κυβερνο-φυσικά συστήματα, τα οποία συνδυάζουν τις υπολογιστικές και φυσικές διεργασίες σε ένα ενιαίο περιβάλλον παραγωγής [20]. Πιο συγκεκριμένα τα κυβερνο-φυσικά συστήματα επιβλέπουν τις φυσικές διαδικασίες στη βιομηχανική παραγωγή, δημιουργούν ένα εικονικό αντίγραφο του φυσικού κόσμου και λαμβάνουν αποκεντρωμένες αποφάσεις.

Η συνεισφορά της βιομηχανίας 4.0 στην διαδικασία κατασκευής και παραγωγής είναι εξαιρετικά σημαντική και υψηλή, καθώς συμβάλλει [16]:

1. Στην καλύτερη διαχείριση και βελτιστοποίηση της αλυσίδας εφοδιασμού. Ειδικότερα οι επιχειρήσεις έχουν τη δυνατότητα να παρέχουν προϊόντα και υπηρεσίες στους καταναλωτές με καλύτερη ποιότητα, γρηγορότερα και φθηνότερα.
2. Στην πρόβλεψη προβλημάτων προτού συμβούν στην πραγματικότητα και συντήρηση.
3. Στη δημιουργία νέων μεθόδων σχεδίασης και παραγωγής προϊόντων χάρις στην 3D εκτύπωση.

Ο μετασχηματισμός του βιομηχανικού κλάδου στη Βιομηχανία 4.0 αναμένεται να ολοκληρωθεί στην εποχή του 6G, καθώς τα ήδη υπάρχοντα δίκτυα δε διαθέτουν τη δυνατότητα για την ικανοποίηση των απαιτήσεων του μετασχηματισμού. Επειδή πολλές νέες βιομηχανικές λειτουργίες απαιτούν αξιοπιστία, επικοινωνία σε πραγματικό χρόνο, σύνδεση πολλαπλών συσκευών στο δίκτυο και εξαιρετικά χαμηλή καθυστέρηση παρατηρούμε ότι οι παραπάνω απαιτήσεις ικανοποιούνται στα δίκτυα έκτης γενιάς.

2.3. Ολογραφικές Επικοινωνίες - Holographic communications

Οι ολογραφικές επικοινωνίες αποτελούν μια εξελισσόμενη τεχνολογία και από τις πιο κρίσιμες και καίριες εφαρμογές του 6G. Η ολογραφική επικοινωνία είναι μια προβολή σε πραγματικό χρόνο τρισδιάστατων (3D) εικόνων ενός αντικειμένου ή ανθρώπου. Για να επιτευχθεί η προβολή του ολογράμματος χρησιμοποιούνται κάμερες από διαφορετικές οπτικές γωνίες για να δημιουργεί το ολόγραμμα του αντικειμένου [21]. Η εικόνα μπορεί να προβληθεί από οποιαδήποτε γωνία, δίνοντας του τη δυνατότητα να κινείται και να μετατοπίζεται ρεαλιστικά. Εκτός από την εικόνα το ολογραφικό ομοίωμα μεταφέρει και τον ήχο, παρέχοντας μοναδικές δυνατότητες.

Τα δίκτυα πέμπτης γενιάς αποτελούν την απαρχή για τη διείσδυση της ολογραφικής επικοινωνίας στη ζωή των ανθρώπων και την αξιοποίηση της σε διάφορους τομείς [22]. Όμως τα δίκτυα έκτης γενιάς λόγω του υψηλού ρυθμού δεδομένων, της εξαιρετικά χαμηλής καθυστέρησης και της αξιοπιστίας που διαθετούν θα ενσωματώσουν τις ολογραφικές επικοινωνίες σε ακόμη μεγαλύτερο βαθμό σε σχέση με τα δίκτυα 5G [23].

Η προσφορά της ολογραφικής επικοινωνίας αναμένεται να φέρει επαναστατικές αλλαγές σε πολλούς τομείς. Ειδικότερα στον τομέα της υγείας, όπως θα αναλυθεί και στο κεφάλαιο 2.5. Ηλεκτρονική Υγειά – Επαυξημένη και Εικονική Πραγματικότητα, η ολογραφική επικοινωνία θα ενισχύσει τα ευφυή συστήματα υγειονομικής περίθαλψης και θα δίνει τη δυνατότητα παροχής ιατρικής περίθαλψης σε όλα τα μέρη του πλανήτη, χωρίς τη φυσική παρουσία γιατρού ή ασθενή. Επιπλέον στον τομέα της διασκέδασης και της ψυχαγωγίας, η ολογραφική επικοινωνία θα παρέχει τη δυνατότητα να παρακολουθήσουμε τα ολογράμματα ενός συγκροτήματος τα οποία πραγματοποιήσουν μια συναυλία σε άλλη χώρα. Επίσης στον τομέα της βιομηχανίας κατασκευών η ολογραφική επικοινωνία θα επιτρέπει την αναπαράσταση του αντικειμένου μέσω ολογράμματος πριν κατασκευαστεί με σκοπό να μελετηθούν οι δυνατότητες του και να προταθούν έγκαιρα αλλαγές πριν αρχίσει η κατασκευή του.

2.4. Συνδεδεμένα Συστήματα Ρομποτικής και Αυτοματισμού - Connected Robotics and Automation Systems

Τα δίκτυα έκτης γενιάς αναμένεται να παρέχουν νέες δυνατότητες μέσω της συνδεδεμένης ρομποτικής και των αυτόνομων συστημάτων. Οι απαιτήσεις που δεν θα ικανοποιούνται από το δίκτυο 5G και θα αποτελέσουν το έναυσμα για την ανάπτυξη του δικτύου 6G θα βοηθήσουν την ανάπτυξη των αυτόνομων συστημάτων και της συνδεδεμένης ρομποτικής [23]. Αυτόνομα συστήματα, τα οποία έχουν ήδη αναπτυχθεί, έχουν ενσωματωθεί και διευκολύνει την καθημερινότητα των ανθρώπων. Στο δίκτυο 6G όμως τα αυτόνομα συστήματα θα ενταχθούν ενεργά στη ζωή των ανθρώπων. Τα μη επανδρωμένα αεροσκάφη ή drones (UAV), τα οποία αποτελούν ένα παράδειγμα αυτόνομων συστημάτων, έχουν

συνεισφέρει στους τομείς του εμπορίου, παράδοσης δεμάτων, γεωργίας, στρατού, αεροφωτογράφισης, διαχείρισης καταστροφών, επιστήμης και αναψυχής. Στα δίκτυα έκτης γενιάς τα UAV εκτός από την υποβοήθηση του δικτύου για την παροχή πλήρης κάλυψης θα παρέχουν μια ευρεία γκάμα εφαρμογών. Επιπλέον τα αυτόνομα οχήματα λόγω της εξαιρετικά χαμηλής καθυστέρησης, της αξιοπιστίας και του υψηλού ρυθμού δεδομένων θα αναπτυχθούν σε μεγάλη κλίμακα και αναμένεται να φτάσουν στο επίπεδο αυτοματοποίησης 5.

2.5. Ηλεκτρονική Υγεία - E-Health – Επαυξημένη και Εικονική Πραγματικότητα – Augmented Reality and Virtual Reality

Τα δίκτυα 6G υπόσχονται να ανοίξουν το δρόμο για μια νέα εποχή στον τομέα της υγείας. Η τηλεϊατρική θα αποτελεί ένα βασικά εργαλείο στα χέρια των γιατρό για την παροχή ιατρικής φροντίδας χωρίς τον περιορισμό του χώρου και χρόνου. Ειδικότερα αξιοποιώντας νέες και καινοτόμες τεχνολογίες, όπως η τεχνητή νοημοσύνη, η ολογραφική επικοινωνία, η επαυξημένη και η εικονική πραγματικότητα (AR & VR), η τηλεϊατρική θα ενισχυθεί και θα παρέχει τις αξιόπιστες υπηρεσίες της στους ασθενείς. Η τεχνητή νοημοσύνη προσφέρει επικοινωνία σε πραγματικό χρόνο, στοιχείο απαραίτητο για την υγειονομική περίθαλψη, καθώς θα βελτιώσει την κλινική διάγνωση και λήψη αποφάσεων [19]. Για να γίνεται κατάλληλη διάγνωση και παροχή φροντίδας στους ασθενείς το δίκτυο θα πρέπει να χαρακτηρίζεται από υψηλή αξιοπιστία, υψηλό ρυθμό δεδομένων, υψηλή συχνότητα λειτουργία και εξαιρετικά χαμηλή καθυστέρηση, χαρακτηριστικά τα οποία ικανοποιούνται στα δίκτυα έκτης γενιάς. Οι παραπάνω απαιτήσεις είναι απαραίτητες στον τομέα της υγείας, καθώς τόσο κρίσιμες υπηρεσίες όσο της υγείας πρέπει να παρέχονται σε πραγματικό χρόνο, χωρίς περιορισμό από το χώρο και το χρόνο [24].

Η επαυξημένη και η εικονική πραγματικότητα συνδέονται στενά όμως δεν είναι τα ίδια. Η επαυξημένη πραγματικότητα (AR) δίνει τη δυνατότητα για προσθήκη ψηφιακού περιεχόμενου (εικόνες, ήχο, κείμενο) σε σκηνές της πραγματικής ζωής [25], ενώ η εικονική πραγματικότητα (VR) είναι η προσομοίωση ενός πραγματικού ή φανταστικού περιβάλλοντος που δημιουργείται από έναν υπολογιστή, στην οποία το άτομο μπορεί να αλληλοεπιδράσει με το τεχνητό τρισδιάστατο περιβάλλον χρησιμοποιώντας ηλεκτρονικές συσκευές [26]. Η προσφορά των δυο παραπάνω τεχνολογιών τόσο στον τομέα της υγείας όσο και σε διάφορους άλλους τομείς θα είναι δυνατή μέσα από τα δίκτυα έκτης γενιάς. Όπως και η ολογραφική επικοινωνία, η επαυξημένη και εικονική πραγματικότητα απαιτούν χαμηλή καθυστέρηση, επικοινωνία σε πραγματικό χρόνο, υψηλό ρυθμό δεδομένων και άμεσες αποκρίσεις. Ο συνδυασμός του AR και της ολογραφικής επικοινωνίας θα βοηθήσουν το γιατρό στην καλύτερη διάγνωση, ενώ το VR στη διεξαγωγή ιατρικών διαδικασιών χωρίς την παρουσία του ασθενή, καθώς και στην εξάσκηση των γιατρών σε δύσκολες χειρουργικές επεμβάσεις [23].

Η τηλεχειρουργική αποτελούσε ένα άπιαστο όνειρο για την ιατρική. Όμως τα δίκτυα έκτης γενιάς υπόσχονται να ανοίξουν το παράθυρο για την έλευση της. Ως τηλεχειρουργική ορίζεται η απομακρυσμένη χειρουργική επέμβαση από γιατρούς. Τα κύρια χαρακτηριστικά που απαιτεί είναι επικοινωνία σε πραγματικό χρόνο, υψηλό ρυθμό δεδομένων και χαμηλή καθυστέρηση, τα οποία ικανοποιούνται στο δίκτυο 6G [27]. Με την βοήθεια της ολογραφικής επικοινωνίας του AR και VR, ο γιατρός μπορεί να είναι εικονικά παρών σε μια χειρουργική επέμβαση. Το Απτικό Διαδίκτυο (Tactile Internet) θα αποτελεί το βασικό εργαλείο για την πραγματοποιήσει χειρουργικής επέμβασης και διάγνωσης από απόσταση. Ειδικότερα το απτικό διαδίκτυο είναι ένα ασύρματο δίκτυο που θα επιτρέψει την αλληλεπίδραση ανθρώπου και μηχανής σε πραγματικό χρόνο. Ο γιατρός θα μπορεί να χρησιμοποιήσει την αίσθηση της αφής χωρίς να είναι φυσικά παρών και να εξετάζει/χειρουργεί τον ασθενή. Η αλληλεπίδραση ανθρώπου – υπολογιστή (Haptic Human-Computer Interaction (HCI)) ταξινομείται σε τρεις κατηγορίες [28]:

1. Desktop: ο απομακρυσμένος γιατρός χρησιμοποιεί εικονικά εργαλεία για τη διάγνωση/επέμβαση.
2. Surface: η κίνηση είναι 2D και ο γιατρός δίνει τις εντολές μέσω μιας επίπεδης οθόνης, όπως το κινητό ή tablet και το ρομπότ αλληλοεπιδρά με τον ασθενή.
3. Wearable: χρησιμοποιούνται φορητές συσκευές για παράδειγμα haptic glove από τον απομακρυσμένο γιατρό για να προσομοιώνει την αίσθηση της αφής στον απομακρυσμένο ασθενή [29].

Τέλος ο τομέας της ιατρικής στα δίκτυα έκτης γενιάς θα ενισχυθεί από τις ευφυείς φορητές συσκευές. Οι ευφυείς φορητές συσκευές συνδέονται με το διαδίκτυο και συλλέγουν δεδομένα σχετικά με την υγεία και την ψυχολογία του χρήστη τους, όπως καρδιακό παλμό, αρτηριακή πίεση, σωματικό βάρος και διατροφή τα οποία στη συνέχεια μεταδίδουν σε κέντρα δοκιμών και παρακολούθησης [30]. Τα πλεονεκτήματα που διαθέτουν οι εν λόγω συσκευές είναι ευρείας κλίμακας, καθώς μπορούν αναλύοντας τα δεδομένα να συμβουλέψουν τον κάτοχο τους να κάνει καλύτερη διατροφή ή να ασκείται περισσότερο βελτιώνοντας έτσι την ποιότητα ζωής του. Επιπλέον στο μέλλον οι ευφυείς φορητές συσκευές θα έχουν τη δυνατότητα να ανιχνεύουν μικρά προβλήματα υγείας και να ενημερώνουν το χρήστη τους ή να αναλύουν τις εξετάσεις του και να εξάγουν τα κατάλληλα αποτελέσματα.

Γίνεται κατανοητό λοιπόν ότι τα δίκτυα έκτης γενιάς θα οδηγήσουν σε μια εποχή ευφυής υγειονομική περίθαλψης. Όμως, καθώς όλες οι προαναφερθέντες τεχνολογίες συλλέγουν, αποθηκεύουν, επεξεργάζονται και μεταδίδουν δεδομένα υγείας τα οποία είναι ευαίσθητα οφείλουν να εγγυούνται στο χρήστη την προστασία των δεδομένων του, την ασφάλεια και το απόρρητο. Οπότε οι εφαρμογές και τεχνολογίες του δικτύου 6G πρέπει να εστιάσουν την προσοχή τους στην προστασία της ιδιωτικής ζωής των χρηστών τους.

2.6. Αυτόνομη Οδήγηση - Autonomous driving

Τα αυτόνομα οχήματα, δηλαδή τα αυτοκίνητα χωρίς οδηγό, έρχονται για να αλλάξουν τον κόσμο και να οδηγήσουν σε μια νέα κοινωνία. Τα αυτόνομα οχήματα θα προσφέρουν ασφαλέστερα και οικονομικότερα ταξίδια, καλύτερη διαχείριση της κυκλοφορίας, μείωση των περιβαλλοντικών επιπτώσεων και μείωση των ατυχημάτων [31]. Όπως είναι ήδη γνωστό το 95% των ατυχημάτων στους δρόμους οφείλεται σε ανθρώπινο λάθος [32]. Η συνεισφορά των αυτόνομων οχημάτων σε συνεργασία με τα δίκτυα έκτης γενιάς θα οδηγήσει σε κάθετη μείωση των ατυχημάτων. Τα αυτόνομα οχήματα κυκλοφορούν ήδη δοκιμάστηκα σε πολλές χώρες του πλανήτη, όμως με την έλευση του δικτύου 6G ποσοστό μεγαλύτερο από το 50% των κατοίκων της γης θα μετακινείται με αυτόνομα οχήματα. Η εξέλιξη της αυτόνομης οδήγησης θα πραγματοποιηθεί σε μαζική κλίμακα. Κάθε αυτόνομο όχημα θα είναι εξοπλισμένο με μεγάλο πλήθος και ποικιλία αισθητήρων, οι οποίοι θα συλλέγουν δεδομένα σε πραγματικό χρόνο και θα τα επεξεργάζονται για την εξαγωγή αποφάσεων. Η ανάγκη για συλλογή και επεξεργασία δεδομένων σε πραγματικό χρόνο, καθώς και η απαίτηση για χαμηλή καθυστέρηση που απαιτείται αποτελούν χαρακτηριστικά τα οποία θα ικανοποιηθούν στα δίκτυα έκτης γενιάς τα οποία θα οδηγήσουν στο Επίπεδο αυτοματοποίησης 5 (πλήρης αυτοματοποίηση οδήγησης).

Σύμφωνα με τα πρότυπα Society of Automotive Engineers (SAE) International τα αυτόνομα οχήματα ιεραρχούνται σε έξι επίπεδα (0-5). Τα παρακάτω έξι επίπεδα έχουν ενστερνιστεί και από την Εθνική Διοίκηση Κυκλοφορικής Ασφάλειας Αυτοκινητοδρόμων των Η.Π.Α. (NHTSA), και είναι τα εξής [33]:

- Επίπεδο 0 (Χωρίς αυτοματοποίηση). Τα οχήματα Επιπέδου 0 είναι χειροκίνητα και δεν διαθέτουν δυνατότητας αυτόνομης οδήγησης. Ο οδηγός έχει τον απόλυτο έλεγχο του οχήματος σε όλο το χρονικό διάστημα της μετακίνησης.

- Επίπεδο 1 (Βοήθεια οδηγού). Τα οχήματα Επιπέδου 1 διαθέτουν αυτοματοποίηση συγκεκριμένων λειτουργιών όπως η υποβοήθηση παράλληλης στάθμευσης, ο έλεγχος πλεύσης του οχήματος και η καθοδήγηση των οριογραμμών. Τα παραπάνω συστήματα υποστηρίζουν την οδήγηση και συλλέγουν πληροφορίες από το περιβάλλον. Επιπλέον ελέγχουν την επιτάχυνση και επιβράδυνση του οχήματος. Όμως το οδηγός είναι υπεύθυνος για όλες τις λειτουργίες του οχήματος και εμπλέκεται πλήρως στη διαδικασία της οδήγησης, καθώς δεν μπορεί να απομακρύνει τα χέρια από το τιμόνι και τα πόδια από τα πεντάλ.

- Επίπεδο 2 (Μερική αυτοματοποίηση). Τα οχήματα Επιπέδου 2 διαθέτουν αυτοματοποίηση πολλαπλών και ολοκληρωμένων λειτουργιών ελέγχου, καθώς είναι εξοπλισμένα, με περισσότερα είδη αυτομάτων συστημάτων, όπως ραντάρ, κάμερες και επικοινωνία μεταξύ άλλων οχημάτων, μέσω δορυφόρου. Στις παραπάνω λειτουργίες συγκαταλέγεται ο

προσανατολισμένος έλεγχος πλεύσης με κέντρωση επί των οριογραμμών των λωρίδων κυκλοφορίας. Ο οδηγός έχει την δυνατότητα να απομακρύνει τα χέρια από το τιμόνι και τα πόδια από τα πεντάλ, όμως πρέπει να ελέγχει τις συνθήκες κυκλοφορίας στο δρόμο και να είναι σε ετοιμότητα για να αναλάβει τον έλεγχο του οχήματος.

- Επίπεδο 3 (Αυτοματοποίηση υπό όρους). Τα οχήματα στο Επίπεδο 3 δίνουν την δυνατότητα στο χειριστή τους να αποδεσμευτεί από τα καθήκοντα του και να μην παρακολουθεί συνεχώς την κυκλοφορία, καθώς το όχημα αναλαμβάνει πλήρως να πραγματοποιήσει το οδικό έργο. Ο οδηγός πρέπει να βρίσκεται εντός του οχήματος ώστε σε περίπτωση ανάγκης να αναλάβει τον έλεγχο του οχήματος. Σύμφωνα με την Volvo απαιτούνται 5 δευτερόλεπτα μέχρι ο άνθρωπος να αναλάβει σε κατάσταση κινδύνου τον πλήρη έλεγχο του οχήματος.

- Επίπεδο 4 (Υψηλός αυτοματισμός). Τα οχήματα Επιπέδου 4 είναι υπεύθυνα για την εκτέλεση όλων των οδικών λειτουργιών και την παρακολούθηση των κυκλοφοριακών συνθηκών κάτω υπό ορισμένες περιπτώσεις. Είναι το πρώτο στάδιο στο οποίο δεν απαιτείται η παρουσία οδηγού εντός του οχήματος, όμως το όχημα κινείται σε προκαθορισμένες περιοχές. Τα οχήματα αυτού του επιπέδου χάρις την αυτοματοποίηση που διαθέτουν μπορούν να χρησιμοποιηθούν από άτομα που δε γνωρίζουν να οδηγούν, άτομα με μειωμένη κινητικότητα ή να μη διαθέτουν καθόλου επιβαίνοντες.

- Επίπεδο 5 (Πλήρης αυτοματοποίηση). Τα οχήματα Επιπέδου 5 είναι υπεύθυνα για την εκτέλεση όλων των οδικών λειτουργιών και την επίβλεψη των κυκλοφοριακών συνθηκών και είναι σε θέση να εκτελέσουν οποιαδήποτε διαδρομή. Το αξιοσημείωτο γεγονός για τα οχήματα αυτού του επιπέδου είναι ότι δεν χρειάζεται να διαθέτουν τιμόνι, οπότε και κατ' επέκταση δεν χρειάζονται την παρουσία οδηγού εντός του οχήματος.

Γενικότερα τα αυτόνομα οχήματα θα οδηγήσουν σε ένα άλμα στην οδική ασφάλεια. Τα οχήματα θα είναι διασυνδεδεμένα μεταξύ τους και θα ενημερώνουν τους χρήστες για τις συνθήκες στο δρόμο. Επιπλέον τα συνεργατικά αυτόνομα οχήματα, δηλαδή τα οχήματα, τα οποία εκτός από τις δικές τους πληροφορίες λαμβάνουν δεδομένα και από οποιαδήποτε άλλη πηγή εκτός τους οχήματος, όπως άλλους αισθητήρες, οχήματα, υποδομές, θα προσφέρουν πολυάριθμα πλεονεκτήματα στους χρήστες τους. Τα συνεργατικά αυτόνομα οχήματα θα είναι διασυνδεδεμένα μεταξύ τους αλλά και με τις υποδομές και θα ενημερώνουν το ένα το άλλο σε πραγματικό χρόνο. Η απόκριση των οχημάτων σε πραγματικό χρόνο συμβάλει στην έγκαιρη αλλαγή πορείας για την αποφυγή εμποδίων.

Αξιοποιώντας την τεχνητή νοημοσύνη και τη μηχανική μάθηση, καθώς και τους αισθητήρες που διαθέτουν τα οχήματα θα αποφεύγουν ατυχήματα τα οποία θα προκαλούνταν από ανθρώπινο σφάλμα κατά την οδήγηση. Τα αυτόνομα οχήματα θα είναι εξοπλισμένα με GPS, αισθητήρες κάμερας, αισθητήρες LiDAR

(Light Detection and Ranging) και αισθητήρες ραντάρ για τη συλλογή δεδομένων και για να κατανοούν το περιβάλλον που επικρατεί γύρω τους [34]. Έπειτα με τη βοήθεια της μηχανικής μάθηση και ειδικότερα της βαθιάς μάθησης (Deep Learning) θα εξάγονται κάποια αποτελέσματα από τα σύνολα δεδομένων τα οποία θα εισάγονται στην ηλεκτρονική μονάδα ελέγχου (Electronic Control Unit) του οχήματος [35]. Το αυτόνομο όχημα στη συνέχεια θα είναι σε θέση να αυξήσει ή να μειώσει την ταχύτητα του, να πατήσει φρένο ή να αλλάξει κατεύθυνση.

Για την βελτιστοποίηση της ασφάλειας στους δρόμους τα αυτόνομα οχήματα θα είναι εξοπλισμένα με εφαρμογές οι οποίες θα πρέπει να επεξεργάζονται τα δεδομένα με υψηλή ταχύτητα για την εξαγωγή και λήψη απόφασης και η καθυστέρηση να είναι αμελητέα. Για την επίτευξη του παραπάνω στόχου το Edge Intelligent (EI) ήρθε για να ενισχύσει και να υποστηρίξει τις εφαρμογές των οχημάτων. Το Edge Intelligent αναφέρεται στη διαδικασία κατά την οποία τα δεδομένα συλλέγονται, αναλύονται και παρέχουν αποτελέσματα κοντά στο σημείο όπου συλλέχθηκαν [36]. Καθώς τα έξυπνα οχήματα υπόσχονται ανάλυση δεδομένων σε πραγματικό χρόνο, τα δεδομένα δε μπορούν να στέλνονται σε κάποιον κεντρικό διακομιστή cloud για να υποστούν επεξεργασία και να γίνει εξαγωγή κάποιας απόφασης.

Μία από αυτές τις καίριες εφαρμογές για τα αυτόνομα οχήματα αποτελεί η ανίχνευση αντικειμένων. Η ικανότητα των αυτόνομων οχημάτων να οδηγήσουν σε μείωση ατυχημάτων και γενικότερα σε ασφαλέστερη οδήγηση βασίζεται στην ικανότητα του να “βλέπει και κατανοεί ” το περιβάλλον στο οποίο βρίσκεται. Το όχημα συλλέγει τα δεδομένα από το περιβάλλον του μέσω GPS, αισθητήρων κάμερας, αισθητήρων LiDAR και αισθητήρων ραντάρ τα οποία αναλύονται μέσω τεχνικών της τεχνητής νοημοσύνης. Οι τρεις προαναφερθείσες κατηγορίες αισθητήρων συνεργάζονται για να βοηθήσουν το όχημα να κρατήσει την κατάλληλη απόσταση από άλλο οχήματα, να αυξήσει η να μειώσει την ταχύτητα του, να σταματήσει κλπ. Καθώς το πλήθος των δεδομένων που συλλέγονται είναι μεγάλο και η επεξεργασία τους πρέπει να γίνει σε πραγματικό χρόνο ώστε το όχημα να μπορεί να προσδιορίσει τα αντικείμενα που το περιβάλλουν κατανοούμε την ανάγκη για το Edge Intelligent. Με το Edge Intelligent το όχημα έχει την δυνατότητα να μεταφέρει μέρος της πληροφορίας που συλλεγεί σε edge servers οι οποίοι βρίσκονται κοντά του, ώστε η ανάλυση να πραγματοποιηθεί με πολύ χαμηλή καθυστέρηση και να υπάρξει υψηλή ακρίβεια στα αποτελέσματα που θα εξαχθούν από τα δεδομένα [35].

Εικόνα 4. Διμοιρία Φορτηγών - Truck Platooning [37].

Η διμοιρία φορτηγών είναι ένα καινοτόμο σύστημα μεταφοράς και θα αποτελέσει το μέλλον στις οδικές μεταφορές καθώς θα βελτιώσει την αποδοτικότητα και θα μειώσει το αποτύπωμα του άνθρακα. Η διμοιρία φορτηγών ή αλλιώς truck platooning είναι η σύνδεση δύο ή περισσότερων φορτηγών σε φάλαγγα αξιοποιώντας τεχνολογία συνδεσιμότητας και αυτοματοποιημένα συστήματα υποστήριξης οδήγησης. Το φορτηγό στην αρχή της φάλαγγας ενεργεί ως αρχηγός και τα φορτηγά που το ακολουθούν αντιδρούν και προσαρμόζονται στις αλλαγές της κίνησης τους [38]. Τα βασικά πλεονεκτήματα της διμοιρία φορτηγών είναι οι ασφαλέστερες και αποτελεσματικές οδικές μεταφορές και επιπλέον η προστασία του περιβάλλοντος. Όμως η διμοιρία φορτηγών δεν έχει αναπτυχθεί σε ευρεία κλίμακα ακόμη, καθώς απαιτούνται περαιτέρω δοκιμές και αλλαγές στη νομοθεσία ώστε η διμοιρία φορτηγών να αποδείξει την ασφάλεια και την αξιοπιστία της όταν χρησιμοποιεί τα δημόσια οδικά δίκτυα. Κάθε όχημα από τη διμοιρία φορτηγών θα πρέπει να γνωρίζει τη σχετική απόσταση και την ταχύτητα των γειτονικών του οχημάτων ώστε να επιτυγχάνεται συντονισμό της επιτάχυνσης και της επιβράδυνσης τους [39]. Ωστόσο εάν η ανταλλαγή πληροφορίων καθυστερήσει τότε η διμοιρία φορτηγών θα τεθεί σε κίνδυνο. Από το 2030 και έπειτα με την έναρξη του 6G δικτύου αναμένεται να αυξηθεί το επίπεδο αυτοματοποίησης και η διμοιρία φορτηγών θα τεθεί σε εφαρμογή εκμεταλλευόμενη τα χαρακτηριστικά του δικτύου 6G.

Όπως έχει προαναφερθεί τα αυτόνομα οχήματα έχουν την ικανότητα να “βλέπουν” χάρη στους αισθητήρες και τις κάμερες που διαθέτουν. Όμως το τεράστιο πλήθος των δεδομένων που συλλέγονται και υπόκεινται σε επεξεργασία, για την σωστή λειτουργία του οχήματος, ενδέχεται να οδηγήσουν σε ζητήματα ασφάλειας και απορρήτου. Πιο συγκεκριμένα το όχημα μπορεί να συλλέγει προσωπικά και ευαίσθητα δεδομένα ανθρώπων οδηγώντας σε παραβίαση της προσωπικής του ζωής.

2.7. Έξυπνα Περιβάλλοντα - Smart Environments

Η έλευση των τεχνολογιών 6G θα οδηγήσει σε βελτιστοποίηση και αύξηση της ποιότητας ζωής των ατόμων στα έξυπνα περιβάλλοντα. Τα έξυπνα περιβάλλοντα έχουν ως στόχο τους να βοηθήσουν τους ανθρώπους στην καθημερινότητα τους. Για να το επιτύχουν αυτό αξιοποιούν υπολογιστές και διάφορες έξυπνες συσκευές τα οποία είναι ενσωματωμένα σε αντικείμενα της καθημερινής ζωής μας. Τα έξυπνα περιβάλλοντα χωρίζονται σε τρείς κατηγορίες: έξυπνο σπίτι (smart home), έξυπνες πόλεις (smart cities) και έξυπνη βιομηχανία (smart manufacturing) [40].

Εικόνα 5. Έξυπνη Πόλη - Smart city [41].

Ο όρος έξυπνη πόλη (smart city) για τον οποίο γίνεται συχνά λόγος τα τελευταία χρόνια αξιοποιεί ψηφιακές και τηλεπικοινωνιακές τεχνολογίες για την ενίσχυση των υπηρεσιών της προς τους πολίτες της και την επίλυση προβλημάτων της πόλης. Η έξυπνη πόλη χρησιμοποιεί την τεχνολογία για να βελτιώσει τις υποδομές της και την ποιότητα ζωής των πολιτών της. Ειδικότερα μια έξυπνη πόλη διαθέτει εκατομμύρια αισθητήρες σε οχήματα, κτίρια, δρόμους, εργοστάσια, σπίτια και άλλες εγκαταστάσεις. Μια έξυπνη πόλη διακατέχεται από κάποιους κύριους στόχου, όπως [42]:

- Βελτίωση των δημόσιων συγκοινωνιών
- Καλύτερη διαχείριση του νερού
- Ηλεκτρονική διακυβέρνηση
- Συμμετοχή των πολιτών
- Βελτίωση των κοινωνικών υπηρεσιών
- Μείωση της σπατάλης

Τα big data και το IoT αποτελούν δύο θεμελιώδη στοιχεία για την έξυπνη πόλη. Η τεχνολογία big data χρησιμοποιείται από την έξυπνη πόλη, καθώς το μεγάλο πλήθος αισθητήρων που βρίσκονται σε αυτήν παράγουν μαζικά μεγάλες ποσότητες δεδομένων τα οποία πρέπει να αναλυθούν για να γίνει εξαγωγή της πληροφορίας. Παράλληλα το διαδίκτυο των πραγμάτων χρησιμοποιείται σε πολλές εφαρμογές της έξυπνης πόλης, όπως βελτίωση της κυκλοφορίας, διαχείριση υδάτων και αποβλήτων, παροχή βασικών υπηρεσιών με έξυπνο τρόπο και βελτίωση της υγειονομικής περίθαλψής, της εκπαίδευσης και της γεωργίας.

Η τεχνολογία 6G, η οποία υπόσχεται να οδηγήσει στην ψηφιοποίηση της κοινωνίας, θα φέρει μια μεγάλη και βαθιά αλλαγή στις έξυπνες πόλεις. Η έξυπνες πόλεις εκμεταλλευόμενες την αξιόπιστη ασύρματη επικοινωνία υψηλή ταχύτητας που θα προσφέρει το δίκτυο 6G θα έχουν την δυνατότητα να υποστηρίξουν νέες κι καινοτόμες εφαρμογές οι οποίες θα συνεργάζονται μεταξύ τους για τη βελτίωση της ποιότητας ζωής του ανθρώπου. Οι εφαρμογές αυτές δεν είναι δυνατόν να ολοκληρωθούν στην εποχή του 5G, καθώς διέπονται από αυστηρές απαιτήσεις, όπως υψηλής αξιοπιστίας επικοινωνία, πανταχού παρούσα συνδεσιμότητα έξυπνων συσκευών, υψηλός ρυθμός δεδομένων και χαμηλή καθυστέρηση οι οποίες ικανοποιούνται από την τεχνολογία 6G. Η προσφορά της τεχνολογία 6G στον τομέα της υγείας και της μεταφοράς σε μια έξυπνη πόλη έχει ήδη αναλυθεί στα προηγούμενα κεφάλαια.

Τα έξυπνα συστήματα που θα χρησιμοποιούνται στις έξυπνες πόλεις χρειάζονται αρκετούς αισθητήρες και ελεγκτές IoT [43]. Μέσω των αισθητήρων θα πραγματοποιείται συλλογή δεδομένων σε ένα ευρύ πεδίο το οποίο θα περιλαμβάνει ανθρώπους, κτίρια, συσκευές και οχήματα. Έπειτα τα δεδομένα θα υποβάλλονται σε ψηφιακή επεξεργασία και θα εξάγουν αποτελέσματα για την καλύτερη παρακολούθηση και διαχείριση των υποδομών, της κυκλοφορία, των δικτύων ύδρευση και άρδευση, των υπηρεσιών κοινής ωφέλειας, των σχολείων, νοσοκομείων και των μονάδων παραγωγής ενέργειας. Παρατηρείται ότι στην έξυπνη πόλη θα υπάρχει διαχείριση των προβλημάτων που μπορεί να προκύψουν σε πραγματικό χρόνο, χάρη στα δίκτυα έκτης γενιάς και η διοίκηση της πόλης θα μπορεί να αλληλοεπιδράσει άμεσα με του πολίτες της. Η τεχνολογία 6G με τις δυνατότητες που θα εμπλουτίσει τις πόλεις θα ανοίξει τον δρόμο για την αυτοματοποίηση των έξυπνων πόλεων. Επιπλέον όσο η τεχνολογία θα εξελίσσεται οι πόλεις θα εξελίσσονται μαζί της αποκτώντας νέες δυνατότητες και αλλάζοντας τη ζωή των ανθρώπων σημαντικά.

Εικόνα 6. Έξυπνο Σπίτι - Smart Home [44].

Ο όρος έξυπνο σπίτι (smart home) αναφέρεται στα σπίτια τα οποία οι συσκευές μπορούν να ελέγχονται αυτόματα από απόσταση μέσω κινητού ή άλλης δικτυακής συσκευής που διαθέτει σύνδεση στο διαδίκτυο [45]. Μέσω των συσκευών και εφαρμογών οι χρήστες ελέγχουν διάφορες λειτουργίες του σπιτιού, όπως τη θερμοκρασία, το φωτισμό, τη θέρμανση κλπ. από απόσταση οποιαδήποτε χρονική στιγμή [46]. Καθώς βρισκόμαστε σε μια εποχή όπου η τεχνολογία αλλάζει και εξελίσσεται με ταχύ ρυθμό η έλευση των δικτυών έκτης γενιάς θα ενισχύσει και εξοπλίσει τα έξυπνα σπίτια με δυνατότητες που μέχρι πριν λίγα χρόνια θεωρούνταν εξωπραγματικές. Αξιοποιώντας την τεχνητή νοημοσύνη και τα big data τα σπίτια γίνονται “πιο έξυπνα” και οι εφαρμογές τους έχουν τη δυνατότητα να προβλέπουν τις ανάγκες των χρηστών τους.

Οι ποικίλες έξυπνες συσκευές που με το πέρασμα των χρόνων γίνονται όλο και πιο εύκολες στη χρήση τους, διαθέτοντας μια φιλική διεπαφή (Interface) για το χρήστη, και παράλληλα μειώνεται και το κόστος τους και είναι ευρέως διαθέσιμες. Οι ήδη υπάρχουσες αυτοματοποιημένες συσκευές όπως τηλεόραση, θερμοστάτης, κάμερες ασφάλειας, ανιχνευτές αερίου και καπνού, πλυντήρια πιάτων και ρούχων, ψυγεία, σκούπες, κλειδαριά πόρτα κλπ. βρίσκονται ήδη στο εμπόριο και σε αρκετές περιπτώσεις σε πολύ προσιτές τιμές. Όπως και στις έξυπνες πόλεις τα έξυπνα σπίτια προκειμένου να αυξήσουν τον βαθμό αυτοματοποίηση τους απαιτούν αρκετούς ασύρματους αισθητήρες και ελεγκτές IoT [47].

Η μετάβαση όμως στη νέα αυτή εποχή όπου οι έξυπνες πόλεις και τα έξυπνα σπίτια θα μπορούν να προβλέπουν και να ικανοποιούν τις ανάγκες των ανθρώπων και να οδηγήσουν σε βελτίωση του βιοτικού επιπέδου εγκυμονεί αρκετούς κινδύνους. Οι αισθητήρες καθώς θα συλλέγουν πλήθος δεδομένων είναι πιθανόν ότι θα συλλέγουν και προσωπικά δεδομένα των χρηστών [48]. Τα δεδομένα αυτά θα υπόκεινται σε επεξεργασία με σκοπό να εξαχθεί μια απόφαση, χωρίς όμως να

έχει ζητηθεί η συγκατάθεση του υποκείμενου των δεδομένων. Παρατηρείται λοιπόν ότι καθώς αυξάνεται η αυτοματοποίηση της κοινωνίας τόσο τα προσωπικά δεδομένα του ανθρώπου κινδυνεύουν να χρησιμοποιηθούν για λάθος σκοπούς.

3. Τεχνολογίες Ενεργοποίησης - Enabling technologies

Τα ασύρματα δίκτυα κινητών επικοινωνιών εξελίσσονται κάθε δεκαετία με στόχο την κάλυψη των συνεχώς αυξανόμενων απαιτήσεων. Τα δίκτυα πέμπτης γενιάς διέπονται από αρκετούς περιορισμούς, όπως έλλειψη παγκόσμιας κάλυψης, υψηλότερη καθυστέρηση, λιγότερη αξιοπιστίας και μη ευρεία χρήση της τεχνητής νοημοσύνης σε σχέση με τα δίκτυα έκτης γενιάς. Αυτοί οι περιορισμοί οδηγούν στην ανάγκη δημιουργίας ενός νέου συστήματος επικοινωνίας που παρέχει περισσότερη χωρητικότητα, εξαιρετικά χαμηλό λανθάνοντα χρόνο, υψηλό ρυθμό μετάδοσης δεδομένων, ασφαλή επικοινωνία χωρίς σφάλματα και πλήρη ασύρματη κάλυψη. Τα μελλοντικά συστήματα ασύρματης επικοινωνίας 6G θα αποτελούν ένα έξυπνο και υπερσύγχρονο δίκτυο, το οποίο θα χαρακτηρίζεται από εξαιρετικά χαμηλή καθυστέρηση και υψηλή ταχύτητα μετάδοσης δεδομένων. Σε αρκετές μελέτες γίνεται λόγος για τις εφαρμογές τις οποίες θα υποστηρίζει το δίκτυο 6G με τη βοήθεια της τεχνητής νοημοσύνης. Η ολογραφική επικοινωνία, η εικονική, μικτή και επαυξημένη πραγματικότητα, τα έξυπνα περιβάλλοντα και τα αυτόνομα οχήματα αποτελούν μόνο μερικές από τις εφαρμογές που θα υποστηρίζουν τα δίκτυα 6G και θα οδηγήσουν την ανθρωπότητα σε μία νέα εποχή.

Οι αναδυόμενες εφαρμογές που θα εξοπλίσουν το δίκτυο 6G θα πρέπει να υποστηρίζονται από κάποιες κύριες τεχνολογίες ενεργοποίησης. Οι τεχνολογίες ενεργοποίησης (enabling technologies) αποτελούν μια καινοτομία η οποία όταν εφαρμοστεί οδηγεί σε μετασχηματισμό και παροχή νέων δυνατοτήτων στο χρήστη. Τα δίκτυα έκτης γενιά θα ενσωματώσουν πλήθος τεχνολογιών ενεργοποίησης για την ικανοποίηση των απαιτήσεων των εφαρμογών και υπηρεσιών που θα παρέχουν.

3.1. Επικοινωνίες Terahertz - Terahertz (THZ) Communications

Η εξέλιξη της τεχνολογίας μας οδηγεί σε μια εποχή μαζικής συνδεσιμότητας συσκευών και μεταφοράς μεγάλου όγκου πληροφοριών. Καθώς το δίκτυο 6G θα παρέχει ποίκιλλες εφαρμογές οι οποίες απαιτούν περισσότερη ευελιξία, υψηλό ρυθμό δεδομένων, μεγάλο εύρος ζώνης και εξαιρετικά χαμηλή καθυστέρηση, η ανάγκη για την εφαρμογή της ζώνης επικοινωνίας THz κρίνεται αναγκαία. Η ζώνη THz αποτελεί τη ζώνη συχνοτήτων από 0,1 έως 10 THz που αντιστοιχεί στο μήκος κύματος 3 και 0,03 mm [49]. Το δίκτυο 6G θα είναι το πρώτο ασύρματο δίκτυο επικοινωνίας το οποίο με τη βοήθεια της THz επικοινωνίας θα υποστηρίζει υψηλό

ρυθμό μετάδοσης μεγέθους Tbps, μέγεθος το οποίο αποτελούσε άπιαστο όνειρο για τεχνολογίες που χρησιμοποιούσαν ζώνες συχνοτήτων κάτω από 0,1 THz. Τα THz waves είναι κύματα υψηλή συχνότητας με αρκετά μικρό μήκος κύματος και μεταφέρουν δεδομένα πιο γρήγορα. Καθώς ο κόσμος οδηγείται μέσω της τεχνολογίας σε μια έξυπνη κοινωνία, η οποία θα διαθέτει καινοτόμες εφαρμογές, και θα απαιτείται σύνθεση μεγάλου αριθμού συσκευών στο δίκτυο και ανταλλαγή υψηλής ποσότητας δεδομένων, για τη διευκόλυνση των πολιτών της γίνεται κατανοητή η ανάγκη μελέτης και κατανόησης της ζώνης THz, η οποία στα ασύρματα δίκτυα θα μειώσει σημαντικά την καθυστέρηση. Η συνεισφορά της τεχνολογίας THz στη μεταφορά βίντεο, χωρίς καθυστέρηση και με υψηλή ευκρίνεια, καθώς και στα αυτόνομα και ρομποτικά συστήματα θα είναι καθοριστική. Επιπλέον τα συστήματα 6G που λειτουργούν στη ζώνη THz διαθέτουν υψηλές δυνατότητες τοποθέτησης, ανίχνευσης και τρισδιάστατης απεικόνισης, τα οποία αποτελούν βασικά στοιχεία για την αυτόνομη οδήγηση. Επίσης η επικοινωνία μεταξύ αυτόνομων οχημάτων (V2V), καθώς και των αυτόνομων οχημάτων με την υποδομή (V2I) απαιτεί υψηλό εύρος ζώνης και σύνδεση υψηλής ταχύτητας τα οποία περιέχονται στην επικοινωνία THz. Τέλος η ολογραφική επικοινωνία και η τηλεχειρουργική θα επωφεληθούν από την επικοινωνία THz, εφόσον τα χαρακτηριστικά της επικοινωνία THz αποτελούν απαιτήσεις για την ολογραφική επικοινωνία και την τηλεχειρουργική.

3.2. Τεχνητή Νοημοσύνη - Artificial Intelligence

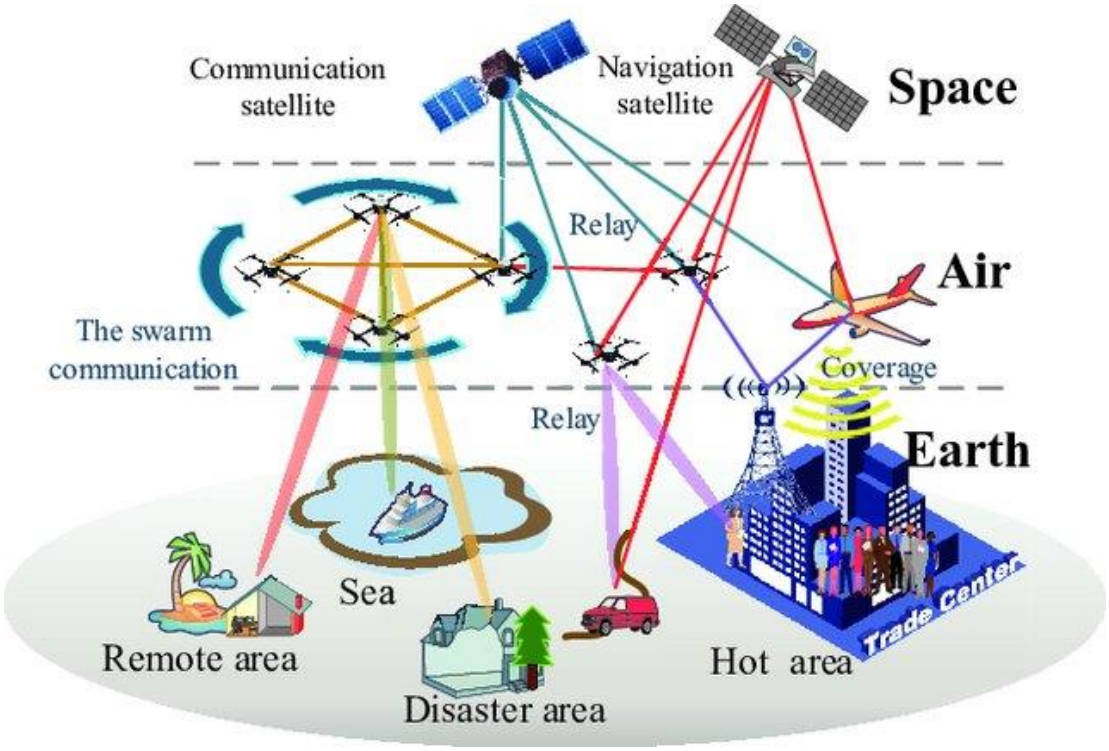
Στη σύγχρονη τεχνολογικά εξελιγμένη κοινωνία το ενδιαφέρον των επιστημόνων στρέφεται στην εφαρμογή της τεχνητής νοημοσύνης σε διάφορους τομείς της καθημερινότητας με σκοπό τη βελτίωση και διευκόλυνση της καθημερινότητας των ανθρώπων μέσω καινοτόμων και μοναδικών εφαρμογών. Η εμφάνιση της τεχνητής νοημοσύνης στα δίκτυα κινητής επικοινωνίας πραγματοποιήθηκε αρχικά στο δίκτυο 5G. Στα δίκτυα έκτης γενιάς η τεχνητή νοημοσύνη και η μηχανική μάθηση θα αποτελέσουν δύο ριζικά στοιχεία του δικτύου. Η είσοδος της τεχνητής νοημοσύνης στις επικοινωνίες θα απλοποιήσει και θα βελτιώσει τη μεταφορά δεδομένων σε πραγματικό χρόνο [50].

Τα δίκτυα 6G θα εκμεταλλευτούν την τεχνητή νοημοσύνη για την παροχή υψηλής αυτοματοποίησης, υψηλής ακρίβειας και απόδοσης δικτύου, διαχείρισης των πόρων και έλεγχο του δικτύου [51]. Όπως έχει ήδη αναλυθεί και στο κεφάλαιο 2 η συνεισφορά της τεχνητή νοημοσύνης στον τομέα της υγείας, μέσω της τηλεχειρουργικής, στον τομέα των μεταφορών, μέσω των αυτόνομων οχημάτων, καθώς και στον τομέα της βιομηχανίας και των έξυπνων πόλεων και σπιτιών θα είναι αξιοσημείωτη. Ειδικότερα τα αυτόνομα οχήματα για να αποκτήσουν αντίληψη του περιβάλλοντος στο οποίο βρίσκονται και να μπορούν να εντοπίσουν αντικείμενα, ώστε να αποφύγουν τα ατυχήματα, αξιοποιούν την τεχνητή νοημοσύνη. Επιπλέον για τη λήψη αυτόνομων αποφάσεων σχετικά με την οδήγηση χρησιμοποιείται η τεχνητή νοημοσύνη. Στον τομέα της υγείας και πιο συγκεκριμένα για την υποστήριξη της τηλεχειρουργικής αλλά και της υγειονομικής περίθαλψης η

τεχνητή νοημοσύνη θα προσφέρει επικοινωνία σε πραγματικό χρόνο. Η επικοινωνία σε πραγματικό χρόνο δεν ήταν εφικτή στα ήδη υπάρχοντα δίκτυα, όμως στα δίκτυα έκτης γενιάς με την υποστήριξη της τεχνητή νοημοσύνης και της εξαιρετικά χαμηλής καθυστέρησης, το άπιαστο αυτό όνειρο αναμένεται να γίνει πραγματικότητα και να αποτελέσει το στυλοβάτη για τη δημιουργία νέων εφαρμογών.

Στον τομέα της ασφάλειας η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για τον εντοπισμό πιθανών απειλών στο δίκτυο. Μέσω κανόνων εκμάθησης αναγνώρισης εισβολών οι οποίοι θα χρησιμοποιούν αλγόριθμούς τεχνητής νοημοσύνης θα μπορούν να ανιχνευτούν επιθέσεις στο δίκτυο.

3.3. Μη Επίγειες Τεχνολογίες - Non – Terrestrial Technologies



Εικόνα 7. Space – Air – Ground Architecture [52].

Η παγκόσμια κάλυψη αναφέρεται στην προσφορά και διαθεσιμότητα υπηρεσιών σε οποιοδήποτε μέρος του πλανήτη χωρίς περιορισμούς. Τα δίκτυα έκτης γενιάς δεν θα περιορίζονται μόνο σε επίγεια δίκτυα επικοινωνίας, τα οποία δεν παρέχουν πλήρη κάλυψη, αλλά θα συνδυάζουν επίγεια και μη επίγεια δίκτυα [53]. Η παγκόσμια κάλυψη που θα παρέχει το δίκτυο 6G θα οδηγήσει σε καλύτερης ποιότητας παροχής υπηρεσιών στο χρήστη. Στα μη επίγεια δίκτυα θα περιλαμβάνονται τα δορυφορικά δίκτυα, τα δίκτυα μη επανδρωμένων εναέριων οχημάτων (UAV) και τα δίκτυα θαλάσσιων επικοινωνιών, τα οποία θα εξασφαλίζουν πλήρη κάλυψη σε όλη τη γη σε συνδυασμό με τα επίγεια δίκτυα και θα παρέχουν ένα δίκτυο επικοινωνίας διάστημα – αέρας – έδαφος – θάλασσα [54].

Η ενοποίηση δορυφορικών, εναέριων, υποθαλάσσιων και επίγειων δικτύων θα ενισχύσει τα δίκτυα 6G με χαρακτηριστικά σημαντικά για τις εφαρμογές που θα παρέχει το δίκτυο 6G. Η ικανοποίηση αιτημάτων με μηδενική καθυστέρηση, η παροχή εξατομικευμένων και "έξυπνων" υπηρεσιών, η βελτίωση της κάλυψης του δικτύου, η βελτίωση της ποιότητα των υπηρεσιών και η διαχείριση της κυκλοφορίας των δεδομένων αποτελούν τα προαναφερθέντα χαρακτηριστικά. Η συμβολή των μη επανδρωμένων εναέριων οχημάτων κρίνεται αναγκαία, καθώς θα οδηγήσει σε γρήγορη απόκριση σε δύσκολα και δυσπρόσιτα περιβάλλοντα. Επίσης θα μπορούν να παρέχουν ασύρματη σύνδεση σε ειδικές εκδηλώσεις όπως συναυλίες, αθλητικές εκδηλώσεις αλλά και σε περίπτωση φυσικών καταστροφών κατά τη διάρκεια των οποίων τα χερσαία δίκτυα μπορεί να έχουν πληγεί. Επιπλέον με το υποθαλάσσιο δίκτυο θα είναι δυνατή η παροχή υπηρεσιών στα πλοία σε οποιοδήποτε μέρος του κόσμου, κάτι το οποίο δεν είναι δυνατό σε πολλές περιπτώσεις στη σύγχρονη εποχή. Τα πλεονεκτήματα που διέπουν την επικοινωνία βασισμένη σε drones είναι το χαμηλό κόστος, η ευελιξία, η βελτίωση της κάλυψης, η βελτίωση της χωρητικότητας του δικτύου, η επεκτασιμότητα, η αυτόνομη λειτουργία και η μειωμένη επίδραση στο φυσικό περιβάλλον. Όμως το περιορισμένο εύρος λειτουργίας, ο περιορισμός της μπαταρίας, η κατανομή των πόρων και οι κίνδυνοι ασφάλειας αποτελούν ορισμένες σημαντικές προκλήσεις για την εισαγωγή των drones στα δίκτυα έκτης γενιάς [55]. Επιπλέον στα δίκτυα 6G οι θαλάσσιες επικοινωνίες θα αναβαθμιστούν σημαντικά ώστε να παρέχουν υπηρεσίες επικοινωνιών υψηλής ποιότητας στα πλοία. Με αυτόν τον τρόπο επιτυγχάνεται η παροχή υπηρεσιών σε περιοχές με περιορισμένες ή χωρίς καθόδου επίγεια υποδομή ή σε περιπτώσεις αδυναμίας λειτουργίας των επίγειων δικτύων όπως σε σεισμούς, καταστροφές ή πολέμους.

Το δίκτυο επικοινωνίας διάστημα – αέρας – έδαφος – θάλασσα αποτελεί ένα έξυπνο και ετερογενές δίκτυο το οποίο διέπετε από υψηλή πολυπλοκότητα με αποτέλεσμα να υπάρχει κίνδυνος για την ασφάλεια. Ειδικότερα το δίκτυο θα πρέπει να ενσωματώσει τεχνολογίες οι οποίες θα εγγυόνται την ασφάλεια των παρεχόμενων υπηρεσιών, καθώς και των δεδομένων που μεταδίδονται στο δίκτυο.

3.4. Οπτικές Ασύρματες Επικοινωνίες - Optical Wireless Communications

Τα δίκτυα οπτικών ινών συνθέτουν το βασικό εργαλείο για τη διασύνδεση όλων των ηπείρων και την ανταλλαγή πληροφορίων με υψηλή ταχύτητα. Η ενσωμάτωση όμως νέων τεχνολογιών και εφαρμογών στα δίκτυα έκτης γενιάς, όπως η εικονική και επαυξημένη πραγματικότητα, τα αυτόνομα οχήματα, η τηλεϊατρική κλπ. έφεραν στην επιφάνεια ότι το φάσμα ραδιοσυχνοτήτων (RF) δε θα μπορεί να καλύψει τις απαιτήσεις των εφαρμογών του δικτύου 6G. Επιπλέον η αύξηση του αριθμού των ασύρματων φορητών συσκευών και της συνδεσιμότητας συσκευών IoT και αυτόνομων οχημάτων στο δίκτυο δεν μπορούσαν να ικανοποιηθούν από τη ζώνη συχνοτήτων mmWave του δικτύου 5G. Τη λύση στο πρόβλημα αναμένεται να φέρουν οι οπτικές ασύρματες επικοινωνίες (Optical

wireless communications). Οι οπτικές ασύρματες επικοινωνίες λειτουργούν ήδη από τα δίκτυα τέταρτης γενιάς όμως αναμένεται να γίνουν περισσότερες μελέτες σχετικά με τις οπτικές ασύρματες επικοινωνίες ώστε να αναπτυχθούν περαιτέρω και να ενισχύσουν το δίκτυο 6G [56]. Επιπλέον οι επικοινωνίες OWC περιλαμβάνουν τρεις διαφορετικές ζώνες συχνοτήτων, την υπέρυθρη ακτινοβολία (IR), την επικοινωνία ορατού φωτός (VLC) και την υπεριώδη ακτινοβολία (UV) [57].

Η επικοινωνία ορατού φωτός αποτελεί την πιο σημαντική συχνότητα των OWC. Οι έξυπνες πόλεις, τα έξυπνα σπίτια, τα αυτόνομα οχήματα καθώς και τα νοσοκομεία επίκειται να χρησιμοποιήσουν το VLC για την αξιόπιστη, ταχύτατη και ασφαλή λειτουργία των συστημάτων τους [58]. Πιο συγκεκριμένα το VLC θα ενισχύσει τη γρήγορη δημιουργία του ασύρματου δικτύου και θα χρησιμοποιηθεί σε ένα ευρύ φάσμα εφαρμογών. Το VLC χρησιμοποιεί διόδους εκπομπής φωτός (LED) και προσφέρει πολλά πλεονεκτήματα σε επικοινωνίες μικρής εμβέλειας σε σύγκριση με την RF. Στα σημαντικά πλεονεκτήματα του VLC συγκαταλέγεται η μη παραγωγή ηλεκτρομαγνητικής ακτινοβολίας (EM) και η μη επιρροή από εξωτερικές ηλεκτρομαγνητικές παρεμβολές [59]. Τα δυο προαναφερθέντα χαρακτηριστικά την καθιστούν ικανή για την ευρεία χρήση της σε εξειδικευμένες εφαρμογές που είναι ευαίσθητες στις ηλεκτρομαγνητικές παρεμβολές όπως στα αεροπλάνα και στα νοσοκομεία. Επιπλέον η ασφάλεια και το απόρρητο αποτελούν ουσιώδες στοιχεία των δικτύων επικοινωνιών. Η επικοινωνία ορατού φωτός είναι πιο ασφαλής, καθώς μπορεί να διατηρήσει την ασφάλεια των πληροφοριών και να αποτρέψει την πρόσβαση κακόβουλων ατόμων σε αυτές. Το εύρος μετάδοσης του δικτύου περιορίζεται σε εσωτερικούς χώρους (κτίρια), καθώς το VLC χρησιμοποιεί ορατό φως το οποίο σημαίνει ότι δεν μπορεί να περάσει από αδιαφανή αντικείμενα, όπως τοίχους, με αποτέλεσμα οι ευαίσθητες πληροφορίες των χρηστών να είναι ασφαλείς και να μην κινδυνεύουν να υποκλαπούν όταν οι χρήστες βρίσκονται σε εσωτερικού χώρους.

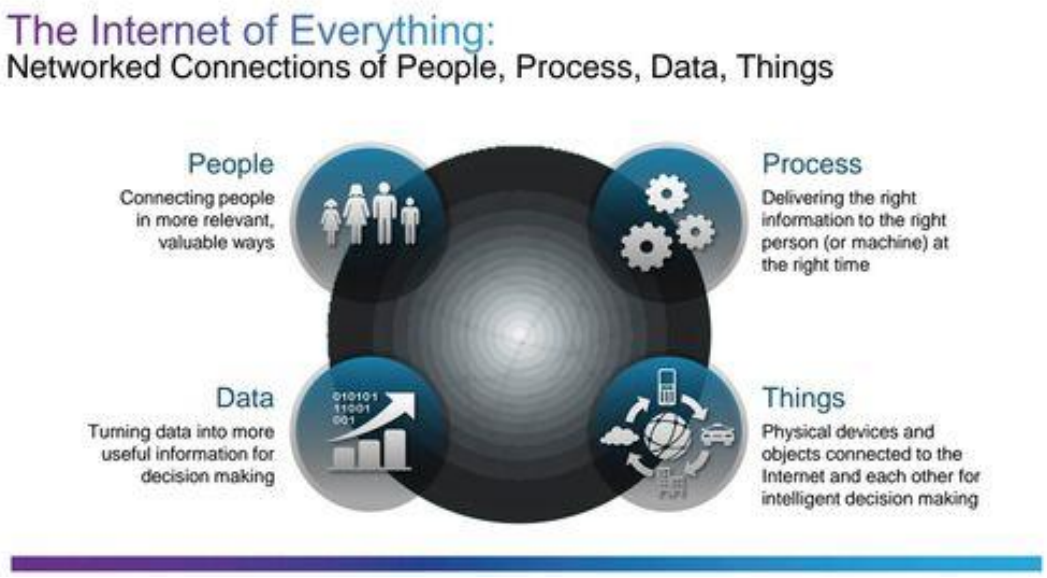
3.5. Edge Intelligence

Τα δίκτυα έκτης γενιάς, όπως είναι ήδη γνωστό, θα περιέχουν ένα εκθετικά αυξανόμενο πλήθος έξυπνων συσκευών που θα παράγουν μεγάλες ποσότητες δεδομένων. Το cloud computing θα αποτελέσει τη βάση για το δίκτυο 6G για την αποθήκευση και επεξεργασία δεδομένων. Η παραπάνω διαδικασία όμως, δηλαδή η μεταφορά μεγάλου όγκου δεδομένων στο cloud για αποθήκευση και επεξεργασία, συνοδεύεται από την κατανάλωση πόρων επικοινωνίας και εύρους ζώνης. Όμως καθώς το πλήθος των συσκευών που θα συνδέονται στο δίκτυο θα αυξάνεται και παράλληλα το δίκτυο 6G θα περιέχει υπηρεσίες σε πραγματικό χρόνο γίνεται κατανοητό ότι η μεταφορά των δεδομένων στο cloud για επεξεργασία δεν αποτελεί ένα αποδοτικό μέτρο. Τη λύση στο πρόβλημα υπόσχεται να φέρει το edge intelligence (EI), το οποίο θα βοηθήσει τα δίκτυα έκτης γενιάς να ικανοποιούν τις απαιτήσεις των χρηστών τους [60]. Η προσφορά του edge intelligent στις εφαρμογές της τεχνητής νοημοσύνης θα καλύπτει ένα ευρύ φάσμα και θα ενισχύσει τον τομέα

της υγειονομικής περίθαλψης, των αυτόνομων οχημάτων, της βιομηχανίας και των έξυπνων πόλεων κα σπιτιών.

Το edge intelligent αποτελεί ένα συνεχώς αυξανόμενο σύνολο συσκευών και συστημάτων που συλλέγουν και επεξεργάζονται δεδομένα κοντά στο χρήστη ή/και την πηγή των δεδομένων [61]. Πιο συγκεκριμένα το edge intelligent αποτελείται από τους κόμβους edge στους οποίους πραγματοποιείται η συλλογή και ανάλυση των δεδομένων και στη συνέχεια λαμβάνουν μια απόφαση σχετικά με την ενέργεια στην οποία θα πρέπει να προβεί η συσκευή/χρήστης [62]. Οι κόμβοι edge θα χρησιμοποιούν αλγόριθμους τεχνητής νοημοσύνης για την ανάλυση των δεδομένων και την εύρεση μοτίβων σε αυτά. Επίσης θα βρίσκονται τοποθετημένοι κοντά στον χρήστη με αποτέλεσμα την ύπαρξη ελάχιστης καθυστέρησης και την παροχή υπηρεσιών σε πραγματικό χρόνο, στοιχεία βασικά για το δίκτυο 6G. Όπως έχει αναλυθεί στο κεφάλαιο 2.6. Αυτόνομη Οδήγηση, καθώς μεταβαίνουμε σε μια νέα εποχή στην οποία το επίπεδο αυτοματοποίησης των οχημάτων αναμένεται να είναι 5 γίνεται κατανοητή η ανάγκη για την επεξεργασία των δεδομένων που συλλέγονται από το όχημα κοντά σε αυτό και όχι στο cloud. Οπότε το edge intelligent αποτελεί το κατάλληλο εργαλείο για τη σωστή λειτουργία των αυτόνομων οχημάτων. Επιπλέον στον τομέα της υγείας οι τεχνολογία edge intelligent θα αξιοποιηθεί από τις ποικίλες ιατρικές συσκευές. Οι συγκεκριμένες συσκευές θα συλλέγουν τα δεδομένα υγείας του χρήστη και θα τα μεταδίδουν στους κόμβους edge για να πραγματοποιηθεί η επεξεργασία τους και να γνωστοποιεί τα αποτελέσματα στον κατάλληλο πρόσωπο (γιατρό, νοσοκόμο, χρήστη). Αξίζει να σημειωθεί ότι μετά την επεξεργασία των δεδομένων στους κόμβους edge τα σημαντικά δεδομένα αποστέλλονται στο cloud για αποθήκευση. Στα πλεονεκτήματα που διέπουν την τεχνολογία edge intelligent περιλαμβάνεται η χαμηλή καθυστέρηση, οι οικονομικά αποδοτικές επικοινωνίες, η αξιοπιστία, η προστασία της ιδιωτικής ζωής και η επεκτασιμότητα.

3.6. Διαδίκτυο των Πάντων - Internet of Everything



Εικόνα 8. Διαδίκτυο των Πάντων - Internet of Everything [63].

Στη σύγχρονη εποχή ο κόσμος κατακλύζεται με μεγάλη συχνότητα από νέες τεχνολογικές εξελίξεις. Η εξέλιξη των δικτύων κινητών επικοινωνιών θα «εξοπλίσει» τους ανθρώπους με νέες δυνατότητες μέσω των καινοτόμων εφαρμογών που θα μπορούν να υποστηρίζουν τα δίκτυα έκτης γενιάς. Το Διαδίκτυο των Πάντων (Internet of Everything – IoE) αναμένεται να ενισχύσει με νέες αναδυόμενες υπηρεσίες τα δίκτυα έκτης γενιάς. Η εκτεταμένη πραγματικότητα (XR) και τα συστήματα τηλεϊατρικής αποτελούν ορισμένες από τις εφαρμογές τους IoE οι οποίες λόγω του υψηλού ρυθμού δεδομένων, της ολοκληρωμένης κάλυψης, του χαμηλού λανθάνοντα χρόνο και της αξιοπιστίας, τα οποία αποτελούν χαρακτηριστικά του δικτύου 6G, θα οδηγήσουν σε μια νέα εποχή.

Ο όρος IoE αποτελεί ένα σχετικά καινούργιο όρο και είναι λιγότερος γνωστός από το IoT. Για το λόγο αυτό συχνά γίνεται συσχέτιση του με τον όρο IoT. Για να γίνει κατανοητή η διαφορά των δύο προαναφερθέντων όρων παρακάτω παρατίθεται ο ορισμός του IoE σύμφωνα με την Cisco το 2013: « Το Διαδίκτυο των Πάντων (IoE) συγκεντρώνει ανθρώπους, διαδικασίες, δεδομένα και πράγματα για να κάνουν τις δικτυωμένες συνδέσεις πιο σχετικές και πολύτιμες από ποτέ, μετατρέποντας τις πληροφορίες σε ενέργειες που δημιουργούν νέες δυνατότητες, πλουσιότερες εμπειρίες και άνευ προηγουμένου οικονομική ευκαιρία για επιχειρήσεις, ιδιώτες και χώρες» [64]. Παρατηρείται λοιπόν ότι το διαδίκτυο των πάντων αποτελεί την εξέλιξη του διαδίκτυου των πραγμάτων και είναι η έξυπνη σύνδεση άτομων, πράγματων, δεδομένων και διεργασίων, ενώ το διαδίκτυο των παργματων συνδέει μόνο φυσικά αντικείμενα (πράγματα). Επιπλέον αξίζει να σημειωθεί ότι σύμφωνα με την Cisco εκτιμάται ότι το 99,4 τοις εκατό των φυσικών αντικειμένων που μπορεί κάποια μέρα να είναι μέρος του Διαδικτύου των πάντων δεν είναι ακόμη συνδεδεμένα [64].

Τα βασικά θεμέλια του διαδίκτυου των πάντων αποτελούν [65]:

- Τα άτομα: σύνδεση ατόμων με πιο σχετικούς και πολίτιμους τρόπους.
- Τα δεδομένα: μεατροπή δεδομένων σε έξυπνα (intelligence) για καλύτερη λήψη αποφάσεων.
- Οι διαδικασίες: παράδοση σωστών πληροφοριών στο σωστό άτομο ή μηχανή την κατάλληλη στιγμή.
- Τα πράγματα: φυσικές συσκευές και αντικείμενα που συνδεονται στο διαδίκτυο και μεταξύ τους για έξυπνη λήψη αποφάσεων (IoT).

Για να γίνει κατανοητεί η διάκριση μεταξύ του διαδίκτυου των πραγμάτων και του διαδίκτου των πάντων πρέπει να μελετηθεί ο τρόπος με τον οποίο λειτουργούν και τα δύο. Αρχικά το διαδίκτυο των πραγμάτων περιλαμβάνει συσκευές, αισθητήρες κλπ. τα οποία δημιουργούν συνδέσεις μεταξύ τους και δημιουργούν ένα δίκτυο. Οι συσκευές συλλέγουν συνεχώς δεδομένα για το περιβάλλον τους και τα κοινοποιούν σε άλλες συσκευές. Συνεπώς το IoT αποτελεί ένα είδος τεχνολογίας επικοινωνίας μηχανής προς μηχανή (machine-to-machine - M2M) [66]. Το διαδίκτυο των πραγμάτων σχετίζεται κυρίως με τις συνδεδεμένες συσκευες, τις δυνατότητες ανίχνευσής τους, τις δυνατότητες επικοινωνίας τους, τα δεδομένα που δημιουργούνται από τη συσκευή τα οποία αναλύονται και αξιοποιούνται για να κατευθύνουν τις διαδικασίες και να τροφοδοτήσουν πολλές πιθανές περιπτώσεις χρήσης του IoT.

Αντίθετα στο διαδίκτυο των πάντων κάθε στοιχείο στον κύκλο IoE είναι αλληλένδετο και δημιουργεί έναν κλειστό βρόγχο που ξεκινά και τελειώνει με ανθρώπους. Ειδικότερα οι άνθρωποι χρησιμοποιούν τα πράγματα που συλλέγουν και παράγουν δεδομένα για την περαιτέρω επεξεργασία (ανάλυση και εξατομίκευση), οπότε, για άλλη μια φορά, τα άτομα μπορούν να το εκμεταλλευτούν για να λαμβάνουν πιο έξυπνες αποφάσεις βάσει δεδομένων [67]. Οπότε το είδος των τεχνολογιών επικοινωνίας που θα μπορεί να υποστηρίζει το δίκτυο είναι άνθρωπος-σε-άνθρωπο (people-to-people (P2P)), μηχανή-σε-άνθρωπο (machine-to-people (M2P)) και μηχανή-σε-μηχανή (machine-to-machine (M2M)) [68]. Παρατηρείται λοιπόν ότι σε αντίθεση με το διαδίκτυο των πράγματων όπου η τεχνολογία είναι στη μηχανή και οι συσκευές «μιλούν» σε άλλες συσκευές με αποτέλεσμα τον αποκλεισμό σε μεγάλο βαθμό του ανθρώπινου παράγοντα. Τέλος, σημειώνεται ότι το διαδίκτυο των πάντων σχεδιάστηκε για να ξεπεράσει την παθητική προσέγγιση (δεδομένα από αισθητήρες) και τη διάσταση μηχανή-σε-μηχανή του IoT σε μια πιο ενεργή.

Το διαδίκτυο των πάντων έχει ως βάση του τη γενική συνδεσιμότητα. Το IoE θα είναι μια ενεργή σύνδεση και θα οδηγήσει στη δημιουργία ενός αλληλένδετου συστήματος. Τα δεδομένα θα μπορούν να ανταλλάσοται με μεγαλύτερη ευκολία και η διαδικασία λήψης αποφάσεων θα είναι πιο γρήγορη και αποτελεσματική.

Βασική προυπόθεση του IoE αποτελεί η εμφύτευση εκατομμυρίων αισθητήρων σε συσκευές, αντικείμενα και μηχανήματα.

Η εποχή του Διαδικτύου των Πραγμάτων αναμένεται να ξεκινήσει με την έλευση του δικτύου 5G, όμως το Διαδίκτυο των Πάντων δεν θα εμφανιστεί μέχρι το 6G. Το διαδίκτυο των πάντων θα συμβάλει στο μετασχηματισμό της κοινωνίας και θα ενισχύσει ποικίλους τομείς. Στον τομέα της υγείας η συνεισφορά αναμένεται να ανοίξει τον χώρο για την παροχή υπηρεσιών υγειονομικής περίθαλψης σε πραγματικό χρόνο και αποτελεί το βασικό παράγοντα για την επιτυχία της υγειονομικής περίθαλψης. Ενώ το IoT έδωσε το έναυσμα για την ευρεία χρήση ασύρματα συνδεδεμένων συσκευών για τη μέτρηση των καρδιακών παλμών, της αρτηριακής πίεσης, του ποσοστού γλυκόζης στο αίμα κλπ., το IoE θα επιτρέψει στις προαναφερθέντες συσκευές να συνδυάζουν και να αναλύουν τα δεδομένα για να κάνουν καλύτερες και πιο στοχευμένες προβλέψεις και να λαμβάνουν εξατομικευμένες αποφάσεις.

Η βιομηχανία, η διαχείριση της ενέργειας, η ψυχαγωγία και ο τραπεζικός τομέας αποτελούν ορισμένους από τους τομείς στους οποίους το IoE αναμένεται να επηρεάσει θετικά και να οδηγήσει στη ριζική τους αλλαγή και εξέλιξη.

Το διαδίκτυο των πραγμάτων θα αρχίσει να εκδηλώνεται με την κυκλοφορία του 5G. Ωστόσο, θα συνεχίσει να εξελίσσεται καθώς αξιοποιούμε τις χρήσεις του σε κάθε κλάδο μέχρι να φτάσουμε επιτέλους στο διαδίκτυο των πάντων. Το διαδίκτυο των πάντων είναι το επόμενο στάδιο ανάπτυξης του διαδικτύου το οποίο υποστηρίζει τη σύνδεση πραγμάτων, ανθρώπων, διαδικασιών και δεδομένων σε ένα τεράστιο κατανεμημένο δίκτυο. Όμως, καθώς οι συσκευές γίνονται πιο συνδεδεμένες και συλλέγουν περισσότερα δεδομένα, οι ανησυχίες για το απόρρητο και την ασφάλεια θα αυξηθούν επίσης. Η προστασία του απορρήτου και της ιδιωτικής ζωής αποτελούν ορισμένα θέματα τα οποία θα πρέπει να μελετηθούν περαιτέρω.

3.7. Multi-access Edge Computing (MEC)

Το Multi-access Edge Computing, παλαιότερα γνωστό ως mobile edge computing, θα έχει πρωταρχικό ρόλο στα δίκτυα έκτης γενιάς, καθώς θα επιτρέπει την ανάλυση δεδομένων σε πραγματικό χρόνο στο σημείο όπου δημιουργούνται χαρακτηριστικό απαραίτητο για τις εφαρμογές του 6G. Αρχικά στα δίκτυα 5G το MEC θα επιτρέπει δυνατότητες υπολογιστικού νέφους στην άκρη των κυψελοειδών δικτύων. Συγκεκριμένα, το MEC επιτρέπει σε κινητές συσκευές με περιορισμένους πόρους να εκφορτώνουν τις εργασίες υπολογισμού τους στην άκρη του δικτύου. Σύμφωνα με την IBM το Multi-access edge computing μπορεί να οριστεί ως «υπηρεσίες cloud που εκτελούνται στην άκρη ενός δικτύου και εκτελούν συγκεκριμένες εργασίες, σε πραγματικό ή σχεδόν πραγματικό χρόνο, που διαφορετικά θα υποβάλλονταν σε επεξεργασία σε κεντρικές υποδομές πυρήνα (core) ή cloud. Το MEC ωθεί τη συλλογή και επεξεργασία δεδομένων να εκτελούνται

πιο κοντά στις συσκευές και κατ' επέκταση στον τελικό χρήστη συμβάλλοντας σε εξαιρετικά χαμηλή καθυστέρηση στις παρεχόμενες υπηρεσίες» [69]. Το 6G αναμένεται να παρέχει υπηρεσίες edge intelligence (EI) μέσω Multi-access edge computing (MEC) σε συσκευές IoT.

Εκτός από την παροχή υπηρεσιών σε πραγματικό χρόνο λόγω της εξαιρετικά χαμηλής καθυστέρησης το MEC μειώνει την ανάγκη για αποστολή περιττών δεδομένων ή πληροφορίων στα κέντρα δεδομένων cloud [70]. Επιπλέον το MEC αναμένεται να χρησιμοποιηθεί για αποτελεσματική διαχείριση των πόρων του δικτύου [71]. Λόγω των προαναφερθέντων χαρακτηριστικών του και του υψηλού εύρους ζώνης το MEC θα επιτρέψει μοναδικές εφαρμογές και υπηρεσίες. Επιπλέον οι τοπικές δυνατότητες προεπεξεργασίας δεδομένων της MEC και η λήψη αποφάσεων στην άκρη του δικτύου θα αποτελέσουν το κλειδί για τις καινοτόμες εφαρμογές του 6G.

Ορισμένες από τις εφαρμογές στις οποίες θα παίξει ζωτικό ρόλο το MEC είναι στα αυτόνομα οχήματα - αυτόνομη οδήγηση, στην ανάλυση βίντεο σε πραγματικό χρόνο, στην αυτόματη αναγνώριση ομιλίας, στην επαυξημένη πραγματικότητα, στις υπηρεσίες τοποθεσίας, στο διαδίκτυο των πραγμάτων, στον τομέα της υγειονομικής περίθαλψής και στις έξυπνες πόλεις-έξυπνα σπίτια [72]. Ειδικότερα στον τομέα της αυτόνομης οδήγησης και των συνδεδεμένων οχημάτων το MEC συμβάλλει στη γρήγορη ανάλυση και επεξεργασία των δεδομένων που συλλέγονται από του αισθητήρες των οχημάτων στην άκρη του δικτύου για την παροχή πληροφορίων με χαμηλή καθυστέρηση στον οδηγό – όχημα για την έγκαιρη λήψη αποφάσεων [73].

Τα δίκτυα έκτης γενιάς, όπως είναι ήδη γνωστό, αναμένεται να αξιοποιήσουν τα drones για την παροχή πανταχού παρούσας συνδεσιμότητας και την παροχή υπηρεσιών. Τα drone με δυνατότητες MEC θα δίνουν τη δυνατότητα στις κινητές συσκευές να εκφορτώσουν τις απαιτητικές υπολογιστικά εργασίες σε αυτά στην άκρη του δικτύου, ώστε να μειωθεί η συμφόρηση του δικτύου και οι υπηρεσίες θα παρέχονται σε γρήγορο χρόνο [55]. Όμως τα drone λόγω των περιορισμών που διαθέτουν στην αποθήκευση και στη διάρκεια της μπαταρίας οδηγούν στη δημιουργία περιορισμών στις δυνατότητες επεξεργασίας επί του σκάφους και στην αποτελεσματική εκτέλεση απαιτητικών εργασιών. Για την επίλυση του προβλήματος έχει προταθεί από ερευνητές η εκφόρτωση και η εκτέλεση των απαιτητικών υπολογισμών από τα drones σε απομακρυσμένους διακομιστές cloud. Πιο συγκριμένα οι διακομιστές cloud θα συμβάλλουν, πρώτον στην αποθήκευση δεδομένων που έχουν συλλεχθεί από τα drones και δεύτερον στην ελαχιστοποίηση του χρόνου επεξεργασίας και της κατανάλωσης της ενέργειας των drones.

4. Εισαγωγή στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ)

Εικόνα 9. General Data Protection Regulation [74].

Η συνεχής αυξανόμενη ποσότητα δεδομένων προσωπικού χαρακτήρα που δημιουργούνται σε καθημερινή βάση και η αναγκαιότητα προσαρμογής στις τεχνολογικές εξελίξεις (profiling, cloud, IoT), οδήγησε στην ανάγκη για ενημέρωση του νομοθετικού πλαισίου για την προστασία των δεδομένων αυτών. Ειδικότερα η ανάγκη για αλλαγή στον τρόπο και την έκταση της επεξεργασίας δεδομένων, λόγω της χρήσης τους από διάφορες εφαρμογές συνέβαλε στη θέσπιση αυστηρότερων κανόνων για τη διαχείριση και επεξεργασία των δεδομένων. Αρχικά η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου του 1995, η οποία αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την ελεύθερη διακίνηση των δεδομένων αυτών, αντικαταστάθηκε από το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων [75].

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου της 27ης Απριλίου 2016 τέθηκε σε άμεση εφαρμογή σε όλα τα Κράτη – Μέλη από τις 25 Μαΐου 2018 [76]. Σκοπός του κανονισμού είναι η αναίρεση των νομικών ασαφειών του προηγούμενου νομικού πλαισίου και η προστασία των φυσικών προσώπων απέναντι στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη διακίνηση αυτών. Η εφαρμογή του πραγματοποιείται σε όλους τους φορείς που διαχειρίζονται, επεξεργάζονται, αποθηκεύουν και διακινούν δεδομένα προσωπικού χαρακτήρα. Τα δεδομένα που σχετίζονται με Ευρωπαϊκούς πολίτες επηρεάζονται από την εφαρμογή του ΓΚΠΔ ανεξάρτητα από την έδρα του φορέα (εντός ή εκτός της Ευρωπαϊκής Ένωσης). Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι υπεύθυνη για τον έλεγχο της συμμόρφωσης με τον GDPR. Σε περίπτωση παραβίασης του Κανονισμού επιβάλλονται οικονομικές κυρώσεις (πρόστιμα).

4.1. Βασικές Έννοιες (Άρθρο 4 του ΓΚΠΔ)

Για την καλύτερη κατανόηση του κανονισμού αλλά και του τόπου εφαρμογής τους κρίνεται απαραίτητη η ανάλυση των βασικών όρων που το διέπουν σύμφωνα με το άρθρο 4 του ΓΚΠΔ [77].

«Δεδομένα προσωπικού χαρακτήρα (προσωπικά δεδομένα)»: ορίζονται στον ΓΚΠΔ ως κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο το οποίο μπορεί να εξακριβωθεί άμεσα ή έμμεσα, ιδίως με αναφορά σε στοιχεία ταυτότητας όπως όνομα, ΑΜΚΑ, ΑΦΜ, αριθμός δελτίου ταυτότητας, δεδομένα θέσης, καθώς και δεδομένα που αφορούν τη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, και πολιτιστική ταυτότητα του ατόμου.

«Ειδικές κατηγορίες δεδομένων (ευαίσθητα δεδομένα)»: αποτελούν τα προσωπικά δεδομένα στα οποία δεν επιτρέπεται η εκτέλεση της επεξεργασίας. Στα δεδομένα αυτά ανήκουν: η φυλετική ή εθνοτική καταγωγή, ο σεξουαλικός προσανατολισμός, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε συνδικαλιστικές οργανώσεις, τα γενετικά ή βιομετρικά δεδομένα υγείας και προσωπικά δεδομένα που σχετίζονται με ποινικές καταδίκες και αδικήματα, εκτός αν η επεξεργασία αυτών επιτρέπεται από τη νομοθεσία της ΕΕ ή της εθνικής νομοθεσίας.

«Γενετικά δεδομένα»: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

«Βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

«Δεδομένα που αφορούν την υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

«Επεξεργασία δεδομένων»: κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοποιημένων μέσων σε δεδομένα προσωπικού χαρακτήρα. Περιλαμβάνει τη συλλογή, καταχώρηση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμός, περιορισμός, διαγραφή ή καταστροφή προσωπικών δεδομένων.

«Περιορισμός της επεξεργασίας»: η επισήμανση αποθηκευμένων δεομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

«Κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνιστάται 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 απόδοσης στην εργασία, την οικονομική κατάσταση, την υγείας, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση και τις μετακινήσεις του εν λόγω φυσικού προσώπου.

«Ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά, μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

«Σύστημα αρχειοθέτησης»: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

«Συγκατάθεση του υποκείμενου των δεδομένων»: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πληρεί επίγνωση, με την οποία το υποκείμενο των δεδομένων δηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα του προσωπικού χαρακτήρα.

«Παραβίαση δεδομένων προσωπικού χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκευτήκαν ή υποβλήθηκαν κατ΄ άλλο τρόπο σε επεξεργασία.

«Υποκείμενο των δεδομένων»: το άτομο στο οποίο ανήκουν τα προσωπικά δεδομένα και το οποίο μπορεί να ταυτοποιηθεί άμεσα ή έμμεσα από αυτά.

«Υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τον σκοπό και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους. Ο υπεύθυνος επεξεργασίας δίνει τις οδηγίες στον εκτελών την επεξεργασίας και φέρει την ευθύνη για τη σωστή εφαρμογή του νόμου.

«Εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου εξεργασίας.

«Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα στα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασίας, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

4.2. Βασικές Αρχές Επεξεργασίας (Άρθρο 5 του ΓΚΠΔ)

Για τη σωστή εφαρμογή του GDPR ο υπεύθυνος επεξεργασίας οφείλει να προσπαθεί να επιτύχει την τήρηση των τριών βασικών αρχών του Κανονισμού κατά την επεξεργασία των δεδομένων. Τις αρχές αυτές αποτελούν [78]:

1. η δίκαιη/θεμιτή και νόμιμη επεξεργασία,
2. ο περιορισμός σκοπού και
3. η ελαχιστοποίηση και διατήρηση δεδομένων .

Πιο συγκεκριμένα σύμφωνα με το άρθρο 5 του ΓΚΠΔ οι βασικές αρχές που θα πρέπει να τηρούνται κατά την επεξεργασία δεδομένων ώστε να είναι νόμιμη η συλλογή και επεξεργασία τους [79]:

Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας: τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο το δεδομένων.

Αρχή του περιορισμού του σκοπού: τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν θα υποβάλλονται σε περαιτέρω επεξεργασία η οποία θα είναι ασύμβατη με τους σκοπούς αυτούς. Η επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικού σκοπού δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς (άρθρο 89 παράγραφος 1)

Αρχή της ελαχιστοποίησης δεδομένων: τα δεδομένα που συλλέγονται και επεξεργάζονται είναι κατάλληλα, συναφή και περιορίζονται στα αναγκαία.

Αρχή της ακρίβειας: τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και επικαιροποιημένα. Επίσης είναι αναγκαίο να ληφθούν μέτρα για την άμεση διαγραφή ή διόρθωση προσωπικών δεδομένων τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Αρχή του περιορισμού της περιόδου αποθήκευσης: τα δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημά που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων

προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα συστήματα, εφόσον αυτά θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς (άρθρο 89 παράγραφος 1) και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο ΓΚΠΔ για την εξασφάλιση των δικαιωμάτων και των ελευθεριών του υποκείμενου των δεδομένων.

Αρχή της ακεραιότητας και εμπιστευτικότητας: τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια τους, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

Αρχή της λογοδοσίας: ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσης με τις παραπάνω Αρχές.

4.3. Πεδίο εφαρμογής του ΓΚΠΔ (Άρθρα 2,3 του ΓΚΠΔ)

Σύμφωνα με το άρθρο 2 του ΓΚΠΔ το ουσιαστικό πεδίο εφαρμογής του ΓΚΠΔ αναφέρει ότι ο ΓΚΠΔ εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται η πρόκειται να περιληφθούν σε συστήματα αρχειοθέτησης [80]. Επιπλέον τονίζει ότι ο ΓΚΠΔ δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα:

a. Στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δίκαιου της Ένωσης,

b. Από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ,

c. Από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας,

d. Από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια.

Ακόμη σύμφωνα με το άρθρο 3 του ΓΚΠΔ σχετικά με το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ [81]:

1. Ο ΓΚΠΔ εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασία

ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

2. Ο ΓΚΠΔ εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκείμενων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωσης, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με :
    a. Την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή
    b. Την παρακολούθηση της συμπεριφορά τους, στο βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.
3. Ο ΓΚΠΔ εφαρμόζεται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας μη εγκατεστημένο στην Ένωση, αλλά σε τόπο όπου εφαρμόζεται το δίκαιο κράτους μέλους δυνάμει του δημοσίου διεθνούς δικαίου.

4.4. Νομιμότητα της επεξεργασίας (Άρθρο 6 του ΓΚΠΔ)

Προκειμένου η επεξεργασία δεδομένων από τους παρόχους υπηρεσιών να χαρακτηρίζεται ως νόμιμη θα πρέπει να ισχύει τουλάχιστον μία από τις ακόλουθες περιπτώσεις σύμφωνα με το άρθρο 6 του ΓΚΠΔ [82]. Αρχικά το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους σκοπούς. Επιπλέον ως νόμιμη κρίνεται και η επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν είναι απαραίτητη για την εκτέλεση σύμβασης, της οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ’ αίτηση του υποκείμενου των δεδομένων πριν από τη σύναψη σύμβασης. Ακόμη η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας. Επίσης νόμιμη είναι η επεξεργασία όταν είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή τρίτου φυσικού προσώπου. Επιπρόσθετα στην περίπτωση που η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας κρίνεται ως νόμιμη επεξεργασίας. Τέλος η επεξεργασία είναι σύννομη όταν είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

4.5. Συγκατάθεση (Άρθρο 7 του ΓΚΠΔ)

Ο ΓΚΠΔ ξεκαθαρίζει τις απαιτήσεις για την απόκτηση και απόδειξη της έγκυρης συγκατάθεσης παρέχοντας λεπτομερείς οδηγίες. Σύμφωνα με το άρθρο 6 του ΓΚΠΔ, η συγκατάθεση αποτελεί μια από τις έξι νόμιμες βάσεις για την συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα [83]:

1. Όταν η επεξεργασία βασίζεται σε συγκατάθεση, ο υπεύθυνος επεξεργασίας είναι σε θέση να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασίας των δεδομένων του προσωπικού χαρακτήρα.

2. Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.

3. Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεση του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησης της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

4. Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση της σύμβασης, συμπεριλαμβανομένης της παροχή μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

4.6. Αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων

Στη σύγχρονη κοινωνία η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ αποτελούν διαδικασίες, οι οποίες εφαρμόζονται σε καθημερινή βάση σε διάφορους τομείς της ζωής του ανθρώπου, χάρη στις δυνατότητες που παρέχουν διάφορες τεχνολογίες, όπως η τεχνητή νοημοσύνη, η μηχανική μάθηση και τα big data. Πιο συγκεκριμένα η υγειονομική περίθαλψη, ο τραπεζικός και χρηματοοικονομικός τομέας, η φορολογία, η ασφάλιση, το μάρκετινγκ και η διαφήμιση αποτελούν τους κυριότερους τομείς στους όποιους το άτομο υπόκειται σε αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ. Όπως θα αναλυθεί και στο κεφάλαιο 5.2. η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ θα αποτελέσουν βασικά στοιχεία για τα δίκτυα έκτης γενιάς. Ειδικότερα τα

προϊόντα της τεχνητής νοημοσύνης θα προβαίνουν σε αυτοματοποιημένη λήψη αποφάσεων και επιπλέον τα δεδομένα που συλλέγονται από τους ετερογενείς αισθητήρες που θα είναι τοποθετημένοι στα αυτόνομα οχήματα, στις υποδομές των έξυπνων πόλεων και στα έξυπνα σπίτια θα αξιοποιούνται για την κατάρτιση προφίλ. Επομένως οι δυο διαδικασίες που αναφέρονται παραπάνω προσφέρουν πλήθος πλεονεκτημάτων, όμως είναι αρκετές οι περιπτώσεις στις οποίες παραβιάζονται τα δικαιώματα και οι ελευθερίες του ατόμου.

Για να κατανοήσουμε καλύτερα το εύρος των παραβιάσεων πρέπει πρώτα να κατανοήσουμε τη σημασία των όρων κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων. Αρχικά ως κατάρτιση προφίλ (profiling) καθορίζεται η διαδικασία κατά την οποία οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα για να αξιολογήσει ορισμένες προσωπικές πτυχές ενός φυσικού προσώπου, ιδίως για την ανάλυσης 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 (άρθρο 4 παράγραφος 4). Επιπλέον ως αυτοματοποιημένη λήψη αποφάσεων ορίζεται η διαδικασία κατά την οποία αυτοματοποιημένα μέσα λαμβάνουν αποφάσεις σχετικές με κάποιο άτομο με τεχνολογικά μέσα και χωρίς την παρέμβαση ανθρώπου. Οι αποφάσεις που λαμβάνονται μπορεί να οφείλονται σε πραγματικά δεδομένα, καθώς και σε ψηφιακά δημιουργημένα προφίλ.

Η αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ αποτελούν το άρθρο 22 του ΓΚΠΔ, στο οποίο αναφέρεται στο δικαίωμα του ατόμου να μην υπόκειται σε αυτοματοποιημένη λήψη απόφασης και κατάρτιση προφίλ [84]. Αξίζει να σημειωθεί ότι η παραπάνω απόφαση δεν εφαρμόζεται όταν, πρώτον είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων, δεύτερον επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή τρίτον βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων.

Η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ αποτελούν δύο πολύ ισχυρά εργαλεία τα όποια χρησιμοποιούνται για να παρέχουν τις κατάλληλες υπηρεσίες και προϊόντα στο κάθε άτομο, με βάση τις ατομικές τους ανάγκες. Στον ασφαλιστικό τομέα, βασιζόμενοι στα δεδομένα του πελάτη και με τη χρήση του κατάλληλου αλγορίθμου παράγεται η απόφαση η οποία είναι θετική ή αρνητική για την ασφάλιση του εκάστοτε πελάτη. Στην περίπτωση που είναι θετική παράγεται και το αποτέλεσμα με το ποσό της ασφάλισης. Η ασφαλιστική εταιρεία ελέγχει την ορθότητα της απόφασης που παρήγαγε ο αλγόριθμος και την ανακοινώνει τον πελάτη της. Η ασφαλιστική εταιρία αρχικά οφείλει να ενημερώσει

τον πελάτη ότι η απόφαση θα ληφθεί με αυτοματοποιημένο τρόπο και στην περίπτωση που δεν συμφωνεί με την απόφαση έχει το δικαίωμα να την προσβάλει. Από το παραπάνω παράδειγμα γίνεται φανερό ότι ελλοχεύουν σημαντικοί κίνδυνοι κατά την εφαρμογή της αυτοματοποιημένη λήψης αποφάσεων και της κατάρτισης προφίλ.

Στα κυριότερα μειονεκτήματα των δύο διαδικασιών είναι η μη ύπαρξη διαφάνειας και ενημέρωσης [85]. Ειδικότερα το υποκείμενο των δεδομένων υπάρχει πιθανότητα να μην γνωρίζει ότι τα δεδομένα του συλλέγονται με σκοπό την δημιουργία προφίλ. Η έλλειψη ενημέρωσης του υποκειμένου οδηγεί σε παραβίαση των δικαιωμάτων του καθώς, η υπηρεσία ή η εφαρμογή που συλλέγει τα δεδομένα οφείλει να ενημερώσει και να προβεί στη συλλογή των δεδομένων μετά τη ρητή συγκατάθεση του υποκείμενου των δεδομένων. Επιπλέον η κατάρτιση προφίλ μπορεί να οδηγήσει στη διαιώνιση υφιστάμενων στερεοτύπων και στην αύξηση του κοινωνικού διαχωρισμού οδηγώντας στη δημιουργία αδικαιολόγητων διακρίσεων. Επίσης μπορεί να οδηγήσει σε άρνηση παροχής υπηρεσιών και προϊόντων, αλλά και σε ανακριβείς προβλέψεις. Από τις παραπάνω περιπτώσεις συμπεραίνουμε ότι η ελευθερία ενός ατόμου μπορεί να υπονομευτεί και για αυτό το λόγο η ύπαρξη νομοθεσίας για την προστασία του ατόμου κρίνεται αναγκαία.

5. Νομικά Ζητήματα των Εφαρμογών και Τεχνολογιών Ενεργοποίησης των Δικτύων 6ης Γενιάς

Η εξέλιξη των δικτύων κινητής τηλεφωνίας αναμένεται να οδηγήσει σε μια νέα εποχή. Τα δίκτυα έκτης γενιάς θα αποτελέσουν το εργαλείο για την υποστήριξη καίριων εφαρμογών και υπηρεσιών οι οποίες μέχρι στιγμής αποτελούσαν άπιαστο όνειρο για την ανθρωπότητα. Το κύριο χαρακτηριστικό τους θα είναι η τεχνητή νοημοσύνη η οποία θα αποτελέσει το θεμέλιο για το δίκτυο 6G. Όμως λόγω της πολυπλοκότητας του δικτύου 6G θα υπάρξουν προκλήσεις σχετικά με την ασφάλεια και πλήθος νομικών ζητημάτων στις εφαρμογές και τις τεχνολογίες που θα ενσωματώνει το 6G. Τεχνολογίες οι οποίες είναι χρήσιμες για την ανάπτυξη του 6G και θα παρέχουν στο δίκτυο χαμηλή καθυστέρηση, αξιοπιστία και υψηλό ρυθμό μετάδοσης θα δημιουργήσουν προβλήματα ασφάλειας και απορρήτου.

Το 6G θα είναι πανταχού παρόν αφού θα διαθέτει πολλές συσκευές, αισθητήρες και αυτόνομες εφαρμογές. Όμως η παραπάνω δυνατότητα του 6G δημιουργεί ζητήματα σχετικά με την προσωπική ζωή αλλά και τη χρήση από άλλους του μεγάλου όγκου δεδομένων που παράγονται. Παρατηρείται λοιπόν ότι οι χρήστες θυσιάζουν εκούσια ή ακούσια το απόρρητο τους για τη χρήση εφαρμογών. Τα θεμελιώδη προβλήματα ασφάλειας και απορρήτου που θα διέπουν το δίκτυο 6G θα πρέπει να μελετηθούν περαιτέρω με στόχο την προσπάθεια επίλυσης τους ώστε να μην υπάρχει έλλειψη εμπιστοσύνης, ιδιωτικότητας και ασφάλειας στα δίκτυα έκτης γενιάς.

5.1. Τεχνητή νοημοσύνη – Artificial Intelligence

Η τεχνητή νοημοσύνη, η οποία φάνταζε κάτι απόκοσμο και η θέση της ήταν μόνο στα σενάρια επιστημονικής φαντασίας, πλέον αποτελεί ένα σημαντικό εργαλείο στα χέρια του ανθρώπου. Ο άνθρωπος βρίσκεται στο κατώφλι μιας νέας εποχής στην οποία η τεχνητή νοημοσύνη θα διαδραματίσει σημαντικό ρολό σε ποικίλους κλάδους. Μέχρι στιγμής τα συστήματα τεχνητής νοημοσύνης έχουν εφαρμοστεί στον κλάδο της ιατρικής, της οικονομίας και της ασφάλισης παρέχοντας νέες υπηρεσίες και προϊόντα τα οποία θα διευκολύνουν την καθημερινότητα των ανθρώπων και θα είναι διαθέσιμα και προσβάσιμα σε όλους. Στον τομέα της τεχνητή νοημοσύνης τα τελευταία χρόνια έχουν συντελεστεί ραγδαίες τεχνολογικές εξελίξεις οι οποίες βοήθησαν και αναμένεται να βοηθήσουν την ανθρωπότητα στη βελτίωση του βιοτικού επίπεδου και των συνθήκων διαβίωσης. Η τεχνητή νοημοσύνη αναμένεται να αποτελέσει το βασικό θεμέλιο λίθο των δικτύων έκτης γενιάς για την παροχή καινοτόμων εφαρμογών και την πυξίδα που θα οδηγήσει την ανθρωπότητα σε μια νέα εποχή. Η μηχανική μάθηση, η αυτοματοποιημένη λήψη αποφάσεων, τα big data, το cloud computing και το IoT αποτελούν βασικές τεχνολογίες οι οποίες σε συνδυασμό με την τεχνητή νοημοσύνη θα οδηγήσουν στην πρόοδο. Όμως η συνεχής εξέλιξη την τεχνητή νοημοσύνης θα πρέπει να συνοδεύεται από μελέτη και κατανόηση του αυξανόμενου αριθμού νομικών ζητημάτων και ζητημάτων ασφάλειας που προκαλεί. Το αντίκτυπο που θα έχει η εξέλιξη της τεχνητή νοημοσύνη στο απόρρητο των ανθρώπων αναμένεται να αποτελέσει ένα πλήγμα για την ιδιωτική τους ζωή, καθώς μπορεί να αποτελέσει το μέσο για την παραβίαση της ιδιωτικής τους ζωής και της ασφαλείας τους.

Στα δίκτυα έκτης γενιάς οι ποικίλες εφαρμογές που θα μπορεί να εκμεταλλευτεί ο άνθρωπος θα διαθέτουν αλγόριθμους τεχνητής νοημοσύνης. Οι διάφορες συσκευές συλλέγουν και επεξεργάζονται ασταμάτητα τα προσωπικά δεδομένα των ανθρώπων και συχνά οι άνθρωποι δεν το συνειδητοποιούν. Η παραπάνω κατάσταση έχει οδηγήσει στη δημιουργία πλήθους νομικών και ηθικών ζητημάτων. Τα κυριότερα ερωτήματα που τίθενται είναι:

- Το ήδη υπάρχον πλαίσιο προστασίας προσωπικών δεδομένων επαρκεί ώστε να γίνεται ορθή συλλογή, επεξεργασία, αποθήκευση και χρήση των προσωπικών δεδομένων;
- Σε πιο βαθμό η τεχνητή νοημοσύνη θα επηρεάζει τα βασικά δικαιώματα και τις ελευθερίες ενός ανθρώπου;
- Αξίζει να σημειωθεί ότι για να λειτουργήσει με ακρίβεια και αποτελεσματικότητα ένας αλγόριθμος τεχνητής νοημοσύνης απαιτεί υπέρογκη ποσότητα προσωπικών δεδομένων για εκπαίδευση του.

Η προστασία των δεδομένων στην Ευρώπη ξεκίνησε με την οδηγία 95/46/ΕΚ. Όμως η ταχεία εξέλιξη της τεχνολογίας και η ψηφιοποίηση της κοινωνίας οδήγησαν στη δημιουργία νέων ερωτημάτων σχετικά με την προστασία των δεδομένων. Την ενίσχυση της προστασίας των προσωπικών δεδομένων στις νέες τεχνολογίες έφερε

ο ΓΚΠΔ. Ειδικότερα ο ΓΚΠΔ επιδιώκει τη διασφάλιση των θεμελιωδών δικαιωμάτων και των ελευθεριών των χρηστών των συστημάτων τεχνητής νοημοσύνης. Ο Κανονισμός δίνει έμφαση στις επιπτώσεις της τεχνητής νοημοσύνης στα ανθρώπινα δικαιώματα και όχι στην τεχνολογική υποδομή. Για τον παραπάνω λόγο οι νομοθέτες επέλεξαν να μην ενσωματώσουν συγκεκριμένη τεχνολογική ορολογία στον κανονισμό. Με αυτόν τον τρόπο εξασφαλίζουν ότι ο Κανονισμός είναι ευέλικτος και θα μπορεί να ακολουθήσει και να συμβαδίσει με τις τεχνολογικές αλλαγές και να μην έχει εφαρμογή μόνο σε συγκεκριμένες τεχνολογίες. Η εφαρμογή του είναι απαραίτητο να γίνεται κατά το στάδιο της συλλογής και επεξεργασίας των δεδομένων από τους αλγόριθμους.

Τα συστήματα τεχνητής νοημοσύνης λειτουργούν με μεγαλύτερη ακρίβεια και βελτιώνουν την απόδοση τους όταν συλλέγουν και επεξεργάζονται όσο το δυνατόν περισσότερα προσωπικά δεδομένα. Μέσω της συλλογής και επεξεργασίας των προσωπικών δεδομένων του χρήστη μπορούν να ανταποκριθούν με μεγαλύτερη ακρίβεια στα ενδιαφέροντα του και να ενισχύσουν την «γνώση» τους. Η υπέρογκη συλλογή προσωπικών δεδομένων όμως δημιουργεί ανησυχίες σχετικά με την μη εφαρμογή των βασικών αρχών της νόμιμης επεξεργασίας (άρθρο 5), καθώς η προστασία των προσωπικών δεδομένων των χρηστών και της ιδιωτικότητας γίνονται όλο και πιο δύσκολα επιτεύξιμοι στόχοι με την εξέλιξη της τεχνολογίας.

Σύμφωνα με το άρθρο 7 του ΓΚΠΔ σχετικά με τις προϋποθέσεις συγκατάθεσης και το άρθρο 8 του ΓΚΠΔ το οποίο αναφέρεται στις προϋποθέσεις για την συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας της πληροφορίας για να πραγματοποιηθεί η συλλογή και επεξεργασία των δεδομένων η συγκατάθεση του υποκείμενου των δεδομένων θα πρέπει να ικανοποιεί ορισμένα κριτήρια για να είναι νόμιμη. Αρχικά ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να γνωστοποιήσει την συγκατάθεση στο υποκείμενο των δεδομένων σε γλώσσα σαφή, απλή και κατανοητή (άρθρο 7 και 8). Όμως στις περισσότερες περιπτώσεις η συλλογή και ανάλυση των δεδομένων πραγματοποιείται αυτόματα χωρίς τη συγκατάθεση του υποκείμενου των δεδομένων. Οι συσκευές δεν ειδοποιούν το χρήστη όταν αρχίζει η συλλογή των δεδομένων του οδηγώντας σε καταπάτηση του δικαιώματος της συγκατάθεσης. Επιπλέον στα περισσότερα προϊόντα τεχνητής νοημοσύνης δεν έχει διευκρινιστεί αν ο χρήστης θα έχει τη δυνατότητα να πραγματοποιήσει ανάκληση της συγκατάθεσης τους.

Μετά τη συλλογή των δεδομένων το υποκείμενο τους αγνοεί τον τρόπο με τον οποίο θα αποτελέσουν αντικείμενο επεξεργασίας, καθώς και που θα πραγματοποιηθεί η επεξεργασία τους. Τα υποκείμενα των δεδομένων θα πρέπει να γνωρίζουν πως επεξεργάζονται τα δεδομένα τους τα συστήματα τεχνητής νοημοσύνης ανεξάρτητα τοποθεσίας. Οι διατάξεις του ΓΚΠΔ ισχύουν κατά την επεξεργασία των προσωπικών δεδομένων ανεξάρτητα αν η επεξεργασία τους πραγματοποιείται εντός ή εκτός της ΕΕ.

Τα συστήματα τεχνητής νοημοσύνης συλλέγουν δεδομένα προκειμένου να ανταποκρίνονται αποτελεσματικά στις ανάγκες των χρηστών τους. Όμως όπως είναι φυσικό έπειτα από κάποιο χρονικό διάστημα ο χρήστης μπορεί να επιθυμεί τα δεδομένα του να τροποποιηθούν (άρθρο 16) ακόμη και να διαγραφούν (άρθρο 17), καθώς μπορεί να μην τον αντιπροσωπεύουν. Δεν είναι γνωστό όμως αν θα μπορεί να πραγματοποιηθεί και διαγραφή/τροποποίηση των ήδη συλλεγμένων δεδομένων. Σύμφωνα με τον ΓΚΠΔ η διαγραφή και η τροποποίηση δεδομένων αποτελούν δικαίωμα του υποκείμενου των δεδομένων. Όμως καθώς η τεχνητή νοημοσύνης είναι ένα εξελισσόμενο πεδίο χωρίς κάποια συγκεκριμένη νομοθεσία για την προστασία των προσωπικών δεδομένων, οι εταιρείες που αναπτύσσουν υπηρεσίες και προϊόντα τα οποία διαθέτουν τεχνητή νοημοσύνη επιλέγουν να μη συμμορφώνονται με τον ΓΚΠΔ. Οπότε ο χρήστης δεν έχει τη δυνατότητα για οριστική διαγραφή των δεδομένων του οδηγώντας σε παραβίαση των δικαιωμάτων του.

Με τη βοήθεια της μηχανικής μάθηση είναι δυνατή η εξαγωγή μοτίβων από τα δεδομένα με αποτέλεσμα την απόκτηση γνώσης για ένα άτομο και τη δημιουργία προφίλ [86]. Μέσω του προφίλ τα προϊόντα της τεχνητής νοημοσύνης μπορούν να λάβουν αποφάσεις για το υποκείμενο του προφίλ βασιζόμενα στις πληροφορίες που περιέχει. Το προφίλ αποτελεί ένα σημαντικό νομικό ζήτημα, καθώς στις περισσότερες περιπτώσεις οι χρήστες δεν έχουν δώσει τη συγκατάθεση τους για να χρησιμοποιηθούν τα δεδομένα τους για την κατάρτιση προφίλ. Επιπλέον η μηχανική μάθηση θα μπορούσε να κατασκευαστεί και να εκπαιδευτεί με τρόπο κατά τον οποίο δεν θα λειτουργούσε με αμερόληπτο τρόπο και θα ακολουθούσε τα κριτήρια κάποιου ανθρώπου με αποτέλεσμα τη δημιουργία διακρίσεων σε βάρος ορισμένων ανθρώπων ή/και ομάδων ανθρώπων.

Οι ανησυχίες σχετικά με την αυξανόμενη παρέμβαση της τεχνητής νοημοσύνης στο απόρρητο των ανθρώπων οδηγεί σε ζητήματα σχετικά με τη θέσπιση ορίων στην παρέμβαση της ιδιωτικής τους ζωής. Στα έξυπνα περιβάλλοντα για παράδειγμα δημιουργούνται μεγάλα σύνολα δεδομένων και καθώς αυξάνονται οι έξυπνες συσκευές ο χρήστης μπορεί να μη συνειδητοποιεί ότι τα δεδομένα του συλλέγονται ανεξέλεγκτα από έξυπνες συσκευές. Επίσης τα αυτόνομα οχήματα θα μπορούν να μεταφέρουν πληροφορίες σχετικά με τη θέση του χρήστη ανά πάσα στιγμή και τα μέρη τα οποία έχει ήδη επισκεφτεί ή προγραμματίζει να επισκεφτεί οδηγώντας σε καταγραφή και παρακολούθηση του χρήστη και γνώση του τι κάνει.

Όπως είναι γνωστό τα συστήματα τεχνητής νοημοσύνης λειτουργούν με βάσει τις πληροφορίες που έχουν ενσωματωθεί στο λογισμικό τους και με την επεξεργασία δεδομένων. Μέσω της επεξεργασίας αποκτούν “εμπειρία”, η οποία τους επιτρέπει να εκτελούν αποτελεσματικά τις εργασίες που τους έχουν ανατεθεί. Το κύριο νομικό ζήτημα που δημιουργείται είναι αν τα προϊόντα τεχνητής νοημοσύνης θα πρέπει να αντιμετωπίζονται ως εργαλεία ή αν θα πρέπει να αρχίσουν να έχουν αντίστοιχες υποχρεώσεις και κυρώσεις όπως οι άνθρωποι; Οι

νέες τεχνολογικές εξελίξεις στον τομέα της τεχνητής νοημοσύνης θα επισημάνουν ορισμένα άλυτα ζητήματα.

Επιπλέον τα συστήματα τεχνητής νοημοσύνης χαρακτηρίζονται με έλλειψη διαφάνειας, καθώς δεν είναι εύκολα αντιληπτός ο τρόπος με τον οποίο οδηγούνται στη λήψη μιας απόφασης [87]. Αν οι αλγόριθμοι τεχνητής νοημοσύνης που λαμβάνουν μια απόφαση δεν βασίζονται σε σωστά και λογικά κριτήρια τότε είναι λογικό να οδηγήσουν σε διακρίσεις. Ακόμη η ύπαρξη προκατάληψης στην αυτοματοποιημένη λήψη αποφάσεων λόγω εκπαίδευσης της μηχανικής μάθησης με σύνολο δεδομένων το οποίο δεν περιέχει αντικειμενικά δεδομένα οδηγεί στη δημιουργία αναξιόπιστης απόφασης.

Το ζήτημα της νομικής ευθύνης αποτελεί ένα από τα σημαντικότερα διλλήματα στα συστήματα τεχνητής νοημοσύνης, καθώς υπάρχει ένα έλλειμα νομοθετικών κανόνων για τον καταλογισμό ευθύνης και χρήζει άμεσης νομοθετικής ρύθμισης. Ειδικότερα είναι αρκετά δύσκολο να προσδιοριστεί εκ των προτέρων πια θα είναι η συμπεριφορά ενός συστήματος τεχνητής νοημοσύνης σε περίπτωση δυσλειτουργίας τους. Οπότε κρίνεται απαραίτητη η δημιουργία ενός πλαισίου που θα καλύπτει πλήρως το φάσμα των κινδύνων που μπορούν να δημιουργήσουν οι νέες τεχνολογικές εξελίξεις. Θα πρέπει να διευκρινιστεί αν ο κατασκευαστής του αλγορίθμου θα είναι υπεύθυνος και για τις μετέπειτα πράξεις του αλγορίθμου, καθώς δεν είναι σαφές αν ένα άτομο θα μπορούσε να προβλέψει την πορεία των αποτελεσμάτων του αλγορίθμου.

Τα προϊόντα και υπηρεσίες της τεχνητής νοημοσύνης έχουν τη δυνατότητα να προσαρμόζονται στον εκάστοτε χρήστη και να ανταποκρίνονται στις απαιτήσεις τους και να τους προσφέρουν ότι τους αρέσει μέσω της ανάλυσης των δεδομένων του που βρίσκονται διαθέσιμα παντού στο διαδίκτυο. Η παραπάνω δυνατότητα της τεχνητής νοημοσύνης διαθέτει πολλά οφέλη και διευκολύνει την καθημερινή ζωή των ανθρώπων. Όμως όπως κάθε τεχνολογικό επίτευγμα η ύπαρξη νομικών ζητημάτων δημιουργεί ανησυχίες στους χρήστες τους. Το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τις κατηγορίες των δεδομένων που συλλέγονται, καθώς και τον σκοπό για τον οποίο θα πραγματοποιηθεί η επεξεργασία τους. Οπότε αποτελεί επιτακτική η ανάγκη κατά την ανάπτυξη εφαρμογών τεχνητής νοημοσύνης να διασφαλίζεται η προστασία των θεμελιωδών δικαιωμάτων των ατόμων. Επιπλέον θα πρέπει να μελετηθεί η επίδραση που θα ασκεί η τεχνητή νοημοσύνη στην εξέλιξη της νομικής επιστήμης.

5.2. Αυτοματοποιημένη Λήψη Αποφάσεων και Κατάρτιση Προφίλ - Automated Decision Making and Profiling

Στη σύγχρονη τεχνολογικά εξελιγμένη εποχή στόχος του ΓΚΠΔ είναι να διευρύνει την προστασία των προσωπικών δεδομένων σε τεχνολογίες όπως το IoT, big data, cloud computing, τεχνητή νοημοσύνη κλπ. Καθώς τα δίκτυα έκτης γενιάς θα εκμεταλλεύονται σε μεγάλο βαθμό τις προαναφερθέντες τεχνολογίες για την

παροχή νεών, καινοτόμων και εξιδεικευμένων υπηρεσιών στους χρήστες τους, κατανοούμε ότι θα υπάρξουν αρκετά νομικά ζητήματα. Η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ αναμένεται να αποτελούν συστατικά στοιχεία των δικτύων 6G, καθώς αυξανόμενες δυνατότητες τους είναι απαραίτητες για τη λειτουργία πολλών τεχνολογιών.

Η αυτοματοποιημένη λήψη αποφάσεων και η κατάρτιση προφίλ δεν αποτελούν χωριστές δραστηριότητες. Δηλαδή αυτοματοποιημένες αποφάσεις μπορούν να λαμβάνονται με ή χωρίς την κατάρτιση προφίλ και η κατάρτιση προφίλ μπορεί να πραγματοποιείται χωρίς την λήψη αυτοματοποιημένων αποφάσεων [88]. Η λειτουργία της αυτοματοποιημένης λήψης αποφάσεων πραγματοποιείται μέσω αλγορίθμου ή συστημάτων τεχνητής νοημοσύνης [89]. Ο αλγόριθμος λειτουργεί με πλήρως ή μερικώς αυτοματοποιημένες αποφάσεις και περιλαμβάνει τις διαδικασίες υπολογισμού, επεξεργασίας, αξιολόγησης δεδομένων και λήψης αποφάσεων. Η τεχνητή νοημοσύνη περιλαμβάνει μηχανική μάθηση και απαιτεί παραγωγή, συλλογή και επεξεργασία μεγάλης ποσότητας δεδομένων.

Όπως έχει ήδη αναφερθεί στην ενότητα 2 η τεχνητή νοημοσύνη και το διαδίκτυο των πράγματων θα διαδραματίσουν θεμελιώδη ρόλο σε πολλούς τομείς, όπως η υγεία, η μετακίνηση, η βιομηχανία, έξυπνα σπίτια και πόλεις κλπ. Όμως για να είναι αξιόπιστες και αποδοτικές οι εφαρμογές που θα φέρουν τα δίκτυα έκτης γενιάς θα πρέπει να διαθέτουν μεγάλο πλήθος και ποικιλία αισθητήρων για συλλογή δεδομένων. Ο αριθμός προσωπικών δεδομένων που θα συλλέγονται και διαμοιράζονται στο διαδίκτυο των πραγμάτων ενισχύει τις ανησυχίες των ανθρώπων για παραβίαση της ιδιωτικής τους ζωής.

Σύμφωνα με το άρθρο 22 του ΓΚΠΔ κάθε άτομο έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας [90]. Επειδή οι νέες καινοτόμες εφαρμογές που θα παρέχει το δίκτυο 6G θα χρησιμοποιούν την αυτοματοποιημένη λήψη αποφάσεων, δημιουργούνται αρκετά νομικά ζητήματα. Αρχικά το εκθετικά αυξανόμενο πλήθος των αισθητήρων που θα χρησιμοποιείται στα δίκτυα έκτης γενιάς για να συλλέγει τα δεδομένα των πολιτών δεν ενδέχεται να έχει περιορισμούς στη συλλογή δεδομένων, οδηγώντας στη συλλογή προσωπικών δεδομένων και στην παραβίαση της προσωπικής ζωής των πολιτών. Καθώς δεν θα υπάρχει ενημέρωση των πολιτών κάθε φορά που ένας αισθητήρας συλλέγει τα δεδομένα τους παραβιάζεται το δικαίωμα στην ενημέρωση (άρθρο 13,14) του ΓΚΠΔ. Επίσης για να είναι νόμιμη η επεξεργασία δεδομένων το υποκείμενο θα πρέπει να έχει δώσει την συγκατάθεση του (άρθρο 6), όμως αρκετές εφαρμογές των δικτυών 6G αναμένεται να επεξεργάζονται τα δεδομένα του υποκειμένου, ακόμη και τα δεδομένα προσωπικού χαρακτήρα χωρίς να έχει ζητηθεί προηγουμένως η συγκατάθεση από το υποκείμενο των δεδομένων. Επιπλέον υπάρχει ο κίνδυνος διαρροής των δεδομένων των χρηστών, καθώς και η εκμετάλλευση τους για μη εξουσιοδοτημένη χρήση οδηγώντας σε παραβίαση του απορρήτου των χρηστών.

5.3. Αυτόνομα οχήματα – Autonomous Driving

Αδιαμφισβήτητα η νέα εποχή στην οποία υπόσχονται να οδηγήσουν τα δίκτυα έκτης γενιάς θα συνοδεύεται από μοναδικά τεχνολογικά επιτεύγματα. Η εξέλιξη της τεχνολογίας σε συνδυασμό με την ανάπτυξη της πληροφορικής έθεσαν τα θεμέλια για τη δημιουργία νέων τεχνολογιών οι οποίες εισβάλλουν στην καθημερινότητα όλων μας. Η τεχνητή νοημοσύνη, η μηχανική μάθηση και η επιστήμη των δεδομένων συνέβαλαν για την εκπλήρωση ενός σεναρίου το οποίο αποτελούσε μέχρι πρώτιστος επιστημονική φαντασία, τα αυτόνομα οχήματα. Τόσο στην Αμερική όσο και στην Ευρώπη κυκλοφορούν ήδη στο δρόμο οχήματα χωρίς την παρουσία οδηγού στην καμπίνα τους. Υπολογίζεται ότι το 95% περίπου των τροχαίων ατυχημάτων στην ΕΕ προξενεύονται από κάποιο ανθρώπινο σφάλμα με αποτέλεσμα να χάνονται ανθρώπινες ζωές [91]. Τα αυτόνομα οχήματα υπόσχονται να αυξήσουν την οδική ασφάλεια και να μειώσουν σημαντικά των αριθμό των ατυχημάτων [92].

Τα αυτόνομα οχήματα, καθώς είναι εξοπλισμένα με νέες και καινοτόμες τεχνολογίες, δεν έχει εξεταστεί και θεσμοθετηθεί ακόμη ειδική νομοθεσία σχετικά με τη χρήση και κατασκευή αυτόνομων οχημάτων. Ένα από τα σημαντικότερα νομικά ζητήματα που περικλείουν τα αυτόνομα οχήματα είναι το ζήτημα της ευθύνης σε περίπτωση σύγκρουσης του αυτόνομου οχήματος με άλλο όχημα, με έμβιο όν αλλά και η πρόκληση υλικών φθορών [93]. Όταν ο οδηγός του οχήματος μεταβιβάζει τα καθήκοντα οδήγησης σε ένα αυτόνομο σύστημα κατανοείται η ανάγκη για την προσαρμογή των ευρωπαϊκών νομοθετικών διατάξεων περί ευθύνης που καθορίζουν ποιος είναι υπεύθυνος σε περίπτωση ατυχήματος. Το κυριότερο ζήτημα που πρέπει να καθοριστεί είναι αν ο κατασκευαστή ή ο οδηγός του αυτόνομου οχήματος είναι φέρει την ευθύνη σε περίπτωση ατυχήματος. Αν και η αυτονομία των οχημάτων έχει εξελιχθεί σε μεγάλο βαθμό, σε ορισμένες περιπτώσεις η σύγκρουση του είναι αναπότρεπτη.

Το trolley problem αποτελεί ένα πείραμα το οποίο περιλαμβάνει ηθικά διλήμματα σχετικά με το αν μπορεί να θυσιαστεί ένα άτομο για να σωθούν περισσότερα άτομα [94]. Το trolley problem βρίσκει εφαρμογή στην αυτόνομη οδήγηση, καθώς κατά το σχεδιασμό ενός αυτόνομου οχήματος μπορεί να απαιτείται ο προγραμματισμός του για να επιλέξει ποιον ή τι θα χτυπήσει όταν βρεθεί σε ένα δίλημμα. Για παράδειγμα αν ένας άνθρωπο πηδήξει μπροστά στο όχημα, τότε το όχημα θα χτυπήσει τον άνθρωπο ή θα επιλέξει να βγει από το δρόμο με κίνδυνο να τραυματίσει ή και να σκοτώσει τους επιβαίνοντες του; Τι θα συμβεί αν στη θέση του ανθρώπου βρισκόταν ένα άλλο όχημα, ένα ζώο ή ένας ποδηλάτης; Αν και τα αυτόνομα οχήματα λόγω των τεχνολογιών που διαθέτουν (αισθητήρες, αλγορίθμους, κλπ.) θεωρείται ότι θα παίρνουν ποιο “σωστές” αποφάσεις σε ένα τέτοιο δίλημμα, το δικαστήριο υπάρχει η περίπτωση να τις αμφισβητήσει. Οπότε κρίνεται αναγκαία η θεσμοθέτηση ενός κοινού νομικού πλαισίου για την αυτόνομη οδήγηση το οποίο θα έχει παγκόσμια ισχύ.

Κάθε αυτόνομο όχημα είναι εξοπλισμένο με μεγάλο πλήθος αισθητήρων. Οι αισθητήρες συλλέγουν και επεξεργάζονται τα δεδομένα σε πραγματικό χρόνο. Καθώς το πλήθος των δεδομένων που συλλέγει το όχημα είναι υπέρογκο τα δεδομένα των ανθρώπων και ειδικότερα τα προσωπικά δεδομένα κινδυνεύουν να συλλέγονται και να υπόκεινται σε επεξεργασία χωρίς τη συγκατάθεση τους, οδηγώντας σε παραβίαση του απορρήτου τους. Τα αυτόνομα οχήματα καταγράφουν πληροφορίες από το γύρω περιβάλλον τους με σκοπό τη λήψη σωστών αποφάσεων για τη λειτουργία και την κίνηση του οχήματος. Στις πληροφορίες που συλλέγουν οι αισθητήρες του οχήματος υπάρχει μεγάλη πιθανότητα να συλλέγονται ευαίσθητα δεδομένα ανθρώπων που κινούνται κοντά στο όχημα. Τα ευαίσθητα δεδομένα τους εκτός από τη συλλογή και την επεξεργασία στην οποία υπόκεινται χωρίς τη συγκατάθεση του υποκείμενου τους, υπάρχει μεγάλος κίνδυνος να διαρρεύσουν. Παρατηρείται ότι η ασφάλεια των δεδομένων και η ιδιωτική ζωή των ανθρώπων διατρέχει μεγάλο κίνδυνο.

Η προστασία των προσωπικών δεδομένων και η πολιτική απορρήτου δημιουργεί πολλές θέτει πέντε βασικά ερωτήματα σχετικά με τα δεδομένα που συλλέγουν τα αυτόνομα οχήματα, τα οποία χρήζουν επιτακτικής απάντησης.

1. Ποιος πρέπει να κατέχει ή να ελέγχει τα δεδομένα του συστήματος;
2. Ποιοι τύποι δεδομένων θα αποθηκεύονται;
3. Με ποιον θα μοιραστούν αυτά τα δεδομένα;
4. Με ποιον τρόπο θα διαθετούν αυτά τα δεδομένα;
5. Για ποιο λόγο θα χρησιμοποιηθούν τα δεδομένα;

Άξιο αναφοράς αποτελεί το γεγονός ότι στον κλάδο της αυτοματοποίησης ισχύουν οι ίδιοι κανόνες προστασίας δεδομένων της ΕΕ. Όμως χωρίς τις σωστές διασφαλίσεις, τα δεδομένα που συλλέγει ένα όχημα μπορεί αν χρησιμοποιηθούν με μη επιτρεπτό τρόπο, όπως υπηρεσίες επιβολής του νόμου με σκοπό τη συνεχή παρακολούθηση και από ασφαλιστικές εταιρίες με σκοπό την ταξινόμηση ενός πιθανού πελάτη ως κατάλληλο ή ακατάλληλο για ασφάλιση ανάλογα με τις περιπτώσεις στις οποίες έχει εμπλακεί σε τροχαίο, σύγκρουση, οδήγηση υπό την επήρεια αλκοόλ κλπ.

Ωστόσο τα αυτόνομα οχήματα δεν αποτελούν μια άτρωτη τεχνολογία. Οι κυβενοεπιθέσεις από χάκερ, τρομοκρατικές οργανώσεις και εχθρικά κράτη αποτελούν ένα σημαντικό ζήτημα για το οποίο θα πρέπει να ληφθούν τα κατάλληλα μέτρα, τα οποία θα εγγυόνται την ασφάλεια και την προστασία των αυτόνομων οχημάτων στον κυβερνοχώρο [95]. Λόγω των νέων τεχνολογιών που θα αξιοποιούν τα αυτόνομα οχήματα και του διαδικτύου στο οποία θα συνεχώς είναι συνδεδεμένα ο κίνδυνος κυβερνοεπιθέσεων αλλά και κλοπής προσωπικών στοιχείων αποτελούν ζητήματα τα οποία θέτουν σε κίνδυνο την ασφάλεια και ιδιωτικότητα του οχήματος, καθώς και των επιβαινόντων του. Ειδικότερα όταν ένα τρίτο άτομο αναλάβει τον

έλεγχο του αυτόνομου οχήματος μπορεί να προκαλέσει ατυχήματα και προβλήματα στην κυκλοφορία.

Επομένως τα δίκτυα έκτης γενιάς θα επιτρέψουν την περαιτέρω καινοτομία στον τομέα της αυτόνομης οδήγησης. Όμως κάθε τεχνολογική εξέλιξη συνοδεύεται από πληθώρα νομικών ζητημάτων. Έτσι και τα αυτόνομα οχήματα διέπονται από αρκετά νομικά ζητήματα καθώς ενσωματώνουν νέες τεχνολογίες οι οποίες ενδέχεται να μην έχουν προβλεφθεί από κάποια ειδική νομοθεσία. Οπότε παρατηρείται ότι για την σωματική ασφάλεια των ανθρώπων αλλά και την ασφάλεια των δεδομένων τους θα πρέπει να υπάρξει μελέτη και δημιουργία ενός νομικού πλαισίου που θα ρυθμίζει την αστική ευθύνη των αυτόνομων οχημάτων.

5.4. Ψηφιακό Δίδυμο - Digital twin body

Τα ψηφιακά δίδυμα αποτελούν μια αναδυόμενη τεχνολογία η οποία βρίσκει εφαρμογή στον τομέα της υγείας, της βιομηχανίας και των έξυπνων πόλεων. Τα digital twin επιτρέπουν σε πραγματικό χρόνο τη γρήγορη ανάλυση και λήψη αποφάσεων μέσω ακριβών αναλυτικών στοιχείων. Η εξέλιξη της τεχνολογίας και η αύξηση των συσκευών IoT ενισχύουν μια μελλοντική εφαρμογή, το ψηφιακό δίδυμο ενός ανθρώπου. Τα πλεονεκτήματα και οι δυνατότητες που θα παρέχει το ψηφιακό δίδυμο ενός ανθρώπου στον τομέα της υγείας είναι εξαιρετικά σημαντικά, καθώς θα δίνει τη δυνατότητα για ανάλυση του ανθρώπινου σώματος σε πραγματικό χρόνο. Παρόλο που το ψηφιακό δίδυμο αποτελεί μια ανέφικτη τεχνολογία η οποία γίνεται εφικτή στα δίκτυα έκτης γενιάς με τη βοήθεια της τεχνητής νοημοσύνης και του IoT, υπάρχουν αρκετά ζητήματα σχετικά με την ασφάλεια και το απόρρητο, τα οποία χρήζουν επιτακτικής μελέτης και επίλυσης [96].

Όπως οι περισσότερες νέες τεχνολογίες έτσι και για το ψηφιακό δίδυμο ο ΓΚΠΔ εγγυάται την ασφάλεια των δεδομένων προσωπικού χαρακτήρα τα οποία συλλέγει και επεξεργάζεται ο ψηφιακός δίδυμος. Όμως οι πάροχοι των υπηρεσιών του ψηφιακού διδύμου οφείλουν να συμμορφώνονται με τον ΓΚΠΔ ώστε να ελαχιστοποιηθούν οι πιθανότητες μη νόμιμης επεξεργασίας και υποκλοπής των δεδομένων του υποκείμενου των δεδομένων. Αξίζει να επισημανθεί ότι από το ψηφιακό δίδυμο προκύπτουν ορισμένα νομικά ζητήματα σχετικά με την προστασία και την ασφάλειας για τα δεδομένα τα οποία συλλέγει, επεξεργάζεται και αποθηκεύει ένα ψηφιακό δίδυμο. Τα ψηφιακά δίδυμα τα οποία βρίσκουν εφαρμογή στον τομέα της υγείας, καθώς περιέχουν τα προσωπικά δεδομένα και ειδικότερα ευαίσθητα δεδομένα ενός ανθρώπου τα οποία σχετίζονται κατά κύριο λόγο με την υγεία του κατανοείται η ανάγκη για την προστασία των δεδομένων αυτών από παράνομη επεξεργασία ή διαρροή. Ο ΓΚΠΔ διασφαλίζει την προστασία και την ασφάλεια των δεδομένων προσωπικού χαρακτήρα, όμως καθώς η τεχνολογία εξελίσσεται ο ΓΚΠΔ θα πρέπει να εξελίσσεται παράλληλα ώστε να εγγυάται την ασφάλειας των προσωπικών δεδομένων και κατά συνέπια της ιδιωτικής ζωής των ανθρώπων από τα διάφορα τεχνολογικά επιτεύγματα.

Καθώς το ψηφιακό δίδυμο αποτελεί ένα ψηφιακό αντίγραφο ενός φυσικού προσώπου, οι γιατροί και οι ερευνητές για να μελετήσουν την επίδραση που θα έχει ένα φάρμακο στο φυσικό πρόσωπο μέσω του ψηφιακού διδύμου θα πρέπει να ενσωματώσουν πλήρως στο ψηφιακό δίδυμο τα δεδομένα του φυσικού προσώπου. Αυτή η συνεχής παροχή δεδομένων στο ψηφιακό δίδυμο ενέχει πολλούς κινδύνους για παραβίαση του απορρήτου του υποκείμενου των δεδομένων, καθώς και για χρήση τους από τρίτους, όπως ασφαλιστικές εταιρίες. Επειδή το ψηφιακό δίδυμο αποτελεί μια λεπτομερή εικόνα των βιολογικών και γενετικών δεδομένων, καθώς και του τρόπου ζωής ενός φυσικού ανθρώπου υπάρχουν αρκετά προκλήσεις σχετικά με τον τρόπο συλλογής και επεξεργασίας των δεδομένων που θα περιέχει ο ψηφιακός δίδυμος.

5.5. Έξυπνα Περιβάλλοντα - Smart environments

Η ενίσχυση των smart environments με τις δυνατότητες του δικτύου 6G θα αποτελέσει ορόσημο για την έναρξη μιας νέας εποχής. Η ενσωμάτωση νέων ψηφιακών τεχνολογιών και του δικτύου έκτης γενιάς θα οδηγήσει στο μετασχηματισμό της έξυπνης πόλης και του έξυπνου σπιτιού, καθώς οι έξυπνες συσκευές θα αποκρίνονται σε πραγματικό χρόνο.

Στον τομέα των smart home οι συσκευές IoT θα κάνουν την λειτουργία του έξυπνου σπιτιού πιο αποτελεσματική και θα διευκολύνουν την καθημερινότητα των κατοίκων του σπιτιού, καθώς οι συσκευές επικοινωνούν μεταξύ τους και αλληλεπιδρούν με το χρήστη και όλες οι λειτουργίες του μπορούν να γίνουν ψηφιακά. Η ανάπτυξη του δικτύου 6G θα ανοίξει των δρόμο για νέες εφαρμογές για τα έξυπνα σπίτια οι οποίες θα έχουν τη δυνατότητα να εκμεταλλευτούν τα πλεονεκτήματα τα οποία θα παρέχει το δίκτυο έκτης γενιάς. Η εκθετική αύξηση των συσκευών IoT σε ένα σπίτι δημιουργεί ανησυχίες σχετικά με τη συνεχής παρακολούθηση των κατοίκων του, το απόρρητο των δεδομένων και την ασφάλεια στον κυβερνοχώρο καθώς ο φόβος της απώλειας ελέγχου του έξυπνου σπιτιού οξύνεται όλο και περισσότερο.

Αρχικά η μεγαλύτερη ανησυχία που εγείρει η ανάπτυξη και ενσωμάτωση όλο και περισσότερων συσκευών IoT σε μια οικία είναι η συλλογή και επεξεργασία προσωπικών δεδομένων[97]. Είναι γνωστό ότι οι συσκευές που διαθέτει ένα έξυπνο σπίτι συλλέγουν υπέρογκες ποσότητες δεδομένων τα οποία αποθηκεύονται και υπόκεινται σε επεξεργασία στο cloud. Δεδομένου ότι στα δεδομένα που συλλέγουν οι συσκευές εκτός από τη θερμοκρασία της κατοικίας περιέχονται και δεδομένα σχετικά με το πόσα άτομα μας επισκέφτηκαν ακόμα και το ποια είναι αυτά τα άτομα γίνεται κατανοητό ότι οι εταιρείες των συσκευών κατέχουν δεδομένα προσωπικού χαρακτήρα. Στις περισσότερες περιπτώσεις το υποκείμενο των δεδομένων δεν γνωρίζει πως η εταιρεία θα χρησιμοποιήσει τα δεδομένα του ακόμη και αν η επεξεργασία τους θα γίνεται με νόμιμο τρόπο και αν ικανοποιούνται οι βασικές αρχές για τη νόμιμη επεξεργασία. Η μαζική συλλογή δεδομένων από τις

συσκευές οδηγεί σε αυξανόμενη εισβολή στην ιδιωτική ζωή και παραβίαση του ιδιωτικού απορρήτου. Καθώς η εξέλιξη της τεχνολογίας γίνεται με γοργά βήματα το νομικό σύστημα δεν είναι σε θέση να καλύψει τις εξελίξεις σε κάθε τομέα της τεχνολογία με αποτελεσματικό τρόπο δίνοντας τη δυνατότητα στις συσκευές εκτός από την εκτέλεση των βασικών τους λειτουργιών να κατασκοπεύουν και τους κατοίκους της οικίας.

Όπως όλες οι συσκευές διαθέτουν κάποια κενά ασφάλειας τα οποία εκμεταλλεύονται χάκερ για την εκτέλεση επιθέσεων, έτσι και οι συσκευές που εξοπλίζουν ένα έξυπνο σπίτι δίνουν τη δυνατότητα σε κακόβουλα άτομα να αποκτήσουν πρόσβαση σε αυτές. Τα συλλεγόμενα δεδομένα σχετικά με τους κατοίκους του σπιτιού αλλά και το ίδιο το σπίτι αποτελούν ένα από τους κυριότερους στόχους των χάκερ. Μέσω των έξυπνων συσκευών έχουν τη δυνατότητα να εκτελέσουν παρακολούθηση των συνομιλιών που πραγματοποιούνται εντός του οικήματος. Επιπλέον ο ακριβής εντοπισμός της τοποθεσίας του σπιτιού μέσω παραβίασης των συσκευών εγείρει σημαντικά ζητήματα σχετικά με την ασφάλεια των κατοίκων του αλλά και την παράνομη είσοδο ενός ξένου σε αυτό, ο όποιος διαθέτει τον έλεγχο των συσκευών. Αξίζει να σημειωθεί ότι ένα σημαντικό ποσοστό συσκευών IoT δεν είναι δοκιμασμένες στις διάφορες ευπάθειες με τις οποίες μπορούν να έρθουν αντιμέτωπες.

Ένα ακόμη αξιοσημείωτο νομικό ζήτημα αποτελεί η χρήση των δεδομένων που συλλέγουν οι συσκευές του έξυπνου σπιτιού για την επιβολή του νόμου. Πιο συγκεκριμένα η χρήση των οικιακών δεδομένων και ειδικότερα των προσωπικών δεδομένων που συλλέγουν οι συσκευές σε ποινικές διώξεις παραβιάζει τα δικαιώματα του υποκείμενου των δεδομένων [98]. Σε αρκετές περιπτώσεις γίνεται λόγος ότι οι αρχές δεν θα χρειάζεται να διαθέτουν ένταλμα για να αποκτήσουν πρόσβαση και να αξιοποιήσουν τα δεδομένα του πολίτη. Το κόστος της παραπάνω ενέργειας για την ιδιωτική ζωή των ανθρώπων θα είναι σημαντικό, καθώς η προσωπική ζωή τους τίθεται σε κίνδυνο.

Οι έξυπνες πόλεις αποτελούν πλέον το μέλλον. Καθώς οι έξυπνες πόλεις εξελίσσονται το όραμα για τη συνεργασία ανθρώπου και τεχνολογίας αποτελεί το μέλλον για την ψηφιοποίηση της κοινωνίας. Χάρη στο διαδίκτυο των πραγμάτων (IoT) και το δίκτυο ασύρματων αισθητήρων (Wireless Sensor Networks) οι έξυπνες πόλεις οδηγούνται σε βελτιστοποίηση των υποδομών, διασύνδεση και καλύτερη διαχείρισης και ανάπτυξη της πόλης. Οι δημόσιες υπηρεσίες αλλά και η ποιότητα ζωής των ανθρώπων θα βελτιωθεί με την χρήση δεδομένων. Ορισμένα παραδείγματα εφαρμογών και τεχνολογιών που θα αξιοποιούν οι έξυπνες πόλεις είναι [99]:

- Τα συνδεδεμένα φανάρια τα οποία λαμβάνουν δεδομένα από αισθητήρες και αυτοκίνητα και προσαρμόζουν τον ρυθμό φωτισμού και το χρόνο που ανταποκρίνονται στην κυκλοφορία σε πραγματικό χρόνο, μειώνοντας την κυκλοφοριακή συμφόρηση.

- Τα συνδεδεμένα οχήματα μπορούν να επικοινωνούν με μετρητές στάθμευσης και σημεία φόρτισης ηλεκτρικών οχημάτων και να κατευθύνουν τους οδηγούς τους στο πλησιέστερο διαθέσιμο. Επίσης τα συνδεδεμένα οχήματα θα μπορούν να επικοινωνούν μεταξύ τους μειώνοντας τα τροχαία ατυχήματα.
- Οι έξυπνοι κάδοι απορριμμάτων στέλνουν αυτόματα δεδομένα σε εταιρείες διαχείρισης αποβλήτων και προγραμματίζουν την παραλαβή τους.

Όμως οι έξυπνες πόλεις αποτελείται από πολλές ετερογενείς μονάδες οι οποίες παράγουν, συλλέγουν, επεξεργάζονται και αναλύουν δεδομένα συνεχώς. Οπότε οι σύγχρονες πόλεις διέπονται από πληθώρα νομικών ζητημάτων λόγω της χρήσης προσωπικών δεδομένων. Παρόλο που υπάρχει συνεχής εξέλιξη στην τεχνολογία και οι οργανισμοί παρέχουν νέες εφαρμογές και υπηρεσίες στους κατοίκους των πόλεων βασική προϋπόθεση για την λειτουργία τους είναι η συνεργασία των πολιτών ώστε να παρέχουν τα δεδομένα τους στις εφαρμογές με σκοπό την ανάλυση και επεξεργασία τους. Όμως θα πρέπει να διασφαλιστεί η δίκαιη ισορροπία μεταξύ της προστασία των δεδομένων και της καινοτομίας.

Η συλλογή δεδομένων μέσω της πληθώρας αισθητήρων που είναι τοποθετημένοι σε διάφορα σημεία της πόλεις όπως φανάρια, κάδους απορριμμάτων και δρόμους αναμένεται να αποτελεί απειλή για την ιδιωτικότητα των ανθρώπων καθώς θα οδηγήσει στην δημιουργία ενός συνεχές συστήματος επιτήρησής [100]. Καθώς οι πόλεις γίνονται περισσότερο διασυνδεδεμένες τα προσωπικά δεδομένα των κατοίκων κινδυνεύουν να συλλέγονται εν αγνοία τους και δίχως τη συγκατάθεση τους.

Τα προσωπικά δεδομένα αποτελούν τη βάση για την έξυπνη πόλη. Δηλαδή αποτελούν την ευφυία-νοημοσύνη της πόλης. Μέσα από την ανάλυση των δεδομένων οι υπηρεσίες μια έξυπνης πόλης βελτιστοποιούνται. Η προστασία των προσωπικών δεδομένων είναι θεμελιώδης προϋπόθεση ώστε οι άνθρωποι να εμπιστευθούν την έξυπνη πόλη. Για αυτόν το λόγο οι εφαρμογές της έξυπνης πόλης θα πρέπει να διασφαλίζουν ότι τα προσωπικά δεδομένα συλλέγονται για συγκεκριμένους, καθορισμένους και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο με αυτούς τους σκοπούς (άρθρο 5) καθώς επίσης και να υποβάλλονται σε νόμιμη επεξεργασία (άρθρο 6). Όμως παρά τις διασφαλίσεις των εταιρειών ότι η συλλογή, επεξεργασία και ανάλυση των προσωπικών δεδομένων πραγματοποιείται σύμφωνα με τον ΓΚΠΔ συχνά τα δεδομένα υπόκεινται σε παράνομη επεξεργασία και αξιοποιούνται από μη εξουσιοδοτημένα μέρη.

Τα δεδομένα που συλλέγονται και αναλύονται στα πλαίσια μιας έξυπνης πόλης όχι μόνο μπορούν να υποκλαπούν αλλά και να χρησιμοποιηθούν για ανεπιθύμητους σκοπούς. Οι έξυπνες τεχνολογίες που ενσωματώνονται σε μια έξυπνη πόλη συχνά παραβιάζονται με αποτέλεσμα τα δεδομένα των πολιτών να κινδυνεύουν και να αξιοποιούνται από τρίτους. Οπότε τα δεδομένα των κατοίκων

μπορούν να αξιοποιηθούν για την κατάρτιση προφίλ με αποτέλεσμα ιδιωτικές εταιρείες να τα εκμεταλλεύονται ώστε να αυξήσουν τα εμπορικά τους κέρδη και επομένως δημιουργούνται θέματα παραβίασης της ιδιωτικότητας μεταξύ των πολιτών, των τεχνολογιών και των οργανισμών. Θα πρέπει λοιπόν να διασφαλιστεί η ανωνυμοποίηση των δεδομένων ώστε να μην μπορεί να εξαχθεί η ταυτότητα των ανθρώπων από αυτά όταν βρεθούν σε λάθος χέρια [101].

Ένα παράδειγμα μια έξυπνης συσκευής στην οποία μπορούν να αποκτήσουν πρόσβαση τρίτα μέρη και να παραβιάσουν την ιδιωτική ζωή των πολιτών είναι οι έξυπνοι μετρητές (smart meters). Οι έξυπνοι μετρητές είναι ηλεκτρονικές συσκευές που παρακολουθούν την κατανάλωση ρεύματος και τα επίπεδα τάσης [102]. Οι έξυπνοι μετρητές αποστέλλουν τις συλλεγόμενες πληροφορίες σε τακτά χρονικά διαστήματα στον καταναλωτή και στους προμηθευτές της ηλεκτρικής ενέργειας. Μέσω των έξυπνων μετρητών ο καταναλωτής μπορεί να ελέγχει την κατανάλωση ρεύματος και το κόστος της. Όμως το σημαντικότερο μειονέκτημα των έξυπνων μετρητών είναι ότι μέσω αυτών οι εταιρείες μπορούν να γνωρίζουν αν υπάρχει κάποιος στο σπίτι ή κάθε πότε κάποιος συχνά σηκώνεται κάποιος τη νύχτα επομένως ο κίνδυνος για την προσωπική ελευθερία είναι σημαντικός. Επιπλέον οι οργανισμοί που δημιουργούν της εφαρμογές και τις έξυπνες συσκευές θα μπορούσαν να είναι ευάλωτοι σε επιθέσεις με αποτέλεσμα στην πρόσβαση μη εξουσιοδοτημένων τρίτων μερών στα δεδομένα και ακόμη τη δημιουργία προφίλ με σκοπό τη στοχευμένη διαφήμιση και μάρκετινγκ [103]. Αξίζει να επισημανθεί ότι εάν οι χρήστες θέλουν να αναλύσουν την κατανάλωση τους οι προμηθευτές για να τους προσφέρουν εναλλακτικά και εξατομικευμένα σχέδια θα πρέπει να μπορούν να συναινέσουν για πρόσβαση στα δεδομένα τους.

Καθώς οδηγούμαστε σε μια ψηφιακή εποχή η οποία βασίζεται στα δεδομένα ο ΓΚΠΔ αποτελεί ένα τρόπο για την προστασία των προσωπικών δεδομένων από παραβιάσεις. Ο ΓΚΠΔ αποτελεί μια πρόκληση για τις έξυπνες πόλεις οι οποίες χρησιμοποιούν τα προσωπικά δεδομένα των πολιτών για να παρέχουν έξυπνες υπηρεσίες. Ο αριθμός των έξυπνων πόλεων αυξάνεται ολοένα και περισσότερο επομένως γεννούνται ερωτήματα στους πολίτες σχετικά με την ασφάλεια και προστασία των προσωπικών τους δεδομένων. Ένα γνωστό ερώτημα αποτελεί το πως οι εταιρίες που δημιουργούν και παρέχουν τις εφαρμογές για τις έξυπνες πόλεις θα εγγυηθούν την απουσία διαρροής ή παραβίασης των συστημάτων τους. Η έξυπνη πόλη θα πρέπει να εγγυάται την ασφάλεια των κατοίκων της ώστε να υπάρξει βεβαιότητα για την ασφάλεια τους.

Η τεχνητή νοημοσύνη αποτελεί τη βάση για τα δίκτυα έκτης γενιάς. Επομένως οι έξυπνες πόλεις αναμένεται να αξιοποιήσουν την τεχνητή νοημοσύνη ώστε να παρέχουν καινοτόμες υπηρεσίες σε πραγματικό χρόνο στους κατοίκους της [104]. Όμως η διαδικασία λήψης αποφάσεων που θα βρίσκεται πίσω από τις αλγοριθμικές τεχνολογίες μπορεί να διακατέχονται από στερεότυπα με αποτέλεσμα να αρνηθούν την παροχή υπηρεσιών σε συγκεκριμένα άτομα και να διαιωνίζουν διακρίσεις μεταξύ των πολιτών. Επιπλέον η λήψη αποφάσεων με βάση αυτοματοποιημένα

μέσα σύμφωνα με τον ΓΚΠΔ επιτρέπεται μόνο σε δύο περιπτώσεις, όπως έχει ήδη αναφερθεί, και επομένως οι κάτοικοι θα πρέπει να γνωρίζουν αν υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων. Παράλληλα η απόφαση που λαμβάνεται θα πρέπει να διασφαλίζει τα δικαιώματα και τις ελευθερίες των πολιτών.

Συνεπώς η ανάπτυξη καινοτομιών στις έξυπνες πόλεις μπορεί να οδηγεί σε βελτιστοποίηση των υπηρεσιών και της διασύνδεσης όμως δημιουργεί ένα μεγάλο ζήτημα σχετικά με το απόρρητο και την ιδιωτική ζωή των πολιτών. Η έξυπνη πόλη πρέπει να δημιουργήσει ένα περιβάλλον στο οποίο θα εγγυάται την ασφάλεια των δεδομένων των πολιτών ώστε να υπάρξει εμπιστοσύνη των κατοίκων στην πόλη. Ακόμη οι εταιρείες και οργανισμοί που δημιουργούν τις εφαρμογές της έξυπνης πόλης οφείλουν να ακολουθούν τον ΓΚΠΔ και να προστατεύουν τα δεδομένα των χρηστών τους.

5.6. Ηλεκτρονική Υγεία - E-Health

Η ταχεία αναβάθμιση και διείσδυση των κινητών συσκευών στην καθημερινότητα των ανθρώπων σε συνδυασμό με συνεχή εξέλιξη των δικτύων κινητών επικοινωνιών (6G) άνοιξαν των δρόμο για στην βελτίωση της υγειονομικής περίθαλψης αλλά και την εύκολη πρόσβαση σε υπηρεσίες υγείας σε πραγματικό χρόνο σε οποιοδήποτε μέρος του πλανήτη, ακόμα και στις αναπτυσσόμενες χώρες. Ειδικότερα η ψηφιοποίηση υπηρεσιών υγείας και οι δημιουργία ποικίλων φορητών συσκευών υγείας δημιουργούν ανοίγουν τον δρόμο για νέες και καινοτόμες υπηρεσίες υγείας.

Ο όρος mHealth αποτελεί υποκατηγορία του e-Health και υποδηλώνει τη χρήση κινητών συσκευών επικοινωνίας όπως smartphones, tablet και φορητών συσκευών όπως smart watches, καθώς και συσκευών που εισάγονται στο ανθρώπινο σώμα για την παρακολούθηση της υγείας ενός ατόμου [105]. Ο όρος mHealth αποτελεί υποκατηγορία του E-Health και δίνει τη δυνατότητα στον απλό πολίτη να συμμετέχει στην υγειονομική του περίθαλψη. Οι συσκευές που ανήκουν στην κατηγορία mHealth γίνονται όλο και πιο δημοφιλής και διατίθενται στο εμπόριο σε μεγάλη ποικιλία και εύρος τιμών. Οι φορητές συσκευές συλλέγουν δεδομένα σε πραγματικό χρόνο σχετικά με την υγεία του χρήστη τους όπως καρδιακός παλμός, αρτηριακή πίεση, σωματικό βάρος, ώρες άσκησης, ποιότητα ύπνου, οξυγόνο και επίπεδα γλυκόζης στο αίμα κλπ. τα οποία στη συνέχεια υποβάλλονται σε επεξεργασία ώστε να παρέχουν χρήσιμες πληροφορίες σχετικά με την υγεία του χρήση τους. Διαθέτουν αρκετά πλεονεκτήματα και το κόστος τους είναι προσιτό ώστε ο μέσος πολίτης να μπορεί κατέχει τουλάχιστον μια φορητή συσκευή υγείας. Υπάρχουν χιλιάδες εφαρμογές για την παρακολούθηση και βελτίωση της υγείας, όμως με τα ανάπτυξη των δικτύων έκτης γενιάς οι εφαρμογές αναμένετε να αυξηθούν αρκετά λόγω των πλεονεκτημάτων που θα διακατέχουν το δίκτυο 6G. Ωστόσο οι προαναφερθέντες συσκευές δημιουργούν αρκετά νομικά

ζητήματα και η ιδιωτική ζωή των χρηστών τους εκτίθεται σε κινδύνους σε αρκετές περιπτώσεις [106].

Αρχικά σκοπός των φορητών συσκευών υγείας (wearable health devices) είναι η συλλογή μεγάλων ποσοτήτων δεδομένων υγείας των χρηστών μέσω των αισθητήρων που διαθέτουν ή/και με εισαγωγή δεδομένων χειροκίνητα από των χρήστη τους. Έπειτα οι συσκευές αποστέλλουν ασύρματα τα ανεπεξέργαστα δεδομένα που συλλέγουν από τους αισθητήρες των συσκευών στους διακομιστές των παρόχων υπηρεσιών με σκοπό τα δεδομένα να αναλυθούν και να παρουσιαστούν στο χρήση τα αποτελέσματα. Ωστόσο οι χρήστες δεν έχουν γνώση για τους κινδύνους τους οποίους κρύβουν οι συσκευές αυτές. Πιο συγκεκριμένα ένα βασικό νομικό ζήτημα είναι σε ποιον ανήκουν / ποιος είναι ο ιδιοκτήτης των δεδομένων που συλλέγει η συσκευή [107]. Αν τα δεδομένα ανήκουν στο χρήστη τότε αυτός αποφασίζει για το ποιος θα έχει πρόσβαση στα δεδομένα του και αν αυτά θα μοιραστούν σε τρίτους από την εταιρεία. Όμως αυτό αποτελεί ένα σχεδόν ουτοπικό σενάριο. Στις περισσότερες περιπτώσεις μετά τη συλλογή των δεδομένων του ο χρήστης παύει να έχει “εξουσία” πάνω στα δικαιώματα του και οι εταιρείες εκμεταλλεύονται τα δεδομένα του προς όφελός τους εντείνοντας τις ανησυχίες των ανθρώπων για διακύβευση της ιδιωτικότητας τους.

Στη σύγχρονη τεχνολογικά εξελιγμένη κοινωνία τα δεδομένα και ειδικότερα τα δεδομένα υγείας αποτελούν την πιο επικερδή επιχείρηση. Οπότε οι φορητές συσκευές, οι οποίες συλλέγουν όλους τους τύπου δεδομένων του χρήστη, γεννούν αξιοσημείωτα νομικά ζητήματα. Αρχικά οι φορητές συσκευές υγείας δεν έχουν περιορισμούς στη συλλογή και επεξεργασία δεδομένων δημιουργώντας ανησυχίες σχετικά με παραβίαση της ιδιωτικής ζωής αλλά και την ασφάλεια των προσωπικών δεδομένων των χρηστών τους. Οι πληροφορίες που συλλέγουν οι συσκευές μπορούν να χρησιμοποιηθούν για την κατάρτιση ενός λεπτομερούς προφίλ για το υποκείμενο των δεδομένων. Το προφίλ θα περιέχει πληροφορίες σχετικά με τις καθημερινές δραστηριότητες και συνήθειες του χρήστης, οδηγώντας σε στοχευμένο μάρκετινγκ από εταιρίες σχετιζόμενες με αθλητικά είδη, διατροφή και γυμναστική. Οι εταιρίες θεωρούν ότι τα δεδομένα που περιέχουν τα προφίλ των χρηστών είναι ο “μαύρος χρυσός”, καθώς τους δίνει τη δυνατότητα να προβάλλουν στο χρήστη στοχευμένα προϊόντα και υπηρεσίες με βάση τόσο τις συνήθειες του αλλά και την κατάσταση της υγείας τους, ώστε να προβεί στην επιλογή τους.

Το βασικό ζήτημα που τίθεται σε αυτό το σημείο είναι αν οι χρήστες θέλουν τρίτα πρόσωπα/εταιρείες να έχουν πρόσβαση στα προσωπικά τους δεδομένα. Η χρήση με αθέμιτο τρόπο των προσωπικών δεδομένων αλλά και η διαρροή και χρήση τους από τρίτους εκτός από την κατάρτιση προφίλ με σκοπό τη χειραγώγηση του χρήστη μέσω μάρκετινγκ και την προβολή στοχευμένων διαφημίσεων οδηγεί και σε ένα ακόμη σημαντικό πρόβλημα. Οι ασφαλιστικές εταιρίες εκμεταλλευόμενες τα δεδομένα που συλλέγουν οι φορητές συσκευές υγείας μπορούν να οδηγήσουν σε επιβολή υψηλών ασφαλίστρων ακόμη και σε απώλεια της ασφαλιστικής κάλυψης. Οπότε γίνεται κατανοητό ότι οι νέες τεχνολογίες εκτός

από ριζικές αλλαγές στον κλάδο της υγείας και ενεργή συμμετοχή του ασθενή στη διαχείριση της υγείας του δημιουργούν ζητήματα τα οποία θα πρέπει να επιλυθούν. Επιπλέον οι εταιρίες και κατ' επέκταση οι συσκευές θα πρέπει να συμμορφώνονται με το νομικό πλαίσιο της ΕΕ για την προστασία των προσωπικών δεδομένων.

Η πολιτική απορρήτου αποτελεί ένα από τα μελανά σημεία των φορητών συσκευών υγείας [109]. Όταν ο χρήστης χρησιμοποιεί για πρώτη φορά μια φορητή συσκευή επιλέγει να μην προβεί στην ανάγνωση της μακροσκελούς πολιτικής απορρήτου κάτι το οποίο εν μέρη είναι κατανοητό. Όμως οι εταιρίες εκμεταλλευόμενες ακριβώς αυτή την αδυναμία του χρήστη διαθέτουν στην πολιτική των συσκευών όρους σχετικά με τη συλλογή και την επεξεργασία των δεδομένων στους οποίος ο χρήστης μπορεί να μην επέλεγε να μη δώσει τη συγκατάθεση του αν του παρουσιαζόντουσαν με απλή και κατανοητή γλώσσα, όπως σύμφωνα με τον ΓΚΠΔ υποχρεούνται να πράξουν οι εταιρείες. Επιπλέον στις περισσότερες περιπτώσεις οι εταιρείες δεν δεσμεύονται ότι θα ειδοποιήσουν τους κατόχους συσκευών τους αν αλλάξει η πολιτική απορρήτου. Την ευθύνη για τον έλεγχο αλλαγή τους απορρήτου τη μεταβιβάζουν στο χρήστη ο οποίος θα πρέπει να ελέγχει μόνος του κάθε φορά αν υπάρχει αλλαγή, με κίνδυνο να μη γνωρίζει ρεαλιστικά τι αλλαγή συνέβη.

Όπως είναι γνωστό οι φορητές συσκευές συλλέγουν προσωπικά δεδομένα, ακόμη και ευαίσθητα δεδομένα τα οποία αποκαλύπτουν πλήρως τη ζωή ενός ατόμου. Όπως είναι φυσικό ένας χρήστης έπειτα από κάποιο διάστημα μπορεί να επιθυμεί τα δεδομένα του να τροποποιηθούν (άρθρο 16) ακόμη και να διαγραφούν (άρθρο 17) από τους διακομιστές της εταιρείας ή την υποδομή cloud στην οποία αποθηκεύονται. Σύμφωνα με τον ΓΚΠΔ οι παραπάνω ενέργειες αποτελούν δικαίωμα του υποκείμενου των δεδομένων. Όμως καθώς οι φορητές συσκευές είναι ένα εξελισσόμενο πεδίο χωρίς κάποια συγκεκριμένη νομοθεσία για την προστασία των προσωπικών δεδομένων, οι εταιρείες επιλέγουν να μη συμμορφώνονται με τον ΓΚΠΔ [109]. Οπότε ο χρήστης δεν έχει τη δυνατότητα για οριστική διαγραφή των δεδομένων του από το σύστημα του παρόχου και τα δεδομένα του διατηρούνται επ΄ αόριστον οδηγώντας σε παραβίαση των δικαιωμάτων του.

Οι φορητές συσκευές αποκαλύπτουν την τοποθεσία μας. Η δυνατότητα τους να καταγράφουν τις διαδρομές μας, καθώς και την ταχύτητα μας, τα βήματα τον ρυθμό και την απόσταση που διανύουμε. Οι πληροφορίες αυτές μπορούν να θέσουν σε κίνδυνο την ασφάλεια μας. Οι περισσότερες φορητές συσκευές υγείας έχουν πρόσβαση σε δεδομένα GPS απευθείας ή μέσω συνδέσμου σε smartphone με σκοπό ο χρήστης να βλέπει την απόσταση που έχει διανύσει, σε ποιες περιοχές πέρασε κλπ. Αυτή δυνατότητα των συσκευών όμως κρύβει τους μεγαλύτερους κινδύνους. Ειδικότερα τα δεδομένα από τις δραστηριότητες του χρήστη μπορούν να συνδυαστούν με τις πληροφορίες τοποθεσίας και να οδηγήσουν σε εξακρίβωση των καθημερινών του δραστηριοτήτων με ακρίβεια ώρας και τοποθεσίας. Η παραβίαση του απορρήτου της τοποθεσίας των χρηστών των συσκευών δημιουργεί πληθώρα

νομικών ζητημάτων και μπορεί να έχει αρνητικές συνέπειες για τον χρήστη, καθώς κάθε στιγμή τρίτα άτομα θα γνωρίζουν την τοποθεσία του.

Οι χρηστές των φορητών συσκευών υγείας δεν γνωρίζουν τι συμβαίνει στα δεδομένα τους μόλις συλλεχθούν, δηλαδή με ποιον τρόπο προστατεύονται στη βάση δεδομένων ή στο cloud και πως γίνεται η επεξεργασία τους. Αυτή η κατάσταση επηρεάζει το ψηφιακό τους απόρρητο, καθώς τα προσωπικά τους δεδομένα μπορεί να παραβιαστούν από χάκερ. Τα δεδομένα μετά τη συλλογή τους θα πρέπει να κρυπτογραφούνται αμέσως και όχι αφού μεταφερθούν στο cloud ή στη βάση δεδομένων, ώστε να αποφευχθεί η παραβίαση και η κλοπή τους. Ακόμη ένα άλλο σημαντικό μέτρο για την προστασία των προσωπικών δεδομένων είναι η ανωνυμοποίηση τους. Μέσω αυτής της διαδικασίας τα δεδομένα δε μπορούν να συσχετιστούν με κάποιο συγκεκριμένο άτομο και να χρησιμοποιηθούν για σκοπούς στοχευμένου marketing. Όμως συχνά οι πάροχοι υπηρεσιών υποστηρίζουν ότι διατηρούν τα δεδομένα των χρηστών που θέλουν να διαγραφούν από την βάση δεδομένων μετατρέποντας τα σε ανωνυμοποιημένα δεδομένα ώστε να μην είναι δυνατός ο συσχετισμός τους με το χρήστη. Οι πάροχοι εκμεταλλεύονται τα ανωνυμοποιημένα δεδομένα για στατιστικούς σκοπούς, όμως όλο και πιο συχνά γίνεται λόγος για δυνατότητα συσχέτισης των ανωνυμοποιημένων δεδομένων με το υποκείμενο τους.

Παρατηρείται λοιπόν ότι παρόλο που τα δίκτυα έκτης γενιάς θα ενισχύσουν τον τομέα της υγείας με ποικίλες εφαρμογές παράλληλα θα υπάρξουν αρκετά νομικά ζητήματα. Ειδικότερα οι φορητές συσκευές υγείας επειδή διαθέτουν πληθώρα αισθητήρων και συλλέγουν προσωπικά δεδομένα αναμένεται να οδηγήσουν σε παραβίαση του απορρήτου και της ιδιωτικής ζωής των κατόχων τους. Επίσης η ανιχνευσιμότητα των ασθενών μέσω των αισθητήρων των συσκευών αποτελεί ένα σημαντικό ζήτημα καθώς μπορεί να οδηγήσει σε υπονόμευση της ελευθερίας τους. Επομένως για να υπάρξει σχέση εμπιστοσύνης μεταξύ των φορητών συσκευών υγείας και των ανθρώπων οι δημιουργοί και οι πάροχοι των συσκευών αυτών θα πρέπει να διασφαλίσουν τη νόμιμη επεξεργασία αλλά και την προστασία των συλλεγόμενων δεδομένων από την παράνομη χρήση και υποκλοπή τους.

5.7. Διαδίκτυο των Πραγμάτων - Internet of Things

Το Διαδίκτυο των Πραγμάτων αναμένεται να παρέχει πλήθος δυνατότητων στους χρήστες τους με την υποστήριξή του από τα δίκτυα έκτης γενιάς. Είναι γνωστό ότι οι συσκευές IoT έχουν οδηγήσει στο μετασχηματισμό του κόσμου και έχουν ενισχύσει διάφορους τομείς με πολλά πλεονεκτήματα, όπως έξυπνα σπίτια και έξυπνες πόλεις, υγειονομική περίθαλψή και φορητές συσκευές υγείας, αυτοματοποιημένα οχήματα κλπ. Όμως όπως και κάθε άλλη τεχνολογία έτσι και το διαδίκτυο των πραγμάτων δημιουργεί νομικά ζητήματα που σχετίζονται με τον νόμο προστασίας δεδομένων. Η ποικιλομορφία και ο όγκος των νέων συσκευών IoT

δημιουργούν αρκετά σημαντικούς κινδύνους ασφάλειας και απορρήτου λόγω της χρήσης τεχνολογιών που συχνά δεν υπόσχονται ένα αποδεκτό επίπεδο ασφάλειας. Ένας από τους βασικότερους κινδύνους στο IoT είναι η κατάρτιση προφίλ, καθώς επιτρέπει την αναγνώριση φυσικών προσώπων μέσω των προσωπικών τους πληροφοριών. Επιπλέον ο αυξανόμενος αριθμός δεδομένων που συλλέγονται από τις συσκευές IoT προκαλεί ανησυχίες σχετικά με την παραβίαση της ιδιωτικής ζωής των χρηστών. Επομένως κρίνεται αναγκαίο να κατανοηθούν οι ανησυχίες που δημιουργεί το διαδίκτυο των πραγμάτων.

Οι πέντε βασικές προκλήσεις που εντοπίζονται στις συσκευών IoT είναι [110]:

1. Τα δεδομένα που συλλέγει μια συσκευή IoT μπορούν να χρησιμοποιηθούν για την κατάρτιση προφίλ. Η δημιουργία προφίλ μπορεί να οδηγήσει σε διακρίσεις σε βάρος του χρήστη και σε αποκάλυψη πτυχών της ιδιωτικής τους ζωής.
2. Προσδιορισμός τοποθεσίας του χρήστη μέσω των συσκευών IoT.
3. Αποκάλυψη προσωπικών δεδομένων των χρηστών σε μη εξουσιοδοτημένα μέρη. Οι χρήστες στις περισσότερες περιπτώσεις δεν είναι σε θέση να ελέγξουν τα δεδομένα που συλλέγει μια συσκευή, καθώς και το που τα μεταδίδει.
4. Οι χρήστες δεν γνωρίζουν ότι τα δεδομένα τους μπορεί να συλλέγονται από κάποια συσκευή. Σε πολλές περιπτώσεις δεν υπάρχει αρχικά ενημέρωση και απουσία συγκατάθεσης για τη συλλογή των δεδομένων των χρηστών.
5. Διαφάνεια και ειλικρίνεια των συσκευών. Ο χρήστης πρέπει να γνωρίζει πότε τα δεδομένα του συλλέγονται, καθώς και σε ποιους θα κοινοποιηθούν και ποιοι θα έχουν πρόσβαση σε αυτά. Πολιτική απορρήτου να ενημερώνει τους χρήστες.

Αρχικά οι πληροφορίες που συλλέγονται από κάθε συσκευή θα μπορούσαν να συγκεντρωθούν και να οδηγήσουν στη δημιουργεί ενός προσωπικού προφίλ το οποίο θα περιείχε ευαίσθητες πληροφορίες του χρήστη των συσκευών [111]. Τα προφίλ αποτελούν στη σύγχρονη εποχή των «μαύρο χρυσό», καθώς είναι περιζήτητα από τις εταιρείες με σκοπό την προβολή στοχευμένων διαφημίσεων στους ανθρώπους και την εξαγωγή συμπερασμάτων για το υποκείμενο των δεδομένων. Σύμφωνα με τον ΓΚΠΔ το άρθρο 22 απαγορεύει την κατάρτιση προφίλ. Επομένως η ανωνυμοποίηση των δεδομένων αποτελεί μια πιθανή λύση, καθώς τα ανωνυμοποιήμενα δεδομένα δε θα μπορούσαν να αποδοθούν άμεσα ή έμμεσα στο φυσικό πρόσωπο στο οποίο ανήκουν.

Ένας ακόμη σημαντικό κίνδυνος των συσκευών IoT αποτελεί η αποκάλυψη της γεωγραφικής τοποθεσίας. Πιο συγκεκριμένα συσκευές όπως τα smartphone, smart watches κλπ. είναι πολύ εύκολο να καθορίσουν με λεπτομέρεια την

τοποθεσία μας. Επίσης η διάδοση της τοποθεσίας σε τρίτους θέτει σε κίνδυνο την ιδιωτική ζωή του χρήστη, καθώς το απόρρητο της τοποθεσίας έχει παραβιαστεί.

Έπειτα αποτελεί ευρέως αποδεκτή ανησυχία το γεγονός ότι ο όγκος των δεδομένων που συλλέγονται και μεταδίδονται μεταξύ των συσκευών και έπειτα στο διαδίκτυο είναι πολύ μεγάλος. Επειδή οι χρήστες δύσκολα ελέγχουν το είδος των δεδομένων που συλλέγεται και μεταδίδεται από συσκευή σε συσκευή η χρήση των συλλεγόμενων πληροφοριών από μη εξουσιοδοτημένα μέρη αποτελεί το μελανό σημείο του διαδικτύου των πραγμάτων. Η συλλογή μεγάλου όγκου πληροφοριών από μια συσκευή δημιουργεί κινδύνους διαρροής των προσωπικών δεδομένων των χρηστών [112]. Η προστασία των προσωπικών δεδομένων των χρηστών από μη εξουσιοδοτημένη χρήση θα πρέπει να αποτελεί ένα από τα κύρια έργα των κατασκευαστών των συσκευών. Επιπλέον τρίτα μέρη στα οποία κοινοποιούνται τα δεδομένα (αστυνομία, εργοδότες και ασφαλιστικές εταιρείας) μπορούν να χρησιμοποιήσουν τα δεδομένα για σκοπούς που δεν έχουν καθοριστεί κατά την αρχική συλλογή των δεδομένων ή/και χωρίς να υπάρχει η συγκατάθεση του χρήστη.

Ο ΓΚΠΔ έχει ως στόχο την ενίσχυση των δικαιωμάτων των χρηστών και τη συμμετοχή τους στην προστασία της ιδιωτικής τους ζωής. Ο ΓΚΠΔ θέτει κανόνες σχετικά με το σκοπό συλλογής των δεδομένων, την περίοδο διατήρησης τους, τον όγκος των δεδομένων που μπορούν να συλλεχθούν από τις συσκευές και την πληροφόρηση των χρηστών σχετικά με τη συλλογή, την επεξεργασία και τον τρόπο χρήσης των δεδομένων τους. Όμως η ποσότητα των δεδομένων που συλλέγουν οι συσκευές έχει δημιουργήσει ανησυχίες στους ανθρώπους σχετικά με τον τρόπο συλλογής και επεξεργασίας των δεδομένων τους. Επομένως είναι απαραίτητη η ευαισθητοποίηση των χρηστών σχετικά με τα δεδομένα που συλλέγουν οι συσκευές. Οι χρήστες των συσκευών θα πρέπει να λάβουν την απόφαση για συγκατάθεση/συναίνεση σχετικά με τα δεδομένα τους μετά από ενημέρωση, ώστε να ενημερωθούν για τους πιθανούς κινδύνους, καθώς και εάν πραγματοποιείται κατάρτιση προφίλ.

Επιπλέον μια σημαντική ανησυχία που δημιουργείτε είναι πως γνωρίζουμε ότι τα δεδομένα που συλλέγονται και αποστέλλονται για επεξεργασία δεν θα χαθούν, τροποποιηθούν κατά την διάρκεια της διαδικασίας. Και το αποτέλεσμα που ανακοινώνεται είναι το αναμενόμενο και σωστό αποτέλεσμα. Καθώς η ενσωμάτωση όλο και περισσότερων έξυπνων συσκευών στην καθημερινή ζωή αποτελεί μια καινούργια καθημερινότητα οι χρήστες των συσκευών συχνά δεν γνωρίζουν τον τρόπο επεξεργασίας των δεδομένων του και υπάρχει έλλειψη διαφάνειας. Επίσης τα βασικά δικαιώματα που διαθέτει το υποκείμενο των δεδομένων δηλαδή δυνατότητα διόρθωση και διαγραφής των ήδη συλλεγμένων δεδομένων στις περισσότερες περιπτώσεις δεν είναι δυνατόν να πραγματοποιηθούν με αποτέλεσμα τα δεδομένα των ανθρώπων να παραμένουν επ’ άπειρον στους διακομιστές των εταιριών που διαχειρίζονται τις συσκευές. Η διαφάνεια αποτελεί το κλειδί για να γνωρίσουν οι χρήστες ότι τα δεδομένα τους συλλέγονται και επεξεργάζονται.

Η τεχνολογία 6G θα φέρει την επανάσταση στην καινοτομία σε ποικίλους τομείς της κοινωνίας με την αξιοποίηση τους διαδικτύου των πραγμάτων όμως θα δημιουργήσει ζητήματα απορρήτου τα οποία ο άνθρωπος δεν έχει ξαναδεί. Ο γεωγραφικός εντοπισμός των ανθρώπων αλλά και η μη νόμιμη επεξεργασία και κοινοποίηση δεδομένων σε μη εξουσιοδοτημένα μέρη αποτελούν ορισμένες από τις βασικές ανησυχίες που διέπουν τις συσκευές IoT. Επομένως με την εξέλιξη των δικτύων κινητών επικοινωνιών θα πρέπει να υπάρξει ο κατάλληλος συντονισμός μεταξύ καινοτομίας και δίκαιου ώστε να μην υπάρξει παραβίαση των ελευθερίων των ατόμων αλλά και παράλληλα τεχνολογική εξέλιξη της κοινωνίας.

5.8. Επαυξημένη πραγματικότητα - Μικτή πραγματικότητα - Εικονική πραγματικότητα - Augmented reality – Mixed reality – Virtual reality

Η εξέλιξη των κινητών δικτύων επικοινωνίας οδηγεί σε ένα πλήρως ψηφιακό κόσμο στον οποίο τα δεδομένα του χρήστη σε συνδυασμό με την τεχνολογία επιτρέπουν στον χρήστη να ζήσει μοναδικές και εξατομικευμένες εμπειρίες προσαρμοσμένες στα ενδιαφέροντα του. Οι τεχνολογίες AR/MR/VR αποτελούνται από μια συλλογή αισθητήρων και οθονών τα οποία λειτουργούν σε συνδυασμό για να παρέχουν στον χρήστη τους μοναδικές εμπειρίες. Τα AR/MR/VR ανήκουν στην κατηγορία της εκτεταμένης πραγματικότητας (XR) [113]. Προκειμένου να μπορέσει ο χρήστης να ζήσει τις μοναδικές αυτές εμπειρίες οι συσκευές AR/MR/VR συλλέγουν υπέρογκες ποσότητες προσωπικών δεδομένων, τα οποία παρέχονται από τους χρήστες αλλά και δημιουργούνται από αυτούς. Για τη δημιουργία της ψευδαίσθησης εικονικών στοιχείων σε τρισδιάστατο φυσικό χώρο (AR) ή στον εικονικό κόσμο (VR) απαιτούνται ορισμένες βασικές πληροφορίες που παρέχονται από τον χρήστη ως σημείο εκκίνησης. Έπειτα μια συνεχή ροή νέων δεδομένων που δημιουργούνται όταν ο χρήστης αλληλοεπιδρά με το εικονικό περιβάλλον ανατροφοδοτεί τις τεχνολογίες AR/MR/VR. Αυτή η συνεχής ροή πληροφορίων ανατροφοδότησης μπορεί να περιλαμβάνει ευαίσθητες πληροφορίες, βιομετρικά στοιχεία και πληροφορίες σχετικά με την τοποθεσία και την κίνηση του χρήστη. Όμως χωρίς τις απαραίτητες διασφαλίσεις η ευρεία συλλογή και επεξεργασία δεδομένων του χρήστη μπορεί να εκθέσει το απόρρητο των ατόμων σε κίνδυνο.

Στην επαυξημένη πραγματικότητα ο πιο αξιοσημείωτος κίνδυνος σχετίζεται με την ιδιωτικότητα του χρήστη. Το απόρρητο ενός χρηστή κινδυνεύει επειδή οι τεχνολογίες AR μπορούν να δουν τι κάνει ο χρήστης. Η επαυξημένη πραγματικότητα συλλέγει μεγάλο όγκο πληροφορίων σχετικά με τον χρήστη και τι κάνει. Στην εικονική πραγματικότητα ο εξαιρετικά προσωπικός χαρακτήρας των συλλεχθέντων δεδομένων (βιομετρικά δεδομένα) αποτελεί ένα ζήτημα μείζονος σημασίας.

Τα σημαντικότερα ερωτήματα που η εγείρουν οι τεχνολογίες AR/MR/VR είναι [114]:

1. Εάν οι χάκερ αποκτήσουν πρόσβαση σε μια συσκευή, η πιθανή απώλεια απορρήτου είναι τεράστια.

2. Πως χρησιμοποιούν οι εταιρείες AR και προστατεύουν τις πληροφορίες που έχουν συλλέξει από τους χρήστες;
3. Πως αποθηκεύουν οι εταιρείες τα δεδομένα τοπικά στη συσκευή ή στο cloud; Εάν τα δεδομένα αποστέλλονται στο cloud κρυπτογραφούνται;
4. Οι εταιρείες AR/MR/VR κοινοποιούν τα δεδομένα των χρηστών σε τρίτους;

Οι συσκευές AR/MR/VR βασίζονται στην πολλαπλή συλλογή δεδομένων από ποικίλες πηγές με σκοπό να προσφέρουν στο χρήστη μοναδικές εμπειρίες. Οι πληροφορίες που συλλέγονται από τους χρήστες των συσκευών μπορούν να ταξινομηθούν στις παρακάτω τέσσερις κατηγορίες [115]:

- Observable: πληροφορίες για ένα άτομο που μπορούν να παρατηρήσουν και να αναπαράγουν οι τεχνολογίες AR/MR/VR καθώς και τρίτα μέρη, όπως ψηφιακά μέσα που παράγει το άτομο ή οι ψηφιακές επικοινωνίες τους.
- Observed: πληροφορίες που παρέχει ή δημιουργεί ένα άτομο, τις οποίες τρίτα μέρη μπορούν να παρατηρήσουν αλλά όχι να αναπαράγουν, όπως βιογραφικές πληροφορίες ή δεδομένα τοποθεσίας.
- Computed: οι νέες τεχνολογίες AR/MR/VR συνάγονται με χειρισμό observable και observed δεδομένων, όπως βιομετρική ταυτοποίηση ή προφίλ διαφημίσεων.
- Associated: πληροφορίες που, από μόνες τους, δεν παρέχουν περιγραφικές λεπτομέρειες για ένα άτομο, όπως όνομα χρήστη ή διεύθυνση IP.

Αξίζει να σημειωθεί ότι ανάλογα με τον τρόπο συλλογής και επεξεργασίας των πληροφορίων ορισμένες πληροφορίες θα μπορούσαν να ανήκουν σε περισσότερους από έναν τύπο δεδομένων. Για παράδειγμα ο καρδιακός ρυθμός και γενικότερα οι βασικές μετρήσεις για την υγεία και τη φυσική κατάσταση ανήκουν στην κατηγορία observed, όμως ο αριθμός των θερμίδων που καίγονται κατά τη διάρκεια μιας δραστηριότητας ανήκει στην κατηγορία των computed δεδομένων.

Οι συσκευές AR/MR/VR για να επιτρέψουν στο χρήστη να δημιουργήσει μια εικονική παρουσία είτε σε πλήρως εικονικούς χώρους που έχουν δημιουργηθεί σε VR είτε σε φυσικούς χώρους ενισχυμένους με εικονικά στοιχεία μέσω AR χρειάζονται την συλλογή ποικίλων τύπων δεδομένων. Για να προβάλλουν τα εικονικά στοιχεία ή τον εικονικό κόσμο οι εφαρμογές AR/MR/VR πρέπει να μπορούν να τοποθετήσουν και να πλοηγήσουν τον χρήστη στο φυσικό χώρο. Ειδικότερα για να εμφανίσουν τα εικονικά στοιχεία οι συσκευές επαυξημένης πραγματικότητας θα πρέπει να γνωρίζουν που βρίσκεται ο χρήστης σε σχέση με τις γεωγραφικές τοποθεσίες και τα φυσικά αντικείμενα ώστε να αποφευχθούν και τα ατυχήματα. Στο ίδιο πλαίσιο οι συσκευές και εφαρμογές εικονικής πραγματικότητας για να διασφαλίσουν την φυσική ασφάλεια του χρήστη πρέπει να γνωρίζουν το περιβάλλον γύρω του. Πληροφορίες από GPS, Inertial Measurement Unit (IMU), δεδομένα γυροσκόπιου ή επιταχυνσιόμετρου καθώς και πληροφορίες για το

περιβάλλον είναι αναγκαία για τη σωστή λειτουργιά και παράλληλα την ασφάλεια του χρήστη όταν χρησιμοποιεί εφαρμογές AR/MR/VR ώστε να γίνεται σωστός προσδιορισμός της τοποθεσίας του και κατανόηση του περιβάλλοντος [116],[117].

Με την αξιοποίηση προηγμένων λειτουργιών, όπως τεχνολογίες παρακολούθησης του βλέμματος και τεχνολογίες διεπαφής εγκεφάλου-υπολογιστή (gaze-tracking and even brain-computer interface (BCI)) που ερμηνεύουν νευρικά σήματα οι συσκευές και εφαρμογές AR/MR/VR εισάγουν νέες πρακτικές για την συλλογή δεδομένων [118]. Όμως οι συνέχειες ροές δεδομένων ενδέχεται να περιέχουν ευαίσθητες πληροφορίες τις οποίες οι συσκευές AR/MR/VR μπορούν να συνδυάσουν για να αποκαλύψουν ή να εξάγουν πρόσθετες λεπτομέρειες και συμπεράσματα για τους χρήστες τους.

Εκτός από τη συλλογή πληροφοριών σχετικά με τη θέση ενός χρήστη στο φυσικό χώρο, οι συσκευές AR/MR/VR παρακολουθούν επίσης ορισμένες κινήσεις και συλλέγουν βιομετρικά δεδομένα, προκειμένου να αναπαράγουν τις ενέργειες ενός χρήστη στον εικονικό χώρο. Τα παραπάνω συλλεγόμενα δεδομένα είναι εξαιρετικά σημαντικά για το VR καθώς ο χρήστης είναι βυθισμένος στον εικονικό κόσμος [119]. Επομένως όσο πιο ρεαλιστικός είναι ο εικονικός κόσμος τόσο πιο συναρπαστική είναι η εμπειρία για τους χρήστες. Για την δημιουργία των καθηλωτικών εμπειριών στον εικονικό κόσμο οι συσκευές συλλέγουν δεδομένα σχετικά με το χρήστη σε πραγματικό χρόνο. Οι τεχνολογίες παρακολούθησης των ματιών (eye tracking), οι οποίες χρησιμοποιούν εσωτερικές κάμερες για τη συλλογή δεδομένων, όπως όπου κοιτάζει ένας χρήστης, αλλαγές στο μέγεθος της κόρης του ματιού τους και εάν τα μάτια τους είναι ανοιχτά ή κλειστά, μπορούν να χρησιμοποιηθούν για τη δημιουργία ακόμη πιο ρεαλιστικών εμπειριών[120]. Για παράδειγμα, αυτά τα δεδομένα επιτρέπουν στα προγράμματα να εμφανίζουν πιο αυθεντικά είδωλα που αντικατοπτρίζουν την πραγματική κίνηση και τις εκφράσεις των χρηστών. Επιπλέον τεχνολογίες παρακολούθησης των χεριών (finger tracking) αξιοποιούνται στις εφαρμογές εικονικής πραγματικότητας καθώς επιτρέπουν την αλληλεπίδραση με τον εικονικό κόσμο χωρίς να απαιτούνται VR controllers [121]. Ειδικότερα οι αισθητήρες συλλέγουν δεδομένα σχετικά με τη θέση, τον προσανατολισμό και την ταχύτητα των χεριών και στη συνέχεια το λογισμικό εντοπισμού χεριών χρησιμοποιεί τα παραπάνω δεδομένα ώστε να δημιουργήσει μια εικονική προσωποποίηση των χεριών σε πραγματικό χρόνο.

Οι βιογραφικές πληροφορίες που παρέχονται από τον χρήστη (π.χ. ηλικία, φύλο, ενδιαφέροντα) επιτρέπουν στις υπηρεσίες να παρέχουν εμπειρίες προσαρμοσμένες στις ανάγκες των μεμονωμένων χρηστών. Εκτός από αυτές τις πληροφορίες που παρέχονται από τον χρήστη, πολλές συσκευές και εφαρμογές AR/MR/VR θα συλλέγουν επίσης δεδομένα σχετικά με τη συμπεριφορά και τις δραστηριότητες του χρήστη εντός του κόσμου. Οι πληροφορίες σχετικά με το τι κάνει ένας χρήστης με τις συσκευές ή τις εφαρμογές AR/MR/VR, πόσο καιρό ξοδεύει σε συγκεκριμένες δραστηριότητες και ποιες εμπειρίες αναζητά και συμμετέχει μπορεί να αποκαλύψει προσωπικά στοιχεία. Επίσης οι συσκευές AR/MR/VR

συλλέγουν εκτεταμένα βιομετρικά δεδομένα τα οποία μπορούν να προσδιορίσουν άτομα και να συνάγουν πρόσθετες πληροφορίες [122].

Αρκετά από τα νομικά ζητήματα που σχετίζονται με τις τεχνολογίες AR/MR/VR προκύπτουν από τα δεδομένα που συλλέγονται από συσκευές και εφαρμογές AR/MR/VR [123]. Τα δεδομένα συλλέγονται μέσω των διαφόρων αισθητήρων που διαθέτουν οι συσκευές AR/MR/VR αλλά και τα δεδομένα που εισάγει ο χρήστης κατά την είσοδο του. Είναι γνωστό ότι οι συσκευές και εφαρμογές AR/MR/VR συλλέγουν δεδομένα σχετικά με συγκεκριμένες δραστηριότητες στις οποίες συμμετέχουν τα άτομα όπως μηνύματα, βίντεο, ήχο και στιγμιότυπα οθόνης. Λόγω του όγκου των πληροφοριών που συλλέγονται, υπάρχει ακόμη μεγαλύτερη διακύμανση στην πρόσβαση τρίτων σε ευαίσθητες πληροφορίες για την ιδιωτική ζωή των χρηστών. Οι κίνδυνοι για τους χρήστες εξαρτιούνται από το πώς, πού και για ποιο σκοπό χρησιμοποιούν τις τεχνολογίες AR/MR/VR τα δεδομένα τους. Τα βιογραφικά και δεδομένα υγείας ενός ασθενούς που χρησιμοποιούν θεραπείες AR/MR/VR πιθανότατα θα θεωρούνται πιο ευαίσθητα από τις ίδιες πληροφορίες που παρέχονται από έναν χρήστη σε μια πλατφόρμα παιχνιδιών ή φυσικής κατάστασης VR.

Τα δεδομένα τα οποία συλλέγονται από τις συσκευές και εφαρμογές AR/MR/VR περιέχουν πολλούς κινδύνους για το απόρρητο των χρηστών και ειδικότερα για την ανωνυμία και την προσωπική αυτονομία των χρηστών [124]. Ειδικότερα όσο περισσότερα τρίτα μέρη επεμβαίνουν στο απόρρητο των χρηστών τόσο η ικανότητα των ατόμων να ελέγχουν πόσα πολλά ή πόσο λίγα μπορούν οι άλλοι να παρατηρήσουν και να αναγνωρίσουν για αυτούς μειώνεται. Οι τεχνολογίες AR/MR/VR συλλέγουν σημαντικό αριθμό ποικίλων τύπων δεδομένων, τα οποία στη συνέχεια μπορούν να ερμηνευθούν για να παρέχουν πιο προηγμένες δυνατότητες και προσαρμοσμένες εμπειρίες. Περιγραφικές πληροφορίες σχετικά με χρήστες, όπως δημογραφικές πληροφορίες, τοποθεσία και συμπεριφορά ή δραστηριότητες εντός του κόσμου μπορούν να συνδυαστούν και να αναλυθούν για να προβάλλουν στοχευμένες διαφημίσεις και περιεχόμενο σε άτομα. Ακόμη τα βιομετρικά στοιχεία μπορούν να δημιουργήσουν πρόσθετες λεπτομέρειες σχετικά με τα φυσικά χαρακτηριστικά του χρήστη ή τις πληροφορίες υγείας. Λόγω της ευαίσθητης φύσης αυτών των βιομετρικά παραγόμενων πληροφοριών, η ασφάλεια των δεδομένων και η δυνατότητα πρόσβασης τρίτων σε αυτές είναι μια αξιοσημείωτη ανησυχία για το απόρρητο [125]. Η πρόσβαση από μη εξουσιοδοτημένα μέρη σε αυτές τις πληροφορίες αναμένεται να οδηγήσει στην δημιουργία προφίλ για το υποκείμενο των δεδομένων με αποτέλεσμα να του προβάλλονται στοχευμένες διαφημίσεις. Επιπρόσθετα η επεξεργασία των δεδομένων σχετικά με την υγεία του χρήστη χωρίς τη συγκατάθεση του μπορεί να οδηγήσει στην αποκάλυψη μελλοντικών προβλημάτων υγείας τα οποία μπορούν να εκμεταλλευτούν ασφαλιστικές εταιρίες αλλά και φαρμακεύτηκες εταιρίες για εξατομικευμένη προβολή ιατρικών προϊόντων.

Στην εικονική πραγματικότητα η γραφική απεικόνιση του χρήστη (avatar) αποτελεί το ενεργό στοιχείο για την αλληλεπίδραση του χρήστη με τον εικονικό κόσμο [126]. Ειδικότερα η εικονική αναπαράσταση ενός χρήστη ή το avatar του μπορούν να αποκαλύψουν συγκεκριμένες πληροφορίες για αυτό όπως τη φυλή, το φύλο του, πληροφορίες σχετικά με τη φυσική εμφάνιση του, τη συμπεριφορά και τις χειρονομίες του. Τα avatar διακρίνονται σε δύο κατηγορίες, πρώτον τα avatar που αντικατοπτρίζουν την φυσική εμφάνιση των χρηστών (πιστό αντίγραφο των κατόχων τους) ή είδωλα που αποκρύπτουν την εμφάνιση ή την ταυτότητα τους. Όμως και στις δυο περιπτώσεις οι κίνδυνοι που διέπουν τα είδωλα είναι εξαιρετικά σημαντικοί. Ο κίνδυνος αυτός είναι μεγάλος για ευάλωτους χρήστες όπως τα παιδία, για εκείνους που χρησιμοποιούν συσκευές AR/MR/VR για την υγεία ή για ιατρικούς σκοπούς και για εκείνους που μοιράζονται ιδιαίτερα ευαίσθητες πληροφορίες στο AR/MR/VR. Επειδή οι χρήστες όταν χρησιμοποιούν την εικονική αναπαράσταση του εαυτού τους βιώνουν το εικονικό σώμα σαν να είναι το δικό τους αλληλεπιδρούν και κινούνται όπως θα έκαναν οι ίδιοι στην πραγματικότητα οδηγώντας στην αποκάλυψη μεγάλου μέρους πληροφορίων για τους εαυτού τους. Επιπρόσθετα τα avatar μπορούν να αποκαλύψουν πλήθος ευαίσθητων πληροφοριών θέτοντας κίνδυνους για το απόρρητο των χρηστών. Όταν η συλλογή, καταγραφή και αναπαραγωγή αυτών των πληροφορίων πραγματοποιείται σε μη εξουσιοδοτημένα μέρη χωρίς τη συγκατάθεση του χρήστη αποκαλύπτοντας ιδιωτικές πληροφορίες για αυτόν τότε παραβιάζονται τα δικαιώματα του υποκείμενου των δεδομένων [127]. Για παράδειγμα η χρήση χωρίς τη συγκατάθεση ηχογραφήσεων ή φωτογραφιών ενός ατόμου μπορούν να οδηγήσουν σε διακρίσεις και να αποκαλύψουν λεπτομέρειες σχετικά με τη ζωή τους. Αξιοσημείωτο είναι το γεγονός ότι κακόβουλα άτομο μπορούν να χρησιμοποιήσουν τα δεδομένα ενός χρήστη για σκοπούς πλαστοπροσωπίας [128]. Πιο συγκεκριμένα ένα κακόβουλο άτομο μπορεί να χρησιμοποιήσει την εικόνα ενός άλλου ατόμου για να τον πλαστοπροσωπήσει σε πλατφόρμες επικοινωνίας. Επιπλέον θα μπορούσε να δημιουργήσει ένα πλήρως διαδραστικό avatar του θύματος και να το χρησιμοποιήσει για να εμπλακεί σε δραστηριότητες τις οποίες δεν έκανε το θύμα προκαλώντας του συναισθηματική βλάβη ή ακόμη και οικονομική ζημία.

Η παρουσίαση του χρήστη και οι αλληλεπιδράσεις του αποτελούν εικονικά δεδομένα με αποτέλεσμα να υπόκεινται σε επεξεργασία. Ειδικότερα οι τεχνολογίες AR/MR/VR απαιτούν την επεξεργασία σημαντικών ποσοτήτων προσωπικών δεδομένων, συμπεριλαμβανομένων των πληροφοριών ταυτότητας των χρηστών, της εμφάνισης, των δεδομένων παρακολούθησης σώματος, της τοποθεσίας, των επικοινωνιών και άλλων συμπεριφορών. Βασιζόμενοι στον ΓΚΠΔ οι υπεύθυνοι επεξεργασίας δεδομένων για τη νόμιμη επεξεργασία των παραπάνω δεδομένων υπάρχει η πιθανότητα να οδηγήσουν στην παροχή μη καθηλωτικών εμπειριών. Επιπλέον τα προϊόντα AR/MR/VR συνήθως χρειάζεται επίσης να επεξεργάζονται βιομετρικά δεδομένα (π.χ. δακτυλικά αποτυπώματα, συστήματα αναγνώρισης προσώπου κλπ.) για να επιτρέψουν τη χρήση αυτών των τεχνολογιών. Η βασική ανησυχία που δημιουργείτε έγκεινται στο γεγονός ότι οι χρήστες μπορεί να μην

έχουν πραγματική επιλογή να συναινέσουν ή όχι στη συλλογή και επεξεργασία των δεδομένων τους σε αυτό το πλαίσιο, όπου η τεχνολογία δεν μπορεί διαφορετικά να χρησιμοποιηθεί χωρίς την επεξεργασία των δεδομένων τους. Σύμφωνα με τον ΓΚΠΔ τα υποκείμενα των δεδομένων θα πρέπει να διαθέτουν σαφείς οδηγίες σχετικά με τον τρόπο αποθήκευσης και επεξεργασίας των δεδομένων τους από τις εφαρμογές AR/MR/VR ώστε να υπάρξει μετριασμό για τους κίνδυνους του απόρρητου τους [129]. Η ενημέρωση των υποκείμενων των δεδομένων είναι αναγκαία καθώς τα δεδομένα που συλλέγουν οι συσκευές και εφαρμογές AR/MR/VR μπορούν να συλλέγονται για κακόβουλους σκοπούς (καταγραφή ατόμων χωρίς την συγκατάθεση τους) οδηγώντας σε παραβίαση του απόρρητου τους και της ιδιωτικής τους ζωής. Για ορισμένους χρήστες, η επεξεργασία των δεδομένων τους χωρίς τη συγκατάθεση τους θα μπορούσε επίσης να οδηγήσει σε επιβλαβείς διακρίσεις. Αυτό δημιουργεί μια αξιοσημείωτη ανησυχία για την προστασία της ιδιωτικής ζωής για άτομα που είναι ευάλωτα σε πρακτικές που εισάγουν διακρίσεις, για παράδειγμα, στην απασχόληση ή την πρόσβαση σε κρίσιμες υπηρεσίες, λόγω χαρακτηριστικών όπως φύλο, ηλικία, φυλή, αναπηρία, σεξουαλικός προσανατολισμός και άλλα. Χωρίς διασφαλίσεις για την προστασία από τέτοιου είδους διακρίσεις, η συνεχής επεξεργασία και κοινοποίηση προσωπικών δεδομένων σε τρίτους μπορούν να προκαλέσουν σημαντική βλάβη.

Η απλή απόκρυψη, ανωνυμοποίηση ή περιορισμός της συλλογής αυτών των δεδομένων θα μείωνε δραστικά την ποιότητα αυτών των υπηρεσιών ή θα τις καθιστούσε αναποτελεσματικές και θα εμπόδιζε την καινοτομία οποιασδήποτε τεχνολογίας που ενδέχεται να απαιτεί πληροφορίες από το χρήστη. Επομένως για τη μείωση των κινδύνων για το απόρρητο και την ιδιωτική ζωή του χρήστη που απορρέουν από την υπέρογκη συλλογή δεδομένων θα πρέπει να υπάρξει εστίαση στον έλεγχο του χρήστη για το πως και πότε τα δεδομένα προβάλλονται και διανέμονται διασφαλίζοντας ότι δεν θα υπάρξει μη εξουσιοδοτημένη πρόσβαση και θεσπίζοντας νόμους και κανονισμούς για την προστασία από την κατάχρηση. Οι συσκευές και εφαρμογές AR/MR/VR θα πρέπει να παρέχουν στους χρήστες διαφάνεια σχετικά τρόπο συλλογής, κοινοποίησης και χρήσης των δεδομένων τους ώστε να υπάρξει εμπιστοσύνη μεταξύ τους. Οι ατομικές ρυθμίσεις απορρήτου επιτρέπουν στους χρήστες να περιορίσουν την πρόσβαση τρίτων στα δεδομένα τους. Για παράδειγμα μπορούν να επιλέξουν ποιοι χρήστες θα βλέπουν τις φωτογραφίες τους. Στο AR/MR/VR θα πρέπει να υπάρξει περιορισμός της πρόσβασης σε εικονικά στοιχεία καθώς και στην δυνατότητα τρίτων να παρατηρούν, ακούνε και καταγράφουν δεδομένα εντός την εφαρμογής/εικονικού κόσμου.

Η διαφάνεια, η αποκάλυψη και η συναίνεση του χρήστη διαδραματίζουν σημαντικό ρόλο στην άμβλυνση των πιθανών παραβιάσεων των τεχνολογιών AR/MR/VR. Όταν οι χρήστες καταλαβαίνουν πώς και γιατί διάφορες υπηρεσίες AR/MR/VR συλλέγουν και μοιράζονται τα δεδομένα τους, μπορούν να λάβουν ενημερωμένες αποφάσεις σχετικά με τις πληροφορίες που επιλέγουν να μοιραστούν. Για παράδειγμα, οι συσκευές AR/MR/VR, όπως αναφέρθηκε και

προηγουμένως, απαιτούν κάποιες πληροφορίες παρακολούθησης κίνησης προκειμένου να αναπαράγουν φυσικές κινήσεις σε εικονικό χώρο, ενώ μια πλατφόρμα αναζήτησης μπορεί να χρησιμοποιεί δεδομένα γεωγραφικής τοποθεσίας για να παρέχει πιο συναφή αποτελέσματα. Σε αυτές τις περιπτώσεις, η διασφάλιση ότι οι χρήστες κατανοούν τον τρόπο με τον οποίο οι συσκευές και οι εφαρμογές χρησιμοποιούν τα δεδομένα τους για την παροχή διαφορετικών υπηρεσιών τους δίνει περισσότερο έλεγχο στα δεδομένα τους και μειώνει την πιθανότητα παραβίαση τους. Όπως και άλλοι τύποι πληροφοριών, η αποκάλυψη και η συναίνεση του χρήστη αποτελούν το θεμέλιο κάθε προσέγγισης μετριασμού για υπολογιστικά δεδομένα. Οι χρήστες πρέπει να κατανοήσουν ποιες πληροφορίες μπορούν να συναχθούν από τα δεδομένα που παρέχουν και πώς χρησιμοποιούνται. Για συμπεράσματα δεδομένων που δεν είναι απαραίτητα για τις βασικές λειτουργίες μιας συσκευής ή εφαρμογής, οι προτιμήσεις απορρήτου των χρηστών μπορούν να επιτρέψουν σε άτομα να εξαιρεθούν από συγκεκριμένη συγκέντρωση δεδομένων και υπολογισμούς. Όταν αυτές οι πληροφορίες είναι απαραίτητες για τη λειτουργικότητα ή την ποιότητα των υπηρεσιών, η διαφάνεια και η αποκάλυψη σχετικά με τον τρόπο και τον λόγο για τον οποίο χρησιμοποιούνται τα συμπεράσματα πληροφοριών μπορούν να διασφαλίσουν ότι οι χρήστες κατανοούν τις πρακτικές δεδομένων που ισχύουν. Επιπλέον σαφείς οδηγίες που περιγράφουν πώς αποθηκεύονται τα δεδομένα και πώς, πότε και από ποιον μπορούν να προσπελαστούν προστατεύουν τους χρήστες από πιθανές προσωπικές βλάβες ή δυσφήμιση που θα μπορούσαν να προκύψουν από μη εξουσιοδοτημένη πρόσβαση.

Οι υπεύθυνοι χάραξης πολιτικής θα πρέπει να δημιουργήσουν ένα ρυθμιστικό περιβάλλον για την προστασία της ιδιωτικής ζωής των χρηστών AR/MR/VR το οποίο παράλληλα θα υποστηρίζει την καινοτομία και την εξέλιξη των προαναφερθέντων τεχνολογιών. Ακόμη θα πρέπει να λάβουν υπόψιν τους διαφορετικούς τύπους πληροφορίων που συλλέγουν οι συσκευές AR/MR/VR και να καθιερώσουν κατάλληλες διασφαλίσεις για την προστασία του απόρρητου των χρηστών από την ευρεία συλλογή δεδομένων [130]. Το κανονιστικό πλαίσιο θα πρέπει να επιτρέπει στις εταιρίες κατασκευής συσκευών AR/MR/VR να συνεχίζουν να καινοτομούν ενώ παράλληλα διασφαλίζουν την προστασία των χρηστών τους.

Συμπεράσματα

Η παρούσα διπλωματική εργασία έχει ως κύριο στόχο τον εντοπισμό και τη διερεύνηση των νομικών ζητημάτων που διέπουν τα δίκτυα έκτης γενιάς. Προκειμένου να εκπληρωθεί ο προαναφερθείς στόχος πραγματοποιήθηκε αρχικά ανάλυση των βασικών εφαρμογών που θα υποστηρίζουν τα δίκτυα 6G και παράλληλα των τεχνολογιών που θα αξιοποιήσουν για την παροχή των υπηρεσιών και εφαρμογών. Έπειτα έγινε παράθεση των βασικών ορισμών και εννοιών του ΓΚΠΔ ώστε να γίνει καλύτερη κατανόηση των παραβιάσεων που θα επιφέρουν τα δίκτυα έκτης γενιάς. Στο κεφάλαιο των νομικών ζητημάτων εντοπίστηκαν και πραγματοποιήθηκε εκτενής ανάλυση των νομικών ζητημάτων των δικτύων έκτης γενιάς.

Όπως παρατηρήθηκε από τη βιβλιογραφική ανασκόπηση τα δίκτυα έκτης γενιάς θα βασίζονται στην τεχνητή νοημοσύνη και στη μηχανική μάθηση. Επιπλέον το πλήθος των αισθητήρων σε διάφορους τομείς όπως υγειονομική περίθαλψη, μεταφορές, έξυπνο σπίτι και πόλη θα αυξηθούν εκθετικά με αποτέλεσμα ο τεράστιος αριθμός προσωπικών δεδομένων που συλλέγονται και κοινοποιούνται στο διαδίκτυο των πράγματων να προκαλεί αυξανόμενες ανησυχίες σχετικά με το απόρρητο των χρηστών. Ο ΓΚΠΔ έχει ως σκοπό να ενισχύσει τα δικαιώματα των χρηστών και να θέσεις τις απαιτήσεις για το χειρισμό των δεδομένων.

Για τον ΓΚΠΔ η συμμετοχή των χρηστών στην προστασία της ιδιωτικής του ζωής αποτελεί βασικό στοιχείο. Μέσω του ΓΚΠΔ επιτεύχθηκε ενίσχυση των ήδη υπάρχοντών δικαιωμάτων των υποκείμενων των δεδομένων. Πιο συγκεκριμένα το δικαίωμα της ενημέρωσης και διαφάνειας, το δικαίωμα της πρόσβασης, το δικαίωμα της διόρθωσης, το δικαίωμα της διαγραφής, το δικαίωμα του περιορισμού της επεξεργασίας, το δικαίωμα της φορητότητας των δεδομένων, το δικαίωμα της εναντίωσης και τέλος το δικαίωμα στη μη αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ. Στη παρούσα διπλωματική παρουσιαστήκαν οι παραβιάσεις των προαναφερθέντων δικαιωμάτων από τις ποικίλες εφαρμογές που θα υποστηρίζουν τα δίκτυα έκτης γενιάς.

Από τα δικαιώματα που προαναφέρθηκαν παρατηρήθηκε ότι τα πιο καίρια νομικά ζητήματα που θα διέπουν τα δίκτυα έκτης γενιάς αφορούν:

- Πως θα χρησιμοποιούν οι εταιρείες και πάροχοι των εφαρμογών/υπηρεσιών τα δεδομένα του χρήστη που συλλέγονται;
- Θα υπάρχει ενημέρωση του χρήστη όταν πραγματοποιηθεί αλλαγή απορρήτου από των πάροχο υπηρεσιών ώστε να ζητήσει εκ νέου την συγκατάθεση του για συλλογή και επεξεργασία των δεδομένων του;
- Σε περίπτωση απώλειας/διαρροής δεδομένων πως θα εγγυώνται οι εταιρείες την ασφάλεια των δεδομένων του υποκείμενου των δεδομένων;
- Τα δεδομένα που αποθηκεύονται στο cloud θα κρυπτογραφούνται;

- Οι εταιρείες που παρέχουν τις εφαρμογές θα κοινοποιούν τα δεδομένα των χρηστών σε τρίτους; Και αν ναι θα υπάρχει ενημέρωση του χρήστη αρχικά ώστε να δώσει την συγκατάθεση του;
- Όταν το υποκείμενο των δεδομένων ζητήσει την διαγραφή των δεδομένων του τότε τα δεδομένα του θα διαγράφονται πραγματικά από τις βάσεις δεδομένων του παρόχου υπηρεσιών;

Η εξέλιξη των δικτύων κινητών επικοινωνιών θα οδηγήσει την ανθρωπότητα σε μια νέα εποχή. Η παροχή υπηρεσιών σε πραγματικό χρόνο, η εξαιρετικά χαμηλή καθυστέρηση, η μαζική συνδεσιμότητα και η αξιοπιστία αποτελούν στοιχεία απαραίτητα για τη σωστή λειτουργία των εφαρμογών των δικτύων 6G. Η ενίσχυση των κλάδων της βιομηχανίας, της υγείας, των μεταφορών, των έξυπνων πόλεων και σπιτιών θα οδηγήσουν σε μια νέα πραγματικότητα. Παρόλα αυτά ο εξελισσόμενος χαρακτήρας των τεχνολογιών και η αύξηση της συλλογής, επεξεργασίας και αποθήκευσης δεδομένων σε βάσεις δεδομένων θα οδηγήσουν στην αύξηση ζητημάτων σχετικά με την ιδιωτικότητα των ατόμων και την παραβίαση/συνεχή καταγραφή της ιδιωτικής τους ζωής. Όταν η τεχνολογία υπόσχεται παγκόσμια συνδεσιμότητα τότε ολόκληρη η ζωή ενός ατόμου κινδυνεύει να παραβιαστεί και τα δεδομένα του να αποκαλυφθούν. Για να υπάρξει σχέση εμπιστοσύνης μεταξύ των εφαρμογών/υπηρεσιών και των ανθρώπων θα πρέπει να υπάρξει διαφάνεια ως προς τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών δεδομένων. Επίσης θα πρέπει πριν την κοινοποίηση των δεδομένων σε τρίτους το υποκείμενο των δεδομένων να έχει δώσει την συγκατάθεση του. Επομένως ο ΓΚΠΔ δεν αποτελεί εμπόδιο στην εξέλιξη και την καινοτομία των δικτύων κινητών επικοινωνιών αλλά το μέσο για την προστασία των δεδομένων των ανθρώπων.

Ακρωνύμια

3D	Three-Dimensional Space
5G	Fifth Generation Telecommunication Networks
6G	Sixth Generation Telecommunication Networks
AI	Artificial Intelligence
AR	Augmented Reality
EI	Edge Intelligence
e-HEALTH	Electronic Health
EM	Electromagnetic
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HCI	Human–Computer Interaction
IR	Infrared
IoE	Internet of Everything
IoT	Internet of Things
LED	Light Emitting Diode
LiDAR	Light Detection and Ranging
M2M	Machine-to-Machine
M2P	Machine-to-People
MEC	Multi-Access Edge Computing
mHEALTH	Mobile Health
mmWave	Millimeter Wave
MR	Mixed Reality
NHTSA	National Highway Traffic Safety Administration
OWC	Optical Wireless Communications
P2P	Peer-to-Peer

RF	Radio Frequency
THZ	Terahertz
UAV	Unmanned Aerial Vehicle
UV	Ultraviolet
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VLC	Visible Light Communication
VR	Virtual Reality
XR	X-Reality

Βιβλιογραφία

[1]https://www.oulu.fi/6gflagship/6g-white-papers

[2]https://searchnetworking.techtarget.com/definition/6G

[3]https://global.chinadaily.com.cn/a/202001/03/WS5e0e4b6ba310cf3e3558226d.html

[4]https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai

[5]https://repository.kallipos.gr/bitstream/11419/3382/1/02_chapter_04.pdf

[6]https://studycare.gr/ti-einai-to-diadiktyo-ton-pragmaton-iot/

[7] Mika Ylianttila, Raimo Kantola, Andrei Gurtov, Lozenzo Mucchi, Ian Oppermann, Zheng Yan, Tri Hong Nguyen, Fei Liu, Tharaka Hewa, Madhusanka Liyanage, Ahmad Ijaz, Juha Partala, Robert Abbas, Artur Hecker, Sara Jayousi, Alessio Martinelli, Stefano Caputo, Jonathan Bechtold, Ivan Morales, Andrei Stoica, Giuseppe Abreu, Shahriar Shahabuddin, Erdal Panayirci, Harald Haas, Tanesh Kumar, Basak Ozan Ozparlak and Juha Röning. “6g white paper: Research challenges for trust, security and privacy”. arXiv preprint arXiv:2004.11665, 2020.

[8]https://www.rfwireless-world.com/Terminology/Difference-between-5G-and-6G.html

[9] Clim, Antonio. “Cyber security beyond the Industry 4.0 era. A short review on a few technological promises”. Informatica Economica, 2019, 23.2: 34-44.

[10]https://electronics360.globalspec.com/article/16447/5g-vs-6g-what-is-it-and-when-will-it-be-here

[11]https://blog.unbelievable-machine.com/en/what-is-a-digital-twin

[12]https://www.fenwickelliott.com/research-insight/annual-review/2020/challenges-legal-implications-digital-twins

[13]https://cmte.ieee.org/futuredirections/2018/06/14/digital-twins-advantages-issues-of-a-powerful-emerging-technology/

[14] Xiaohu You, Cheng-Xiang Wang, Jie Huang, Xiqi Gao, Zaichen Zhang, Mao Wang, Yongming Huang, Chuan Zhang, Yanxiang Jiang, Jiaheng Wang, Min Zhu, Bin Sheng, Dongming Wang, Zhiwen Pan, Pengcheng Zhu, Yang Yang, Zening Liu, Ping Zhang, Xiaofeng Tao, Shaoqian Li, Zhi Chen, Xinying Ma, Chih-Lin I, Shuangfeng Han, Ke Li, Chengkang Pan, Zhimin Zheng, Lajos Hanzo, Xuemin (Sherman) Shen, Yingjie Jay Guo, Zhiguo Ding, Harald Haas, Wen Tong, Peiying Zhu, Ganghua Yang, Jun Wang, Erik G. Larsson, Hien Quoc Ngo, Wei Hong, Haiming Wang, Debin Hou, Jixin Chen, Zhe Chen, Zhangcheng Hao, Geoffrey Ye Li, Rahim Tafazolli, Yue Gao, H. Vincent Poor, Gerhard P. Fettweis and Ying-Chang Liang. “Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts”. Science China Information Sciences, 2021, 64.1: 1-74.

[15]https://www.ge.com/news/reports/these-engineers-are-building-the-industrial-internet-for-the-body

[16]https://medium.com/o4s-io/industry-4-0-the-new-building-block-of-manufacturing-79c9ecbb053f

[17]https://www.epicor.com/en/resource-center/articles/what-is-industry-4-0/

[18]https://www.thebest.gr/article/493218-

[19] Amin Shahraki, Mahmoud Abbasi, Md. Jalil Piran, Mingzhe Chen and Shuguang Cui. “A Comprehensive Survey on 6G Networks: Applications, Core Services, Enabling Technologies, and Future Challenges”. arXiv preprint arXiv:2101.12475, 2021.

[20]https://el.wikipedia.org/wiki/%CE%92%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AF%CE%B1_4.0

[21] Nayak Sabuzima and Patgiri Ripon. “6G communication technology: A vision on intelligent healthcare”. In: Health Informatics: A Computational Perspective in Healthcare. Springer, Singapore, 2021. p. 1-18.

[22] https://awtg.co.uk/enabling-holographic-communication

[23] https://spectrum.ieee.org/6g-haptic-holography

[24] Faiza Nawaz, Jawwad Ibrahim, M. Awais, M. Junaid, Sabila Kousar and Tamseela Parveen. “A review of vision and challenges of 6G technology”. International Journal of Advanced Computer Science and Applications, 2020, 11.2.

[25]https://www.threekit.com/blog/what-is-augmented-reality

[26]https://www.investopedia.com/terms/v/virtual-reality.asp

[27]https://5g.co.uk/guides/what-is-the-tactile-internet/

[28] D. Wang, Y. Guo, S. Liu, Yuru Zhang, Weiliang Xu and Jing Xiao. "Haptic display for virtual reality: progress and challenges". Virtual Reality & Intelligent Hardware, 2019, 1.2: 136-162.

[29]https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/s2008/crs54_tz36/crs54_tz36/twocolumn.html

[30] Feng Liu, Jing-Long Han, Ji Qi, Yu Zhang, Jia-Luo Yu, Wen-Peng Li, Dong Lin, Ling-Xin Chen and Bo-Wei Li. "Research and application progress of intelligent wearable devices". Chinese Journal of Analytical Chemistry, 2021, 49.2: 159-171.

[31]https://www.pencilonthemoon.gr/ta-aftonoma-ochimata-erchontai-gia-na-allaksoun-ton-kosmo/

[32]https://www.europarl.europa.eu/news/el/headlines/economy/20190110STO23102/autonoma-autokinita-stin-ee-apo-epistimoniki-fantasia-se-apti-pragmatikotita

[33]https://el.omatomeloanhikaku.com/what-are-the-different-self-driving-car-levels-of-autonomy-6900

[34] Jianhua He, Kun Yang and Hsiao-Hwa Chen. "6G cellular networks and connected autonomous vehicles". IEEE Network, 2020.

[35] Bo Yang, Xuelin Cao, Kai Xiong, Chau Yuen, Yong Liang Guan, Supeng Leng, Lijun Qian and Zhu Han. "Edge Intelligence for Autonomous Driving in 6G Wireless System: Design Challenges and Solutions". IEEE Wireless Communications, 2021, 28.2: 40-47.

[36]https://www.medianova.com/en-blog/2020/02/28/what-on-earth-is-edge-intelligence

[37]https://simonlawpc.com/trucking-accident/autonomous-truck-platooning-legal-in-your-state/

[38]https://www.acea.auto/files/Platooning_roadmap.pdf

https://www.ericsson.com/en/blog/2017/5/how-will-the-transportation-system-benefit-from-iot-enabled-platooning

[39] Tengchan Zeng, Omid Semiari, Walid Saad and Mehdi Bennis. "Joint communication and control for wireless autonomous vehicular platoon systems". IEEE Transactions on Communications, 2019, 67.11: 7907-7922.

[40]https://en.wikipedia.org/wiki/Smart_environment

[41]https://www.mobilize.org.br/noticias/12397/mais-de-40-das-pessoas-podem-trocar-suas-cidades-por-uma-smart-city.html

[42]http://smartcityhub.com/governance-economy/what-is-a-smart-city/

[43] Zaheer Allam and David S. Jones. "Future (post-COVID) digital, smart and sustainable cities in the wake of 6G: Digital twins, immersive realities and new urban economies". Land Use Policy, 2021, 101: 105201.

[44]https://qz.com/1482503/what-our-tech-habits-reveal-about-the-future-of-smart-homes/

[45]https://www.investopedia.com/terms/s/smart-home.asp

[46]https://iotnews.asia/wp-content/uploads/2017/01/The-Battle-for-the-Smart-Home-Open-to-All.pdf

[47] Karan Sheth, Keyur Patel, Het Shah, Sudeep Tanwar, Rajesh Gupta and Neeraj Kumar. "A taxonomy of AI techniques for 6G communication networks". Computer Communications, 2020, 161: 279-303.

[48] John McKinlay and Edinburgh Peter McLaughlin. "The Smart Home Legal Framework". DLA Piper.

[49] Mohammed H. Alsharif, Mahmoud A. M. Albreem, Ahmad A. A. Solyman and Sunghwan Kim. "Toward 6G Communication Networks: Terahertz Frequency Challenges and Open Research Issues". Computers, Materials & Continua, 2021, 66.3: 2831-2842.

[50] Lauri Loven, Teemu Leppänen, Ella Peltonen, Juha Partala, Erkki Harjula, Pawani Porambage, Mika Ylianttila and Jukka Riekki. "EdgeAI: A Vision for Distributed, Edge-native Artificial Intelligence in Future 6G Networks". The 1st 6G Wireless Summit, 2019, 1-2.

[51] Helin Yang, Arokiaswami Alphones, Zehui Xiong, Dusit Niyato, Jun Zhao and Kaishun Wu. "Artificial-Intelligence-Enabled Intelligent 6G Networks". IEEE Network, 2020, 34.6: 272-280.

[52] Jianwei Zhao, Feifei Gao, Guoru Ding, Tao Zhang, Weimin Jia and Arumugam Nallanathan. "Integrating Communications and Control for UAV Systems: Opportunities and Challenges". IEEE Access, 2018, 6: 67519-67527.

[53] Shangwei Zhang, Jiajia Liu, Hongzhi Guo, Mingping Qi and Nei Kato. "Envisioning Device-to-Device Communications in 6G". IEEE Network, 2020, 34.3: 86-91.

[54] Tongyi Huang, Wu Yang, Jun Wu, Jin Ma, Xiaofei Zhang and Daoyin Zhang. "A Survey on Green 6G Network: Architecture and Technologies". IEEE Access, 2019, 7: 175758-175768.

[55] Emilio Calvanese Strinati, Sergio Barbarossa, Taesang Choi, Antonio Pietrabissa, Alessandro Giuseppi, Emanuele De Santis, Josep Vidal, Zdenek Becvar, Thomas Haustein, Nicolas Cassiau, Francesca Costanzo, Junhyeong Kim and

Ilgyu Kim. “6G in the sky: On-demand intelligence at the edge of 3D networks”. arXiv preprint arXiv:2010.09463, 2020.

[56] Mostafa Zaman Chowdhury, Md. Shahjalal, Shakil Ahmed and Yeong Min Jang. “6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions”. IEEE Open Journal of the Communications Society, 2020, 1: 957-975.

[57] Yang Lua and Xianrong Zhengb. “6G: A survey on technologies, scenarios, challenges, and the related issues”. Journal of Industrial Information Integration, 2020, 100158.

[58] Lina Bariah, Lina Mohjazi, Sami Muhaidat, Paschalis C. Sofotasios, Gunes Karabulut Kurt, Halim Yanikomeroglu and Octavia A. Dobre. “A Prospective Look: Key Enabling Technologies, Applications and Open Research Topics in 6G Networks”. IEEE Access, 2020, 8: 174792-174820.

[59] Latif Ullah Khan. “Visible light communication: applications, architecture, standardization and research challenges”. Digital Communications and Networks, 2017, 3.2: 78-88.

[60] Ella Peltonen, Mehdi Bennis, Michele Capobianco, Merouane Debbah, Aaron Ding, Felipe Gil-Castiñeira, Marko Jurmu, Teemu Karvonen, Markus Kelanti, Adrian Kliks, Teemu Leppänen, Lauri Lovén, Tommi Mikkonen, Ashwin Rao, Sumudu Samarakoon, Kari Seppänen, Paweł Sroka, Sasu Tarkoma and Tingting Yang.
“6G white paper on edge intelligence”. arXiv preprint arXiv:2004.14850, 2020.

[61] https://azure.microsoft.com/en-us/overview/future-of-cloud/

[62] Rajesh Gupta, Dakshita Reebadiya and Sudeep Tanwar. “6G-enabled Edge Intelligence for Ultra -Reliable Low Latency Applications: Vision and Mission”. Computer Standards & Interfaces, 2021, 77: 103521.

[63]https://honim.typepad.com/biasc/2014/06/the-internet-of-everything-course.html

[64]https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-index-faq.pdf

[65]https://www.bbvaopenmind.com/en/technology/digital-world/the-internet-of-everything-ioe/

[66] https://www.i-scoop.eu/internet-of-things-guide/internet-of-everything/

[67]https://emerline.com/blog/iot-vs-ioe

[68] Prafulla Kumar Padhi and Feranando Charrua-Santos. “6G Enabled Industrial Internet of Everything: Towards a Theoretical Framework”. Applied System Innovation, 2021, 4.1: 11.

[69]https://www.ibm.com/cloud/blog/what-is-multi-access-edge-computing

[70]https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

[71] Hiroyuki Tanaka, Masahiro Yoshida, Koya Mori and Noriyuki Takahashi. "Multi-access Edge Computing: A Survey". Journal of Information Processing, 2018, 26: 87-97.

[72] https://www.etsi.org/technologies/multi-access-edge-computing

[73] Haixia Peng, Qiang and Xuemin Shen. "Spectrum Management for Multi-Access Edge Computing in Autonomous Vehicular Networks". IEEE Transactions on Intelligent Transportation Systems, 2019, 21.7: 3001-3012.

[74] http://usolutions.gr/v3/news/international-news/gdpr-

[75]https://www.taxheaven.gr/circulars/27607/arora-ti-einai-o-gdpr-kai-poies-oi-ypoxrewseis-twn-epixeirhsewn

[76]https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-99-genikos-kanonismos-gia-tin-prostasia-dedomenon-enarxi

[77]https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-4-genikos-kanonismos-gia-tin-prostasia-dedomenon-orismoi

[78]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_el

[79] https://www.dpa.gr/el/foreis/arxes_nomimotitas

[80]https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-2-genikos-kanonismos-gia-tin-prostasia-dedomenon

[81]https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-3-genikos-kanonismos-gia-tin-prostasia-dedomenon-edafiko

[82]https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-6-genikos-kanonismos-gia-tin-prostasia-dedomenon

[83] https://www.lawspot.gr/gdpr/consent

[84] https://www.privacy-regulation.eu/el/22.htm

[85]https://www.lawspot.gr/nomika-nea/odigies-gia-tin-katartisi-profil-hriston-profiling-symfona-me-ton-geniko-kanonismo-gdpr

[86] Lilian Mitrou. "Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-

Proof'?". Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof, 2018.

[87]https://dspace.lib.uom.gr/bitstream/2159/23990/4/PanagiotidouMarina-EuthymiaMsc2020.pdf

[88] https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf

[89] Stavroula Rizou, Eugenia Alexandropoulou-Egyptiadou and Kostas E. Psannis. "Taxonomy about the Stages of Performing Automated Decision-Making Processing under GDPR in the Light of 6G Networks". In: 2020 3rd World Symposium on Communication Engineering *(*WSCE*)*. IEEE, 2020. p. 23-27.

[90]https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/can-i-be-subject-automated-individual-decision-making-including-profiling_el

[91]https://www.europarl.europa.eu/news/el/headlines/society/20190410STO36615/ta-thanatifora-trochaia-atuchimata-stin-ee-me-arithmous-grafima

[92] https://blog.spotawheel.gr/osa-prepei-na-kserete-gia-ta-autonoma-au/

[93] https://ikee.lib.auth.gr/record/302315/files/GRI-2019-23393.pdf

[94] https://en.wikipedia.org/wiki/Trolley_problem

[95] Minghao Wanga, Tianqing Zhub, Tao Zhanga, Jun Zhangc, Shui Yua and Wanlei Zhoua. "Security and privacy in 6G networks: new areas and new challenges". Digital Communications and Networks, 2020, 6.3: 281-291.

[96] Aidan Fuller, Zhong Fan, Charles Day and Chris Barlow. "Digital Twin: Enabling Technologies, Challenges and Open Research". IEEE access, 2020, 8: 108952-108971.

[97]https://www.nahb.org/advocacy/legal-issues/Smart-Home-Technology

[98]https://jolt.law.harvard.edu/digest/smart-homes-deserve-the-same-treatment-as-smartphones

[99]https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/smart-cities

[100]https://www.amnesty.gr/news/articles/article/22368/exypnes-poleis-ena-oneiro-poy-mporei-na-metatrapei-se-efialti

[101] Geffray Edouard, and Jean-Bernard Auby. "The political and legal consequences of smart cities". Interview with Edouard Geffray/Legal perspective with Jean-Bernard Auby. Field Actions Science Reports. The journal of field actions, 2017, Special Issue 16: 11-15.

[102] https://en.wikipedia.org/wiki/Smart_meter

[103]https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-2-smart-meters-smart-homes_en

[104] Yuanyuan Sun, Jiajia Liu, Jiadai Wang, Yurui Cao and Nei Kato. “When Machine Learning Meets Privacy in 6G: A Survey”. IEEE Communications Surveys & Tutorials, 2020, 22.4: 2694-2724.

[105] https://en.wikipedia.org/wiki/MHealth

[106] Pawani Porambage, Gürkan Gür, D. Osorio, Madhusanka Liyanage, A. Gurtov and M. Ylianttila. “The Roadmap to 6G Security and Privacy”. IEEE Open Journal of the Communications Society, 2021, 2: 1094-1122.

[107] Cilliers Liezel. “Wearable devices in healthcare: Privacy and information security issues”. Health information management journal 49.2-3 (2020): 150-156.

[108] Paul Greig and James Irvine. “Privacy implications of wearable health devices”. In: Proceedings of the 7th International Conference on Security of Information and Networks. 2014. p. 117-121.

[109] Kauffman Marcos E. and Marcelo Negri Soares. "New technologies and data ownership: wearables and the erosion of personality rights." Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE) 6.1 (2018): 512-538.

[110] Sandra Wachter. “Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR”. Computer law & security review, 2018, 34.3: 436-449.

[111] Fabiano Nicola. “Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation”. Athens JL, 2017, 3: 201.

[112] Alexia Dini Kounoudes and Georgia M. Kapitsaki. “A mapping of IoT user-centric privacy preserving approaches to the GDPR”. Internet of Things, 2020, 11: 100179.

[113] https://xrgo.io/en/x-reality-introduction/

[114]https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr

[115]https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality

[116]https://hellodarwin.com/blog/virtual-reality-data-collection

[117]https://www.vectornav.com/resources/inertial-navigation-articles/what-is-an-inertial-measurement-unit-imu

[118]http://psychologyinrussia.com/volumes/index.php?article=6646

[119]https://eclass.upatras.gr/modules/document/file.php/PN1441/%CE%95%CF%81%CE%B3%CE%B1%CF%83%CF%84%CE%AE%CF%81%CE%B9%CE%BF/8_Virtual_Reality.pdf

[120] Clay Viviane, König Peter, Koenig Sabine. "Eye tracking in virtual reality". Journal of Eye Movement Research, 2019, 12.1.

[121] Markopoulos Evangelos, et al. "Finger tracking and hand recognition technologies in virtual reality maritime safety training applications". In: 2020 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom). IEEE, 2020. p. 000251-000258.

[122]https://medium.com/xrlo-extended-reality-lowdown/biometrics-level-up-vr-and-provide-the-next-leap-forward-in-human-computer-interaction-293c03983f15

[123] Adams Devon, et al. "Ethics emerging: the story of privacy and security perceptions in virtual reality". In: Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018). 2018. p. 427-442.

[124]https://iapp.org/news/a/establishing-privacy-controls-for-virtual-reality-and-immersive-technology/

[125] Miller Mark Roman, et al. "Personal identifiability of user tracking data during observation of 360-degree VR video". Scientific Reports, 2020, 10.1: 1-10.

[126]https://www.techopedia.com/definition/4624/avatar

[127]https://www.dentons.com/en/insights/articles/2019/october/18/virtual-reality-top-data-protection-issues-to-consider

[128]https://er.educause.edu/articles/2018/5/securing-your-reality-addressing-security-and-privacy-in-virtual-and-augmented-reality-applications

[129]https://medium.com/@thomaswickens/virtual-reality-and-data-privacy-860aa266dd7e

[130] Bagheri Roya. "Virtual Reality: The Real Life Consequences". UC Davis Bus. LJ, 2016, 17: 101.