ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

«**ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ**»

“ARTIFICIAL INTELLIGENCE IN THE INTERNET OF THINGS”

Διπλωματική Εργασία

Της

Αφροδίτης Ζιώγου

Θεσσαλονίκη, Μάρτιος 2023

«ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

Αφροδίτη Ζιώγου

Πτυχίο Νομικής, ΑΠΘ 2012

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής: Ψάννης Κωνσταντίνος
Συνεπιβλέπουσα Καθηγήτρια: Μυλώση Μαρία

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2023

ΨΑΝΝΗΣ ΚΩΝ/ΝΟΣ	ΜΥΛΩΣΗ ΜΑΡΙΑ	ΣΤΑΥΡΙΔΟΥ ΣΥΛΒΙΑ
.....	.....	.....

Αφροδίτη Ζιώγου

Περίληψη

Καθώς η ψηφιακή τεχνολογία καθίσταται ολοένα και πιο κεντρικό στοιχείο κάθε πτυχής της ζωής, οι άνθρωποι θα πρέπει να μπορούν να την εμπιστεύονται. Η τεχνητή νοημοσύνη θεωρείται πλέον επίκεντρο του διεθνούς ανταγωνισμού. Σήμερα πάρα πολλές επιχειρήσεις χρησιμοποιούν την τεχνητή νοημοσύνη, η οποία σε συνδυασμό με τα οφέλη του Διαδικτύου των Πραγμάτων, μπορεί πραγματικά να απογειώσει την ανάπτυξή τους. Ωστόσο αυτή η ραγδαία ανάπτυξη της τεχνολογίας των πληροφοριών έχει επιτείνει ταυτόχρονα την ανάγκη για ισχυρή προστασία των δεδομένων προσωπικού χαρακτήρα, αλλά και της γενικότερης ασφάλειας των συστημάτων AI και IoT. Στο παρόν πόνημα παρουσιάζονται οι τεχνολογίες της τεχνητής νοημοσύνης και του διαδικτύου των πραγμάτων, οι κατηγορίες τους, οι τεχνολογίες με τις οποίες συνεργάζονται, συχνά παραδείγματα εφαρμογής, καθώς και τα οφέλη και οι κίνδυνοι αμφότερων των τεχνολογιών. Εν συνεχεία, γίνεται αναφορά στην τεχνητή νοημοσύνη των πραγμάτων (AIoT) και ειδικά στα οφέλη που προκύπτουν από το συνδυασμό των δύο αυτών τεχνολογιών με παρουσίαση κάποιων παραδειγμάτων πραγματικής εφαρμογής. Τέλος χαρτογραφείται το νομικό πλαίσιο που τις διέπει ιδιαίτερα από τη σκοπιά της προστασίας του δικαιώματος των προσωπικών δεδομένων σε Ευρώπη και Ελλάδα.

Λέξεις Κλειδιά: Τεχνητή Νοημοσύνη, Διαδίκτυο των Πραγμάτων, Τεχνητή Νοημοσύνη των Πραγμάτων, IoT, AIoT

Abstract

As digital technology becomes more and more a centerpiece to every aspect of life, people should be able to trust it. Artificial intelligence is now seen as the epicenter of international competition. Today too many businesses are using artificial intelligence, which combined with the benefits of the Internet of Things, can really take off their growth. However, this rapid development of information technology has simultaneously increased the need for strong protection of personal data, but also of the general security of AI and IoT systems. This paper presents AI and IoT technologies, their categories, the technologies they work with, common application examples, and the benefits and risks of both technologies. Subsequently, reference is made to the artificial intelligence of things (AIoT) and especially to the benefits arising from the combination of these two technologies with the presentation of some examples of real application. Finally, the legal framework that governs them is mapped, especially from the point of view of the protection of the right to personal data in Europe and Greece.

Keywords: Artificial Intelligence, Internet of Things, Artificial Intelligence of Things , IoT, AIoT

Πρόλογος – Ευχαριστίες

Η παρούσα Μεταπτυχιακή Διπλωματική Εργασία, με τίτλο «Τεχνητή Νοημοσύνη στο Διαδίκτυο των Πραγμάτων», πραγματοποιήθηκε στα πλαίσια της ολοκλήρωσης των σπουδών μου για τη λήψη του μεταπτυχιακού μου διπλώματος, από το Πρόγραμμα Μεταπτυχιακών Σπουδών, «Δίκαιο και Πληροφορική», του Τμήματος Εφαρμοσμένης Πληροφορικής, του Πανεπιστημίου Μακεδονίας. Σκοπός της εργασίας, η όσο το δυνατόν, τεκμηριωμένη, επιστημονικά ορθή έρευνα, βασισμένη σε βιβλιογραφικές πηγές και αρθρογραφία, για την Τεχνητή Νοημοσύνη στο Διαδίκτυο των Πραγμάτων.

Καθότι η πρώτη μου επαφή με τον τομέα των ΤΠΕ έγινε μέσω του μεταπτυχιακού προγράμματος, η παρούσα εργασία δεν θα μπορούσε να περιλαμβάνει τεχνικές λεπτομέρειες επί του θέματος. Η προσέγγισή του έγινε κυρίως από τη σκοπιά του νομικού, η οποία με οδήγησε στην αναγκαία συσχέτιση του θέματος με την παραβίαση των προσωπικών δεδομένων και τη νομοθεσία των νέων τεχνολογιών.

Ένα μεγάλο ευχαριστώ οφείλω στους καθηγητές μου και τη διευθύντρια του μεταπτυχιακού κ. Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία, οι οποίοι κατέβαλλαν κάθε δυνατή προσπάθεια να ολοκληρωθεί ο εξ αποστάσεως κύκλος των μαθημάτων εν μέσω της πανδημίας του κορωνοϊού, κάτω από ιδιαίτερες συνθήκες που κανείς μας προηγουμένως δεν είχε αντιμετωπίσει. Ιδιαίτερες ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Ψάννη Κωνσταντίνο, αλλά και τη συνεπιβλέπουσα κ. Μυλώση Μαρία, οι οποίοι με καθοδήγησαν με τις πολύτιμες συμβουλές τους όποτε χρειάστηκε κατά τη συγγραφή της παρούσας.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου και τον σύζυγό μου Πέτρο, οι οποίοι στάθηκαν δίπλα μου σε όλη αυτή τη διαδρομή και με στήριξαν με κάθε δυνατό τρόπο. Το μεγαλύτερο ευχαριστώ το οφείλω στην κόρη μου Μαρία, για την κατανόηση που έδειξε όλο το χρονικό διάστημα που αναγκάστηκα να της στερήσω πολύτιμο χρόνο με τη μητέρα της.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

1 / Εισαγωγή

Η τεχνητή νοημοσύνη είναι μια ταχέως αναπτυσσόμενη τεχνολογία που συναντάμε όλο και πιο συχνά πλέον γύρω μας, η οποία παρέχει καινοτόμες λύσεις σε πολλά και σύνθετα προβλήματα. Οι εξελιγμένες δυνατότητες που προσφέρει, μιμούμενη την ανθρώπινη συμπεριφορά, έχουν ως αποτέλεσμα να ενισχύουν και να εκσυγχρονίζουν τις λειτουργίες των συσκευών που συνδέονται στο λεγόμενο διαδίκτυο των πραγμάτων.

Ταυτόχρονα, η συλλογή μεγάλων ποσοτήτων δεδομένων έχει αυξηθεί κατακόρυφα τα τελευταία χρόνια μέσω των συσκευών IoT που χρησιμοποιούμε στην καθημερινότητά μας. Η Τεχνητή Νοημοσύνη ενισχύει τις δυνατότητες του IoT εφαρμόζοντας μηχανική εκμάθηση, κατά την οποία οι συσκευές IoT μαθαίνουν από τα δεδομένα και την εμπειρία τους, με σκοπό τη βελτίωση της λήψης αποφάσεων. Η σύγκλιση αυτή των δύο τεχνολογιών αναφέρεται ως Τεχνητή Νοημοσύνη των Πραγμάτων ή AIoT.

Υπάρχει μεγάλη μερίδα πολιτών σε όλο τον κόσμο που χρησιμοποιούν και εμπιστεύονται τις τεχνολογίες αυτές, εντούτοις δεν είναι λίγοι και εκείνοι που είτε δεν γνωρίζουν, είτε δεν κατανοούν τι ακριβώς είναι η Τεχνητή Νοημοσύνη, το Διαδίκτυο των Πραγμάτων και το AIoT. Από την άλλη, η συνεχόμενη εξέλιξη και ενσωμάτωσή τους στη ζωή μας, οφείλει να διέπεται από κανόνες, προκειμένου να αντιμετωπίζεται αποτελεσματικά το σύνολο των νομικών και ηθικών προκλήσεων που προκύπτουν από τη χρήση τους, γεγονός ιδιαίτερα περίπλοκο, αν σκεφτεί κανείς τις πιθανές συγκρούσεις μεταξύ των κανονισμών AI, IoT και GDPR. Για παράδειγμα, η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για τη λήψη αποφάσεων σχετικά με τα δεδομένα ενός ατόμου, ο GDPR όμως διασφαλίζει ότι το άτομο έχει δικαίωμα πρόσβασης και ελέγχου των δεδομένων του. Επιπλέον, η δυνατότητα της ΤΝ για πιο παρεμβατικές και στοχευμένες εκστρατείες μάρκετινγκ μπορεί να δημιουργήσει μια σύγκρουση μεταξύ των προσωπικών δικαιωμάτων απορρήτου, και της ανάγκης των επιχειρήσεων να βγάλουν κέρδος.

Τίθενται λοιπόν ερωτήματα σχετικά με το αν η τεχνητή νοημοσύνη στο διαδίκτυο των πραγμάτων συνιστά ευκαιρία ή απειλή, αφενός μεν διότι η χρήση της μπορεί να συμβάλλει μεταξύ άλλων, στην πρόληψη και αναγνώριση τυχόν επιθέσεων ή απάτης και γενικότερα στην βελτίωση της ζωής των ανθρώπων, αφετέρου διότι τα δεδομένα, στα οποία στηρίζεται η όλη ιδέα αυτών των τεχνολογιών, έχουν αποκτήσει πλέον τέτοια αξία, που για διάφορες εταιρίες, αλλά ακόμη και κυβερνοεγκληματίες είναι πρόκληση η

απόκτησή τους, εγείροντας έτσι ζητήματα ασφάλειας και ιδιωτικότητας λόγω της παραβίασής τους.

1.1 Σκοπός -Στόχοι

Στόχος της παρούσας διπλωματικής εργασίας είναι μέσα από την παρουσίαση εργασιών άλλων ερευνητών και τη στοχευμένη έρευνα, να γίνει μια περιεκτική ανάλυση των σημαντικότερων στοιχείων και πληροφοριών των δύο μεγάλων τεχνολογιών που αφορά, ήτοι της Τεχνητής Νοημοσύνης και του Διαδικτύου των Πραγμάτων, προκειμένου ο αναγνώστης, μέσα από την ανάλυση σχετικών ορισμών και την καταγραφή των κυριότερων εφαρμογών, να κατανοήσει καλύτερα τις λειτουργίες τους. Επίσης η αναφορά των οφελών καθώς και των πιθανών κινδύνων, αλλά και του νομοθετικού πλαισίου που τις διέπει, θα του επιτρέψουν να αποφασίσει, αν θα υιοθετήσει και ο ίδιος τέτοιες λύσεις στην καθημερινότητά του, γνωρίζοντας πλέον που θα πρέπει να εστιάσει, ώστε η χρήση τους να είναι όσο ασφαλέστερη γίνεται.

Σκοπός της γράφουσας είναι η δημιουργία ενός χαρτοφυλακίου που θα περιέχει όλες τις απαραίτητες πληροφορίες σχετικά με την τεχνητή νοημοσύνη και το διαδίκτυο των πραγμάτων, ξεκινώντας από το πότε εμφανίστηκαν, τι είναι και πως λειτουργούν, τι προσφέρουν και πως θα χρησιμοποιηθούν αυτές τις τεχνολογίες νόμιμα και με ασφάλεια. Έτσι, μέσα από τη συνολική παρουσίαση όλων των παραπάνω, θα δημιουργηθεί ένας πρόχειρος κατάλογος με προκλήσεις και θέματα για μελλοντική έρευνα.

1.2 Βασική Ορολογία

Προς αποφυγή ασκόπων επαναλήψεων και για λόγους συντομίας, στην παρούσα διπλωματική εργασία, λέξεις και φράσεις που επαναλαμβάνονται συχνά, εμφανίζονται με τα ακρωνύμιά τους, όπως:

IOT: Internet of Things ή στην ελληνική εκδοχή: **ΔτΠ**: Διαδίκτυο των Πραγμάτων

AI: Artificial Intelligence ή στην ελληνική εκδοχή: **ΤΝ**: Τεχνητή Νοημοσύνη

AIoT: Artificial Intelligence of Things ή στην ελληνική εκδοχή: **ΤΝτΠ**: Τεχνητή Νοημοσύνη των Πραγμάτων

GDPR: General Data Protection Regulation ή **ΓΚΠΔ**: Γενικός Κανονισμός Προστασίας Δεδομένων

1.3 Διάρθρωση της μελέτης

Η διπλωματική εργασία απαρτίζεται από 7 Κεφάλαια. Στο Κεφάλαιο 1. γίνεται μια εισαγωγή του θέματος που πραγματεύεται η παρούσα, παρουσιάζεται ο σκοπός και οι στόχοι της και γίνεται μια πρώτη αναφορά της βασικής ορολογίας, καθώς και της Μεθοδολογίας που ακολουθήθηκε για τη συγγραφή της εργασίας. Το Κεφάλαιο 2 περιέχει μια Ιστορική Αναδρομή της Τεχνητής Νοημοσύνης, τις κατηγορίες της ΤΝ, τις τεχνολογίες που χρησιμοποιεί, όπως επίσης αναφέρονται οι εφαρμογές της και σχετικά παραδείγματα, τα οφέλη της, καθώς και οι κίνδυνοι και οι προκλήσεις της ΤΝ. Αντίστοιχα, στο Κεφάλαιο 3 παρουσιάζεται μια Ιστορική Αναδρομή του Διαδικτύου των Πραγμάτων μαζί με τις κατηγορίες, και τις τεχνολογίες που χρησιμοποιεί, αναπτύσσονται οι εφαρμογές και τα παραδείγματα του ΔτΠ , τα οφέλη του, οι κίνδυνοι και οι προκλήσεις. Στη συνέχεια στο Κεφάλαιο 4 παρουσιάζεται η λεγόμενη Τεχνητή Νοημοσύνη των Πραγμάτων ή AIoT, τα οφέλη της και πραγματικά παραδείγματα εφαρμογής. Ακολουθεί το Κεφάλαιο 5 στο οποίο γίνεται αναφορά στην προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση και την Ελλάδα, ενώ στο Κεφάλαιο 6 γίνεται μια σύντομη αναφορά στο ισχύον νομοθετικό πλαίσιο εντός Ελλάδος και Ευρωπαϊκής Ένωσης. Η παρούσα διπλωματική εργασία ολοκληρώνεται με το Κεφάλαιο 7, στο οποίο αντί επιλόγου γίνεται μια σύνοψη με αναφορά στα συμπεράσματα που εξήχθησαν από τη μελέτη κατά τη συγγραφή της, καθώς και προτείνονται Μελλοντικές Επεκτάσεις σε νέους ερευνητές που θα ασχοληθούν μελλοντικά με το θέμα της Τεχνητής Νοημοσύνης στο Διαδίκτυο των Πραγμάτων.

1.4 / Μεθοδολογία

Στην προσπάθεια μια σφαιρικής και ολοκληρωμένης κάλυψης του θέματος της διπλωματικής εργασίας, αρχικά έγινε μια πρώτη έρευνα στο διαδίκτυο σχετικά με την τεχνητή νοημοσύνη και το διαδίκτυο των πραγμάτων. Στη συνέχεια πραγματοποιήθηκε αναλυτική μελέτη των ελληνικών και ξενόγλωσσων άρθρων και μελετών που συλλέχθηκαν από αναζήτηση κυρίως στις βάσεις δεδομένων Science Direct, Scopus, Google Scholar, Elsevier. Τέλος, πολλές πληροφορίες αντλήθηκαν από ελληνική και ξένη αρθρογραφία, καθώς και από τη μελέτη συγγραμμάτων νομικού περιεχομένου. Το σύνολο της νομοθεσίας παρατέθηκε από την ΤΝΠ «NOMOS» και τον ιστότοπο της ΕΕ.

2 / Τεχνητή νοημοσύνη (Artificial Intelligence)

2.1 Τι είναι η τεχνητή νοημοσύνη – Ιστορική αναδρομή

Η μελέτη του μηχανικού ή «τυπικού» συλλογισμού εγκαινιάστηκε από αρχαίους φιλοσόφους και μαθηματικούς, ιδιαιτέρως από τον George Boole[1] και τον Friedrich Ludwig Gottlob Frege[2], οι οποίοι εμπνεύστηκαν από το όνειρο του Leibniz[3] για μια καθολική «γλώσσα εννοιών» και το αρχαίο λογικό σύστημα (συλλογιστική μέθοδο) του Αριστοτέλη[4]. Ήδη από την εποχή του Ομήρου, οι άνθρωποι είχαν την ιδέα μιας μηχανής με ανθρώπινη συμπεριφορά και γνωστικές ικανότητες[5]. Στην Ηλιάδα του Ομήρου, ο κινητικά ανάπηρος Θεός Ήφαιστος, φέρεται να υποστηριζόταν από χρυσά ανθρωποειδή που ήταν προικισμένα με δύναμη, λογική και δεξιότητες, πάνω στις οποίες τους εκπαίδευσε ο ίδιος[6].

Με την πάροδο του χρόνου, η μελέτη της μαθηματικής λογικής οδήγησε απευθείας στη θεωρία υπολογισμού του Alan Turing, με την οποία ισχυριζόταν ότι, οι μηχανές μπορούν να προσομοιώσουν κάθε διαδικασία τυπικής σκέψης, γνωστή ως Thesis Turing

---

[1] Η «Μαθηματική Ανάλυση της Λογικής» από το 1847, ήταν απλά η βάση ώστε το 1854 ο Μπουλ να τελειοποιήσει τις απόψεις του περί της λογικής, δημοσιεύοντας τη Διερεύνηση των Νόμων της Σκέψης. Ο Μπουλ στηρίχθηκε στις βασικές αρχές της λογικής του Αριστοτέλη και προσπάθησε να τις συστηματοποιήσει και να επεκτείνει το φάσμα των εφαρμογών τους. Durand-Richard, MJ. (2022). «*Boole's Symbolized Laws of Thought Facing Empiricism*». In: Béziau, JY., Desclés, JP., Moktefi, A., Pascu, A.C. (eds) Logic in Question. Studies in Universal Logic. Birkhäuser, Cham. https://doi.org/10.1007/978-3-030-94452-0_6 Διαθέσιμο: https://link.springer.com/chapter/10.1007/978-3-030-94452-0_6 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[2] Ο Φρίντριχ Λούντβιχ Γκότλομπ Φρέγκε, Γερμανός μαθηματικός, λογικολόγος και φιλόσοφος, πατέρας της αναλυτικής φιλοσοφίας και της σύγχρονης λογικής, το 1879 πρότεινε ένα σύστημα αυτοματοποιημένης συλλογιστικής και έθεσε τις βάσεις του κατηγορηματικού λογισμού. Thiel, C. (2022). «*Gottlob Frege: Die Abstraktion*». In *Fregeana*. Leiden, The Netherlands: Brill | mentis. doi: https://doi.org/10.30965/9783969752654_009 Διαθέσιμο: https://brill.com/edcollchap/book/9783969752654/BP000009.xml [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[3] Ο Λάιμπνιτς υπήρξε ένας από τους σημαντικότερους επιστήμονες της λογικής, για πολλούς «ιδιοφυία». Look, Brandon C., "Gottfried Wilhelm Leibniz", *The Stanford Encyclopedia of Philosophy* (Spring 2020 Edition), Edward N. Zalta (ed.), Διαθέσιμο: https://plato.stanford.edu/archives/spr2020/entries/leibniz/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[4] Dixon Chris, «How Aristotle created the computer», Διαθέσιμο: https://www.theatlantic.com/technology/archive/2017/03/aristotle-computer/518697/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[5] Τάλως, το πρώτο ρομπότ στην ιστορία, Διαθέσιμο: http://users.sch.gr/jenyk/index.php/robotics/robotics-historicalreview/37-talos [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[6] Στη Ραψωδία Σ, στίχοι 417-420 της Ιλιάδας του Ομήρου αναφέρεται *«…και ανάλαφρα τον κύριον εστηρίζαν θεράπαινες ολόχρυσες, σαν ζωντανά κοράσια. Δύναμιν έχουν και φωνήν, νουν έχουν εις τες φρένες, και τεχνουργήματ' έμαθαν από τους αθανάτους»* http://www.mikrosapoplous.gr/iliada/BIBLIO_18_323_467.htm [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

του Church[7]. Μάλιστα το 1950, ο ίδιος ο μαθηματικός Alan Turing, πατέρας της θεωρίας υπολογισμού και προπάτορας της τεχνητής νοημοσύνης, πρότεινε το τεστ Τούρινγκ[8] μία δοκιμασία, η οποία ηδύνατο να εξακριβώσει αν μία μηχανή είναι έξυπνη[9], συμμετέχοντας απρόσκοπτα σε μια ανθρώπινη συνομιλία. Επιτυχές θα ήταν, αν από τις απαντήσεις που έδιναν οι μηχανές δεν θα μπορούσε να διαπιστώσει κάποιος ότι αυτές δεν προέρχονται από άνθρωπο.

Λίγο αργότερα, το 1956 στη διάσκεψη του Ντάρτμουθ[10], ο μαθηματικός John McCarthy όρισε για πρώτη φορά την «τεχνητή νοημοσύνη», ως την «*επιστήμη και μεθοδολογία της δημιουργίας νοούντων μηχανών*»[11], «ιδιαίτερα ευφυών προγραμμάτων υπολογιστών»[12].

Η πρώτη γενιά των ερευνητών μεταξύ των δεκαετιών 1960 και 1970 ήταν υπερβολικά αισιόδοξοι ότι εντός σύντομου χρονικού διαστήματος, θα κατάφερναν τελικά να δημιουργήσουν μια μηχανή με τεχνητή γενική νοημοσύνη[13]. Ο Χέρμπερτ Σάιμον προέβλεψε, «*οι μηχανές θα είναι ικανές, μέσα σε είκοσι χρόνια, να κάνουν οποιαδήποτε δουλειά μπορεί να κάνει ένας άνθρωπος*»[14]. Την ίδια περίοδο είχαν ξεκινήσει και σχετικές χρηματοδοτήσεις των διερευνητικών ερευνών στην τεχνητή νοημοσύνη, ωστόσο μόλις τη δεκαετία του 1970, η τεχνητή νοημοσύνη δέχτηκε επικρίσεις λόγω της αποτυχίας υλοποίησης όσων υποσχέθηκαν οι ερευνητές, που οδήγησαν στη διακοπή τους,

[7]Copeland Jack, «The Church-Turing Thesis» Διαθέσιμο: http://www.alanturing.net/turing_archive/pages/Reference%20Articles/The%20Turing-Church%20Thesis.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[8] https://www.turing.org.uk/scrapbook/test.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[9] Davenport, T. & Ronanki, R. (2018). «*Artificial Intelligence for the real world. Harvard Business Review*» Διαθέσιμο: https://www.bizjournals.com/boston/news/2018/01/09/hbr-artificial-intelligence-for-the-real-world.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[10] Στο συνέδριο μαθηματικών που πραγματοποιήθηκε το 1956 στο Dartmouth College στο Χάνοβερ των ΗΠΑ με τη συμμετοχή των Αμερικανών επιστημόνων του τομέα John McCarthy, Marvin Minsky και Claude Shannon. θεμελιώθηκε ο όρος «τεχνητή νοημοσύνη».

[11] Βόρρας Α /. Μήτρου Λ, 2018, «Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679», ΔΙΤΕ (π. ΔΙΜΕΕ), Τεύχος 4/2018

[12] *J. McCarthy, "What is AI? / Basic Questions, Professor John McCarthy / Stanford». Διαθέσιμο: http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html.* [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[13] Jiang, Y., Li, X., Luo, H. *et al.* «*Quo vadis artificial intelligence*?». *Discov Artif Intell* **2**, 4 (2022). https://doi.org/10.1007/s44163-022-00022-8 . [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[14] Simon, Herbert (1965), «*The Shape of Automation for Men and Management*» , σελ. 96

σηματοδοτώντας με αυτόν τον τρόπο, το έτος 1974 την έναρξη του λεγόμενου «πρώτου χειμώνα της τεχνητής νοημοσύνης»[15], [16].

Το τέλος της περιόδου αυτής, κατά την οποία η εξασφάλιση χρηματοδότησης για έργα τεχνητής νοημοσύνης ήταν δύσκολη, ήρθε λίγα χρόνια μετά, περίπου το 1980, με την εμπορική επιτυχία των «έμπειρων συστημάτων»[17], μια μορφή προγράμματος τεχνητής νοημοσύνης που προσομοίωσε τη γνώση και τις αναλυτικές δεξιότητες των ειδικών σε ανθρώπους. Το 1985 η αγορά για την τεχνητή νοημοσύνη είχε ξεπεράσει το ένα δισεκατομμύριο δολάρια. Ωστόσο, το 1987, μετά την αποτυχία και του Lisp Machine[18] της Symbolics, ξεκίνησε ένας δεύτερος χειμώνας για την τεχνητή νοημοσύνη που διήρκησε έως το 1993, μετά τον οποίο, και περί τα τέλη της δεκαετίας 1990 με αρχές 2000 ανέκτησε σταδιακά τη φήμη της.

Καθώς δεν υπάρχει ένας κοινά αποδεκτός ορισμός της τεχνητής νοημοσύνης, το 2019 η ομάδα Εμπειρογνωμόνων σε ζητήματα Τεχνητής Νοημοσύνης της Ευρωπαϊκής Ένωσης (AI HLEG), πρότεινε ένα ολοκληρωμένο ορισμό της Τεχνητής Νοημοσύνης ως εξής: «*Τα συστήματα τεχνητής νοημοσύνης (AI) είναι συστήματα λογισμικού (και πιθανώς και υλικού) σχεδιασμένα από ανθρώπους που, δεδομένου ενός πολύπλοκου στόχου, δρουν στη φυσική ή ψηφιακή διάσταση αντιλαμβανόμενα το περιβάλλον τους μέσω της καταγραφής δεδομένων, ερμηνεύοντας τα συλλεγμένα δομημένα ή αδόμητα δεδομένα. καταλήγοντας σε συμπεράσματα ή επεξεργαζόμενα τις πληροφορίες, που προέρχονται από αυτά τα δεδομένα και αποφασίζοντας την καλύτερη ενέργεια ή τις καλύτερες ενέργειες για την επίτευξη του δεδομένου στόχου. Τα συστήματα AI μπορούν είτε να χρησιμοποιήσουν συμβολικούς κανόνες είτε να μάθουν ένα αριθμητικό μοντέλο και μπορούν επίσης να προσαρμόσουν τη συμπεριφορά τους αναλύοντας πώς επηρεάζεται το περιβάλλον από τις προηγούμενες ενέργειές τους»*[19].

---

[15] *Crevier, Daniel (1993). «AI: The Tumultuous History of the Search for Artificial Intelligence», σελ. 100-144 Διαθέσιμο online:* *https://www.researchgate.net/publication/233820788_AI_The_Tumultuous_History_of_the_Search_for_Artificial_Intelligence [τελευταία ανάκτηση 15 Ιανουαρίου 2023]*

[16] *Russell, Stuart J .; Norvig, Peter (2010), «Artificial Intelligence: A Modern Approach» (3rd Edition), σελ 21-22. Διαθέσιμο online:* *http://repo.darmajaya.ac.id/3800/1/Artificial%20Intelligence%20A%20Modern%20Approach%20%283rd%20Edition%29.pdf%20%28%20PDFDrive%20%29.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]*

[17] Lindsay RK, Buchanan BG, Feigenbaum EA, Lederberg J. «*DENDRAL: a case study of the first expert system for scientific hypothesis formation*». Artif Intell. 1993;61(2):209–61. Διαθέσιμο: https://www.sciencedirect.com/science/article/abs/pii/000437029390068M [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[18] Kim, H. (2022). «*Historical Sketch of Artificial Intelligence. In: Artificial Intelligence for 6G».* Springer, Cham., pp 3–14 https://doi.org/10.1007/978-3-030-95041-5_1 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[19]*AI HLEG (2019)* A Definition of AI: Main Capabilities and Disciplines. *Διαθέσιμο:*

Στο Αγγλικό Λεξικό της Οξφόρδης, δίπλα στο λήμμα «Artificial intelligence»[20], ορίζεται ότι τεχνητή νοημοσύνη είναι «η *ικανότητα των υπολογιστών ή άλλων μηχανών να επιδεικνύουν ή να προσομοιώνουν έξυπνη συμπεριφορά, το πεδίο σπουδών που αφορά αυτό*».

Η Encyclopædia BRITANNICA αναφέρει ότι «*τεχνητή νοημοσύνη είναι η ικανότητα ενός υπολογιστή ή ενός ρομπότ που ελέγχεται από έναν υπολογιστή να κάνει εργασίες που συνήθως εκτελούνται από ανθρώπους επειδή απαιτούν ανθρώπινη νοημοσύνη και διάκριση. Αν και δεν υπάρχει τεχνητή νοημοσύνη που να μπορεί να εκτελέσει τη μεγάλη ποικιλία εργασιών που μπορεί να κάνει ένας συνηθισμένος άνθρωπος, ορισμένη τεχνητή νοημοσύνη μπορεί να ταιριάζει με ανθρώπους σε συγκεκριμένες εργασίες*».[21] Έχουσα λοιπόν ως στόχο την μίμηση της ανθρώπινης ευφυΐας, η τεχνητή νοημοσύνη για να λειτουργήσει, απαιτεί το συνδυασμό πολλών επιστημών, όπως η πληροφορική, η ψυχολογία, η φιλοσοφία, η γλωσσολογία. Σήμερα πλέον η χρήση της είναι διαδεδομένη σε όλη τη βιομηχανία της τεχνολογίας, χάρη στην αύξηση ισχύος του υπολογιστή, αλλά και στην πιο εστιασμένη αντιμετώπιση των προβλημάτων, που πραγματοποιήθηκε με συνεργασία με άλλους τομείς, όπως η στατιστική, η οικονομία και τα μαθηματικά.

Η τεχνητή νοημοσύνη είναι η επιστήμη της ενστάλαξης νοημοσύνης στις μηχανές, έτσι ώστε να είναι σε θέση να κάνουν εργασίες που παραδοσιακά απαιτούσαν το ανθρώπινο μυαλό. Τα συστήματα που βασίζονται στην τεχνητή νοημοσύνη εξελίσσονται με ταχείς ρυθμούς όσον αφορά την εφαρμογή, την προσαρμογή, την ταχύτητα επεξεργασίας και τις δυνατότητες. Οι μηχανές γίνονται όλο και πιο ικανές να αναλαμβάνουν λιγότερο συνηθισμένες εργασίες. Ενώ η ανθρώπινη νοημοσύνη στην πραγματικότητα «λαμβάνει» μια τέλεια απόφαση την κατάλληλη στιγμή, η τεχνητή νοημοσύνη αφορά απλώς την «επιλογή» μιας σωστής απόφασης την κατάλληλη στιγμή (Ghosh et al., 2018)[22].

Σύμφωνα με την αποσαφήνιση του όρου της ΤΝ που περιλαμβάνεται στη Λευκή Βίβλο για την ΤΝ, τα κύρια στοιχεία σύνθεσής της είναι τα δεδομένα και οι αλγόριθμοι.

---

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341,[τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[20] https://www.oed.com/viewdictionaryentry/Entry/271625 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[21]Copeland, B.J.. "artificial intelligence". *Encyclopedia Britannica*, 11/11/2022, Διαθέσιμο: https://www.britannica.com/technology/artificial-intelligence [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[22] Ghosh, A., Chakraborty, D. and Law, A. (2018), *«Artificial intelligence in Internet of things»*. CAAI Trans. Intell. Technol., 3: 208-218 https://doi.org/10.1049/trit.2018.1008 Διαθέσιμο: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/trit.2018.1008 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Η τεχνητή νοημοσύνη δύναται να ενσωματωθεί στο υλισμικό και να χρησιμοποιηθεί για την εκπαίδευση αλγορίθμων να συνάγουν μοτίβα από δεδομένα προκειμένου να επιτευχθεί ένας συγκεκριμένος στόχος. Αυτοί οι αλγόριθμοι συνεχίζουν να μαθαίνουν ενώ χρησιμοποιούνται και ενώ τα προϊόντα που βασίζονται σε τεχνητή νοημοσύνη μπορούν να ενεργούν αυτόνομα, η συμπεριφορά τους καθορίζεται σε μεγάλο βαθμό από τους προγραμματιστές τους, οι οποίοι θέτουν τους στόχους για τη βελτιστοποίηση του συστήματος[23].

Διάφοροι τομείς όπως η φιλοσοφία, η επιστήμη των υπολογιστών, τα μαθηματικά, η στατιστική, η βιολογία, η φυσική, η κοινωνιολογία, η ψυχολογία και πολλοί άλλοι έχουν συγκεντρωθεί για να ενισχύσουν τη διεπιστημονική φύση της τεχνητής νοημοσύνης. Η νοημοσύνη προέρχεται από όλα τα δεδομένα που παράγονται σε καθέναν από αυτούς τους τομείς. Η ανάλυση αυτών των δεδομένων είναι σημαντική για να αναδείξει τις αρχές πίσω από αυτήν. Ο ανθρώπινος εγκέφαλος είναι ικανός να το κάνει εύκολα, αλλά χρειάζεται πολύ χρόνο (Ghosh et al., 2018), λόγω του τεράστιου όγκου τους, της αδόμητης φύσης τους, των ποικίλων πηγών προέλευσής τους, αλλά και της συνεχούς μεταβολής τους.

Αξίζει να σημειωθεί ότι το πρώτο έργο που αναγνωρίζεται ευρέως ως τεχνητή νοημοσύνη, είναι οι «τεχνητοί νευρώνες» των Warren McCullouch and Walter Pitts' το 1943[24], οι οποίοι μπορούσαν να μαθαίνουν και να υπολογίζουν κάθε συνάρτηση.

2.2 Κατηγορίες της τεχνητής νοημοσύνης

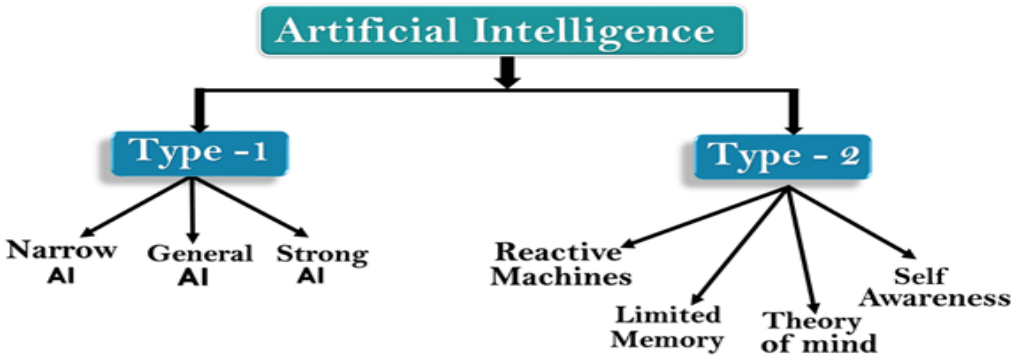
Η Τεχνητή Νοημοσύνη μπορεί να χωριστεί σε διάφορους τύπους. Η κύρια κατηγοριοποίηση γίνεται με βάση τις δυνατότητες ή με βάση τα λειτουργικά της τεχνητής νοημοσύνης. Γενικά, η τεχνητή νοημοσύνη που εκτελεί περισσότερες ανθρώπινες λειτουργίες με ισοδύναμα επίπεδα επάρκειας θεωρείται ως πιο εξελιγμένος τύπος τεχνητής νοημοσύνης, ενώ μια τεχνητή νοημοσύνη που έχει περιορισμένη λειτουργικότητα και απόδοση θεωρείται απλούστερος και λιγότερο εξελιγμένος τύπος[25].

---

[23] «Λευκή Βίβλος για την ΤΝ», σελ 20-21, Διαθέσιμο: https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[24] McCulloch, W.S., Pitts, W. «*A logical calculus of the ideas immanent in nervous activity*. *Bulletin of Mathematical Biophysics*» 5, 115–133 (1943) Διαθέσιμο: https://link.springer.com/article/10.1007/BF02478259#citeas *[*τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[25]https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=716dee29233e [τελευταία ανάκτηση 15 Ιανουαρίου 2023]



Εικόνα 1: Τύποι και κατηγορίες της τεχνητής νοημοσύνης

Πηγή: javatpoint.com

Ο τύπος 1 υποδιαιρείται σε τρεις κατηγορίες (Berryhill J. et al 2019, Bostrom N. 2014, Carriço Z. 2018, OECD 2019)[26]:

- **Τεχνητή Στενή Νοημοσύνη ή ασθενής νοημοσύνη (Artificial Narrow Intelligence – ANI**) αφορά συστήματα τεχνητής νοημοσύνης που σχεδιάστηκαν για να εκτελέσουν μια αποκλειστική εργασία με ευφυία. Παραδείγματα ANI είναι η αναγνώριση ομιλίας ή εικόνας, τα αυτοοδηγούμενα αυτοκίνητα, όπως και ο εικονικός βοηθός Apple Siri.

- **Τεχνητή Γενική Νοημοσύνη (Artificial General Intelligence - AGI)** αναφέρεται σε μηχανές που είναι έξυπνες όπως ο άνθρωπος, ικανές να εκτελέσουν πνευματική εργασία όπως ο άνθρωπος. Δεν υπάρχει παράδειγμα, καθώς είναι σε ερευνητικό στάδιο ακόμα η δημιουργία τέτοιων συστημάτων μηχανικής αναπαράστασης των διαδικασιών που συμβαίνουν στον ανθρώπινο εγκέφαλο από τους επιστήμονες του τομέα. Και αυτό διότι είναι εξαιρετικά δύσκολο τεχνικά να προσομοιωθεί με ακρίβεια ο ανθρώπινος εγκέφαλος, καθώς για την επίτευξη του σκοπού αυτού απαιτείται ένας ισχυρός υπολογιστής, δεδομένου ότι ο εγκέφαλος ενός ανθρώπου διαθέτει δισεκατομμύρια συνδέσεις νευρώνων που λέγονται συνάψεις. Κάθε νευρώνας έχει κατά μέσο όρο 7.000 συνδέσεις με άλλους νευρώνες και υπολογίζεται ότι ο εγκέφαλος μπορεί να επεξεργαστεί

[26] https://www.javatpoint.com/types-of-artificial-intelligence [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

100 τρισεκατομμύρια συναπτικές ενημερώσεις ανά δευτερόλεπτο. Οι υπερυπολογιστές εκτιμάται ότι μόλις τώρα φτάνουν στο ίδιο επίπεδο υπολογιστικών δυνατοτήτων με τον ανθρώπινο εγκέφαλο[27].

- **Τεχνητή Υπερ-Νοημοσύνη (Artificial Super- Intelligence - ASI)** περιλαμβάνει τα συστήματα που ξεπερνούν την ανθρώπινη νοημοσύνη και μπορούν να εκτελέσουν οποιαδήποτε εργασία καλύτερα από τον άνθρωπο με γνωστικές ιδιότητες, χάρη στη συντριπτικά αυξημένη μνήμη που διαθέτουν, στη δυνατότητα ταχύτερης επεξεργασίας, καθώς και ανάλυσης δεδομένων και των δυνατοτήτων λήψης αποφάσεων. Προφανώς είναι μια υποθετική έννοια της τεχνητής νοημοσύνης, καθώς πιθανολογείται ότι η ανάπτυξη τέτοιων συστημάτων ενδεχομένως να απειλήσει αν όχι την ανθρωπότητα, τουλάχιστον τον τρόπο ζωής.

Ο τύπος 2 υποδιαιρείται σε τέσσερις κατηγορίες[28]:

- **Αντιδραστικές μηχανές (Reactive Machines)**

  Το πρώτο είδος τεχνητής νοημοσύνης είναι οι αντιδραστικές μηχανές (Jackson, 2019). Αφορά τις παλαιότερες μορφές συστημάτων τεχνητής νοημοσύνης, με εξαιρετικά περιορισμένες δυνατότητες, αφού μια τέτοια συσκευή είναι προγραμματισμένη να ανταποκρίνεται πάντα σε παρόμοιες καταστάσεις με τον ίδιο ακριβώς τρόπο κάθε φορά, μη δυνάμενη να αποθηκεύει μνήμες ή προηγούμενες εμπειρίες για μελλοντικές ενέργειες. Από τα πιο γνωστά παραδείγματα αντιδραστικής μηχανής AI είναι το Deep Blue της IBM , ένα μηχάνημα που κέρδισε τον Grandmaster του σκακιού Garry Kasparov το 1997[29].

[27] Κιρίκος Ε. «Γενική Τεχνητή Νοημοσύνη, Τι είναι», Διαθέσιμο: https://www.athinodromio.gr/γενική-τεχνητή-νοημοσύνη-τι-είναι/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[28] Marr Bernard, «*Understanding the 4 types of Artificial Intelligence*» Διαθέσιμο: https://bernardmarr.com/understanding-the-4-types-of-artificial-intelligence/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[29] Ο περιορισμένης νοημοσύνης υπολογιστής Deep Blue της IBM κατάφερε να νικήσει τον παγκόσμιο πρωταθλητή σκάκι Γκάρι Κασπάροφ, όντας σχεδιασμένος για αυτό μόνο: να νικήσει τον αντίπαλο στο παιχνίδι σκάκι.

- **Περιορισμένη μνήμη (Limited memory)**

  Οι περιορισμένης μνήμης μηχανές μπορούν να ανακαλέσουν προηγούμενα γεγονότα και να βασιστούν σε αυτές τις αναμνήσεις για να πληροφορηθούν κρίσεις σχετικά με το μέλλον (Jackson, 2019). Παράδειγμα εφαρμογής αυτής της κατηγορίας τεχνητής νοημοσύνης, είναι τα chatbots, οι εικονικοί βοηθοί και τα αυτοοδηγούμενα οχήματα.

- **Θεωρία του Νου (Theory of mind)**

  Πρόκειται για το επόμενο επίπεδο συστημάτων τεχνητής νοημοσύνης, που θα πρέπει να κατανοεί τα ανθρώπινα συναισθήματα, τους ανθρώπους, τις πεποιθήσεις και θα μπορεί να αλληλεπιδρά κοινωνικά όπως οι άνθρωποι.

- **Αυτογνωσία (Self awareness)**

  Η ανάπτυξη της Τεχνητής Νοημοσύνης που μπορεί να κατανοήσει και να προκαλέσει συναισθήματα είναι ακόμα μακριά. Αυτός ο τύπος τεχνητής νοημοσύνης θα έχει τα δικά του συναισθήματα, ανάγκες, πεποιθήσεις και πιθανώς επιθυμίες. Θα μπορούσε να είναι τόσο προηγμένο που να ξεπερνά την ανθρώπινη νοημοσύνη και ενδεχομένως να καταλάβει την ανθρωπότητα.

2.3 Τεχνολογίες της Τεχνητής Νοημοσύνης

Στους τομείς της επιστήμης των υπολογιστών και της τεχνολογίας, η Τεχνητή Νοημοσύνη αποτελεί τη βάση για έναν σημαντικό αριθμό σημαντικών εννοιών. Τα θέματα αυτά αναφέρονται με λέξεις όπως μηχανική μάθηση, βαθιά μάθηση, ρομπότ, όραση υπολογιστών, διαδίκτυο, συστήματα συστάσεων και επεξεργασία φυσικής γλώσσας (Ashley, 2017- Jackson, 2019 – Πράσσος, 2022).

Εικόνα 2: 6 βασικοί κλάδοι της ΤΝ

Πηγή: analyticssteps.com/

Αναλυτικά οι 6 αυτοί βασικοί κλάδοι της τεχνητής νοημοσύνης είναι[30]:

1. Ο όρος **μηχανική μάθηση ή machine learning** αναφέρεται στην τεχνική που δίνει την δυνατότητα στους υπολογιστές να μαθαίνουν χωρίς να είναι προγραμματισμένοι[31]. Βασικός στόχος της Μηχανικής Μάθησης είναι η δημιουργία μοντέλων ή προτύπων από ένα σύνολο δεδομένων, τα οποία ονομάζονται δεδομένα εκπαίδευσης. Τα μοντέλα αυτά χρησιμοποιούνται για επίλυση διάφορων τύπων προβλημάτων, όπως ομαδοποίηση δεδομένων, παλινδρόμησης, πρόβλεψης και άλλα. Η επιστήμη των δεδομένων είναι άρρηκτα συνδεδεμένη με τη μηχανική μάθηση (Schmidt et al., 2019). Σύμφωνα με τον Acemoglu, η μηχανική μάθηση θα επιτρέψει στους υπολογιστές να μαθαίνουν αυτόματα μια ποικιλία πραγμάτων χωρίς τη βοήθεια του ανθρώπου (Restrepo, 2018 – Πράσσος, 2022). Η μηχανική μάθηση μπορεί να χωριστεί σε τρεις κατηγορίες: εποπτευόμενη μάθηση, μάθηση χωρίς επίβλεψη και διαδοχική μάθηση. Ο στόχος στην εποπτευόμενη μάθηση είναι η επισήμανση νέων παρατηρήσεων. Η μάθηση χωρίς επίβλεψη

[30] Neelam Tyagi, 6 Major Branches of Artificial Intelligence (AI), Διαθέσιμο: https://www.analyticssteps.com/blogs/6-major-branches-artificial-intelligence-ai [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[31] Το 1959 ο Άρθουρ Σάμουελ έδωσε τον παρακάτω ορισμό για τη μηχανική μάθηση: "*Πεδίο μελέτης που δίνει στους υπολογιστές την ικανότητα να μαθαίνουν, χωρίς να έχουν ρητά προγραμματιστεί*".

προσδιορίζει υποκείμενες σχέσεις ή πρότυπα. Στη διαδοχική μάθηση, οι αλγόριθμοι χρησιμοποιούν επανειλημμένα εξωτερικές παρατηρήσεις για να επιτύχουν τη βέλτιστη απόφαση σχετικά με το περιβάλλον στο οποίο αλληλεπιδρούν (Stergiou et al., 2022)[32]

2. Τα **Νευρωνικά Δίκτυα ή Neural Networks** αποτελούν ένα σύνολο αλγορίθμων σχεδιασμένο να εντοπίζει βασικές συνδέσεις μεταξύ ομάδων δεδομένων, αναπαράγοντας τον τρόπο που λειτουργεί ο ανθρώπινος εγκέφαλος.

3. Η **ρομποτική ή Robotics** είναι κλάδος της ΤΝ που εστιάζει στην ανάπτυξη, παραγωγή, λειτουργία και χρήση ρομπότ. Περιλαμβάνει τη χρήση συστημάτων υπολογιστών για τον έλεγχο των ρομπότ, την παραγωγή έξυπνων αποτελεσμάτων και την επεξεργασία δεδομένων.

4. Τα **Συστήματα Εμπειρογνωμόνων ή Expert Systems**, τα οποία είναι εξειδικευμένα υπολογιστικά συστήματα ικανά να μιμούνται την ανθρώπινη νοημοσύνη κατά τη διαδικασία λήψης αποφάσεων. Όσο περισσότερες πληροφορίες και δεδομένα συλλέγει, τόσο μεγαλύτερη είναι η αποτελεσματικότητά του.

5. Η **Ασαφής Λογική ή Fuzzy Logic** είναι μια τεχνική που χρησιμοποιείται για την αναπαράσταση και την τροποποίηση αβέβαιων πληροφοριών. Λειτουργεί με τη μέτρηση του βαθμού στον οποίο μια υπόθεση είναι σωστή, με βάση τα διαθέσιμα δεδομένα, επιτρέποντας την πραγματοποίηση ακριβέστερων προβλέψεων, χάρη στη συνεχή ενημέρωση και βελτίωση των δεδομένων.

6. Η **Επεξεργασία φυσικής γλώσσας ή natural languange processing** είναι ένας κλάδος της επιστήμης των υπολογιστών και της τεχνητής

[32] K. D. Stergiou, G. M. Minopoulos, V. A. Memos, C. L. Stergiou, M. P. Koidou, K. E. Psannis, "A Machine Learning-based Model for Epidemic Forecasting and Faster Drug Discovery", MDPI, Applied Sciences, vol. 12, issue: 21, October 2022. [DOI: 10.3390/app122110766] Διαθέσιμο: https://www.mdpi.com/2076-3417/12/21/10766 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

νοημοσύνης που επιτρέπει στους υπολογιστές να κατανοούν και να επικοινωνούν με τους ανθρώπους χρησιμοποιώντας τη φυσική γλώσσα. Είναι μια τεχνική υπολογιστικής επεξεργασίας ανθρώπινων γλωσσών, που επιτρέπει σε έναν υπολογιστή να διαβάζει και να ερμηνεύει δεδομένα μιμούμενος τον τρόπο που οι άνθρωποι χρησιμοποιούν τη φυσική γλώσσα.

2.4 Εφαρμογές Τεχνητής Νοημοσύνης και παραδείγματα

Εικόνα 3: Παραδείγματα χρήσης τεχνητής νοημοσύνης

Πηγή: europarl.europa.eu/

Σήμερα όλο και περισσότερο στην καθημερινότητα μας συναντάμε την τεχνητή νοημοσύνη, σε διάφορες εφαρμογές. Σύμφωνα με το Statista, τα έσοδα από την αγορά λογισμικού τεχνητής νοημοσύνης παγκοσμίως αναμένεται να φτάσουν τα 126 δισεκατομμύρια δολάρια μέχρι το 2025[33].

Τεχνολογίες τεχνητής νοημοσύνης όπως είναι τα συστήματα ανάγνωσης πινακίδων της αστυνομίας, ή οι εικονικοί βοηθοί στα κινητά μας, μέχρι την πραγματική

[33]«Revenues from the artificial intelligence (AI) software market worldwide from 2018 to 2025» https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

τεχνητή νοημοσύνη που σώζει ζωές, βοηθώντας στην ενεργοποίηση μηχανισμών ασφαλείας (αυτόματο φρενάρισμα σε αυτοκίνητα ή ακόμα και οχήματα με αυτοοδήγηση) είναι ήδη ενσωματωμένες στο λογισμικό και το υλικό γύρω μας. Η πραγματική τεχνητή νοημοσύνη μάς βοηθά να βελτιστοποιούμε τις διαδικασίες ή να προβλέψουμε αστοχίες, βελτιώνοντας την αποτελεσματικότητα και μειώνοντας τα περιβαλλοντικά απόβλητα. Ο μόνος λόγος για τον οποίο υπάρχουν εκατοντάδες εταιρείες τεχνητής νοημοσύνης και χιλιάδες ερευνητές και μηχανικοί μελετούν σε αυτόν τον τομέα, είναι επειδή στοχεύουν στην παραγωγή λύσεων που βοηθούν τους ανθρώπους και βελτιώνουν τη ζωή μας (Richardson, 2017) [34].

Σε μια έρευνα της εταιρίας Boston Consulting Group (BCG) σε συνεργασία με την Microsoft που διεξήχθη στην Ελλάδα με τον τίτλο «Harnessing the Power of AI in Greece. Embarking on the path to value» δηλαδή «Αξιοποιώντας την δύναμη της τεχνητής νοημοσύνης στην Ελλάδα», της οποίας τα αποτελέσματα δημοσιεύτηκαν τον Σεπτέμβριο του 2020[35], διαπιστώθηκε ότι τουλάχιστον 35 ελληνικές επιχειρήσεις εφαρμόζουν την τεχνητή νοημοσύνη, μεταξύ των οποίων είναι η COSMOTE, EUROBANK, ΕΛΛΗΝΙΚΑ ΠΕΤΡΕΛΑΙΑ, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, ΠΑΠΑΣΤΡΑΤΟΣ, ΤΡΑΠΕΖΑ ΠΕΙΡΑΙΩΣ, TITAN ΤΣΙΜΕΝΤΑ, VODAFONE κ.α. με σκοπό έκαστη εξ αυτών να μειώσουν το κόστος λειτουργίας και παραγωγής, και να βελτιώσουν την παροχή υπηρεσιών προς τους πελάτες τους.

Μια αξιόλογη περίπτωση εφαρμογής ΤΝ είναι της εταιρίας Deepmind AI της Google, στην οποία θα πρέπει να γίνει ιδιαίτερη αναφορά. Συγκεκριμένα, τον περασμένο χρόνο παρουσίασε το «*ITHACA*»[36], ένα βαθύ νευρωνικό δίκτυο για την κειμενική αποκατάσταση, τη γεωγραφική απόδοση και τη χρονολογική απόδοση αρχαιοελληνικών επιγραφών[37], με ένα από τα πρώτα της αποτελέσματα να απεικονίζεται στην εικόνα 4.

---

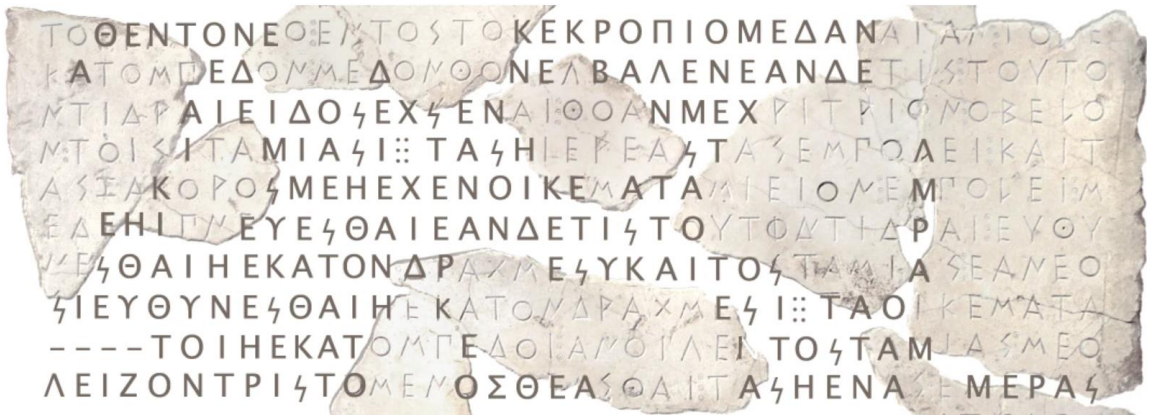
[34] Peter J. Bentley, «*Should we fear artificial intelligence? – In depth analysis*», European Parliament, European Parliamentary research service, STOA, March 2018, σελ. 6 Διαθέσιμο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA%282018%29614547_EN.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[35] Chryssos Kavounides, Markos Giakoumelos, Evdokia Kaffe, «*Harnessing the Power of AI in Greece. Embarking on the path to value*» Διαθέσιμο: https://web-assets.bcg.com/93/be/5ac6b7ff4d698947da09681332db/harnessing-the-power-web-final.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[36]Οποιοσδήποτε μπορεί να δοκιμάσει το ITHACA στο σύνδεσμο: https://ithaca.deepmind.com/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[37] Assael, Y., Sommerschield, T., Shillingford, B. et al., «*Restoring and attributing ancient texts using deep neural networks*», Nature 603, 280–283 (2022). Διαθέσιμο: https://doi.org/10.1038/s41586-022-04448-z [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Με μοντέλα όπως η Ιθάκη, τεχνητή νοημοσύνη και ιστορικοί μπορούν να συνεργαστούν, επηρεάζοντας μεταμορφωτικά τον τρόπο με τον οποίο μελετάμε και γράφουμε για μια από τις πιο σημαντικές περιόδους της ανθρώπινης ιστορίας.



Εικόνα 4: Αποκατάσταση κατεστραμμένης επιγραφής με το νευρωνικό δίκτυο ITHAKA

Πηγή: ithaca.deepmind.com

2.4.1 Υγεία και Ιατρική

Η τεχνητή νοημοσύνη στον ιατρικό τομέα είναι σε θέση να εκτελεί εργασίες γρήγορα και με χαμηλότερο κόστος, καθώς εφαρμόζεται με τη χρήση μοντέλων μηχανικής μάθησης για την εξαγωγή, την ενσωμάτωση και την ανάλυση μη δομημένων και ασυνεπών δεδομένων ασθενών για ακριβέστερες και ταχύτερες προβλέψεις και καλύτερες κλινικές αποφάσεις. Επίσης, ενσωματώνεται με μοντέλα που βασίζονται στη φυσική και μοντέλα που βασίζονται σε δεδομένα, και χρησιμοποιείται για την υποκατάσταση των χειρουργών και την παροχή ακριβών χειρουργικών επεμβάσεων (Minopoulos et al., 2022)[38]. Πλέον η εφαρμογή της στον ιατρικό τομέα αποτελεί αναπόσπαστο μέρος της σύγχρονης υγειονομικής περίθαλψης με χρήση αλγόριθμων τεχνητής νοημοσύνης για την υποστήριξη των ιατρικών επαγγελματιών σε κλινικά περιβάλλοντα και σε συνεχή έρευνα[39].

Χαρακτηριστικό παράδειγμα τέτοιου AI αλγορίθμου είναι ο Naïve Bayes, ένας από τους πιο αποτελεσματικούς αλγόριθμους μηχανικής μάθησης για ταξινόμηση. Βασίζεται

[38] Minopoulos GM, Memos VA, Stergiou CL, Stergiou KD, Plageras AP, Koidou MP, Psannis KE. «*Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System*». *Applied Sciences*. 2022; 12(12):5859. https://doi.org/10.3390/app12125859 Διαθέσιμο: https://www.mdpi.com/2076-3417/12/12/5859 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[39] https://www.ibm.com/topics/artificial-intelligence-medicine [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

στο θεώρημα του Bayes με την υπόθεση της ισχυρής ανεξαρτησίας μεταξύ των παρατηρούμενων χαρακτηριστικών. Επί του παρόντος χρησιμοποιείται για ταξινόμηση ιατρικών δεδομένων και πρόβλεψη ασθενειών[40].

Ενδεικτικά στον τομέα της υγείας, η χρήση της τεχνητής νοημοσύνης, μεταξύ άλλων προσφέρει και τα εξής οφέλη[41]:

- Τα εργαλεία που κατασκευάζονται με βάση την τεχνητή νοημοσύνη βοηθούν στην αναγνώριση της ασθένειας από την οποία πάσχει το άτομο σε προγενέστερο στάδιο. Χαρακτηριστική περίπτωση η έγκαιρη αναγνώριση του καρκίνου (προσυμπτωματικός έλεγχος καρκίνου)[42].

- Οι ρομποτικοί χειρουργοί σε λεπτές χειρουργικές επεμβάσεις μπορούν λόγω της τεχνητής νοημοσύνης να χειρουργήσουν με μεγαλύτερη ακρίβεια έναν ασθενή, καθώς και να προσφέρουν τρισδιάστατη μεγέθυνση του σημείου εγχείρησης[43].

- Η τεχνητή νοημοσύνη έχει τη δυνατότητα να αποθηκεύει όλες τις πληροφορίες των ασθενών με οργανωμένο τρόπο για να έχει μια καλύτερη και σαφέστερη εικόνα όλων των λεπτομερειών τους και μπορεί να αναλύσει αυτά τα δεδομένα πολύ πιο γρήγορα από οποιονδήποτε άνθρωπο, συμπεριλαμβανομένων κλινικών μελετών, ιατρικών αρχείων και γενετικών πληροφοριών που μπορούν να βοηθήσουν τους επαγγελματίες γιατρούς να

[40] https://www.turing.com/kb/an-introduction-to-naive-bayes-algorithm-for-beginners [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[41] Sai dyuti Vaishnavi Vaddiparthi, ADVANTAGES OF AI IN THE MODERN WORLD, (2021), διαθέσιμο: https://www.researchgate.net/publication/348687836_ADVANTAGES_OF_AI_IN_THE_MODERN_WORLD [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[42] Στο Πανεπιστήμιο Tulane, μια ομάδα ερευνητών χρησιμοποίησε τεχνητή νοημοσύνη για να αναλύσει σαρώσεις ιστών για να επιταχύνει τη διαδικασία διάγνωσης του καρκίνου. Η έρευνα περιελάμβανε τη συλλογή 13.000 εικόνων καρκίνου του παχέος εντέρου από περισσότερα από 8.000 άτομα από ανεξάρτητα ιατρικά κέντρα που βρίσκονται στην Ασία, την Ευρώπη και τις Ηνωμένες Πολιτείες. Ανέπτυξαν ένα μοντέλο μηχανικής μάθησης που σημείωσε μεγαλύτερη ακρίβεια στη διάγνωση από τους ανθρώπινους γιατρούς. https://news.tulane.edu/pr/tulane-university-study-uses-artificial-intelligence-detect-colorectal-cancer [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[43] Χειρουργοί στο Ιατρικό Κέντρο του Πανεπιστημίου του Μάαστριχτ, Κάτω Χώρες, χρησιμοποίησαν ρομποτική υποβοηθούμενη από AI για να ράψουν πολύ στενά αιμοφόρα αγγεία από 0,03 έως ,08 mm. https://www.maastrichtuniversity.nl/news/world%E2%80%99s-first-super-microsurgery-operation-%E2%80%98robot-hands%E2%80%99 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

έρθουν σε διάγνωση ή να προβούν σε προσομοίωση περιβάλλοντος για πρόβλεψη ιατρικών αποτελεσμάτων[44].

- Στα πλαίσια γήρανσης του πληθυσμού της Ευρώπης, η ρομποτική και η ΤΝ συνιστούν πολύτιμα εργαλεία για τη συνδρομή των παρόχων φροντίδας[45], την υποστήριξη της φροντίδας των ηλικιωμένων και την παρακολούθηση της κατάστασης των ασθενών σε πραγματικό χρόνο[46], σώζοντας ζωές (AI HLEG, 2019).

2.4.2 Χρηματοοικονομικές Επιχειρήσεις – Αυτοκινητοβιομηχανία-Εφοδιαστική Αλυσίδα – Επιχειρήσεις Λιανικής

Η τεχνητή νοημοσύνη στις χρηματοοικονομικές επιχειρήσεις μπορεί να προσφέρει ασφάλεια κατά πιθανών περιστατικών απάτης, αλλά και βελτιστοποίηση των διαδικασιών μέσω του αυτοματισμού.

Στις εταιρίες της λεγόμενης εφοδιαστικής αλυσίδας, η ΤΝ μπορεί να βελτιώσει τη διαδικασία διαχείρισης αποθεμάτων, των μεταφορών και των παραδόσεων.

Όσον αφορά τις αυτοκινητοβιομηχανίες όπως η Volvo, Toyota, Audi και Tesla, χρησιμοποιούν μηχανική μάθηση για να μαθαίνουν στους υπολογιστές που τοποθετούν στα αυτοκίνητα παραγωγής τους να σκέφτονται σαν άνθρωποι. Η δυσκολία σε αυτό το εγχείρημα είναι πολύ μεγαλύτερη διότι, το αυτοκίνητο καλείται σε πραγματικές συνθήκες να αποφεύγει εμπόδια ώστε να μην γίνονται ατυχήματα και να ακολουθεί τους κανόνες του κώδικα οδικής κυκλοφορίας.

Ωστόσο η χρήση της τεχνητής νοημοσύνης στον τομέα της αυτοκινητοβιομηχανίας έχει τα εξής οφέλη:

- Ασφάλεια: Η τεχνητή νοημοσύνη μπορεί να βοηθήσει να γίνουν τα οχήματα ασφαλέστερα μειώνοντας τα ατυχήματα και βελτιώνοντας την ασφάλεια του οδηγού.
- Αποδοτικότητα: Η τεχνητή νοημοσύνη μπορεί να συμβάλει στη βελτίωση της απόδοσης καυσίμου και στη μείωση των εκπομπών.

---

[44] https://www.maastrichtuniversity.nl/news/artificial-intelligence-chooses-best-treatment-option-breast-cancer [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[45] http://caressesrobot.org/en/project/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[46] www.myhealthavatar.eu [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

- Απόδοση: Η τεχνητή νοημοσύνη μπορεί να βοηθήσει στη βελτίωση της απόδοσης του οχήματος βελτιστοποιώντας την απόδοση του κινητήρα
- Κόστος: Η τεχνητή νοημοσύνη μπορεί να βοηθήσει στη μείωση του κόστους κατασκευής και επισκευής οχημάτων.
- Ικανοποίηση πελατών: Η τεχνητή νοημοσύνη μπορεί να βοηθήσει στη βελτίωση της ικανοποίησης των πελατών[47].

Τέλος, στις επιχειρήσεις λιανικού εμπορίου δεδομένα που λαμβάνονται από κάμερες και αισθητήρες του χώρου, μπορούν να χρησιμοποιηθούν για την παρακολούθηση των κινήσεων των πελατών και την πρόβλεψη πότε θα φτάσουν στη γραμμή ταμείου, το οποίο μπορεί να φανεί χρήσιμο κατά τη στελέχωση του προσωπικού, αλλά και τη λιγότερο χρονοβόρα εξυπηρέτηση στα ταμεία.

2.4.3 Έξυπνες κατοικίες, πόλεις και δημόσιες υποδομές

Όλο και περισσότεροι άνθρωποι μετατρέπουν την οικία ή και την επιχείρηση τους σε έξυπνες, υιοθετώντας την τεχνολογία της τεχνητής νοημοσύνης, με σκοπό την μείωση κατανάλωσης ενέργειας, την εξοικονόμηση χρημάτων, την βελτιστοποίηση της καθημερινής τους ζωής κ.α.

Σε μεγαλύτερες ομάδες όπως οι έξυπνες πόλεις, συναντάμε την τεχνητή νοημοσύνη σε έξυπνα συστήματα φωτισμού για την εξοικονόμηση ενέργειας και χρημάτων, σε ευφυή συστήματα άρδευσης/ύδρευσης, ακόμα και ρύθμισης της κυκλοφορίας για τη μείωση της κυκλοφοριακής συμφόρησης[48]. Η χρήση της Τεχνητής Νοημοσύνης στα Ευφυή Συστήματα Μεταφορών συμβάλλει στη μείωση του χρόνου αναμονής, στη βελτιστοποίηση της δρομολόγησης και στην αύξηση της ανεξαρτησίας των ατόμων με προβλήματα όρασης. Επιπλέον, η τεχνητή νοημοσύνη χρησιμοποιείται για τη βελτιστοποίηση ενεργειακά αποδοτικών κινητήρων, οι οποίοι με τη σειρά τους συμβάλλουν στη μείωση των εκπομπών άνθρακα και του περιβαλλοντικού αποτυπώματος της κοινωνίας. Αυτό οδηγεί σε μια πιο βιώσιμη και φιλική προς το περιβάλλον κοινωνία.

[47] https://orelit.com/benefits-of-artificial-intelligence-in-automotive-industry/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[48] https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

2.4.4 Εικονικοί βοηθοί - Chatbots

Σύμφωνα με την IBM, chatbot είναι ένα πρόγραμμα υπολογιστή που χρησιμοποιεί τεχνητή νοημοσύνη και επεξεργασία φυσικής γλώσσας για να κατανοήσει τις ερωτήσεις των πελατών και να αυτοματοποιήσει τις απαντήσεις σε αυτές, προσομοιώνοντας την ανθρώπινη συνομιλία.

Ένας εικονικός βοηθός λειτουργεί ως προσωπικός βοηθός, παρέχοντας στους χρήστες προσαρμοσμένες και βελτιστοποιημένες ρυθμίσεις. Μπορεί να απαντά σε ερωτήσεις, να δίνει συμβουλές και να υπενθυμίζει στους χρήστες επερχόμενες συναντήσεις. Είναι επίσης ένας διαδραστικός συνομιλητής που μπορεί να προσαρμοστεί στα ατομικά χαρακτηριστικά ενός συγκεκριμένου ατόμου, λαμβάνοντας υπόψη το περιβάλλον, τα ενδιαφέροντα και τις συνήθειες του χρήστη. Παραδείγματα εικονικών βοηθών είναι η Siri της Apple και η Alexa της Amazon.

Το Νοέμβριο του 2022 κυκλοφόρησε ένα πρόγραμμα ΤΝ που έχει προκαλέσει ιδιαίτερη εντύπωση στους χρήστες, το «Chat GPT» της OpenAi[49]. Ουσιαστικά πρόκειται για ένα εξελιγμένο chatbot, που βασίζεται στο NLP (Natural Language Processing), το οποίο μπορεί να γράψει ποιήματα, λογοτεχνικά κείμενα ή μουσική, να λύσει εξισώσεις μαθηματικών ή φυσικής, να κάνει σύγκριση προϊόντων, ακόμα και να συνομιλήσει στην αγγλική γλώσσα υποκαθιστώντας πραγματικά πρόσωπα. Αντίστοιχο παράδειγμα είναι η εφαρμογή Historical Figures της Apple, με την οποία ο χρήστης μπορεί να «συνομιλήσει» με προσωπικότητες που δεν είναι πλέον εν ζωή!

2.4.5 Καθημερινότητα- Αυτόματες μεταφράσεις κ.α

Στην καθημερινή ζωή όσοι χρησιμοποιούν υπολογιστή ή έξυπνο κινητό, είναι σίγουρα χρήστες εφαρμογών ΤΝ ακόμη και εν αγνοία τους. Αυτό φυσικά συμβαίνει διότι τη συναντάμε σε πράγματα, τα οποία πλέον για τους περισσότερους είναι αυτονόητα, όπως παραδείγματος χάρη συμβαίνει με τις προγνωστικές αναζητήσεις κατά τη χρήση της μηχανής αναζήτησης του περιηγητή της Google, οι οποίες με χρήση αλγορίθμων μαθαίνουν και προσαρμόζουν τα αποτελέσματα της αναζήτησης στα ενδιαφέροντα του χρήστη. Επίσης και στα λογισμικά αυτόματης μετάφρασης και υποτιτλισμού, όπως το google translate, γίνεται χρήση ΤΝ για την παροχή και βελτίωση μεταφράσεων. Το ίδιο

[49] https://openai.com/ *[τελευταία ανάκτηση 15 Ιανουαρίου 2023]*

συμβαίνει και με την εφαρμογή Google maps ή χάρτες, κατά τη χρήση της οποίας οι αλγόριθμοι υπολογίζουν τη βέλτιστη διαδρομή προς το σημείο προορισμού.

2.4.6 Αγροτικές εφαρμογές

Στον αγροτικό τομέα συναντάμε την τεχνητή νοημοσύνη στα έξυπνα συστήματα άρδευσης ή ψεκασμού με τη βοήθεια αισθητήρων και άλλων μέσων ενσωματωμένων σε drones και ρομπότ κ.α. Με την χρήση της τεχνολογίας επιτυγχάνεται εξοικονόμηση της υπερβολικής χρήσης νερού, φυτοφαρμάκων, ζιζανιοκτόνων, διατήρηση της γονιμότητας του εδάφους, ενώ αυξάνεται η παραγωγικότητα και βελτιώνεται η ποιότητα.[50]

2.4.7 Ανθρωποειδή ρομπότ

Σήμερα πολλές εταιρίες έχουν προχωρήσει σε δημιουργία ανθρωποειδών ρομπότ, τα οποία λειτουργούν με τεχνητή νοημοσύνη. Ανάμεσα στα πιο γνωστά ρομπότ συναντάμε το Pepper, το οποίο σύμφωνα με την επίσημη ιστοσελίδα της εταιρίας Aldebaran που το κατασκεύασε, είναι το πρώτο κοινωνικό ανθρωποειδές ρομπότ παγκοσμίως που έχει τη δυνατότητα αναγνώρισης προσώπων και των βασικών ανθρώπινων συναισθημάτων, έχει βελτιστοποιηθεί για ανθρώπινη αλληλεπίδραση και είναι σε θέση να αλληλεπιδρά με ανθρώπους μέσω της συνομιλίας και της οθόνης αφής του. Είναι μαζικής παραγωγής, καθώς διατίθεται σήμερα σε επιχειρήσεις και σχολεία για να καλωσορίζει, να ενημερώνει και να καθοδηγεί τους επισκέπτες με καινοτόμο τρόπο[51]. Το συναντάμε και στο αεροδρόμιο Ελ. Βενιζέλος, όπου ενημερώνει και ψυχαγωγεί τους ταξιδιώτες σε ελληνικά, αγγλικά και κινέζικα!

Ένα ακόμη γνωστό ρομπότ με τεχνητή νοημοσύνη είναι η Sophia, που σχεδιάστηκε από τη Hanson Robotics για να βοηθήσει ανθρώπους σε πραγματικές χρήσεις όπως η ιατρική και η εκπαίδευση, και να υπηρετήσει την έρευνα της τεχνητής νοημοσύνης[52].

---

[50] *Tanha Talaviya, Dhara Shah, Nivedita Patel, Hiteshri Yagnik, Manan Shah, «Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides», Artificial Intelligence in Agriculture, Volume 4, 2020, σελ. 58-73, ISSN 2589-7217, https://doi.org/10.1016/j.aiia.2020.04.002. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S258972172030012X [τελευταία ανάκτηση 15 Ιανουαρίου 2023]*

[51] https://www.aldebaran.com/en/pepper [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[52] https://www.hansonrobotics.com/sophia/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Στο Consumer Electrics Show 2022, ένα από τα μεγαλύτερα τεχνολογικά γεγονότα στον κόσμο, παρουσιάστηκε το ανθρωποειδές ρομπότ Ameca της βρετανικής εταιρίας Engineered Arts που μπορεί να μιλήσει και να αναγνωρίσει πρόσωπα[53].

Ο Elon Musk, ιδιοκτήτης της εταιρίας Tesla, παρουσίασε κατά τη διάρκεια της Ημέρας Τεχνητής Νοημοσύνης της Tesla, το πρωτότυπο ανθρωποειδές ρομπότ Optimus, το οποίο κατά δήλωσή του, αναμένεται να βγει σε μαζική παραγωγή τα επόμενα έτη[54].

Τέλος, στη μεγαλύτερη τεχνολογική εκδήλωση στον κόσμο, το Gitex, που έλαβε χώρα στο Παγκόσμιο Κέντρο Εμπορίου του Ντουμπάι, από τις 10 έως τις 14 Οκτωβρίου 2022 παρουσιάστηκε από την εταιρία Uniccon Group of Companies, η Omeife, ένα θηλυκό, αφρικανικό ανθρωποειδές ρομπότ ύψους 1,80 μέτρων, πολλαπλών χρήσεων και βοήθειας. Μιλάει αφρικανικές γλώσσες και είναι προγραμματισμένη να κατανοεί βαθιά την αφρικανική κουλτούρα και τα πρότυπα συμπεριφοράς[55].

2.4.8 Εκπαίδευση

Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί και για τις ανάγκες της εκπαίδευσης, καθώς μπορεί να επιταχύνει την εξατομικευμένη μάθηση, να παρέχει στους μαθητές συνεχή αξιολόγηση και ανατροφοδότηση και να εφαρμόσει τη μαθησιακή αναλυτική για τη διαφοροποίηση της μαθησιακής διαδικασίας, ώστε να προσαρμόζεται στις ατομικές ανάγκες των μαθητών σε πραγματικό χρόνο (UNESCO, 2020)[56].

Οι (Memos et al, 2020) στην εργασία τους, προτείνουν την δημιουργία μιας Επαναστατικής Διαδραστικής Έξυπνης Τάξης (Revolutionary Interactive Smart Classroom) RISC, η οποία χρησιμοποιώντας τις τελευταίες τεχνολογίες θα μπορεί να προσφέρει όλα τα παραπάνω και να συνεισφέρει θετικά σε διάφορους τομείς, όπως στην εκπαίδευση και την κοινωνία, δίνοντας τη δυνατότητα σε μαθητές με ειδικές ανάγκες ή σε μαθητές απομακρυσμένων περιοχών να εκπαιδευτούν, αλλά και στο περιβάλλον εφόσον θα απαιτείται λιγότερο χαρτί, στον οικονομικό τομέα και στον πολιτιστικό τουρισμό αφού το RISC μπορεί να προσελκύσει ξένα σχολεία και ιδρύματα για εκπαιδευτικούς σκοπούς,

[53] https://www.engineeredarts.co.uk/robot/ameca/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[54] https://www.bbc.com/news/technology-63100636 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[55] https://www.africa.com/africas-first-humanoid-robot-omeife-unveiled-at-gitex/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[56] Dugan Steven - UNESCO, «*Ai in Education, Change at the speed of learning*», Διαθέσιμο: https://iite.unesco.org/wp-content/uploads/2020/11/Steven_Duggan_AI-in-Education_2020.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

και ως εκ τούτου, είναι μια εξαιρετική ευκαιρία για αυτά να εξερευνήσουν και την πολιτιστική κληρονομιά της Θεσσαλονίκης και περιχώρων[57].

2.5 Οφέλη της τεχνητής νοημοσύνης

Όπως ήδη ειπώθηκε, η χρήση της τεχνητής νοημοσύνης αυξήθηκε κατακόρυφα, και τουλάχιστον την τελευταία δεκαετία είναι παντού γύρω μας. Μάλιστα η ΤΝ, όχι μόνο διευκολύνει τη ζωή μας, αλλά μας βοηθά επίσης να αντιμετωπίσουμε μερικά από τα πιο πιεστικά ζητήματα που αντιμετωπίζει ο κόσμος σήμερα, όπως η καταπολέμηση χρόνιων ασθενειών, η μείωση των θανάτων από τροχαία, η καταπολέμηση της κλιματικής αλλαγής και η πρόβλεψη απειλών για την ασφάλεια στον κυβερνοχώρο.

Αν και μία μερίδα του κόσμου ενίσταται για κατάχρηση της τεχνητής νοημοσύνης, όταν αυτή χρησιμοποιείται με μέτρο, μπορεί να προσφέρει αμέτρητα πλεονεκτήματα, συνιστώντας ένα πολύτιμο εργαλείο στην εύρεση λύσης σε πολύπλοκα ζητήματα.

Η μηχανή που τροφοδοτείται από την ΤΝ είναι ικανή να εκτελεί ταυτόχρονα πολλαπλά καθήκοντα- σε σύγκριση με τους ανθρώπους, είναι λιγότερο δαπανηρή, πιο ακριβής και πιο αποτελεσματική (Πράσσος, 2022). Για να επωφεληθεί ο εκάστοτε χρήστης αυτής από τις δυνατότητες που παρέχει, οφείλει να μάθει να την χειρίζεται όσο καλύτερα γίνεται, ώστε να επωφεληθεί από τα πλεονεκτήματα που του προσφέρει. Η λίστα είναι μεγάλη και διαφοροποιείται ανάλογα με το πεδίο εφαρμογής, ωστόσο κάποια από τα σημαντικότερα οφέλη της ΤΝ είναι τα εξής[58, 59]:

- **ελαχιστοποίηση λαθών**: με το σωστό προγραμματισμό η επεξεργασία των δεδομένων μέσω κατάλληλων αλγορίθμων μειώνει τα λάθη στις αποφάσεις
- **μείωση κινδύνου**: Τα ρομπότ ΤΝ μπορούν να χρησιμοποιηθούν σε επικίνδυνες καταστάσεις όπως εξουδετέρωση βόμβας, εξόρυξη πετρελαίου κτλ
- **εξοικονόμηση χρόνου και χρήματος**: μείωση λειτουργικού κόστους, πχ μισθού υπαλλήλου, με περικοπή των ωρών εργασίας του

[57] V. A. Memos, G. Minopoulos, C. Stergiou, K. E. Psannis, Y. Ishibashi, "A Revolutionary Interactive Smart Classroom (RISC) with the Use of Emerging Technologies", in Proceedings of 2nd International Conference on Computer Communication and the Internet (ICCCI 2020), 26-28 June 2020, Nagoya Institute of Technology, Japan. [DOI: 10.1109/ICCCI49374.2020.9145987] Διαθέσιμο: https://www.researchgate.net/publication/339933375_A_Revolutionary_Interactive_Smart_Classroom_RISC_with_the_Use_of_Emerging_Technologies [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[58] https://www.javatpoint.com/advantages-and-disadvantages-of-artificial-intelligence [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[59] https://www.procon.org/headlines/artificial-intelligence-ai-top-3-pros-and-cons/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

- **ταχύτερη λήψη αποφάσεων**: ο συνδυασμός των τεχνολογιών που χρησιμοποιεί η ΤΝ βοηθάει στη γρήγορη λήψη αποφάσεων. Όσο περισσότερο εκτελεί αντίστοιχες ενέργειες επεξεργαζόμενη τα δεδομένα μέσω αλγορίθμων, τόσο βελτιώνεται σε ακρίβεια, ταχύτητα και ποιότητα ανάλυσης αυτών
- **αμεροληψία**: το γεγονός ότι τα δεδομένα επεξεργάζονται από μια μηχανή, ελλείψει ανθρώπινης παρεμβάσεως και συναισθημάτων, μπορεί να προσφέρει στο χρήστη αμερόληπτες αποφάσεις
- **προβλέψεις**: η ανάλυση ολοένα και περισσότερων δεδομένων της επιτρέπει τον εντοπισμό μοτίβων και κατ' επέκταση προβλέψεων, τις οποίες ο άνθρωπος δεν δύναται να πραγματοποιήσει με την ίδια ταχύτητα και ακρίβεια
- **Εκτέλεση επαναλαμβανόμενων ενεργειών**: πολλές φορές η επανάληψη κάποιας εργασίας απωθεί τον άνθρωπο που καλείται να τη φέρει εις πέρας, εν αντιθέσει με τη μηχανή που απλώς την προγραμματίζεις κατά βούληση και επαναλαμβάνει τις ίδιες εργασίες
- **Διαθεσιμότητα πάντα**: η χρήση ενός συστήματος τεχνητής νοημοσύνης δεν έχει χρονικούς περιορισμούς, ούτε απαιτεί διαλείμματα, σε αντίθεση με τον άνθρωπο, πχ. chatbot
- **Νέες εφευρέσεις**: η χρήση προηγμένων τεχνολογιών βασισμένων στην ΤΝ διευκολύνει κάθε τομέα να προχωρήσει σε νέες εφευρέσεις, ιδιαίτερα στην υγειονομική περίθαλψη, την ιατρική, την εκπαίδευση και τον αθλητισμό.
- **Βελτίωση καθημερινής ζωής**: η χρήση της στο σύστημα πλοήγησης, στο ψυγείο του σπιτιού μας ή στην παρακολούθηση και καταγραφή της αθλητικής μας δραστηριότητας, διευκολύνει την καθημερινότητα του χρήστη, πολλώ δε μάλλον όταν ο χρήστης είναι άτομο με αναπηρίες.

Στην αιχμή της κυβερνοασφάλειας επίσης, βρίσκεται η Τεχνητή Νοημοσύνη, η οποία χρησιμοποιείται για την ανάπτυξη πολύπλοκων αλγορίθμων για την προστασία δικτύων και συστημάτων, συμπεριλαμβανομένων των συστημάτων IoT (Kuzlu et al. 2021)[60].

[60] Kuzlu, M., Fair, C. & Guler, O. «Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity», (2021). https://doi.org/10.1007/s43926-020-00001-4 Διαθέσιμο: https://link.springer.com/article/10.1007/s43926-020-00001-4 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Η χρήση της τεχνητής νοημοσύνης για την προστασία των δεδομένων και των πληροφοριακών συστημάτων τους γίνεται όλο και πιο συνηθισμένη στις σημερινές πολυεθνικές εταιρείες και άλλες μεγάλες επιχειρήσεις (Πράσσος, 2022).

Γενικότερα, η ΤΝ μπορεί να χρησιμοποιηθεί για τον εντοπισμό πιθανών κινδύνων ασφαλείας και την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, όπως και για την κρυπτογράφηση δεδομένων, τον εντοπισμό κακόβουλων δραστηριοτήτων και την πρόληψη της διαρροής δεδομένων. Ακόμη, για τον εντοπισμό μη φυσιολογικών δραστηριοτήτων και την ειδοποίηση των χρηστών για πιθανές απειλές. Επίσης η ΤΝ έχει τη δυνατότητα να βελτιώσει την ασφάλεια και το απόρρητο στα ψηφιακά δίδυμα σενάρια, τα οποία χρησιμοποιούνται για τον εντοπισμό κινδύνων και την παροχή προληπτικών λύσεων (Stergiou et al., 2023)[61].

2.6 Κίνδυνοι και προκλήσεις της τεχνητής νοημοσύνης

Η τεχνητή νοημοσύνη όπως προαναφέρθηκε, συνιστά ένα ταχέως αναπτυσσόμενο τομέα της πληροφορικής που επηρεάζει τη ζωή μας σε καθημερινό επίπεδο. Σε συνδυασμό με τα συστήματα μηχανικής μάθησης, εφαρμόζεται πλέον καινοτόμα σε διάφορους τομείς, όπως η υγειονομική περίθαλψη, ο οικονομικός προγραμματισμός και η πρόβλεψη φυσικών καταστροφών κ.α. Όμως παράλληλα με τις μεγάλες ευκαιρίες που προσφέρει, ενέχει και κάποιους κινδύνους που χρήζουν κατάλληλης και αναλογικής αντιμετώπισης, διαφορετικά η χρήση της ΤΝ μπορεί να οδηγήσει σε υλικές και άυλες ζημίες. Η υλική ζημία μπορεί να περιλαμβάνει βλάβη στην ασφάλεια και την υγεία των ανθρώπων, συμπεριλαμβανομένης της απώλειας ζωής, καθώς και περιουσιακές ζημίες. Η άυλη ζημία μπορεί να συνεπάγεται απώλεια της ιδιωτικής ζωής, περιορισμό του δικαιώματος στην ελευθερία έκφρασης και προσβολή της ανθρώπινης αξιοπρέπειας, όπως διακρίσεις στην πρόσβαση στην εργασία. Αυτοί οι κίνδυνοι συνδέονται με ένα ευρύ φάσμα θεμάτων, συμπεριλαμβανομένης της εφαρμογής κανόνων για την προστασία των θεμελιωδών δικαιωμάτων, όπως τα προσωπικά δεδομένα και η προστασία της ιδιωτικής ζωής, η μη διάκριση, η ασφάλεια και η ευθύνη.

[61] C. L. Stergiou, E. Bompoli, K. E. Psannis, "Security & privacy issues in IoT-based Big Data Cloud systems in a Digital Twin scenario", MDPI, Applied Sciences, vol. 13, issue: 2, January 2023. [DOI: 10.3390/app13020758] Διαθέσιμο: https://www.mdpi.com/2076-3417/13/2/758 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Γνωστές προσωπικότητες έχουν συμμετάσχει και στις δύο πλευρές της συζήτησης. Για παράδειγμα, ο Έλον Μασκ μοιράστηκε τις ανησυχίες ότι η τεχνητή νοημοσύνη αποτελούσε υπαρξιακή απειλή για την ανθρώπινη φυλή, ενώ ο Μπιλ Γκέιτς απάντησε ότι η τεχνολογία θα μας κάνει πιο παραγωγικούς και δημιουργικούς. Αμφότεροι ωστόσο αναγνωρίζουν ότι η τεχνητή νοημοσύνη παρουσιάζει ένα ευρύ φάσμα ευκαιριών και προκλήσεων και καλούν για προβληματισμό σχετικά με το πώς μπορούμε να διαχειριστούμε την ανάπτυξή της με τρόπο που να μεγιστοποιεί τα οφέλη της χωρίς να μας εκθέτει σε κίνδυνο[62].

Βέβαια, οι ελπίδες και οι φόβοι για την τεχνητή νοημοσύνη δεν αφορούν μόνο το μακρινό μέλλον. Συχνά αφορούν τη σημερινή τεχνητή νοημοσύνη, που έχει ήδη μια ουσιαστική επιρροή στη ζωή μας, και φαινομενικά και για το καλύτερο και το χειρότερο. Για παράδειγμα, η τεχνητή νοημοσύνη αποτελεί και μέρος του προβλήματος αλλά και λύση στην αντιμετώπιση των ψεύτικων ειδήσεων. Αλγόριθμοι τεχνητής νοημοσύνης έχουν χρησιμοποιηθεί για να υποστηρίξουν μια πιο αμερόληπτη ποινική δικαιοσύνη, ωστόσο κατηγορούνται για φυλετική προκατάληψη κ.α. Ειδικά το τελευταίο διάστημα που έχουν κάνει δυναμική εμφάνιση τα προγράμματα AI Image Generators, όπως DALL-E, Stable Diffusion, MidJourney κλπ. είναι σαφές ότι τροφοδοτούν τα αντιθετικά ζεύγη (generative adversarial) μέσω των οποίων "μαθαίνουν" με φωτογραφίες προσώπων προκειμένου να δημιουργούν τεχνητά πρόσωπα με "δανεισμένα" και παραλλαγμένα χαρακτηριστικά τα οποία όμως μοιάζουν άκρως ρεαλιστικά. Οι πιθανές εμπορικές εφαρμογές είναι τεράστιες, από την άλλη τίθενται ζητήματα προστασίας πνευματικών δικαιωμάτων[63]. Αντίστοιχα ζητήματα πνευματικών δικαιωμάτων αλλά και παραπληροφόρησης δημιουργούν και τα ψηφιακά deepfakes[64].

---

[62] Philip Boucher, «*Should we fear artificial intelligence? – In depth analysis*», European Parliament, European Parliamentary research service, STOA, March 2018, σελ. 5 Διαθέσιμο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA%282018%29614547_EN.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[63]Καλδής Π., «*Ειδική Νομοθεσία από την Ευρωπαϊκή Ένωση για την Τεχνητή Νοημοσύνη*», Διαθέσιμο: https://www.photo.gr/blogs/eidiki-nomothesia-apo-evropaiki-enosi-gia-tin-techniti-noimosyni/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[64] Τα deepfakes είναι αληθοφανή προϊόντα πολυμέσων, με ήχο, βίντεο και φωτογραφίες, που δημιουργούνται μέσω της τεχνητής νοημοσύνης και εμφανίζουν ανθρώπους να λένε ή να πράττουν συγκεκριμένα πράγματα. Ουσιαστικά πρόκειται για πιο σύνθετα και πιο δύσκολα εντοπίσιμα fake news. Διαθέσιμο: https://www.iefimerida.gr/kosmos/deepfakes-psifiako-mellon-parapliroforisis [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Γενικά, θα μπορούσαμε να αναφέρουμε ότι η τεχνητή νοημοσύνη έχει τα εξής μειονεκτήματα[65]:

- **Υψηλό κόστος παραγωγής**: Προκειμένου να σημειώνουν πάντα υψηλές επιδόσεις τα συστήματα ΤΝ απαιτούν συχνές ενημερώσεις λογισμικού και υλικού που συνεπάγονται υψηλό κόστος.
- **Κίνδυνος ανεργίας**: λόγω της αντικατάστασης θέσεων εργασίας από ρομπότ, πχ. chatbot αντί των ανθρώπων.
- **Μείωση πνευματικής και σωματικής δραστηριότητας του ανθρώπου:** Οι δυνατότητες που προσφέρει η Τεχνητή Νοημοσύνη με τους αυτοματισμούς, δημιουργούν εξάρτηση στους ανθρώπους, με αποτέλεσμα λόγω τεμπελιάς να αυξηθούν μελλοντικά τα προβλήματα ανεργίας και υγείας.
- **Απουσία συναισθημάτων:** λόγω του ότι τα ρομπότ δεν έχουν ανθρώπινα συναισθήματα, δεν μπορούν να λειτουργήσουν σαν ομάδα για την ολοκλήρωση ενός στόχου
- **Έλλειψη δημιουργικότητας:** ίσως το μεγαλύτερο μειονέκτημα της Τεχνητής Νοημοσύνης καθώς βασίζεται πλήρως σε προφορτωμένα δεδομένα
- **Έλλειψη ηθικής:** όπως και τα συναισθήματα έτσι και η ηθική είναι προνόμιο των ανθρώπων. Δίχως αυτή και με την ανεξέλεγκτη χρήση της τεχνητής νοημοσύνης σε κάθε τομέα, μπορεί να απειληθεί η ανθρωπότητα με εξαφάνιση.

Δεδομένων των πλεονεκτημάτων και μειονεκτημάτων των προϊόντων τεχνητής νοημοσύνης, δεν φαίνεται να προκαλεί έκπληξη το γεγονός ότι ορισμένοι άνθρωποι αποδέχονται πιο εύκολα την εμφάνιση προϊόντων τεχνητής νοημοσύνης και αναγνωρίζουν τα πλεονεκτήματά τους για τον άνθρωπο. Σε αντίθεση με αυτό, άλλοι φαίνεται να είναι αμφίθυμοι ή ακόμη και δύσπιστοι και φοβισμένοι σχετικά με την άνοδο των προϊόντων τεχνητής νοημοσύνης (LINK Institut -2018)[66].

[65] https://www.javatpoint.com/advantages-and-disadvantages-of-artificial-intelligence [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[66] Sindermann, C., Sha, P., Zhou, M. *et al.* «*Assessing the Attitude Towards Artificial Intelligence: Introduction of a Short Measure in German, Chinese, and English Language*», *Künstl Intell*, (2021) Διαθέσιμο: https://link.springer.com/article/10.1007/s13218-020-00689-0#citeas [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

2.6.1 Κοινωνικός περιορισμός και φόβοι στην εφαρμογή της ΤΝ

Μελέτες από διάφορους τομείς δείχνουν ότι υπάρχουν ατομικές διαφορές στη στάση και την εμπιστοσύνη στην τεχνητή νοημοσύνη, οι οποίες πιθανότατα οφείλονται στις διάφορες αρνητικές και θετικές συνέπειες της ενσωμάτωσης της τεχνητής νοημοσύνης στην καθημερινή ζωή.

Μια έρευνα της Ελληνικής εταιρίας Focus Bari που έγινε τον Δεκέμβριο 2021 σε δείγμα 1.001 ατόμων 18-74 ετών, έδειξε ότι το 48% στη χώρα μας εκφράζουν σκεπτικισμό ή αμφιβολία για την τεχνητή νοημοσύνη, το 32% διακατέχεται από θετικά συναισθήματα, ενώ το 20% είναι αρνητικό απέναντί της. Επίσης το 28% δηλώνει ότι νιώθει φόβο ή/και άγχος όταν ακούει τον όρο «Τεχνητή Νοημοσύνη», το 23% αποδοχή, το 21% αισιοδοξία, το 18% ελπίδα και το 15% σύγχυση, ενώ το 17% θεωρεί τελείως περιττή την ΤΝ. Σημειώνεται ότι μεταξύ των 18 χωρών που έλαβαν μέρος στην έρευνα, η Ελλάδα έχει το υψηλότερο ποσοστό του συναισθήματος σκεπτικισμού, ενώ ακολουθεί η Γερμανία με 40%, η Αγγλία και οι ΗΠΑ με 39% και η Γαλλία με 37%. Αναφορικά με το ποσοστό αποδοχής της ΤΝ στην Ελλάδα ανέρχεται περίπου στον διεθνή μέσο όρο, ενώ όσον αφορά το ποσοστό φόβου απέναντι στην ΤΝ η Ελλάδα έρχεται δεύτερη μετά την Πολωνία (29%).[67]

Σε έρευνα που έγινε μεταξύ Γερμανών (Ulm University - Γερμανία) και Κινέζων πολιτών (Πανεπιστήμιο Ηλεκτρονικής Επιστήμης και Τεχνολογίας της Κίνας -UESTC, και Πανεπιστήμιο Πολιτικών Μηχανικών και Αρχιτεκτονικής του Πεκίνου, Κίνα) διαπιστώθηκε ότι υπάρχει υψηλότερη αποδοχή της τεχνητής νοημοσύνης στους Κινέζους σε σύγκριση με το γερμανικό δείγμα[68]. Πιθανολογείται δε, όσον αφορά τα υψηλότερα επίπεδα αποδοχής στο κινεζικό έναντι του γερμανικού δείγματος, ότι οφείλεται στο γεγονός ότι η κινεζική κυβέρνηση υποστηρίζει σθεναρά εδώ και αρκετό καιρό την ανάπτυξη τεχνολογιών τεχνητής νοημοσύνης, όπως αναλύεται αμέσως παρακάτω.

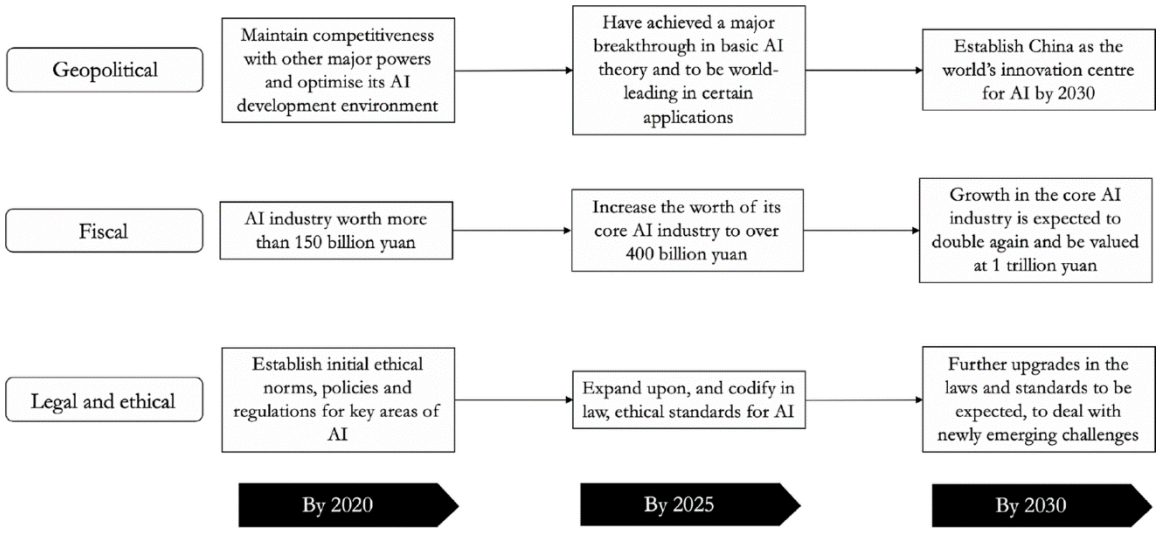
[67] https://focusbari.gr/wp-content/uploads/2022/02/GREEKS-AND-ARTIFICIAL-INTELLIGENCE_EN.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[68] Sindermann, C., Sha, P., Zhou, M. *et al.* Assessing the Attitude Towards Artificial Intelligence: Introduction of a Short Measure in German, Chinese, and English Language. *Künstl Intell*, (2021) Διαθέσιμο: https://link.springer.com/article/10.1007/s13218-020-00689-0#citeas [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

2.6.2 The (new) next generation artificial intelligence development plan (AIDP) της Κίνας

Το λεγόμενο «*Σχέδιο Ανάπτυξης Τεχνητής Νοημοσύνης (νέας) Επόμενης Γενιάς*[69]», έχει ως στόχο να καταστήσει την Κίνα ηγέτη στην έρευνα τεχνητής νοημοσύνης. Είναι ένα ενοποιημένο έγγραφο, το οποίο κυκλοφόρησε τον Ιούλιο του 2017 από το Κρατικό Συμβούλιο της Κίνας, και περιγράφει τους στόχους πολιτικής της για την τεχνητή νοημοσύνη. Μάλιστα στα κινεζικά μέσα ενημέρωσης αναφέρθηκε ως «*το πρώτο έτος της στρατηγικής ανάπτυξης AI της Κίνας*» (China AI Development Report 2018, Σελ. 63).

Πρωταρχικός στόχος της πολιτικής, όπως καθορίζεται στο AIDP, είναι να καταστήσει την Κίνα το παγκόσμιο κέντρο της καινοτομίας της τεχνητής νοημοσύνης έως το 2030 και να καταστήσει την τεχνητή νοημοσύνη «*την κύρια κινητήρια δύναμη για τη βιομηχανική αναβάθμιση και τον οικονομικό μετασχηματισμό της Κίνας*» (AIDP 2017). Το σχέδιο υπογραμμίζει επίσης τη σημασία της χρήσης της τεχνητής νοημοσύνης στους τομείς άμυνας και κοινωνικής πρόνοιας, και τονίζει την ανάγκη ανάπτυξης προτύπων και ηθικών κανόνων για τη χρήση της ΤΝξ. Συνολικά, το Σχέδιο παρέχει μια ολοκληρωμένη στρατηγική AI και προκαλεί άλλες κορυφαίες δυνάμεις σε πολλούς βασικούς τομείς[70].



Εικόνα 5: Οπτικοποίηση του AIDP της Κίνας

Πηγή: link.springer.com

[69] http://fi.china-embassy.gov.cn/eng/kxjs/201710/P020210628714286134479.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[70] Roberts, H., Cowls, J., Morley, J. *et al.* «*The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*» , (2021) Διαθέσιμο: https://link.springer.com/article/10.1007/s00146-020-00992-2#citeas [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

2.6.3 Αποτελέσματα έρευνας πανεπιστήμιου Timișoara σχετικά με την ΤΝ

Ιδιαίτερο ενδιαφέρον παρουσιάζει μια μελέτη που διεξήχθη στο Πανεπιστήμιο της Τιμισοάρα της Ρουμανίας. Τα δεδομένα συλλέχθηκαν από 929 απαντήσεις φοιτητών μεταξύ 5 Μαρτίου και 26 Απριλίου 2018, με περιθώριο σφάλματος 3%, ενώ επιλέχθηκαν φοιτητές με υψηλό μορφωτικό επίπεδο και πρόσβαση σε τέτοιου είδους πληροφορίες. Το ερωτηματολόγιο κάλυπτε τόσο τα τεχνικά όσο και τα ανθρωπιστικά μαθήματα στο πανεπιστήμιο[71].

Η μελέτη διαπίστωσε ότι το 84,6% των ανθρώπων γνωρίζει τι είναι η τεχνητή νοημοσύνη, ενώ το 12% απάντησε ότι δεν ξέρει τι είναι και το 3,4% λέει ότι δεν γνωρίζει ή δεν απαντά. Διαφορές στις απαντήσεις βρέθηκαν ανά φύλο και εξειδίκευση. Η μεταβλητή φύλου έδειξε ότι οι άνδρες είναι πιο πιθανό από τις γυναίκες να γνωρίζουν τι σημαίνει η έννοια της τεχνητής νοημοσύνης (σε ποσοστό 89,5% έναντι 82,3%). Οι σπουδαστές κλήθηκαν να απαντήσουν μια σειρά ερωτήσεων σχετικά με πόσο αρνητικά θα μπορούσε να επηρεάσει η τεχνητή νοημοσύνη στην κοινωνία. Τα αποτελέσματα της έρευνας επιβεβαιώνουν τις πιθανές ανησυχίες που προκαλεί η AI στην κοινωνία.

Ειδικότερα, από την έρευνα προέκυψε ότι ένα ποσοστό 59,8% απάντησε καταφατικά στην ερώτηση "*Οι συσκευές τεχνητής νοημοσύνης θα επηρεάσουν αρνητικά τις διαπροσωπικές σχέσεις;*", ποσοστό 38% απάντησε επίσης θετικά στην ερώτηση "*Η τεχνητή νοημοσύνη θα προκαλέσει οικονομική κρίση;*", όπως και το 64,1% στην ερώτηση "*Οι συσκευές τεχνητής νοημοσύνης θα κυριαρχήσουν στην ανθρωπότητα;*" καθώς επίσης και το 37,7% στην ερώτηση "*Η τεχνητή νοημοσύνη θα καταστρέψει την ανθρωπότητα*". Τέλος, ένας στους τρεις φοιτητές επιβεβαίωσε τους φόβους του σχετικά με τον αντίκτυπο της τεχνητής νοημοσύνης στην κοινωνία.

2.6.4 Νομικά και ηθικά ζητήματα της Τεχνητής Νοημοσύνης

Παράλληλα με την ανάπτυξη των ψηφιακών τεχνολογιών αιχμής, υπάρχει πάντα μια μερίδα του κόσμου που εκφράζει τις ανησυχίες του για παραβιάσεις δεδομένων, αλλά ταυτόχρονα υπογραμμίζει την ανάγκη για αλγοριθμική διαφάνεια και ασφάλεια.

[71] Gherhes, Vasile. (2018). «*Why Are We Afraid of Artificial Intelligence (Ai)?. European Review Of Applied Sociology*», Διαθέσιμο: https://www.researchgate.net/publication/330678764_Why_Are_We_Afraid_of_Artificial_Intelligence_Ai [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Τα νομικά και ηθικά ζητήματα που αντιμετωπίζει η κοινωνία λόγω της Τεχνητής Νοημοσύνης περιλαμβάνουν το απόρρητο και την επιτήρηση, την προκατάληψη ή τις διακρίσεις και ενδεχομένως η φιλοσοφική πρόκληση είναι ο ρόλος της ανθρώπινης κρίσης (Naik, et.al)[72].

2.6.4.1 Η περίπτωση του αλγόριθμου COMPAS

Αναφορικά με το ζήτημα των προκαταλήψεων/διακρίσεων από τη χρήση της τεχνητής νοημοσύνης, ως παράδειγμα θα μπορούσε να αναφερθεί ο αλγόριθμος που αναπτύχθηκε από την ιδιωτική εταιρία Northpointe (νυν Equivant), COMPAS (Correctional Offender Management Profiling for Alternative Sanctions)[73], ένας αλγόριθμος λήψης αποφάσεων με τεχνητή νοημοσύνη που εξακολουθεί να χρησιμοποιείται σήμερα στο δικαστικό σύστημα των Ηνωμένων Πολιτειών. Αυτό το λογισμικό προβλέπει τον κίνδυνο (υποτροπιασμού) του κατηγορουμένου να διαπράξει πλημμέλημα ή κακούργημα εντός 2 ετών από την αξιολόγηση από 137 χαρακτηριστικά σχετικά με ένα άτομο και το προηγούμενο ποινικό μητρώο του ατόμου.

Το 2016 η ρεπόρτερ Julia Angwin και οι συνεργάτες της στο ProPublica ανέλυσαν τις εκτιμήσεις COMPAS για περισσότερους από 7.000 συλληφθέντες στην κομητεία Broward της Φλόριντα και δημοσίευσαν μια έρευνα[74], υποστηρίζοντας ότι ο αλγόριθμος ήταν προκατειλημμένος εναντίον Αφροαμερικανών. Σύμφωνα με την έρευνα, η συνολική ακρίβεια της COMPAS για λευκούς κατηγορούμενους είναι 67,0%, ελαφρώς υψηλότερη από την ακρίβειά της 63,8% για τους μαύρους κατηγορούμενους. Τα λάθη που έγιναν από την COMPAS, ωστόσο, επηρέασαν διαφορετικά τους ασπρόμαυρους κατηγορούμενους: Οι μαύροι κατηγορούμενοι που δεν υποτροπίασαν είχαν εσφαλμένα προβλεφθεί ότι θα επαναλάβουν τα αδικήματα σε ποσοστό 44,9%, σχεδόν δύο φορές υψηλότερο από τους λευκούς ομολόγους τους στο 23,5%, ενώ οι λευκοί κατηγορούμενοι που υποτροπίασαν, είχε λανθασμένα προβλεφθεί ότι δεν θα επαναλάβουν το αδίκημα σε ποσοστό 47,7%, σχεδόν δύο φορές υψηλότερο από τους μαύρους ομολόγους τους στο 28,0%!!

---

[72] Naik Nithesh, et.al, 'Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?', Frontiers in Surgery Vol.9, 2022 Διαθέσιμο: https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[73] Räz, T. «*COMPAS: zu einer wegweisenden Debatte über algorithmische Risikobeurteilung*.» *Forens Psychiatr Psychol Kriminol* **16**, 300–306 (2022). https://doi.org/10.1007/s11757-022-00741-9 Διαθέσιμο: https://link.springer.com/article/10.1007/s11757-022-00741-9 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[74] https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Εν συνεχεία διεξήχθη μια έρευνα από τους Julia Dressel και Hany Farid του Dartmouth College[75], σχετικά με τη συνολική ακρίβεια και προκατάληψη στην ανθρώπινη αξιολόγηση σε σχέση με την αλγοριθμική αξιολόγηση του COMPAS, η οποία κατέληξε στο ότι ο αλγόριθμος πρόβλεψης COMPAS, δεν είναι πιο ακριβής ή δίκαιος από τις προβλέψεις που γίνονται από άτομα με λίγη ή καθόλου εμπειρία στην ποινική δικαιοσύνη, τουναντίον, είναι ισοδύναμος με έναν απλό γραμμικό ταξινομητή! Οι ερευνητές υποστήριξαν ότι, παρά την εντυπωσιακή συλλογή 137 χαρακτηριστικών στον COMPAS, ένας γραμμικός ταξινομητής που βασίζεται σε μόνο 2 χαρακτηριστικά—ηλικία και συνολικό αριθμό προηγούμενων παραβάσεων—είναι το μόνο που απαιτείται για να αποδώσει την ίδια ακρίβεια πρόβλεψης με το COMPAS!

2.6.4.2 Κατηγορίες ηθικών προκλήσεων ΤΝ

Σύμφωνα με τον Bernd Carsten Stahl το πανεπιστημίου του De Montfort, οι ηθικές προκλήσεις της τεχνητής νοημοσύνης μπορούν να ομαδοποιηθούν σε τρεις κατηγορίες[76]:

Πίνακας 1 - Τρεις κατηγορίες ηθικών θεμάτων τεχνητής νοημοσύνης

1. Ζητήματα που προκύπτουν από τη μηχανική μάθηση	
Προστασία απορρήτου και δεδομένων	Έλλειψη ιδιωτικότητας, Κατάχρηση προσωπικών δεδομένων, Προβλήματα ασφαλείας
Αξιοπιστία	Έλλειψη ποιοτικών δεδομένων, Έλλειψη ακρίβειας δεδομένων Προβλήματα ακεραιότητας
Διαφάνεια	Έλλειψη λογοδοσίας και ευθύνης, Έλλειψη διαφάνειας, Μεροληψία και διακρίσεις, Έλλειψη ακρίβειας προγνωστικών συστάσεων Έλλειψη ακρίβειας μη μεμονωμένων συστάσεων
Ασφάλεια	Βλάβη στη σωματική ακεραιότητα
2. Ζητήματα ζώντας σε έναν ψηφιακό κόσμο	

[75] Dressel J, Farid H. «*The accuracy, fairness, and limits of predicting recidivism*», 2018 Διαθέσιμο: https://www.science.org/doi/10.1126/sciadv.aao5580 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[76] Stahl, Bernd. (2021). «*Ethical Issues of AI*», Διαθέσιμο: https://www.researchgate.net/publication/350145020_Ethical_Issues_of_AI [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Οικονομικά θέματα	Εξαφάνιση θέσεων εργασίας, Συγκέντρωση οικονομικής δύναμης, Κόστος για την καινοτομία
Δικαιοσύνη (Justice) και δικαιοσύνη (fairness)	Αμφισβητούμενη ιδιοκτησία δεδομένων, Αρνητικές επιπτώσεις στο δικαστικό σύστημα, Έλλειψη πρόσβασης σε δημόσιες υπηρεσίες, Παραβίαση των θεμελιωδών ανθρωπίνων δικαιωμάτων των τελικών χρηστών, Παραβίαση των θεμελιωδών ανθρωπίνων δικαιωμάτων στην εφοδιαστική αλυσίδα, Αρνητικές επιπτώσεις στις ευάλωτες ομάδες Αδικία
Ελευθερία	Έλλειψη πρόσβασης και ελευθερίας στην πληροφόρηση, Απώλεια της ανθρώπινης λήψης αποφάσεων, Απώλεια ελευθερίας και ατομικής αυτονομίας
Ευρύτερα κοινωνικά ζητήματα	Άνισες σχέσεις εξουσίας, Ασυμμετρίες ισχύος, Αρνητικό αντίκτυπο στη δημοκρατία, Προβλήματα ελέγχου και χρήσης δεδομένων και συστημάτων, Έλλειψη ενημερωμένης συναίνεσης, Έλλειψη εμπιστοσύνης, Δυνατότητα για στρατιωτική χρήση, Αρνητικές επιπτώσεις στην υγεία, Μείωση της ανθρώπινης επαφής, Αρνητικές επιπτώσεις στο περιβάλλον
Θέματα αβεβαιότητας	Απρόβλεπτες, απρόβλεπτες δυσμενείς επιπτώσεις, Προτεραιοποίηση των «λάθος» προβλημάτων, Δυνατότητα εγκληματικής και κακόβουλης χρήσης
3. Μεταφυσικά θέματα	
○ Μηχανική συνείδηση ○ «Ξύπνημα» της τεχνητής νοημοσύνης ○ Αυτόνομοι ηθικοί παράγοντες ○ Υπερ-ευφυΐα ○ Μοναδικότητα ○ Αλλαγές στην ανθρώπινη φύση	

Το πρώτο σύνολο θεμάτων αποτελείται από αυτά που προκύπτουν από τα χαρακτηριστικά της μηχανικής μάθησης. Πολλές από τις τεχνικές μηχανικής μάθησης που οδήγησαν στην τρέχουσα επιτυχία της τεχνητής νοημοσύνης βασίζονται σε τεχνητά νευρωνικά δίκτυα. Τα χαρακτηριστικά αυτών των προσεγγίσεων που προκαλούν ηθικές

ανησυχίες είναι η αδιαφάνεια, η απρόβλεπτη ικανότητα και η ανάγκη για μεγάλα σύνολα δεδομένων για την εκπαίδευση των τεχνολογιών (Stahl, 2021).

Το δεύτερο σύνολο ηθικών θεμάτων αποτελείται από εκείνα που σχετίζονται με τα κατά τον Stahl «Συγκλίνοντα κοινωνικο-τεχνικά συστήματα AI», τα οποία έχουν τα χαρακτηριστικά της αυτονομίας, του κοινωνικού αντίκτυπου και της χειραγώγησης. Η εν λόγω διάκριση είναι αναλυτική, καθώς τα συγκλίνοντα κοινωνικο-τεχνικά συστήματα δεν είναι ξεχωριστά από τα συστήματα μηχανικής μάθησης, αλλά τείνουν να τα περιλαμβάνουν και να βασίζονται σε μηχανική μάθηση και άλλες δυνατότητες τεχνητής νοημοσύνης. Η διαφορά αφορά περισσότερο την προοπτική, όπου ο όρος «μηχανική μάθηση» χρησιμοποιείται για να επικεντρωθεί σε συγκεκριμένες τεχνολογίες για καθορισμένες εφαρμογές, ενώ τα συγκλίνοντα κοινωνικοτεχνικά συστήματα τείνουν να περιλαμβάνουν πολυάριθμες τεχνολογίες και η εστίασή τους είναι στον κοινωνικό αντίκτυπο που προκαλούν.

Η τρίτη και τελευταία κατηγορία ηθικών θεμάτων, είναι η αποκαλούμενη «μεταφυσικά ζητήματα», και θεωρείται η πιο ανοιχτή και ανεξερεύνητη. Τα ζητήματα εδώ συνδέονται άμεσα με θεμελιώδεις πτυχές της πραγματικότητας της φύσης του όντος και της ανθρώπινης ικανότητας να το κατανοήσει αυτό. Αυτά τα μεταφυσικά ζητήματα σχετίζονται κυρίως με την τεχνητή γενική νοημοσύνη (AGI) ή την καλή παλιομοδίτικη τεχνητή νοημοσύνη (GOFAI), η οποία συνήθως εννοείται με όρους συμβολικής και λογικής αναπαράστασης του κόσμου . Η ιδέα είναι ότι το AGI θα εμφανίζει ανθρώπινες συλλογιστικές ικανότητες[77].

2.6.4.3 Κινδυνεύουν τα θεμελιώδη δικαιώματα, η ιδιωτικότητα και τα προσωπικά μας δεδομένα από την ΤΝ;

Η χρήση της ΤΝ μπορεί να έχει αντίκτυπο στις αξίες στις οποίες βασίζεται η ΕΕ, οδηγώντας ενδεχομένως σε παραβιάσεις θεμελιωδών δικαιωμάτων όπως η ελευθερία έκφρασης, η ελευθερία του συνέρχεσθαι, η ανθρώπινη αξιοπρέπεια και η μη διάκριση κ.α.[78].

[77] Stahl, Bernd. (2021). «*Ethical Issues of AI*», Διαθέσιμο: https://www.researchgate.net/publication/350145020_Ethical_Issues_of_AI [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[78] Από την έρευνα του Συμβουλίου της Ευρώπης με τίτλο «Algorithms and human rights – Study on the human rights dimensions of automated data processing techniques and possible regulatory implecations» προκύπτει ότι η χρήση της ΤΝ θα μπορούσε να επηρεάσει μεγάλο αριθμό θεμελιωδών δικαιωμάτων,

Όσο η τεχνολογία αυτή εξελίσσεται, συλλέγοντας ολοένα περισσότερα δεδομένα, τόσο αυξάνεται και ο κίνδυνος παραβίασης του προσωπικού απορρήτου. Αυτό συμβαίνει διότι η τεχνητή νοημοσύνη έχει τη δυνατότητα να συλλέγει δεδομένα από άτομα χωρίς τη γνώση ή τη συγκατάθεσή τους και να χρησιμοποιεί αυτά τα δεδομένα για τη λήψη αποφάσεων σχετικά με την προσωπική τους ζωή. Μάλιστα η δυνατότητα της ΤΝ να χρησιμοποιείται για την ανάλυση μεγάλων ποσοτήτων δεδομένων και τον εντοπισμό των συνδέσεων μεταξύ τους, οδηγεί σε νέους κινδύνους για την προστασία των προσωπικών δεδομένων, ακόμη και όταν το σύνολο δεδομένων δεν περιλαμβάνει προσωπικά δεδομένα.

Σε μια μελέτη των Dilmaghani et al. (2019), διερεύνησαν τη δυνατότητα της τεχνητής νοημοσύνης να παραβιάζει το προσωπικό απόρρητο, εξετάζοντας πώς τα συστήματα τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για την αναγνώριση ατόμων. Διαπίστωσαν ότι η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την αναγνώριση ατόμων με υψηλό βαθμό ακρίβειας και ότι η ακρίβεια αυτή, αυξάνεται με τον όγκο των διαθέσιμων δεδομένων. Αυτό σημαίνει ότι σε όσο περισσότερα δεδομένα έχει πρόσβαση ένα σύστημα ΤΝ, τόσο πιο ακριβές μπορεί να είναι στην αναγνώριση ατόμων, γεγονός που αποτελεί σοβαρή απειλή για το προσωπικό απόρρητο, καθώς τα συστήματα ΤΝ μπορούν να συλλέγουν μεγάλους όγκους δεδομένων χωρίς τη συγκατάθεση ή τη γνώση ενός ατόμου. Ως εκ τούτου, είναι σημαντικό να ληφθούν υπόψη οι πιθανές επιπτώσεις της τεχνολογίας ΤΝ στο προσωπικό απόρρητο και να ληφθούν μέτρα για να διασφαλιστεί ότι δεν γίνεται κατάχρηση των προσωπικών δεδομένων[79].

Επιπλέον, η χρήση της ΤΝ από διαδικτυακές μηχανές αναζήτησης για να ιεραρχήσουν τις πληροφορίες που παρουσιάζουν στους χρήστες τους και να παρουσιάσουν επιλεκτικά το περιεχόμενό τους, μπορεί να επηρεάσει τα δικαιώματα της ελεύθερης έκφρασης, την προστασία των προσωπικών δεδομένων, το απόρρητο και τις πολιτικές ελευθερίες, ανάλογα με τα επεξεργασμένα δεδομένα, τον σχεδιασμό της εφαρμογής και το εύρος ανθρώπινης παρέμβασης.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) είναι ένα σύνολο κανόνων που έχουν σχεδιαστεί για την προστασία της ιδιωτικής ζωής των ατόμων. Δεν

Διαθέσιμο: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[79] S. Dilmaghani, M. R. Brust, G. Danoy, N. Cassagnes, J. Pecero and P. Bouvry, "Privacy and Security of Big Data in AI Systems: A Research and Standards Perspective," *2019 IEEE International Conference on Big Data (Big Data)*, Los Angeles, CA, USA, 2019, pp. 5737-5743, doi: 10.1109/BigData47090.2019.9006283. Διαθέσιμο: https://ieeexplore.ieee.org/document/9006283 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

αφορά άμεσα τη χρήση τεχνολογικών συστημάτων ΤΝ, αλλά χρειάζεται να συμβαδίζει με τον γρήγορο ρυθμό των τεχνολογικών προόδων. Ο GDPR επιδιώκει να διασφαλίσει ότι τα θεμελιώδη δικαιώματα και οι ελευθερίες των ατόμων γίνονται σεβαστά, ενώ παράλληλα επιτρέπει την καινοτομία και την τεχνολογική πρόοδο. Ο κανονισμός πρέπει να εφαρμόζεται κατά τη συλλογή και την επεξεργασία δεδομένων, ανεξάρτητα από την τεχνολογία που χρησιμοποιείται. Το επίκεντρο του κανονισμού δεν είναι η ίδια η τεχνολογία, αλλά ο αντίκτυπος που έχει στα ανθρώπινα δικαιώματα και επιδιώκει να βρει μια ισορροπία μεταξύ των δύο. (Μπακόλας, 2018).

Σύμφωνα με την Μήτρου, η αποχή από την ειδική για την τεχνολογία ορολογία και διατάξεις φαίνεται να είναι μια συνειδητή επιλογή που πρέπει να αποδοθεί στην «*προσέγγιση της τεχνολογικής ουδετερότητας*». Με τον GDPR, οι ευρωπαίοι νομοθέτες τηρούν ρητά την προσέγγιση της τεχνολογικής ουδετερότητας, καθώς η αιτιολογική σκέψη 15 αναφέρει ότι «*η προστασία των φυσικών προσώπων πρέπει να είναι τεχνολογικά ουδέτερη»*, μη εξαρτώμενη από τις τεχνικές που χρησιμοποιούνται. Ο GDPR εφαρμόζεται τόσο στην ανάπτυξη όσο και στη χρήση της τεχνητής νοημοσύνης, με στόχο την ανάλυση και τη λήψη αποφάσεων σχετικά με τα άτομα. Παραχωρεί στους χρήστες ορισμένα δικαιώματα σχετικά με την επεξεργασία των προσωπικών τους δεδομένων, ενώ παράλληλα επιβάλλει υποχρεώσεις στον υπεύθυνο επεξεργασίας για την ανάπτυξη και την εφαρμογή της ΤΝ. Ιδιαίτερη σημασία για το περιβάλλον τεχνητής νοημοσύνης έχουν οι κανονισμοί που αφορούν τον σκοπό της εφαρμογής, τη νομική βάση επεξεργασίας, τις αρχές προστασίας δεδομένων και την αυτοματοποιημένη λήψη αποφάσεων (Mitrou, 2018).

Περαιτέρω, η τεχνητή νοημοσύνη και η αυτοματοποιημένη λήψη αποφάσεων εγείρουν ερωτήματα σχετικά με την ευθύνη των παραβιάσεων που έχουν αντίκτυπο στην προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων, σε περίπτωση που δεν μπορούν να αποδοθούν με ακρίβεια η πολυπλοκότητα και ο όγκος των επεξεργασμένων δεδομένων. Όταν η τεχνητή νοημοσύνη και οι αλγόριθμοι θεωρούνται προϊόντα, τίθενται ζητήματα μεταξύ της προσωπικής ευθύνης, (η οποία ρυθμίζεται βάσει του Γενικού Κανονισμού για την Προστασία Δεδομένων και συνεπάγεται ευθύνη τόσο για τον υπεύθυνο επεξεργασίας όσο και για τον εκτελούντα την επεξεργασία), αλλά και της ευθύνης λόγω ελαττωματικών προϊόντων, η οποία δεν ρυθμίζεται από τον ΓΚΠΔ[80]. Το

[80] Ευρωπαϊκό Κοινοβούλιο, European Civil Law Rules in Robotics, Γενική Διεύθυνση Εσωτερικών Πολιτικών (Οκτώβριος 2016), σ. 14 Διαθέσιμο:

Σεπτέμβριο του 2022 έγινε προσπάθεια κάλυψης του κενού με τη νέα πρόταση Οδηγίας για την εξωσυμβατική αστική ευθύνη[81].

Η Μήτρου υποστηρίζει ότι τα προσωπικά δεδομένα και η τεχνητή νοημοσύνη είναι «*αμφίδρομος δρόμος*»: τα προσωπικά δεδομένα τροφοδοτούν την τεχνητή νοημοσύνη και η τεχνητή νοημοσύνη παράγει περισσότερα συναγόμενα δεδομένα. Αυτό σημαίνει ότι όσο αυξάνονται τα δεδομένα, τόσο καλύτερα αποδίδει η ΤΝ. Εντούτοις παρατηρούμε ότι αυτό έρχεται άμεσα σε αντίθεση με την αρχή ελαχιστοποίησης των δεδομένων του άρθρου 5 ΓΚΠΔ, σύμφωνα με την οποία θα πρέπει να συλλέγονται τα απολύτως απαραίτητα δεδομένα για την εκπλήρωση του σκοπού της επεξεργασίας. Το ίδιο συμβαίνει και όταν η ΤΝ αλλάζει το σκοπό και τη χρήση τους[82].

Η πολυπλοκότητα και το απρόβλεπτο πολλών τεχνολογιών τεχνητής νοημοσύνης, καθώς και η εν μέρει αυτόνομη συμπεριφορά τους, μπορεί να καταστήσουν δύσκολη τη διασφάλιση της συμμόρφωσης με την υφιστάμενη νομοθεσία της ΕΕ που έχει σχεδιαστεί για την προστασία των θεμελιωδών δικαιωμάτων. Αυτό οφείλεται στην έλλειψη διαφάνειας (αδιαφάνεια της ΤΝ) αυτών των τεχνολογιών, γεγονός που καθιστά δύσκολο τον εντοπισμό και την απόδειξη τυχόν παραβιάσεων του νόμου, συμπεριλαμβανομένων εκείνων που σχετίζονται με την προστασία των θεμελιωδών δικαιωμάτων. Επιπλέον, είναι δύσκολο να προσδιοριστεί ποιος ευθύνεται για τυχόν παραβάσεις και ποιες προϋποθέσεις πρέπει να πληρούνται για να διεκδικηθεί αποζημίωση. Αναφορικά με την έλλειψη αλγοριθμικής διαφάνειας, οι Desai και Kroll (2017) αναφέρουν παραδείγματα ανθρώπων που είτε τους αρνήθηκαν την χορήγηση δανείου, είτε κάποια θέση εργασίας κ.α, χωρίς να γνωρίζουν «*γιατί συνέβη αυτό, παρά μονάχα ότι η απόφαση ελήφθη μέσω κάποιου λογισμικού*»!

Τέλος, στη μελέτη τους οι Aizenberg και Van Den Hoven (2020), υποστήριξαν επίσης ότι τα συστήματα τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν για τη λήψη αποφάσεων που έχουν σημαντικές επιπτώσεις στα ανθρώπινα δικαιώματα. Αυτές οι αποφάσεις μπορεί να περιλαμβάνουν την παρακολούθηση ή την επιτήρηση ατόμων ή

---

https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[81] Ανακοίνωση του Ευρωπαϊκού Κοινοβουλίου σχετικά με το αίτημα προς την Επιτροπή για υποβολή πρότασης σχετικά με τη θέσπιση κανόνων για την αστική ευθύνη στους τομείς της ρομποτικής και της τεχνητής νοημοσύνης Διαθέσιμο: https://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[82] Σύμφωνα με τους Βόρρα -Μήτρου « *Η Τεχνητή Νοημοσύνη επιτρέπει τη συλλογή και την αξιοποίηση μεγάλου όγκου δεδομένων αλλάζοντας τον σκοπό και τη χρήση τους*». (Βόρρας-Μήτρου, 2018).

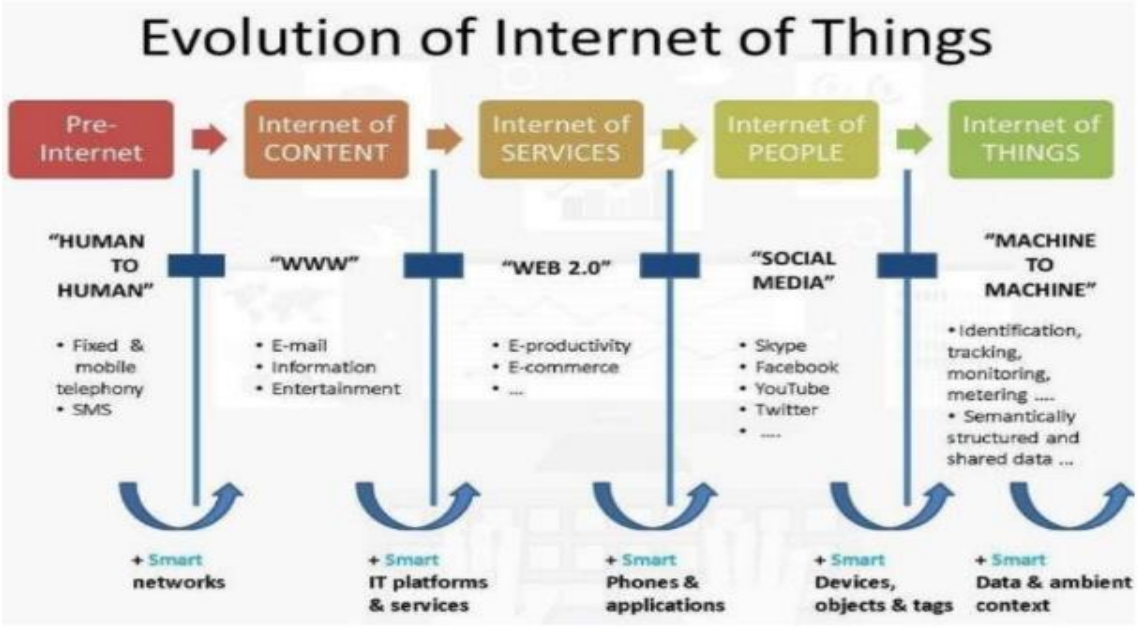
ομάδων ή τον εντοπισμό προτύπων συμπεριφοράς που μπορεί να είναι ενδεικτικές εγκληματικής δραστηριότητας. Επιπλέον, η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την γρήγορη επεξεργασία μεγάλων ποσοτήτων δεδομένων, λαμβάνοντας αποφάσεις για λογαριασμό ατόμων ή οργανισμών που μπορεί να έχουν ανεπιθύμητες συνέπειες. Ως εκ τούτου, είναι σημαντικό να ληφθούν μέτρα για να διασφαλιστεί ότι οι αποφάσεις που βασίζονται στην τεχνητή νοημοσύνη λαμβάνονται με τρόπο που σέβεται τα ανθρώπινα δικαιώματα και ότι τυχόν πιθανοί κίνδυνοι ή βλάβες ελαχιστοποιούνται. Οι συγγραφείς κατέληξαν στο συμπέρασμα ότι ο πιθανός αντίκτυπος της τεχνητής νοημοσύνης στα ανθρώπινα δικαιώματα είναι ένα σημαντικό ζήτημα που πρέπει να αντιμετωπιστεί και ότι απαιτείται περαιτέρω έρευνα για να κατανοηθούν τα αποτελέσματά της και να διασφαλιστεί ότι τα ανθρώπινα δικαιώματα γίνονται σεβαστά και προστατεύονται[83].

3 / Διαδίκτυο των πραγμάτων (Internet Of Things)

3.1 Τι είναι το IoT - Ιστορική αναδρομή

Το Διαδίκτυο των Πραγμάτων (IoT) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων (Stergiou et al., 2016)[84]. Ουσιαστικά συμβολίζει μια γενική αντίληψη για την ικανότητα των συσκευών δικτύου να αντιλαμβάνονται και να συλλέγουν δεδομένα από τον κόσμο και εν συνεχεία να συνεισφέρουν αυτά τα δεδομένα στο διαδίκτυο, όπου μπορούν να υποβληθούν σε επεξεργασία και να αναπτυχθούν για διάφορους ενδιαφέροντες λόγους[85].

[83] Aizenberg, E., & van den Hoven, J. (2020). Designing for human rights in AI. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720949566 Διαθέσιμο: https://journals.sagepub.com/doi/10.1177/2053951720949566 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[84] Stergiou, C., Psannis, K. E., Kim, B.-G. & Gupta, B., 2016. «*Secure integration of IoT and Cloud Computing*», Διαθέσιμο: https://ruomo.lib.uom.gr/bitstream/7000/79/1/1-s2.0-S0167739X1630694X-main%281%29.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[85] Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, 2014, «*Internet of Things for Smart Cities»,* Διαθέσιμο: https://ieeexplore.ieee.org/document/6740844 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]



Εικόνα 6: Η εξέλιξη του IoT

Πηγή: researchgate.net

Η σύλληψη της ιδέας του IoT έγινε αρχικά το 1982, όταν ένα τροποποιημένο μηχάνημα αυτόματης πώλησης Coca-Cola στο Πανεπιστήμιο Carnegie Mellon έγινε η πρώτη συνδεδεμένη στο ARPANET συσκευή, αναφέροντας το απόθεμά της και τη θερμοκρασία των φρεσκογεμισμένων ποτών[86]. Ωστόσο, ήταν ο Mark Weiser που το 1991 με το έργο του «Ο υπολογιστής του 21ου αιώνα»[87] και τα ακαδημαϊκά UbiComp και PerCom παρήγαγαν το σύγχρονο όραμα του IoT. Μάλιστα, το 1994 ο Reza Raji όρισε την ιδέα ως «*μεταφορά μικρών πακέτων δεδομένων σε μια τεράστια ποικιλία κόμβων, έτσι ώστε να ενσωματωθούν και να αυτοματοποιηθούν τα πάντα, από οικιακές συσκευές μέχρι τεράστια εργοστάσια*»[88].

Η φράση «Διαδίκτυο των πραγμάτων» και η ιδέα του προέκυψαν αρχικά σε μια ομιλία που δόθηκε από τον Peter T. Lewis τον Σεπτέμβριο του 1985 στην Ουάσιγκτον, DC, στο 15ο Ετήσιο Νομοθετικό Σαββατοκύριακο του Ιδρύματος Μαύρων Κογκρέσου[89].

---

[86] https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[87] Weiser, Mark (1991). *«The Computer for the 21st Century»*, Διαθέσιμο: https://web.archive.org/web/20150311220327/http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

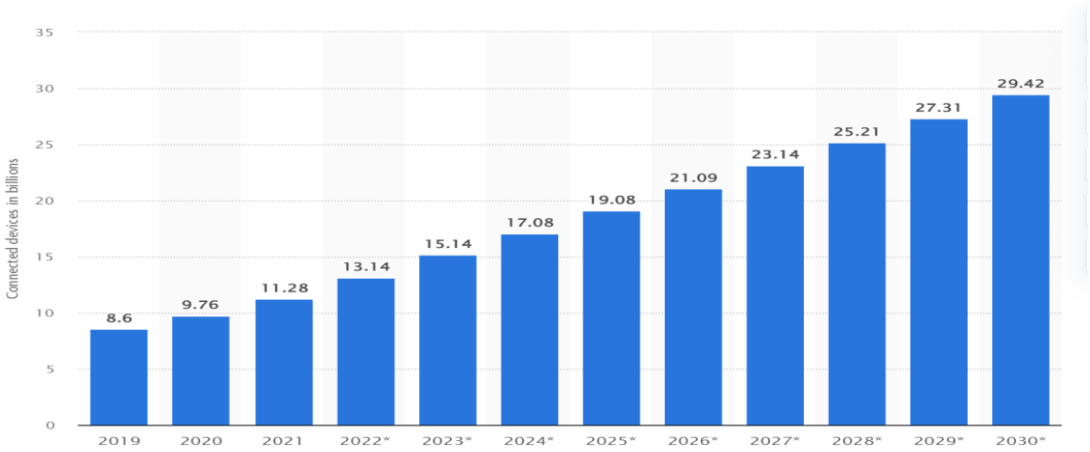
[88] *Raji, R.S. (1994). "Smart networks for control". IEEE Spectrum. 31 (6): 49–55, διαθέσιμο https://www.semanticscholar.org/paper/Smart-networks-for-control-Raji/f7b3654bc95a8a4c490d9d41c1ec63cf4cb37730* [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[89] CHETAN SHARMA, *«CORRECTING THE IOT HISTORY», 2016, http://www.chetansharma.com/correcting-the-iot-history/* [προσπέλαση 2 Αυγούστου 2021]

Σύμφωνα με τον Lewis, το Διαδίκτυο των Πραγμάτων, είναι «*η ενοποίηση ανθρώπων, διαδικασιών και τεχνολογίας με συνδεόμενες συσκευές και αισθητήρες για να καταστεί δυνατή η απομακρυσμένη παρακολούθηση, η κατάσταση, η τροποποίηση και η αξιολόγηση τάσεων τέτοιων πραγμάτων*».

Λίγα χρόνια αργότερα, ο Kevin Ashton της Procter & Gamble, και αργότερα του MIT, επινόησε τη φράση "Internet of things" το 1999[90]. Αλλά μόνο όταν η Gartner πρόσθεσε το IoT στη λίστα με τις νέες αναδυόμενες τεχνολογίες το 2011, άρχισε να αποκτά παγκόσμια δυναμική.

Σύμφωνα με την Statista υπολογίζεται ότι σήμερα υπάρχουν περίπου 15.14 δισεκατομμύρια συνδεδεμένες συσκευές IoT, ενώ ο αριθμός αναμένεται να διπλασιαστεί μέχρι το 2030[91].



Εικόνα 7: Εκτιμώμενος αριθμός συνδεδεμένων IoT συσκευών 2019-2030
Πηγή: statista.com

Γενικά, πρωταρχικός στόχος του Διαδικτύου των Πραγμάτων είναι να επιτρέψει νέες μορφές επικοινωνίας μεταξύ ανθρώπων και πραγμάτων καθώς και μεταξύ των ίδιων των πραγμάτων, ενσωματώνοντας κινητούς πομποδέκτες μικρής εμβέλειας σε μια ποικιλία συσκευών και καθημερινών αντικειμένων.

Σύμφωνα με τη Cisco Systems, το Διαδίκτυο των Πραγμάτων «γεννήθηκε» μεταξύ 2008 και 2009, με την αναλογία πραγμάτων/ανθρώπων να αυξάνεται από 0,08 το 2003 σε

[90] Ashton Kevin, That 'Internet of Things' Thing, 2009, διαθέσιμο: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[91] https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

1,84 το 2010. Η ίδια όρισε το IoT ως *ουσιαστικά το χρονικό σημείο όπου περισσότερα «πράγματα ή αντικείμενα» ήταν συνδεδεμένα με το Διαδίκτυο παρά οι άνθρωποι*[92].

Η ORACLE περιγράφει το Διαδίκτυο των Πραγμάτων ως το δίκτυο φυσικών αντικειμένων — «πράγματα» — που είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες με σκοπό τη σύνδεση και την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα μέσω του Διαδικτύου. Αυτές οι συσκευές κυμαίνονται από συνηθισμένα οικιακά αντικείμενα έως εξελιγμένα βιομηχανικά εργαλεία[93].

Για την AMAZON, ο όρος IoT, ή Internet of Things, αναφέρεται στο συλλογικό δίκτυο των συνδεδεμένων συσκευών και στην τεχνολογία που διευκολύνει την επικοινωνία μεταξύ συσκευών και του cloud, καθώς και μεταξύ των ίδιων των συσκευών. Χάρη στην εμφάνιση των φθηνών τσιπ υπολογιστών και των τηλεπικοινωνιών υψηλού εύρους ζώνης, έχουμε πλέον δισεκατομμύρια συσκευές συνδεδεμένες στο διαδίκτυο. Αυτό σημαίνει ότι οι καθημερινές συσκευές όπως οι οδοντόβουρτσες, οι ηλεκτρικές σκούπες, τα αυτοκίνητα και οι μηχανές μπορούν να χρησιμοποιούν αισθητήρες για τη συλλογή δεδομένων και την έξυπνη απόκριση στους χρήστες[94].

Σύμφωνα δε με το άρθρο 31 παρ. 5 του Νόμου 4961/2022 περί αναδυόμενων τεχνολογιών πληροφορικής και επικοινωνιών, το Διαδίκτυο των Πραγμάτων είναι «*κάθε τεχνολογία η οποία: α) επιτρέπει σε συσκευές ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών, μέσω της σύνδεσής τους με το διαδίκτυο, να εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων, συμπεριλαμβανομένης της τεχνολογίας εκείνης που αφορά στη διασύνδεση φυσικών πραγμάτων, ιδίως συσκευών, οχημάτων και κτιρίων, με ηλεκτρονικά εξαρτήματα, λογισμικό, αισθητήρες (sensors), ελεγκτές ενεργοποίησης (actuators), ραδιοζεύξεις και σύνδεση δικτύου και β) επιτρέπει τη συλλογή και ανταλλαγή ψηφιακών δεδομένων, προκειμένου να προσφέρουν ποικίλες υπηρεσίες στους χρήστες, με ή χωρίς την ανθρώπινη συμμετοχή.*».

Το IoT ως μια από τις πιο σημαντικές τεχνολογίες του 21ου αιώνα διευκολύνει τη σύνδεση καθημερινών αντικειμένων, συσκευών κουζίνας, αυτοκινήτων, θερμοστατών, βρεφικών οθονών κτλ στο διαδίκτυο, μέσω ενσωματωμένων συσκευών, επιτρέποντας την

[92] Evans, Dave, 2011, «The Internet of Things How the Next Evolution of the Internet Is Changing Everything», Cisco white paper, Διαθέσιμο: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[93] https://www.oracle.com/internet-of-things/what-is-iot/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[94] https://aws.amazon.com/what-is/iot/?nc1=h_ls [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

επικοινωνία μεταξύ ανθρώπων, διαδικασιών και πραγμάτων[95]. Κατ' αυτό τον τρόπο πραγματοποιείται μεταξύ τους η συλλογή και επεξεργασία των δεδομένων αυτόματα, χάρη στις υπηρεσίες cloud, big data, Machine learning κ.α., που τους επιτρέπουν να προσαρμόζουν κάθε αλληλεπίδραση μεταξύ των συνδεδεμένων πραγμάτων.

Αναφορικά με τα συνολικά ετήσια έσοδα παγκοσμίως του IoT, αυτά βάσει της Statista για φέτος υπολογίζεται να ανέλθουν στα 293.2 δισεκατομμύρια δολάρια Αμερικής, ενώ το 2030 αναμένεται να έχουν διπλασιαστεί[96].

3.2 Κατηγορίες του Διαδικτύου των Πραγμάτων

Σύμφωνα με το Cloud Credential Council, κορυφαίο πάροχο προγραμμάτων πιστοποίησης των επαγγελματιών πληροφορικής στον ψηφιακό μετασχηματισμό, υπάρχουν δύο τύποι Διαδικτύου των Πραγμάτων (IoT), το IIoT (Industrial Internet Of Things) και το CIoT (Consumer Internet Of Things), δηλαδή το Βιομηχανικό και το Καταναλωτικό Διαδίκτυο των Πραγμάτων αντίστοιχα[97].

Το Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT), χρησιμοποιώντας μηχανική μάθηση και την τεχνολογία μεγάλων δεδομένων για να επεξεργάζεται τα δεδομένα των αισθητήρων, σε συνδυασμό με τις τεχνολογίες αυτοματισμού, αυξάνει την αποτελεσματικότητα, την παραγωγικότητα μιας επιχείρησης, συνεπώς οι πελάτες της είναι ευχαριστημένοι.

Από την άλλη το Καταναλωτικό Διαδίκτυο των Πραγμάτων CIoT, που απευθύνεται σε μεμονωμένα άτομα ή μικρές ομάδες ατόμων, μπορεί να προσφέρει σε αυτούς άνεση, ασφάλεια, ποιότητα, ευκολία, αποτελεσματικότητα.

Η Syntegra, ένας παγκόσμιος πάροχος λύσεων επικοινωνίας CPaaS, παρουσιάζει πέντε τύπους Διαδικτύου των Πραγμάτων (IoT)[98]:

---

[95] F. Mattern and C. Floerkemeier, «*From the Internet of Computers to the Internet of Things*» Διαθέσιμο: https://link.springer.com/chapter/10.1007/978-3-642-17226-7_15 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[96]Internet of Things (IoT) total annual revenue worldwide from 2020 to 2030 (in billion U.S. dollars) Διαθέσιμο: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[97]https://www.cloudcredential.org/blog/knowledge-byte-the-different-types-of-iot/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[98] https://syntegra.net/internet-of-things-the-five-types-of-iot/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Πίνακας 2 - Τύποι IoT σύμφωνα με τη Syntegra

ΤΥΠΟΙ ΙΟΤ	ΠΕΡΙΓΡΑΦΗ
Industrial Internet Of Things	Το Industrial IoT (IIoT), είναι ίσως η πιο δυναμική πτέρυγα της βιομηχανίας IoT. Η εστίασή του είναι στην ενίσχυση των υφιστάμενων βιομηχανικών συστημάτων, καθιστώντας τα τόσο πιο παραγωγικά όσο και πιο αποδοτικά. Οι αναπτύξεις IIoT βρίσκονται συνήθως σε μεγάλης κλίμακας εργοστάσια και εργοστάσια παραγωγής και συχνά συνδέονται με βιομηχανίες όπως η υγειονομική περίθαλψη, η γεωργία, η αυτοκινητοβιομηχανία και η εφοδιαστική.
Consumer Internet Of Things	Το Consumer IoT (CIoT) αναφέρεται στη χρήση του IoT για εφαρμογές και συσκευές καταναλωτών. Τα κοινά προϊόντα CIoT περιλαμβάνουν smartphone, wearables, έξυπνους βοηθούς, οικιακές συσκευές
Military Internet Of Things	Το Internet of Battlefield Things ή απλά IoBT. Το IoMT είναι ακριβώς αυτό που ακούγεται - η χρήση του IoT σε στρατιωτικές ρυθμίσεις και καταστάσεις σε πεδία μάχης. Αποσκοπεί κυρίως στην αύξηση της επίγνωσης της κατάστασης, στην ενίσχυση της αξιολόγησης κινδύνου και στη βελτίωση των χρόνων απόκρισης.
Commercial Internet Of Things	Ενώ το CIoT τείνει να επικεντρώνεται στην ενίσχυση των προσωπικών και οικιακών περιβαλλόντων, το Commercial IoT προχωρά λίγο παραπέρα, προσφέροντας τα οφέλη του IoT σε μεγαλύτερους χώρους. Πχ: εμπορικά κτίρια γραφείων, σούπερ μάρκετ, καταστήματα, ξενοδοχεία, εγκαταστάσεις υγειονομικής περίθαλψης και χώροι ψυχαγωγίας
Infrastructure Internet Of Things	Το Infrastructure IoT ασχολείται με την ανάπτυξη έξυπνων υποδομών που ενσωματώνουν τεχνολογίες IoT για την ενίσχυση της αποδοτικότητας, την εξοικονόμηση κόστους, τη συντήρηση κ.λπ. Αυτό περιλαμβάνει τη δυνατότητα παρακολούθησης και ελέγχου λειτουργιών αστικών και

	αγροτικών υποδομών, όπως γέφυρες, σιδηροδρομικές γραμμές και και υπεράκτια αιολικά πάρκα.

Το 2019 παρουσιάστηκε στο Journal of Advanced Research in Dynamical and Control Systems[99] μια κριτική για τους τύπους του IoT, οι οποίοι σύμφωνα με τους συγγραφείς έχει ως εξής[100]:

Πίνακας 3 - Τύποι IoT σύμφωνα με το Journal of Advanced Research

ΤΥΠΟΙ ΙΟΤ	ΠΕΡΙΓΡΑΦΗ
Internet of Everything (IoE)	Το Internet of Everything (IoE) είναι μια νέα εποχή στο IoT. Το Διαδίκτυο των Πραγμάτων (IoT) αφορά τα πράγματα (Φυσικά Αντικείμενα), ενώ το Διαδίκτυο των Πάντων (IoE) αφορά τα πράγματα, τους ανθρώπους και τις διαδικασίες και τα δεδομένα. Το IoE συνεπάγεται Διαδίκτυο για τα πάντα.
Internet of Nano Things (IoNT)	Το Internet of Nano Things (IoNT) θα επικεντρωθεί στη διασύνδεση των νανο-συσκευών με το διαθέσιμο δίκτυο επικοινωνίας. Οι συσκευές νανο με νανο-εξαρτήματα είναι ενσωματωμένες σε μία μόνο συσκευή για την εκτέλεση πολλών εργασιών. Θα λειτουργεί σύμφωνα με τον τρόπο που συνδέουμε συσκευές μέσω Διαδικτύου. Οι κύριες διαφορές μεταξύ του Internet of Things (IoT) και Internet of Nano Things (IoNT) είναι ότι τα νανοστοιχεία δεν θα είναι επιτεύξιμα στο IoT.
Internet of Mission Critical Things (IoMCT)	Το Internet of Mission Critical Things (IoMCT) ενθαρρύνεται από τη σύγκλιση ανίχνευσης, επικοινωνίας, υπολογισμού και ελέγχου. Ο κύριος στόχος του IoMCT είναι να βελτιωθεί η χρήση της επιτήρησης δικτύου και όχι η μίξη διαφορετικών προϊόντων αισθητήρων. Για να μειωθούν οι επιβαρύνσεις στο ανθρώπινο σώμα, η μέθοδος

[99] https://www.jardcs.org/abstract.php?id=20 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[100] Srinivasan, C.R. & Bodduna, Rajesh & Saikalyan, P. & Premsagar, K. & Yadav, Eadala Sarath. (2019). «*A review on the different types of internet of things (IoT)»,* Διαθέσιμο: https://www.researchgate.net/publication/332153657_A_review_on_the_different_types_of_internet_of_things_IoT [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

	προσαρμογής, διαχείρισης και αναδιοργάνωσης των πηγών πληροφοριών, των συσκευών και του δικτύου θα πρέπει να είναι εξειδικευμένη ξεχωριστά. Το Internet of Machine Critical Things (IoMCT) πλησιάζει σε κρίσιμες αποστολές όπως πεδίο μάχης, περιπολία συνόρων, έρευνα και διάσωση, παρακολούθηση και επιτήρηση κρίσιμων δομών κ.λπ.
Internet of Mobile Things (IoMT)	Η ποιότητα των ψηφιακών συσκευών όπως τα τηλέφωνα μας χρησιμοποιεί εδώ και πολύ καιρό. Στα κινητά, οι ενσωματωμένοι αισθητήρες αυξάνονται με την αύξηση των φορητών συσκευών. Τώρα μπορούμε να επικοινωνήσουμε μεταξύ μας μέσω της συσκευής και με τους αισθητήρες τους. Η κύρια διαφορά μεταξύ του IoT και του IoMT, όσον αφορά την κινητικότητα των πραγμάτων, οι αλλαγές συμβαίνουν σε α) πλαίσιο β) συνδεσιμότητα γ) διαθεσιμότητα ενέργειας δ) ιδιωτικότητα και ασφάλεια.

3.3 Τεχνολογίες του Διαδικτύου των Πραγμάτων

Η ιδέα του IoT έχει δώσει στον κόσμο υψηλότερο επίπεδο προσβασιμότητας, ακεραιότητας, διαθεσιμότητας, επεκτασιμότητας, εμπιστευτικότητας και διαλειτουργικότητας όσον αφορά τη συνδεσιμότητα συσκευών[101]. Για τη μεταξύ τους σύνδεση το IoT χρησιμοποιεί διάφορες τεχνολογίες, οι οποίες ταξινομούνται σε δύο μεγάλες κατηγορίες, την Τεχνολογία αναγνώρισης και την Τεχνολογία επικοινωνίας.

3.3.1 Τεχνολογία Αναγνώρισης

Οι τεχνολογίες αναγνώρισης χρησιμοποιούνται για σκοπούς εντοπισμού και παρακολούθησης. Σε αυτές περιλαμβάνονται οι ετικέτες RFID που περιέχουν έναν αναγνώστη για τη συλλογή των πληροφοριών, και έναν πομπό για τη μετάδοση των

[101] Y. Lu and L. D. Xu, *«Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics»* 2019, doi: 10.1109/JIOT.2018.2869847. Διαθέσιμο: https://ieeexplore.ieee.org/abstract/document/8462745 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

πληροφοριών, το WSN wearable sensing devices, ο κωδικός QR, γραμμωτοί κώδικες, ευφυείς αισθητήρες κ.α.

3.3.2 Τεχνολογία Επικοινωνίας

Οι τεχνολογίες επικοινωνίας παρέχουν οδηγίες που πρέπει να ακολουθούνται για τη μεταφορά δεδομένων. Ορισμένα παραδείγματα τεχνολογιών επικοινωνίας που για διευθυνσιοδότηση χρησιμοποιούν IPv4 είτε IPv6 είναι:

- το πρωτόκολλο μικρής εμβέλειας ZigBee που χρησιμοποιείται για τη δημιουργία μικρών οικιακών δικτύων,
- το ασύρματο πρωτόκολλο μεγάλης εμβέλειας Z-wave που χρησιμοποιείται επίσης στον οικιακό αυτοματισμό,
- το πρωτόκολλο MQTT (Message Queue Telemetry Transport) που μπορεί να μεταδώσει πληροφορίες από μια πηγή σε πολλούς χρήστες μέσω ενός ενδιάμεσου κόμβου,
- το πρωτόκολλο μικρής εμβέλειας Bluetooth που χρησιμοποιείται πχ. στα έξυπνα κινητά για μεταφορά αρχείων στην αντιστοιχισμένη συσκευή,
- το ασύρματο πρωτόκολλο μικρής εμβέλειας Li-fi ,
- το δίκτυο μεσαίας εμβέλειας Wi-fi,
- το πρωτόκολλο δικτύωσης πολύ μικρής εμβέλειας NFC (Near Field Communication),
- το πρωτόκολλο μεσαίας εμβέλειας HaLow ,
- το ενσύρματο δίκτυο μεγάλης εμβέλειας Power line network area.

3.4 Εφαρμογές του Διαδικτύου των Πραγμάτων και παραδείγματα

Την εποχή που διανύουμε, υπάρχουν δισεκατομμύρια δικτυωμένα «έξυπνα» φυσικά αντικείμενα γύρω μας, που συλλέγουν και μοιράζονται δεδομένα μέσω του Διαδικτύου, δίνοντάς τους έτσι ένα επίπεδο ψηφιακής νοημοσύνης και αυτονομίας.

Το 2019 σύμφωνα με την McKinsey, περίπου το ένα τέταρτο των επιχειρήσεων χρησιμοποιούσαν τεχνολογίες IoT, από 13% το 2014. Σήμερα μάλιστα, υπάρχουν περισσότερες συνδεδεμένες συσκευές από ό, τι οι άνθρωποι στον κόσμο, σύμφωνα με την έκθεση State of the Connected World του Παγκόσμιου Οικονομικού Φόρουμ και

προβλέπεται ότι έως το 2025, 41,6 δισεκατομμύρια συσκευές θα συλλέγουν δεδομένα σχετικά με τον τρόπο με τον οποίο ζούμε, εργαζόμαστε, κινούμαστε μέσα στις πόλεις μας με τον τρόπο που λειτουργούμε και συντηρούμε τα μηχανήματα από τα οποία εξαρτόμαστε[102].

Οι εφαρμογές του IoT ποικίλλουν από ένα μικρό δίκτυο όπως ο οικιακός αυτοματισμός, σε μεγάλο δίκτυο όπως η εφαρμογή βιομηχανίας που βασίζεται στο cloud[103].

Ακολουθούν μερικές από τις πιο δημοφιλείς εφαρμογές του Διαδικτύου των Πραγμάτων:

3.4.1 Υγειονομική περίθαλψη

Το σημαντικότερο παράδειγμα εφαρμογής IoT στην υγεία είναι η απομακρυσμένη παρακολούθηση ασθενών στα πλαίσια της υγειονομικής περίθαλψης.

Στο Healthcare IoT (HIoT) ή αλλιώς Internet of Medical Things (IMoT) οι συσκευές περιέχουν ιατρικούς αισθητήρες με τους οποίους μπορούν να συλλέγουν αυτόματα μετρήσεις υγείας, όπως οξυγόνο, γλυκόζη, καρδιακούς παλμούς, αρτηριακή πίεση, θερμοκρασία και άλλα, από ασθενείς που δεν είναι φυσικά παρόντες σε μια μονάδα υγειονομικής περίθαλψης, εξαλείφοντας την ανάγκη να ταξιδεύουν οι ασθενείς στους παρόχους ή οι ασθενείς να τις συλλέγουν οι ίδιοι[104]. Υπάρχουν και αισθητήρες που εμφυτεύονται μέσα στο σώμα, όταν η υγεία των ασθενών πρέπει να παρακολουθείται συνεχώς.

3.4.1.1 Fitness ή Activity tracker και Έξυπνα ρολόγια – Smart Watches

Οι συσκευές αυτές περιλαμβάνουν βιοαισθητήρες που μπορούν να τοποθετηθούν απευθείας στο δέρμα για να παρέχουν μια στιγμιαία ένδειξη του καρδιακού ρυθμού, να

[102] https://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

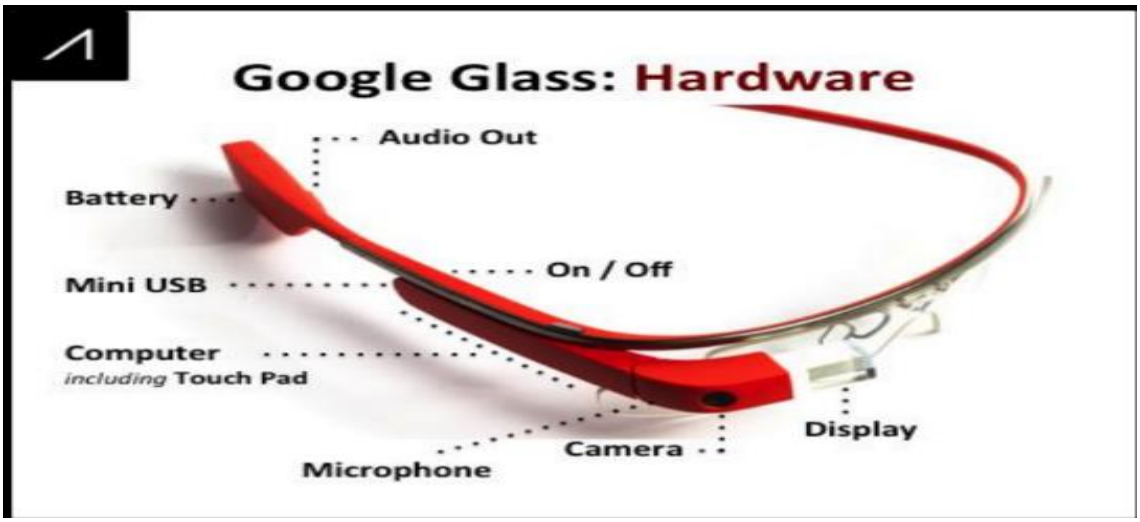
[103] Kotha, Harika & Gupta, V.. (2018). «*IoT Application, A Survey*», Διαθέσιμο: https://www.researchgate.net/publication/325116647_IoT_Application_A_Survey [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[104] Al-Shargabi, Bassam & Abuarqoub, Simak. (2020). «*IoT-Enabled Healthcare: Benefits, Issues and Challenges»,* 10.1145/3440749.3442596. Διαθέσιμο: https://www.researchgate.net/publication/351391253_IoT-Enabled_Healthcare_Benefits_Issues_and_Challenges [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

εντοπίζουν επερχόμενες καρδιακές προσβολές και να επιτρέπουν την έγκαιρη αναγνώριση τυχόν ανωμαλιών στον καρδιακό ρυθμό.

3.4.1.2 Έξυπνα γυαλιά – Smart glasses

Ακόμα ένα είδος συσκευής IoT είναι τα Wearable computer-glasses, τα οποία ουσιαστικά είναι ένας υπολογιστής που μπορεί να φορεθεί ως γυαλιά. Ωφελεί όλους τους τομείς, αλλά πολύ περισσότερο την επιστήμη της υγείας, καθώς επιτρέπει στους γιατρούς εν ώρα χειρουργείου, να παρακολουθούν τις ζωτικής σημασίας μετρήσεις, όπως είναι οι παλμοί της καρδιάς, τα ποσοστά οξυγόνου και η αρτηριακή πίεση, χωρίς να κοιτάξουν στο monitor.



Εικόνα 8: Google Glass in healthcare

Πηγή: researchgate.net

Η χρήση των έξυπνων γυαλιών θα δίνουν επίσης τη δυνατότητα στο χρήστη να ανιχνεύει τις κινήσεις των χεριών του, μετατρέποντας οποιαδήποτε επιφάνεια σε οθόνη αφής, αλλά και να μεταφράζει σε πραγματικό χρόνο το κείμενο που διαβάζει , προβάλλοντας τη μετάφραση πάνω στο περιοδικό που έχει μπροστά του[105].

Σύμφωνα με την επίσημη ιστοσελίδα του Metaverse τα έξυπνα γυαλιά θα γίνουν πύλες εισόδου στο μετασύμπαν, επιτρέποντας στο χρήστη να εγγράφει βίντεο και ήχο με

[105] Μυλώση, Μ.: Τα «έξυπνα γυαλιά» στην εποχή της επαυξημένης πραγματικότητας. Προστατεύοντας τα προσωπικά δεδομένα ως «κόρην οφθαλμού». International Conference «NEW TECHNOLOGIES IN HEALTH: MEDICAL, LEGAL AND ETHICAL ISSUES", Θεσσαλονίκη 20-21 Νοεμβρίου 2019, Εργαστήριο μελέτης ιατρικού δικαίου και βιοηθικής, ΑΠΘ, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ (2021) σελ. 255-265

ένα μόνο άγγιγμα και να προσθέσει ακμές εικονικής πραγματικότητας (AR) στον κόσμο γύρω του[106].

3.4.1.3 Link – Neuralink

Ένα ακόμη πολλά υποσχόμενο παράδειγμα εφαρμογής IoT στον τομέα της υγείας είναι το Link της Neuralink, ένα εμφύτευμα που διαβάζει νευρολογικά σήματα, με σκοπό να βοηθήσει τα άτομα με παράλυση να ανακτήσουν τον έλεγχο του σώματός τους[107].

3.4.2 Βιομηχανία – Εφοδιαστικές Αλυσίδες- Μεταφορές - Logistics

Οι βιομηχανίες με την εφαρμογή του IoT μπορούν να αυξήσουν την παραγωγικότητα τους και την ποιότητα των προϊόντων τους μειώνοντας στο ελάχιστο το κόστος και την σπατάλη των πόρων τους. Εταιρίες που δραστηριοποιούνται στην ενέργεια, τη γεωργία, τις μεταφορές και επιχειρήσεις κοινής ωφέλειας, εργάζονται σε έργα IoT που συνδέουν δισεκατομμύρια συσκευές και προσφέρουν αξία σε μια ποικιλία περιπτώσεων χρήσης, συμπεριλαμβανομένων των αναλύσεων πρόβλεψης ποιότητας και συντήρησης, κατάσταση περιουσιακών στοιχείων παρακολούθηση και βελτιστοποίηση της διαδικασίας[108].

Οι βιομηχανίες που δραστηριοποιούνται στις μεταφορές προσαρτώντας ετικέτες RFID ή γραμμωτούς κώδικες στο όχημα, μπορούν να παρακολουθούν τις πληροφορίες σε πραγματικό χρόνο των οχημάτων, όπως την τοποθεσία του οχήματος ή την ταχύτητά του. Με τον ίδιο τρόπο μια παλέτα ή ακόμη και ένα container που εξοπλίζεται με αισθητήρες μπορεί να δώσει πληροφορίες τόσο για την γεωγραφική του θέση ανά πάσα στιγμή, όσο και για τις περιβαλλοντικές συνθήκες που επικρατούν (θερμοκρασία, υγρασία κλπ). Η αξιοποίηση των εν λόγω δεδομένων συμβάλλει στην βελτίωση της αποδοτικότητας της εφοδιαστικής αλυσίδας, αλλά και στην εξασφάλιση της ποιότητας ευαίσθητων αγαθών όπως φάρμακα, τρόφιμα κ.α.

---

[106] https://about.meta.com/metaverse/#smart-glasses [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[107] https://neuralink.com/approach/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[108]Goundar, Sam & Bhardwaj, Akashdeep & Nur, Safiya & Kumar, Shonal & Harish, Rajneet. (2021). «*Industrial Internet of Things: Benefit, Applications, and Challenges*», 10.4018/978-1-7998-3375-8.ch010. Διαθέσιμο: https://www.researchgate.net/publication/348132641_Industrial_Internet_of_Things_Benefit_Applications_and_Challenges [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Στα logistics, οι εταιρίες μπορούν να παρακολουθούν την εισροή και την εκροή των προϊόντων χρησιμοποιώντας barcodes.

3.4.2.1 Έξυπνες αποθήκες – Smart warehouses

Στην κατηγορία αυτή ανήκουν τα Smart warehouses ή αλλιώς έξυπνες αποθήκες, οι οποίες στοχεύουν στην αύξηση της συνολικής ποιότητας υπηρεσιών, της παραγωγικότητας και της αποδοτικότητας της αποθήκης, ελαχιστοποιώντας ταυτόχρονα το κόστος και τις αστοχίες[109]. Για το σκοπό αυτό με τα χρόνια υιοθέτησαν έξυπνες τεχνολογίες ώστε να μπορούν να ανταπεξέλθουν στον όγκο των παραγγελιών, την ταξινόμηση των προϊόντων κ.α.

3.4.2.2 Amazon Prime Air

Με την εξέλιξη των ρομπότ, εταιρίες ηλεκτρονικού εμπορίου όπως η Amazon, ως κορυφαία εταιρία ηλεκτρονικού εμπορίου και υπολογιστικού νέφους, ανακοίνωσε την κυκλοφορία του Amazon Prime Air που είναι ένα αυτοματοποιημένο σύστημα παράδοσης. Το σύστημα χρησιμοποιεί drones (μικροσκοπικά μη επανδρωμένα οχήματα αέρος) (MUAVs) για να διανείμει τα δέματα στον συγκεκριμένο πελάτη σε λιγότερο από μισή ώρα[110].

Ήδη από το Δεκέμβριο του 2022 η Amazon έχει αρχίσει να παραδίδει παραγγελίες με drone στην περιοχή Lockeford της Καλιφόρνια και College Station του Τέξας, παραδίδοντας έναν μικρό αριθμό πακέτων ακριβώς στην ώρα των Χριστουγέννων[111].

---

[109] Geest, Maarten & Tekinerdogan, Bedir & Catal, Cagatay. (2021). «*Smart Warehouses: Rationale, Challenges and Solution Directions*», Διαθέσιμο: https://www.researchgate.net/publication/357372387_Smart_Warehouses_Rationale_Challenges_and_Solution_Directions [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[110] https://www.aboutamazon.com/news/transportation/amazon-prime-air-prepares-for-drone-deliveries [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[111] https://arstechnica.com/gadgets/2022/12/amazon-begins-drone-deliveries-in-california-and-texas/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Εικόνα 9: Drone της εταιρίας Amazon που παραδίδει πακέτα

Πηγή: aboutamazon.com

3.4.3 Στρατός

Το Internet of Military Things (IoMT) ή το Internet of Battlefield Things (IoBT) είναι μια κατηγορία Internet of Things (IoT) για σύγχρονες επιχειρήσεις μάχης και έξυπνο πόλεμο. Αναφέρεται σε φυσικά αντικείμενα στον στρατιωτικό τομέα, τα οποία είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες. Αυτά τα αντικείμενα επικοινωνούν μεταξύ τους για να συλλέξουν και να μεταφέρουν δεδομένα μέσω του Διαδικτύου για να ολοκληρώσουν ένα ευρύ φάσμα δραστηριοτήτων με πιο αποτελεσματικό και ενημερωμένο τρόπο[112].

Ανάμεσα στα οφέλη του IoT στον στρατό είναι η αυτόματη εξαγωγή πληροφοριών από το πεδίο μάχης, η συνεχής παρακολούθηση των ζωτικών στοιχείων στρατιωτών, οι έξυπνες και αυτάρκεις στρατιωτικές βάσεις και η δυνατότητα προσομοίωσης μαχών.

3.4.3.1 Project Crimson

Στα πλαίσια της ετήσιας αμερικάνικης στρατιωτικής άσκησης που έλαβε χώρα από τα τέλη Σεπτεμβρίου έως το Νοέμβριο 2022, στρατιώτες πολλών εθνών συνεργάστηκαν για να εξερευνήσουν νέες τεχνολογίες στην υπηρεσία του πολέμου. Τότε στην έρημο νότια

[112]Kott, Alexander & Swami, Ananthram & West, Bruce. (2016). «*The Internet of Battle Things*», Διαθέσιμο: https://www.researchgate.net/publication/311215660_The_Internet_of_Battle_Things [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

της Death Valley, στη στρατιωτική βάση Fort Irwin California, πραγματοποιήθηκε μια άσκηση προσομοίωσης πολέμου με τον τίτλο «Project Crimson», κατά τη διάρκεια του οποίου παραδόθηκαν φιάλες ψεύτικου αίματος με drones σε δήθεν τραυματίες του πεδίου μάχης[113].

Δοκιμάζοντας την παράδοση ιατρικών προμηθειών με drone, σε συνδυασμό με άλλη τεχνολογία, ο στρατός αναζητά τρόπους για να διασφαλίσει την επιβίωση των στρατιωτών μετά από τραυματισμούς μάχης, ακόμη και σε περιπτώσεις όπου δεν είναι ασφαλές να στέλνεις ανθρώπους με τα πόδια για βοήθεια.

3.4.4 Αγροτικές εφαρμογές

Ο παγκόσμιος πληθυσμός πρόκειται να φτάσει τα 9,5 δισεκατομμύρια μέχρι το έτος 2040. Για να επιβιώσει λοιπόν αυτός ο μεγάλος πληθυσμός και η ζήτηση για πολλά τρόφιμα να ικανοποιηθεί, θα πρέπει η αγροτική βιομηχανία να αποδεχθεί το IoT. Με τον τρόπο αυτό θα αντιμετωπίσει καλύτερα και τις προκλήσεις, όπως οι ακραίες κλιματικές συνθήκες, αύξηση θερμοκρασίας και περιβαλλοντικές επιπτώσεις που προκύπτουν από πρακτικές εντατικής γεωργίας[114].

Το IoT στη γεωργία χρησιμοποιεί ρομπότ, drones, απομακρυσμένους αισθητήρες σε συνδυασμό με μηχανική μάθηση (Machine learning) και αναλυτικά εργαλεία, για την παρακολούθηση των καλλιεργειών (κατάσταση εδάφους - παρακολούθηση μετρήσεων του εδάφους, της υγρασίας και του νερού) και την καλύτερη εκμετάλλευση των αγροτικών πόρων[115].

Στην υδατοκαλλιέργεια χρησιμοποιείται για τον έλεγχο της δράσης των θερμαντικών σωμάτων που χρησιμοποιούνται σε δεξαμενές ψαριών για παροχή οξυγόνου. Με τη χρήση χημικών αισθητήρων ο αγρότης μπορεί να πάρει τις πληροφορίες σχετικά με το νερό και τη θερμοκρασία του[116].

---

[113] https://www.dailymail.co.uk/sciencetech/article-11453187/US-Army-tests-DRONES-deliver-blood-medical-supplies-dangerous-battlefield-situations.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

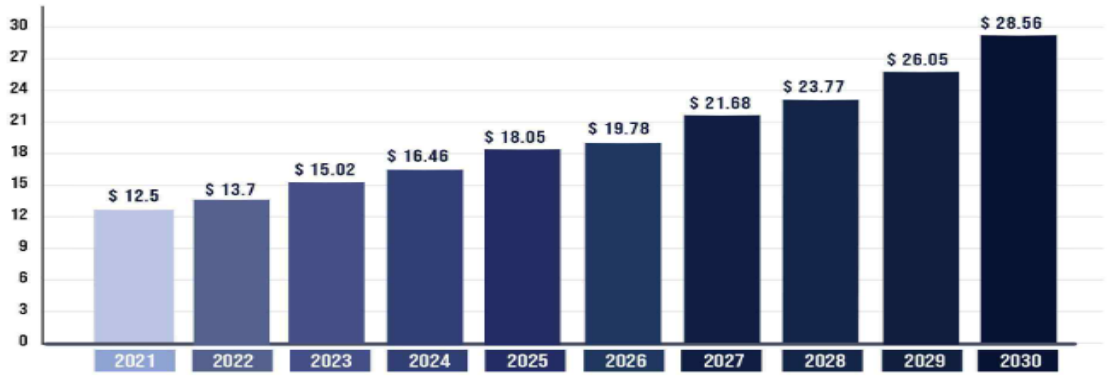
[114] https://www.researchgate.net/publication/357809791_IOT_IN_AGRICULTURE [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[115] Verdouw, Cor & Wolfert, Sjaak & Tekinerdogan, Bedir. (2016). «*Internet of Things in agriculture*», Διαθέσιμο: https://www.researchgate.net/publication/312164156_Internet_of_Things_in_agriculture [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[116] Kotha, Harika & Gupta, V.. (2018). *«IoT Application, A Survey»*, Διαθέσιμο: https://www.researchgate.net/publication/325116647_IoT_Application_A_Survey [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

3.4.4.1 AgrIOT - Farmsensors

Ιδανικό παράδειγμα η AgrIOT, η οποία χρησιμοποιεί κινητά και ασύρματα δίκτυα αισθητήρων (farm sensors) για τη συλλογή και ανάλυση δεδομένων οπωροφόρων δέντρων μεγάλης κλίμακας αξιόπιστα, έγκαιρα και αποτελεσματικά, με σκοπό την αύξηση της παραγωγικότητας, τη μείωση των απωλειών λόγω παρασίτων και τη βελτιστοποίηση της αποδοτικότητας χρήσης του νερού[117].



Εικόνα 10: Αγορά IoT στην γεωργία 2021-2030

Πηγή: precedenceresearch.com

Σύμφωνα με τον παγκόσμιο οργανισμό έρευνας αγοράς και παροχής συμβουλών Precedenceresearch, το παγκόσμιο Διαδίκτυο των πραγμάτων (IoT) στη γεωργική αγορά αποτιμήθηκε σε 13,7 δισεκατομμύρια δολάρια ΗΠΑ το 2022 και προβλέπεται ότι θα αξίζει περίπου 28,56 δισεκατομμύρια δολάρια μέχρι το 2030 με καταγεγραμμένο CAGR[118] 9,62% από το 2022 έως το 2030[119].

3.4.5 Οικιακός αυτοματισμός - Έξυπνα σπίτια

Στα έξυπνα σπίτια το IoT μπορεί να προσφέρει σημαντική εξοικονόμηση χρημάτων από τον έλεγχο της κατανάλωσης ενέργειας με έξυπνο θερμοστάτη. Αυτό επιτυγχάνεται με τη χρήση ενός κεντρικού διανομέα που συνήθως είναι ένα έξυπνο

[117] https://www.smartfarmsensing.com/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[118] Compound annual growth rate (CAGR) – ετήσιος αριθμός ανάπτυξης
[119] https://www.precedenceresearch.com/iot-in-agriculture-market [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

τηλέφωνο με αισθητήρες, στο οποίο θα συνδεθεί χρησιμοποιώντας NFC, Bluetooth, ή άλλα πρωτόκολλα μικρής εμβέλειας.

Με την ίδια λογική λειτουργεί και η έξυπνη κλειδαριά, το έξυπνο ψυγείο ή το κλιματιστικό κ.α.

3.4.6 Έξυπνη πόλη

Η χρήση της τεχνολογίας IoT στην πόλη διευκολύνει τη ζωή μας, αφού μας παρέχει βιώσιμη ανάπτυξη και υψηλή ποιότητα ζωής. Ορισμένες από τις εφαρμογές της είναι ο έξυπνος φωτισμός που προσαρμόζεται ανάλογα με τις συνθήκες που επικρατούν, η διαχείριση απορριμμάτων, οι έξυπνοι δρόμοι κ.α.

Υπάρχουν πολλές πόλεις στην Ελλάδα όπως η Αθήνα, η Θεσσαλονίκη ή τα Τρίκαλα Θεσσαλίας, οι οποίες έχουν εδώ και χρόνια υιοθετήσει έξυπνες εφαρμογές εύρεσης θέσης στάθμευσης ή διαχείρισης κυκλοφορίας.

Στο εξωτερικό η Βαρκελώνη είναι μία από τις πόλεις που θεωρούνται πλέον «έξυπνες», καθώς έχει υιοθετήσει λύσεις IoT όπως, έξυπνο φωτισμό, με τα φώτα LED να διαθέτουν αισθητήρες που μπορούν να ανιχνεύσουν την κίνηση, τον καιρό, τη ρύπανση και τον θόρυβο. Μεταξύ άλλων εφαρμόζει μέσω αισθητήρων εντοπισμό αυξημένης κυκλοφοριακής κίνησης, και έξυπνο parking.

3.4.7 Περιβάλλον

Διάφορα είδη αισθητήρων χρησιμοποιούνται για κάθε περιβαλλοντική ανάγκη. Για παράδειγμα για την ανάλυση της ατμοσφαιρικής ρύπανσης χρησιμοποιούνται αισθητήρες σκόνης και αισθητήρες αερίων[120]. Η ανίχνευση παραμέτρων όπως η θερμοκρασία γίνεται με αισθητήρες RTD ή θερμόμετρο. Με τη χρήση των τεχνολογιών e-Tonge (ηλεκτρονική γλώσσα) και e – Nose (ηλεκτρονική μύτη) μπορεί να εντοπιστεί η παρουσία χημικών ουσιών. Αυτές οι τεχνολογίες κάνουν χρήση λογισμικού αναγνώρισης προτύπων και χρησιμοποιούνται στις πόλεις για την παρακολούθηση των επιπέδων

[120] Chodorek, Agnieszka, Robert Ryszard Chodorek, and Alexander Yastrebov. 2022. «*The Prototype Monitoring System for Pollution Sensing and Online Visualization with the Use of a UAV and a WebRTC-Based Platform*», Διαθέσιμο: https://pubmed.ncbi.nlm.nih.gov/35214478/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

ρύπανσης[121]. Στις εφαρμογές για το περιβάλλον μπορεί να προστεθεί η πυρανίχνευση δασικών περιοχών, η ανίχνευση σεισμικών δονήσεων κ.α.

3.5 Οφέλη του Διαδικτύου των Πραγμάτων (IoT)

Είναι πια βέβαιο πως το IoT, ως ένα δίκτυο συνδεδεμένων συσκευών που αλληλεπιδρούν μεταξύ τους ανταλλάσσοντας δεδομένα, αποτελεί μία τεχνολογία με πολλές προεκτάσεις που συνεχώς εξελίσσεται. Τα πλεονεκτήματα που προσφέρει η χρήση του IoT διαφοροποιούνται ανάλογα με τον τομέα εφαρμογής του και εξαρτώνται από πολλούς παράγοντες. Καθημερινά συναντούμε πολλές εφαρμογές IoT, όπως τα έξυπνα wearables, τα έξυπνα κινητά, οι τηλεοράσεις και άλλες συσκευές, την έξυπνη παρακολούθηση υγείας, τα ρομπότ σε νοσοκομεία κ.λ.π., οι οποίες διευκολύνουν την καθημερινότητα μας, προσφέροντας μας πολλές λειτουργίες.

Μερικά λοιπόν από τα οφέλη που προσφέρει το IoT είναι ενδεικτικά τα εξής[122, 123, 124]:

- **Ασφάλεια και Προσωπική βοήθεια**

Η συνεχής παρακολούθηση, μέσω έξυπνων συσκευών, των σπιτιών, πόλεων κτλ ενισχύει την ασφάλεια και προσφέρει προσωπική προστασία. Επίσης μέσω των κατάλληλων προγραμματισμών ενός συστήματος από το χρήστη, μπορούν να πραγματοποιούνται αυτόματα οι απαραίτητες αναβαθμίσεις, αυξάνοντας έτσι την ασφάλειά του. Για παράδειγμα, το GM OnStar[125], είναι μια ενσωματωμένη συσκευή που το σύστημα εντοπίζει ένα τροχαίο ατύχημα ή ένα ατύχημα στο δρόμο. Κάνει αμέσως μια κλήση εάν εντοπιστεί ατύχημα ή ατύχημα.

- **Εξοικονόμηση χρόνου και μείωση κόστους**

Η χρήση του IoT δίνει τη δυνατότητα αυτοματοποίησης καθημερινών χρονοβόρων λειτουργιών, εξοικονομώντας περισσότερο χρόνο στον χρήστη, αλλά και λιγότερο κόστος

---

[121] Kotha, Harika & Gupta, V.. (2018). «*IoT Application, A Survey*», Διαθέσιμο: https://www.researchgate.net/publication/325116647_IoT_Application_A_Survey [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[122] https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[123] https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[124] https://techvidvan.com/tutorials/advantages-and-disadvantages-of-iot/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[125] https://www.onstar.com/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

πχ. γλυτώνει την αμοιβή που θα πλήρωνε σε κάποιον, ο οποίος θα ήταν επιφορτισμένος με την ολοκλήρωση διάφορων ενεργειών, τις οποίες τώρα αναλαμβάνει το IoT.

- **Πρόβλεψη αποτελεσμάτων**

Η συλλογή τωρινών και παρελθοντικών δεδομένων μπορεί να συμβάλει στην πρόβλεψη πιθανών μελλοντικών αποτελεσμάτων (predictive analytics).

- **Βελτίωση καθημερινής ζωής**

Το σύνολο των εφαρμογών αυτής της τεχνολογίας έχει κοινό παρανομαστή, τη βελτίωση ποιότητας ζωής, καθώς προσφέρει αυξημένη άνεση, ευκολία και καλύτερη διαχείριση σε καθημερινές δραστηριότητες.

3.6 Κίνδυνοι και προκλήσεις του Διαδικτύου των Πραγμάτων

Η κατανόηση των κινδύνων που σχετίζονται με την ανάπτυξη του Διαδικτύου των πραγμάτων είναι όλο και πιο σημαντική, αφού παράλληλα με όλα τα θετικά που έφερε, άνοιξε και το «κουτί της Πανδώρας» για το έγκλημα στον κυβερνοχώρο, κλέβοντας προσωπικές πληροφορίες και ταυτότητα, κατασκοπεύοντας την επαγγελματική και ιδιωτική ζωή των ανθρώπων καθώς και άλλα συναφή ζητήματα (Olinder et al.)[126].

Πολλοί άνθρωποι σήμερα εκφράζουν τις ανησυχίες τους σχετικά με τη χρήση του IoT, υποστηρίζοντας ότι η ανεξέλεγκτη χρήση του οδηγεί αναπόφευκτα σε μειωμένη πνευματική και σωματική δραστηριότητα των ανθρώπων, τα οποία μπορούν να προκαλέσουν σοβαρά προβλήματα υγείας.

Εκτός από αυτό, αρκετοί έχουν την πεποίθηση ότι λόγω της αντικατάστασης των ανθρώπων από ρομπότ σε ορισμένες θέσεις εργασίας, ο κίνδυνος της αύξησης της ανεργίας είναι υπαρκτός, με συνεπακόλουθο τη μείωση αποδοχών ακόμα και των πιο εξειδικευμένων εργατών.

3.6.1 Ζητήματα ασφάλειας δεδομένων, απορρήτου και ιδιωτικότητας

Ήδη από το 2014 η Γαλλική Αρχή Προστασίας Δεδομένων, με αφορμή την κυκλοφορία των «έξυπνων γυαλιών», όρισε το ανθρώπινο σώμα ως το καινούριο

[126] Nina Olinder, Konstantin Fedyakin, Elena Korneeva «*Personal Data Protection in the Internet of Things »,* Διαθέσιμο: https://www.researchgate.net/publication/350375595_Personal_Data_Protection_in_the_Internet_of_Things [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

διασυνδεδεμένο αντικείμενο, «*LE CORPS, NOUVEL OBJET CONNECTÉ*»[127], υπογραμμίζοντας ότι η γνώση πληροφοριών που αφορούν τον χρήστη, προέρχεται από την ανάλυση αλγορίθμων πρόβλεψης και την ανάλυση δεδομένων μεγάλης κλίμακας (big data) που επιτρέπουν την εξαγωγή έμμεσων πληροφοριών και συμπερασμάτων για τη ζωή του χρήστη μέσω των αισθητήρων που τα γυαλιά φέρουν και αφορούν για παράδειγμα τον αριθμό των βημάτων που ο χρήστης διανύει. Σύμφωνα με τη Γαλλική Αρχή, η αυξανόμενη «μυστικότητα» χρήσης αυτών των αισθητήρων, του σώματος του χρήστη και του άμεσου περιβάλλοντός του, είναι τάση που ακολουθείται από τα έξυπνα γυαλιά της Google. Σε αυτό το πλαίσιο είναι πιθανό να επηρεάζεται πέρα από την ιδιωτικότητα του ιδίου του χρήστη των γυαλιών και η ιδιωτικότητα των ατόμων που βρίσκονται γύρω του, στην εμβέλεια της συσκευής και ηχογραφούνται ή βιντεοσκοπούνται εν αγνοία τους, το δε περιεχόμενο καταγραφής (φωνή, ήχος, εικόνα), είναι πιθανό να διαμοιράζεται σε τρίτους διαμέσου του υπολογιστικού νέφους ή των μέσων κοινωνικής δικτύωσης. (Μυλώση, 2019)[128].

Τα κύρια ζητήματα που σχετίζονται με την προστασία δεδομένων αφορούν την ποσότητα και την ποικιλία των προσωπικών δεδομένων που υφίστανται επεξεργασία, καθώς και την επεξεργασία και τα αποτελέσματά της. Η χρήση πολύπλοκων αλγορίθμων και λογισμικού για τη μετατροπή μεγάλων ποσοτήτων δεδομένων σε πόρο για τη λήψη αποφάσεων έχει άμεση επίδραση σε άτομα και ομάδες, ιδιαίτερα σε περιπτώσεις δημιουργίας προφίλ ή επισήμανσης, και αυτό τελικά εγείρει μια σειρά από ανησυχίες για την προστασία των δεδομένων[129].

Το Διαδίκτυο των Πραγμάτων εξαρτάται σε μεγάλο βαθμό από τον συνδυασμό φυσικών αισθητήρων και τη δύναμη του Διαδικτύου. Οι αισθητήρες χρησιμοποιούνται για τη συλλογή δεδομένων από το εξωτερικό περιβάλλον, τα οποία στη συνέχεια

---

[127] CAHIERS IP, «LE CORPS, NOUVEL OBJET CONNECTÉ DU QUANTIFIED SELF À LA M-SANTÉ : LES NOUVEAUX TERRITOIRES DE LA MISE EN DONNÉES DU MONDE», Nr. 2, Cnil 2014, σελ.19, Διαθέσιμο: https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[128] Μυλώση, Μ.: Τα «έξυπνα γυαλιά» στην εποχή της επαυξημένης πραγματικότητας. Προστατεύοντας τα προσωπικά δεδομένα ως «κόρην οφθαλμού». International Conference «NEW TECHNOLOGIES IN HEALTH: MEDICAL, LEGAL AND ETHICAL ISSUES", Θεσσαλονίκη 20-21 Νοεμβρίου 2019, Εργαστήριο μελέτης ιατρικού δικαίου και βιοηθικής, ΑΠΘ, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ (2021) σελ. 255-265

[129] Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων, 23 Ιανουαρίου 2017, σ. 2

συνδυάζονται με πληροφορίες που είναι αποθηκευμένες στο cloud[130]. Στη συνέχεια, αυτά τα δεδομένα αναλύονται στο σύνολό τους για να δημιουργήσουν δράσεις με βάση τα συμφραζόμενα ή να παράσχουν συμφραζόμενες συμβουλές. Όσο περισσότερα δεδομένα είναι διαθέσιμα, τόσο πιο ακριβή θα είναι τα αποτελέσματα, καθώς το σύστημα είναι σε θέση να λαμβάνει καλύτερες αποφάσεις με βάση τον μεγαλύτερο όγκο πληροφοριών (Bastos et al., 2018)[131]. Φυσικά ο όγκος δεδομένων που παράγονται από συσκευές IoT καθιστούν δύσκολη την επίβλεψη, τη διαχείριση και την προστασία δεδομένων.

Σήμερα δε, υπάρχουν αισθητήρες για τη λήψη σχεδόν κάθε πληροφορίας από το περιβάλλον. Μερικά παραδείγματα αισθητήρων είναι: εικόνα, βίντεο, ήχος, τοποθεσία, εγγύτητα, θερμοκρασία, υγρασία, επιτάχυνση, πίεση, αέριο και καρδιακός παλμός (Bastos et al., 2018). Για παράδειγμα στις «έξυπνες πόλεις» συλλέγονται διάφορα προσωπικά δεδομένα των πολιτών πολλές φορές εν αγνοία τους: Από δημογραφικά δεδομένα (γεννήσεις/θάνατοι/γάμοι), μέχρι εργασιακά δεδομένα, δεδομένα δημοσκοπήσεων αλλά και καμερών. Τα παραπάνω συλλέγονται μέσω αισθητήρων και καμερών που βρίσκονται σε κάδους απορριμμάτων, σε φανάρια ρύθμισης κυκλοφορίας, στους δρόμους, σε φρεάτια, ή και κατά τη χρήση του δωρεάν Wi-Fi, ενώ η συλλογή και επεξεργασία αυτών γίνεται συνήθως για στατιστικούς και διαφημιστικούς λόγους, αλλά ενδεχομένως και για λόγους επιτήρησης. Πρόκειται ουσιαστικά για μια διαρροή πληροφοριών η οποία λαμβάνει χώρα μέσω της διασύνδεσης συστημάτων χωρίς απαραίτητα τα υποκείμενα των δεδομένων να το επέτρεψαν.

Μια τέτοια συλλογή και επεξεργασία δεδομένων μπορεί δυνητικά να οδηγήσει σε ταυτοποίηση ενός φυσικού προσώπου. Αυτό δύναται να συμβεί με τη συσχέτιση κάποιου αναγνωριστικού χαρακτηριστικού με το άτομο ή με δεδομένα που το αφορούν, ταυτοποιώντας το κατ' αυτό τον τρόπο, στα οποία συμπεριλαμβάνεται και ο εντοπισμός θέσης χρήστη μέσω GPS ή IP διεύθυνσης. Παραδείγματος χάρη, τα wearables συλλέγουν και περαιτέρω δεδομένα εκτός από αυτά για τα οποία προορίζονται, με αποτέλεσμα η συλλογή αυτή από πολλές συσκευές αισθητήρων να βοηθά στη δημιουργία μοναδικών αποτυπωμάτων και σταθερότερων αναγνωριστικών στοιχείων, τα οποία στη συνέχεια

[130] Το Cloud είναι μια τεχνολογία αποθήκευσης οποιασδήποτε μορφής πληροφορίας όχι τοπικά αλλά διαδικτυακά σε Data Centers ή Server Farms, η οποία προσφέρει πλεονεκτήματα στους χρήστες της όπως, ασφάλεια δεδομένων,Back up, χωρητικότητα, ευκολία, αξιοπιστία, μικρό κόστος κ.α.

[131] Bastos, Daniel & Giubilo, Fabio & Shackleton, Mark & El-Mousa, Fadi. (2018). «*GDPR Privacy Implications for the Internet of Things*». Διαθέσιμο: https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

μπορούν να αντιστοιχιστούν με συγκεκριμένα άτομα από τα ενδιαφερόμενα μέρη του ΔτΠ.

Ο τεράστιος όγκος των προσωπικών δεδομένων που παράγονται από τις διασυνδεδεμένες συσκευές IoT ενέχει κίνδυνο για το απόρρητο και την προστασία των δεδομένων. Η ευρωπαϊκή νομοθεσία για την προστασία δεδομένων δίνει έμφαση στη διαφάνεια, αλλά με τόσες πολλές συνδεδεμένες συσκευές, δεν είναι πάντα σαφές ποιος συλλέγει τα δεδομένα, έχει πρόσβαση σε αυτά και τα χρησιμοποιεί[132]. Επιπλέον, ο μεγάλος όγκος δεδομένων που παράγονται από το IoT, σε συνδυασμό με σύγχρονες τεχνικές ανάλυσης δεδομένων και διασταύρωσης, μπορεί να επιτρέψει τη χρήση των δεδομένων για δευτερεύοντες σκοπούς, όπως η εξαγωγή συμπερασμάτων σχετικά με τις προτιμήσεις ή τις καταναλωτικές συνήθειες κάποιου, που μπορεί να οδηγήσει σε δημιουργία προφίλ/μοτίβων, όπως αυτή ορίζεται στο άρθρο 4 παρ. 4 ΓΚΠΔ[133].

Σύμφωνα μάλιστα με την Γνώμη 8/2014 της Ομάδας εργασίας του άρθρου 29, η χρήση των συσκευών οικιακού αυτοματισμού εγείρει συγκεκριμένες προκλήσεις σε σχέση με την προστασία των δεδομένων και της ιδιωτικής ζωής, καθώς η ανάλυση των συνήθων τρόπων χρήσης σε ένα τέτοιο πλαίσιο είναι πιθανό να αποκαλύπτει λεπτομέρειες για τον τρόπο ζωής, τις συνήθειες ή τις επιλογές των ενοίκων – ή απλά την παρουσία τους στο σπίτι. Γι' αυτό ειδικά οι λύσεις IoT που χρησιμοποιούνται σε σπίτια (και όχι μόνο), απαιτούν ισχυρούς ελέγχους προστασίας δεδομένων και απορρήτου, ώστε να επιτυγχάνεται κατάλληλο επίπεδο κυβερνοασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής τους και να αποτρέπονται απόπειρες μη εξουσιοδοτημένων τρίτων να αλλοιώσουν τη χρήση ή τις επιδόσεις τους κ.α.

Στα πλαίσια συμμόρφωσης με τον ΓΚΠΔ που θα αναλυθεί σε επόμενο κεφάλαιο, προκειμένου η όποια επεξεργασία δεδομένων ενός ατόμου να είναι σύννομη, θα πρέπει να συντρέχουν κάποιες προϋποθέσεις (άρθρο 6 ΓΚΠΔ), μεταξύ των οποίων η συγκατάθεση του υποκειμένου των δεδομένων. Σε αρκετές περιπτώσεις ο χρήστης ενδέχεται να μην είναι ενήμερος για την επεξεργασία των δεδομένων του από τις συσκευές του IoT και αυτή

[132] Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2017), Understanding the Internet of Things,

[133] Άρθρο 4 παρ. 4 του Γενικού Κανονισμού για την Προστασία Δεδομένων – Ορισμοί: «…4) «*κατάρτιση προφίλ»: οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου*»

η έλλειψη ενημέρωσης συνιστά σημαντικό εμπόδιο για την παραχώρηση έγκυρης συγκατάθεσης του. Η έλλειψη της (προσήκουσας) συγκατάθεσης αποτελεί ένα από τα κυριότερα προβλήματα του IoT. Και αυτό διότι σύμφωνα με το άρθρο 7 ΓΚΠΔ, η συγκατάθεση πρέπει να προκύπτει από δήλωση ή σαφή θετική ενέργεια, να είναι ελεύθερη, συγκεκριμένη και εν πλήρει επιγνώσει, να ανακαλείται τόσο εύκολα όσο παρέχεται, να δίδεται σε γραπτή, ηλεκτρονική ή προφορική μορφή και βέβαια να μπορεί να αποδειχθεί από τον υπεύθυνο επεξεργασίας και μάλιστα υπό την προϋπόθεση της προηγούμενης πλήρους ενημέρωσης του υποκειμένου για την επεξεργασία των δεδομένων του. Για τον παραπάνω λόγο θα πρέπει να δημιουργηθούν νέοι μέθοδοι απόκτησης της έγκυρης συναίνεσης από τον τελικό χρήστη , όπως «privacy proxies»[134] και οι πολιτικές «συγκόλλησης» δεδομένων - «sticky policies»[135].

Επιγραμματικά, η συμμόρφωση με τον GDPR σε περιβάλλον IoT απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων, ενώ κρίνεται απαραίτητη και η ελαχιστοποίηση δεδομένων, δηλαδή η συλλογή μόνο των εκείνων των δεδομένων που χρειάζονται για την εκπλήρωση του σκοπού που συλλέχθηκαν. Επίσης θα πρέπει να υπάρχει διαφανής επεξεργασία, δηλαδή η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση, αλλά και το δικαίωμα στη λήθη, ήτοι η δυνατότητα διαγραφής των δεδομένων που αφορούν το υποκείμενο. Φυσικά η αναφορά τυχόν παραβίασης είναι απαραίτητη, όπως και το απόρρητο από τη σχεδίαση των συσκευών IoT, συνοδευόμενο από την εκτίμηση αντικτύπου του άρθρου 35 παρ.1 ΓΚΠΔ.

Όταν εταιρείες ή οργανισμοί επιδιώκουν να εφαρμόσουν μια νέα κατασκευαστική ή βιομηχανική πρωτοβουλία IoT ή να συνδέσουν υπάρχουσα τεχνολογία για αυτοματοποιημένη και απομακρυσμένη παρακολούθηση ή πρόσβαση, είναι σημαντικό να ληφθούν υπόψη οι πιθανοί κίνδυνοι και οι φορείς επίθεσης που σχετίζονται με αυτές τις αποφάσεις. Αυτό σημαίνει ότι λαμβάνεται υπόψη η ασφάλεια του συστήματος, η δυνατότητα για κακόβουλους παράγοντες να αποκτήσουν πρόσβαση στο σύστημα και η

[134] Τα privacy proxies ή proxies υψηλής ανωνυμίας προσφέρουν τη μεγαλύτερη ασφάλεια σε έναν χρήστη. Αποκρύπτουν τη διεύθυνση IP του χρήστη και δεν προσδιορίζονται ως διακομιστές μεσολάβησης σε διακομιστές ιστού (σε αντίθεση με τους ανώνυμους διακομιστές μεσολάβησης). Αυτοί οι διακομιστές μεσολάβησης αλλάζουν τακτικά τις διευθύνσεις IP όταν υποβάλλουν αιτήματα σε διακομιστές ιστού, επιτρέποντας υψηλό επίπεδο απορρήτου.

[135] Οι sticky policies ή σταθερές πολιτικές αντιπροσωπεύουν μια προσέγγιση για τη βελτίωση του ελέγχου των ιδιοκτητών στα δεδομένα τους. Σε μια τέτοια προσέγγιση, πολιτικές αναγνώσιμες από μηχανή επισυνάπτονται στα δεδομένα. Ονομάζονται «κολλώδη» καθώς ταξιδεύουν μαζί με δεδομένα, καθώς τα δεδομένα ταξιδεύουν σε πολλούς τομείς διαχείρισης.

πιθανότητα παραβίασης δεδομένων ή άλλων κακόβουλων δραστηριοτήτων. Είναι επίσης σημαντικό να ληφθεί υπόψη η πιθανότητα μη εξουσιοδοτημένης πρόσβασης στο σύστημα, καθώς και η πιθανότητα χειραγώγησης ή κλοπής δεδομένων. Λαμβάνοντας υπόψη αυτούς τους κινδύνους, οι εταιρείες και οι οργανισμοί μπορούν να διασφαλίσουν ότι τα συστήματά τους είναι ασφαλή και ότι τα δεδομένα τους προστατεύονται. Ιδιαίτερα μάλιστα με την τάση που επικρατεί τελευταία για «εμπορευματοποίηση» των προσωπικών δεδομένων των ανθρώπων, τυχόν αποτυχία εξασφάλισης επαρκών μέτρων ασφαλείας κατά της παραβίασης, ή αδυναμία συμμόρφωσης με όλα τα ισχύοντα πρότυπα προστασίας δεδομένων, τα πρωτόκολλα κρυπτογράφησης και άλλους κανονισμούς και τεχνολογίες που έχουν σχεδιαστεί για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητα δεδομένα, μπορεί να επιφέρει δαπανηρές και καταστροφικές συνέπειες, όπως κλοπές ταυτότητας, απώλεια εταιρικών μυστικών, εξοπλισμού ή προϊόντων, δολιοφθορά κ.λπ.[136].

Επιπλέον, η υλοποίηση της υποδομής IoT απαιτεί σε επιχειρηματικές επενδύσεις τη δημιουργία, συντήρηση και επέκταση ενός δικτύου πολλών έξυπνων συσκευών και τη σχετική τεχνική υποδομή, συμπεριλαμβανομένου του δικτύου τροφοδοσίας και του δικτύου επικοινωνίας, αλλά επίσης και έμπειρα άτομα που εξειδικεύονται σε λύσεις IoT για να αποφευχθεί η παρεμβολή στη λειτουργικότητα των έξυπνων συσκευών και η πρόκληση του «φαινόμενου χιονοστιβάδας»[137].

3.6.2 Ζητήματα ασφάλειας δικτύων και συστημάτων υπολογιστών

Η συνεχής αύξηση των διασυνδεδεμένων συσκευών, αυξάνει και τα «σημεία εισόδου» που μπορούν να εκμεταλλευτούν χάκερς και κυβερνοεγκληματίες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και χωρίς δικαίωμα πρόσβαση σε κάποιο σύστημα (hacking). Τέτοιες «κυβερνοεπιθέσεις» έχουν πάντοτε αρκετές αρνητικές επιπτώσεις. Ένας επιτιθέμενος μπορεί να εντοπίσει πιθανά κενά ασφαλείας των συστημάτων, τα οποία θα μπορούσαν μεταξύ άλλων να είναι:

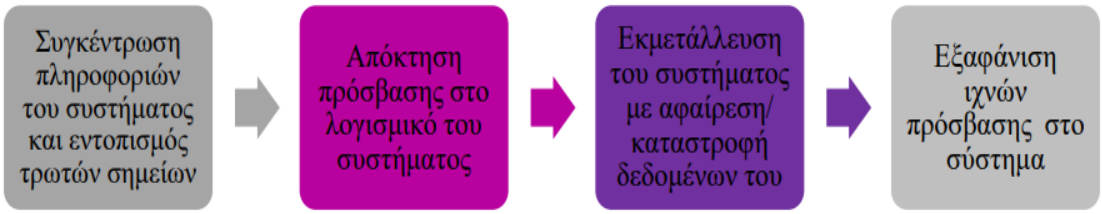
- η **ελλιπής πιστοποίηση** ή εξουσιοδότηση, δηλαδή περιπτώσεις αδύναμου κωδικού πρόσβασης,

[136] https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[137] https://light-it.net/blog/9-prominent-benefits-of-iot-for-business/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

- η **απώλεια κρυπτογράφησης** κατά τη μεταφορά δεδομένων που συμβαίνει διότι συνήθως οι IoT συσκευές είναι φθηνές συσκευές χαμηλής επεξεργαστικής ισχύος με αποτέλεσμα την αδυναμία εφαρμογής κρυπτογράφησης των δεδομένων ή ισχυρών αλγόριθμων ασφαλούς επικοινωνίας
- το **επισφαλές λογισμικό**, ήτοι το λογισμικό κάποιων IoT συσκευών που δεν δέχεται ενημερώσεις και αναβαθμίσεις
- τα **αδύναμα διαπιστευτήρια**

Ειδικότερα, τα στάδια μιας τέτοιας επίθεσης σε ένα σύστημα IoT είναι τα εξής:



Όταν εκτελείται μια επίθεση, μπορεί να οδηγήσει σε παραβιάσεις δεδομένων, με αποτέλεσμα απώλεια ή χειραγώγηση δεδομένων. Εκτός από το γεγονός ότι το φυσικό ή νομικό πρόσωπο που υπέστη την επίθεση, υφίσταται οικονομικές απώλειες, κλονίζεται και η εμπιστοσύνη των πελατών και ταυτόχρονα η φήμη του.

Για τους λόγους αυτούς, προκειμένου να περιορίσουμε τις επιθέσεις στον κυβερνοχώρο, εφαρμόζουμε την ασφάλεια στον κυβερνοχώρο, δηλαδή μια μέθοδο προστασίας των δικτύων, των συστημάτων υπολογιστών και των στοιχείων τους από μη εξουσιοδοτημένη ψηφιακή πρόσβαση, που αλλιώς ονομάζεται «κυβερνοασφάλεια».

3.6.2.1 Είδη κακόβουλων επιθέσεων

Οι εισβολείς ή «hackers» ενίοτε χρησιμοποιούν διαφορετικά είδη επίθεσης σε συστήματα προκειμένου να αποκτήσουν πρόσβαση σε αυτά, μερικά από τα οποία είναι τα εξής:

- **«αυτοαναπαραγόμενα κακόβουλα λογισμικά (malicious software/malware/badware)»** με ή χωρίς ξενιστή, που υποκλέπτουν πληροφορίες ή κρυπτογραφούν δεδομένα, ή παρακολουθούν ενέργειες του χρήστη ανάλογα με τη μορφή που έχει προσβληθεί το πληροφοριακό σύστημα,

- **«ιούς (viruses)»** οι οποίοι αποτελούν το συνηθέστερο και πιο γνωστό είδος κακόβουλου λογισμικού και απαιτεί ξενιστή. Ουσιαστικά πρόκειται για ένα πρόγραμμα-εκτελέσιμο αρχείο το οποίο «μολύνει» το σύστημα, επισυνάπτοντας τον εαυτό του σε αρχεία τα οποία υπάρχουν σε αυτόν, και τροποποιεί τη λειτουργία τους.
- **«σκουλήκια (worms)»,** κακόβουλο λογισμικό το οποίο πολλαπλασιάζεται δίχως την ενέργεια του χρήστη, μέσω διαδικτύου ή δικτύου υπολογιστών.
- **«δούρειος ίππος (trojan horse)»,** καμουφλαρισμένο πρόγραμμα που ξεγελά το χρήστη κάνοντάς τον να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία, ενώ στην πραγματικότητα αποκτά πρόσβαση στα αρχεία του υπολογιστή και τα χρησιμοποιεί κατά βούλησή του ο δράστης, πχ. εγκαθιστώντας στον υπολογιστή του θύματος κακόβουλα προγράμματα, τις λεγόμενες «κερκόπορτες». Με τη χρήση τους οι «hackers» προβαίνουν στη λεγόμενη «Distributed denial of service (DDoS attack)», όπου σε μία δεδομένη στιγμή συντονίζουν όλους τους υπολογιστές να απαιτήσουν δεδομένα και υπηρεσίες από ένα συγκεκριμένο σύστημα, το οποίο και φυσικά μετά από την υπερβολική ζήτηση που αντιμετωπίζει, καταρρέει.
- **«Botnet»** λογισμικό που επιτρέπει στο δράστη να μολύνει πλήθος υπολογιστών άλλων χρηστών, να τους καθιστά «όργανά» του (υπολογιστές «ζόμπι» και στη συνέχεια μέσω αυτού του λογισμικού πραγματοποιεί ενέργειες όπως «Distributed denial of service (DDoS attacks)»
- **«λογισμικά παρακολούθησης (spyware)[138]»** είδος κακόβουλου λογισμικού το οποίο φορτώνεται κρυφά (με ύπουλο τρόπο) σε έναν υπολογιστή χωρίς να το ξέρει ο χρήστης και εκτελείται στο παρασκήνιο κάνοντας διάφορα πράγματα πίσω από την πλάτη του χρήστη. Το Spyware κρύβεται ώστε να μην μπορεί το θύμα να τον εντοπίσει εύκολα, συγκεντρώνει στοιχεία σχετικά με το χρήστη (ιστοσελίδες που επισκέπτεται, κωδικούς πρόσβασης, ακόμη και αριθμούς πρόσβασης πιστωτικών καρτών). Επίσης αλλάζει ρυθμίσεις και εκτελεί άλλες κακόβουλες και ενοχλητικές δραστηριότητες.
- **«καταγραφή πλήκτρων (key logger)[139]»** , είναι η δράση της καταγραφής των πλήκτρων που πατήθηκαν σε ένα πληκτρολόγιο, συνήθως κρυφά, έτσι ώστε το άτομο που χρησιμοποιεί το πληκτρολόγιο να μην γνωρίζει ότι οι ενέργειές του παρακολουθούνται

[138] https://usa.kaspersky.com/resource-center/threats/spyware [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[139] https://www.kaspersky.com/resource-center/definitions/keylogger [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

- **«logic bombs»** κώδικας ενσωματωμένος σε κάποιο κανονικό πρόγραμμα που είναι προγραμματισμένος να εκραγεί όταν ικανοποιούνται συγκεκριμένες συνθήκες
- **«ransomware[140]»** είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος σε αυτά, μέχρι να δοθούν λύτρα από το θύμα
- **«Pharming»** ο δράστης (pharmer) εκμεταλλεύεται το τρωτό σημείο κάποιου λογισμικού και αφού επέμβει σε αυτό, ανακατευθύνει τον ανυποψίαστο επισκέπτη μιας ιστοσελίδας σε μία άλλη κατασκευασμένη από τον ίδιο με σκοπό εκεί να του αποσπάσουν εμπιστευτικές πληροφορίες.
- **«Phishing» (ηλεκτρονικό ψάρεμα)** ο δράστης (phisher) με την αποστολή πχ. ηλεκτρονικών μηνυμάτων email προσπαθεί να αποσπάσει εμπιστευτικές πληροφορίες που ανήκουν στον παραλήπτη του μηνύματος, πχ. ζητάει τα στοιχεία πιστωτικής κάρτας ή πρόσβασης στην ηλεκτρονική τραπεζική (e-banking) προκειμένου να αποσπάσει χρήματα.
- **«Denial of service (DoS attack)»**: σε αυτή την περίπτωση ο hacker τρέχει από έναν υπολογιστή πολλαπλά προγράμματα με αυτοματοποιημένη αποστολή μηνυμάτων και εντολών τα οποία βομβαρδίζουν το δίκτυο με δεδομένα και έτσι το υπερφορτώνει ώστε να αδυνατεί να ανταποκριθεί, σε αντίθεση με την «Distributed denial of service (DDoSS attack)» που πραγματοποιείται από περισσότερους υπολογιστές[141].
- **«DNS Spoofing ή DNS cache poisoning[142]»**: Εδώ ο hacker τροποποιεί το Domain Name Code που είναι η αριθμητική, δυαδική ψηφιοποιημένη διεύθυνση ενός ιστότοπου. Αυτό σημαίνει ότι όταν ένας χρήστης πληκτρολογεί την αριθμητική διεύθυνση ενός ιστότοπου, μπορεί να ανακατευθυνθεί σε διαφορετικό ιστότοπο. Αυτό μπορεί να είναι επιζήμιο για τον ιστότοπο που αρχικά προσπαθούσε να επισκεφτεί ο χρήστης, καθώς μπορεί να οδηγήσει σε απώλεια εσόδων. Επιπλέον, ο χάκερ μπορεί να δημιουργήσει έναν ιστότοπο mirror, ο οποίος είναι ακριβές αντίγραφο του ιστότοπου, και να τον χρησιμοποιήσει για να εξάγει ευαίσθητα προσωπικά δεδομένα από τον χρήστη, ο οποίος πιστεύει ότι τα δίνει στον πραγματικό ιστότοπο.

---

[140] https://cyberalert.gr/ransomware/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[141] Tripathi, Nikhil & Mehtre, Babu. (2013). «*DoS and DDoS Attacks: Impact, Analysis and Countermeasures»,* Διαθέσιμο: https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Impact_Analysis_and_Countermeasures [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[142] https://www.kaspersky.com/resource-center/definitions/dns [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

- **«IP Spoofing[143]»:** αναφέρεται στην δημιουργία πακέτων IP με ψεύτικη διεύθυνση προέλευσης ούτως ώστε να συγκαλυφθεί η ταυτότητα του αποστολέα του πακέτου και ο παραλήπτης να νομίζει ότι προήλθε από άλλον υπολογιστή
- **«Email Spoofing»:** είναι η δημιουργία μηνυμάτων ηλεκτρονικού ταχυδρομείου με μία πλαστή διεύθυνση αποστολέα[144]
- **«Packet Sniffers»:** Ο ανιχνευτής πακέτων είναι ένας τύπος προγράμματος που επιτρέπει στον χρήστη να λαμβάνει και να ερμηνεύει πακέτα πληροφοριών που μεταδίδονται μέσω του Διαδικτύου. Τα πακέτα είναι μικρά κομμάτια δεδομένων που αποστέλλονται μέσω ενός δικτύου υπολογιστών, όπως όνομα χρήστη, κωδικός σύνδεσης ή email. Αυτά τα πακέτα αποστέλλονται χρησιμοποιώντας το πρωτόκολλο μετάδοσης Ethernet, που σημαίνει ότι κάθε μηχάνημα στο δίκτυο μπορεί να δει το πακέτο. Κάθε πακέτο έχει μια κεφαλίδα Ethernet, η οποία είναι μια αριθμητική διεύθυνση που διασφαλίζει ότι το σωστό μηχάνημα λαμβάνει τις σωστές πληροφορίες. Ωστόσο, ο ανιχνευτής πακέτων είναι ένας τύπος λογισμικού που επιτρέπει σε έναν χάκερ ή έναν διαχειριστή δικτύου να υποκλέψει πληροφορίες που δεν προορίζονται για τη διεύθυνσή τους. Αυτός ο τύπος λογισμικού μπορεί να χρησιμοποιηθεί για την απόκτηση πρόσβασης σε εμπιστευτικές πληροφορίες, γι' αυτό είναι σημαντικό να υπάρχουν μέτρα ασφαλείας για την προστασία από το sniffing πακέτων.

3.6.3 Αποτελέσματα έρευνας σχετικά με την τεχνολογία IoT

Σε μια έρευνα του τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Δυτικής Μακεδονίας[145] που διεξήχθη τον Νοέμβριο του 2020, 458 άτομα ερωτήθηκαν σχετικά με το IoT, εκ των οποίων 283 γυναίκες και 175 άντρες.

---

[143] https://www.kaspersky.com/resource-center/threats/ip-spoofing [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[144]Babu, P. & Bhaskari, Lalitha & CH.Satyanarayana,. (2011). «*A Comprehensive Analysis of Spoofing*». Διαθέσιμο: https://www.researchgate.net/publication/49597043_A_Comprehensive_Analysis_of_Spoofing [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[145] Maria Papatsimouli, Lazaros Lazaridis, Dimitris Ziouzios, Minas Dasygenis, George Fragulis « *Internet Of Things (IoT) awareness in Greece*», SHS Web Conf., 139 (2022) 03013 DOI: https://doi.org/10.1051/shsconf/202213903013 Διαθέσιμο: https://www.shs-conferences.org/articles/shsconf/abs/2022/09/shsconf_etltc2022_03013/shsconf_etltc2022_03013.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Στην πρώτη ερώτηση «*Σε ποιο βαθμό αντιπροσωπεύονται οι τεχνολογίες IoT στην Ελλάδα*;» οι ερωτηθέντες απάντησαν ότι το 47,6% αυτών έχει χρησιμοποιήσει, ενώ το 52,4% απάντησε αρνητικά.

Στη συνέχεια ερευνήθηκε ποιο από τα δύο φύλα είναι πιο εξοικειωμένο με το IoT. Τα αποτελέσματα έδειξαν ότι 118 από το σύνολο των αντρών, δηλαδή ποσοστό 67,4% και 138 από το σύνολο των γυναικών, δηλαδή ποσοστό 48,8% ήταν εξοικειωμένοι. Αυτό σημαίνει ότι οι άντρες είναι περισσότερο εξοικειωμένοι από τις γυναίκες με τις τεχνολογίες IoT.

Τελευταία ερώτηση ήταν αν το εισόδημα συνδέεται με τη γνώση των IoT. Σύμφωνα με τα αποτελέσματα της έρευνας, οι ερωτηθέντες που είχαν εισόδημα μεταξύ 501-1500 ευρώ και γνωρίζουν τις τεχνολογίες IoT, ήταν σχεδόν διπλάσιοι σε αριθμό από εκείνους που δεν τη γνωρίζουν.

Στα πλαίσια της έρευνας εξετάστηκε επίσης αν οι εργαζόμενοι ή οι άνεργοι είναι πιο εξοικειωμένοι με τις τεχνολογίες IoT. Τα αποτελέσματα έδειξαν ότι δύο στους τρεις εργαζόμενους γνωρίζουν την τεχνολογία, ενώ ένας στους δύο ανέργους όχι.

Με την ίδια μέθοδο ερευνήθηκε κατά πόσο οι συμμετέχοντες που γνωρίζουν το IoT το χρησιμοποιούν και τα αποτελέσματα έδειξαν ότι 205, ήτοι ποσοστό 94% των ερωτηθέντων γνωρίζει το IoT και το χρησιμοποιεί, ενώ μόλις το 6% δεν έχει κάνει χρήση.

3.7 Μέτρα ασφαλείας πληροφοριακών συστημάτων και κατ' επέκταση του IoT

Για την αποφυγή τυχόν παραβιάσεων, η ασφάλεια των συστημάτων θα πρέπει να είναι προτεραιότητα των κατασκευαστών από τον σχεδιασμό και την παραγωγή των αισθητήρων έως και την υλοποίησή του, όπως πλέον προβλέπει και η σχετική νομοθεσία.

Η ασφάλεια λοιπόν των πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές ιδέες, την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα (Mcclure et al., 2009)

- *ακεραιότητα* (integrity), δηλαδή η απόλυτη (ακέραιη) διατήρηση των πληροφοριών και η μη εξουσιοδοτημένη μεταβολή τους,
- *διαθεσιμότητα* (availability), δηλαδή η δυνατότητα εκμαίευσης πληροφοριών χωρίς δυσκολίες και καθυστερήσεις ενός πληροφοριακού συστήματος,

- *εμπιστευτικότητα* (confidentiality) δηλαδή η προστασία των δεδομένων από άτομα που δεν έχουν καμία εξουσιοδότηση για πρόσβαση σε αυτά τα δεδομένα.

Ανάλογα με το είδος των συστημάτων, ορισμένα μπορούν περισσότερο και άλλα λιγότερο να εφαρμόσουν χαρακτηριστικά ασφαλείας. Ωστόσο, για ένα ασφαλές σύστημα θα πρέπει κανείς να φροντίσει για τα εξής :

- φυσική ασφάλεια του συστήματος ή *physical security*, ήτοι την προστασία του υλικού αντικειμένου,
- ασφάλεια υπολογιστικού συστήματος ή *computer security*, ήτοι την προστασία του λειτουργικού συστήματος και των δεδομένων ή εφαρμογών
- ασφάλεια των βάσεων δεδομένων ή *database security*, ήτοι τη προστασία των περιεχόμενων μιας τέτοιας βάσης
- ασφάλεια των δικτύων επικοινωνιών ή *network security*, ήτοι τη προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω δικτύων

Τα μέτρα ασφαλείας, ή μέτρα προστασίας, ή αντίμετρα συμπληρώνουν την πολιτική ασφαλείας. Αφορούν όλες τις διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος. Τα μέτρα ασφαλείας χωρίζονται σε τέσσερις μεγάλες κατηγορίες (Mcclure et al., 2009):

- *πρόληψη,* όπου τα αντίμετρα προσπαθούν να μειώσουν τον κίνδυνο,
- *διασφάλιση*, με εργαλεία, ελέγχους και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων,
- *ανίχνευση*, με προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών,
- *επαναφορά*, με διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον μετά από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε.

Η επιτυχής εφαρμογή των μέτρων ασφαλείας απαιτεί ένα σχέδιο που περιγράφει συγκεκριμένες διαδικασίες για συνεχείς ενημερώσεις. Μόλις τεθεί σε ισχύ το σχέδιο ασφαλείας, θα πρέπει να δημιουργηθεί ένα ολοκληρωμένο σχέδιο έκτακτης ανάγκης, το οποίο θα πρέπει να περιλαμβάνει ένα σχέδιο αποκατάστασης από καταστροφή και ένα σχέδιο επιχειρηματικής ανάκαμψης. Η εφαρμογή της ασφάλειας σε ένα σύστημα πληροφοριών είναι μια προκλητική και περίπλοκη διαδικασία που απαιτεί προσεκτική εξέταση και σχεδιασμό (Τσουραμάνης, 2005).

Η τεχνολογία IoT συνοδεύεται από πολλά τρωτά σημεία, τα οποία μπορούν να απειλήσουν την προσωπική και δημόσια ασφάλεια. Το Internet of Things διαθέτει μεγάλο αριθμό πρωτοκόλλων που ποικίλλουν ανάλογα με τις συνδεδεμένες συσκευές, αυξάνοντας έτσι την πολυπλοκότητα μιας συνεπούς λύσης ασφαλείας. Τα ζητήματα της προστασίας του IoT και της διαχείρισης ασφάλειας μπορούν να χωριστούν σε τρία επίπεδα: συσκευή, δίκτυο και cloud. Το πιο σημαντικό ζήτημα στην ασφάλεια του IoT είναι η προστασία των δεδομένων που μεταδίδονται, ανταλλάσσονται και αποθηκεύονται επειδή τα πρωτόκολλα για την προστασία δεδομένων είναι περιορισμένα (Papatsimouli et al, 2022).

4 / Η Τεχνητή Νοημοσύνη των Πραγμάτων (AIoT)

4.1 Τι είναι το AIoT (Artificial Intelligence of Things);

Η Τεχνητή Νοημοσύνη των Πραγμάτων ή AIoT αναφέρεται στη σύγκλιση των τεχνολογιών τεχνητής νοημοσύνης (AI) με υποδομή Διαδικτύου των πραγμάτων (IoT) για την επίτευξη πιο αποτελεσματικών λειτουργιών IoT, τη βελτίωση των αλληλεπιδράσεων ανθρώπου-μηχανής και τη βελτίωση της διαχείρισης και ανάλυσης δεδομένων.

Το IoT και η AI είναι ανεξάρτητες τεχνολογίες που έχουν αντίκτυπο σε διάφορους κλάδους. Είναι το μέλλον του βιομηχανικού αυτοματισμού και της 4ης Βιομηχανικής Επανάστασης (Industry 4.0)[146].

Όπως ήδη αναφέρθηκε εκτενώς, στόχος του IoT είναι η επίτευξη της συνδεσιμότητας των πάντων όπου είναι δυνατόν, με σκοπό την αυτοματοποίηση, τη βελτίωση των αλληλεπιδράσεων ανθρώπου-μηχανής, μηχανής- μηχανής, αλλά και της διαχείρισης και ανάλυσης δεδομένων, ενώ της τεχνητής νοημοσύνης η μίμηση της ανθρώπινης ευφυΐας.

Καθώς ο αριθμός των συσκευών IoT και τα δεδομένα που δημιουργούν αυξάνονται διαρκώς, η κύρια πρόκληση στο IoT θα είναι να χρησιμοποιηθούν αυτά τα δεδομένα με

[146] Η Industry 4.0 αποτελείται από τις σύγχρονες τεχνολογίες αιχμής, που προωθούν την ψηφιακή μηχανοργάνωση της παραγωγής και μεταποίησης προϊόντων και υπηρεσιών μέσω της ανάλυσης, επεξεργασίας και εκμετάλλευσης του τεραστίου όγκου ψηφιακών δεδομένων (Big Data), σε συνδυασμό με την τεράστια υπολογιστική δύναμη των σημερινών υπολογιστών, που έχουν τη δυνατότητα της ταχύτατης επεξεργασίας πολύπλοκων αλγορίθμων. Κύριος στόχος της είναι η πλήρης αυτοματοποίηση και ο ψηφιακός μετασχηματισμός του μελλοντικού «έξυπνου εργοστασίου» (Smart Factory), αλλά και ολόκληρης της κοινωνίας γενικότερα.

ουσιαστικό τρόπο. Σύμφωνα με έρευνα της Gartner[147], το 87% των οργανισμών έχουν περιορισμένη επιχειρηματική ευφυΐα και ωριμότητα αναλυτικών στοιχείων. Ως εκ τούτου, οι περισσότεροι οργανισμοί αξιοποιούν ελάχιστα τα δεδομένα τους και αποτυγχάνουν να λάβουν αξία από αυτά. Στις περιπτώσεις αυτές, η ενσωμάτωση λύσεων σε εφαρμογές IoT που βασίζονται σε τεχνητή νοημοσύνη, θα βοηθήσει τις εταιρίες/οργανισμούς να επιτύχουν καλύτερες δυνατότητες διαχείρισης δεδομένων και ανάλυσης.

Στην πραγματικότητα, η ενσωμάτωση της τεχνητής νοημοσύνης στο Διαδίκτυο των Πραγμάτων ξεκλειδώνει τις πραγματικές δυνατότητες του IoT δημιουργώντας πολύ πιο έξυπνα συστήματα και επιτρέποντας στα δίκτυα και τις συσκευές να μαθαίνουν από προηγούμενες αποφάσεις, να προβλέπουν μελλοντικές δραστηριότητες και να βελτιώνουν συνεχώς την απόδοση και τις δυνατότητες λήψης αποφάσεων χωρίς την ανάγκη ανθρώπινης παρέμβασης.

Και αυτό διότι η τεχνητή νοημοσύνη είναι αυτή που δίνει τη δυνατότητα σε μια IoT συσκευή να είναι έξυπνη, παρέχοντάς της δεξιότητες συλλογιστικής και ανάληψης αποφάσεων βασισμένες σε παρελθόντα δεδομένα και γεγονότα. Βεβαίως τα δεδομένα, για να είναι χρήσιμα για τη λήψη αποφάσεων, πρέπει να συλλέγονται, να αποθηκεύονται, να υποβάλλονται σε επεξεργασία και να αναλύονται. Όσο περισσότερα δεδομένα συλλέγονται, δημιουργείται τεράστιος όγκος δεδομένων που οδηγεί σε καθυστέρηση και συμφόρηση των συσκευών IoT.

Η καινοτομία στο AIoT είναι η προσθήκη του 5G δικτύου. Το δίκτυο πέμπτης γενιάς, 5G, έχει σχεδιαστεί για να επιτρέπει ταχύτερη μεταφορά μεγάλων αρχείων δεδομένων σε συσκευές IoT, μέσω του υψηλότερου εύρους ζώνης και της χαμηλότερης καθυστέρησης[148].

4.2 Πως λειτουργεί το AIoT;

Για να καταλάβουμε πως λειτουργεί το AIoT θα πρέπει να γνωρίζουμε αφενός μεν ότι η τεχνητή νοημοσύνη είναι η όλη διαδικασία του τρόπου με τον οποίο μια μηχανή,

[147] «*Gartner Data Shows 87 Percent of Organizations Have Low BI and Analytics Maturity*» https://www.gartner.com/en/newsroom/press-releases/2018-12-06-gartner-data-shows-87-percent-of-organizations-have-low-bi-and-analytics-maturity [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[148] C. -X. Wang, M. D. Renzo, S. Stanczak, S. Wang and E. G. Larsson, *«Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges»,* 2020, doi: 10.1109/MWC.001.1900292. Διαθέσιμο: https://ieeexplore.ieee.org/abstract/document/9023918 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

συσκευή ή σύστημα μαθαίνει και εκτελεί μια συγκεκριμένη εργασία, αφετέρου ότι το Διαδίκτυο των πραγμάτων αναφέρεται στη διασύνδεση συσκευών μεταξύ τους και με το Διαδίκτυο, για συλλογή, αποστολή και επεξεργασία δεδομένων.

Στην Τεχνητή Νοημοσύνη των Πραγμάτων συλλέγονται δεδομένα και νοημοσύνη, με σκοπό οι πληροφορίες αυτές, με κατάλληλους αλγορίθμους, να αξιολογηθούν και να εκτελεστούν οι εργασίες ή να προβαίνουν σε ενέργειες (λήψη «*αυτοματοποιημένων αποφάσεων*») χωρίς ανθρώπινη παρέμβαση.

Ειδικότερα, η ροή εργασιών του AIoT είναι η εξής:

- **Συλλογή δεδομένων:**

Οι συσκευές IoT δημιουργούν δεδομένα, τα οποία συλλέγονται με τη βοήθεια αισθητήρων που υπάρχουν στις συσκευές για τη συλλογή πολλαπλών συνόλων δεδομένων.

- **Μεταφορά δεδομένων:**

Τα δεδομένα που συλλέγονται, αποθηκεύονται στα αντίστοιχα σύνολα συνήθως στο cloud για λόγους ευκολίας αλλά και εξοικονόμησης χρόνου και χρημάτων.

- **Επεξεργασία δεδομένων:**

Τα αποθηκευμένα στους διακομιστές cloud δεδομένα υποβάλλονται σε επεξεργασία σε φάσεις με βάση την εξαγωγή και τον καθαρισμό σημαντικών δεδομένων.

- **Ανάλυση δεδομένων:**

Τα επεξεργασμένα δεδομένα μεταδίδονται μέσω διαφορετικών δικτύων., όπου συγκεντρώνονται και αναλύονται σε πληροφορίες που μπορούν να χρησιμοποιηθούν.

- **Εκτέλεση πληροφοριών:**

Οι πληροφορίες που συλλέγονται με δυνατότητα δράσης χρησιμοποιούνται στη συνέχεια σε πρακτική χρήση[149].

4.3 Εφαρμογές, οφέλη και παραδείγματα της Τεχνητής Νοημοσύνης των Πραγμάτων

Ο συνδυασμός διαδικτύου των πραγμάτων και των έξυπνων συστημάτων καθιστά το AIoT ένα ισχυρό και σημαντικό εργαλείο για πολλές εφαρμογές. Η σύγκλιση αυτή οδηγεί στην εξάλειψη των τεχνολογικών εμποδίων μεταξύ των συστημάτων και μπορεί να

[149] https://www.hitechnectar.com/blogs/future-of-aiot-technologies/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

επαναπροσδιορίσει τον τρόπο λειτουργίας των βιομηχανιών, των επιχειρήσεων και της οικονομίας γενικότερα, ενώ τα οφέλη είναι πολλαπλά, από εξοικονόμηση πόρων μέχρι μείωση περιβαλλοντικών επιπτώσεων κ.α.

Η τεχνητή νοημοσύνη βελτιώνει τις εφαρμογές IoT σε δύο βασικές διαστάσεις: α) στην ενεργοποίηση απαντήσεων σε πραγματικό χρόνο, για παράδειγμα μέσω μιας απομακρυσμένης βιντεοκάμερας που διαβάζει πινακίδες κυκλοφορίας ή αναλύει πρόσωπα και β) στην επεξεργασία μετά το συμβάν, όπως η αναζήτηση μοτίβων στα δεδομένα με την πάροδο του χρόνου και η εκτέλεση προγνωστικών αναλύσεων.

Ωστόσο η αλληλεξάρτηση μεταξύ IoT και AI λειτουργεί και αντίστροφα. Η ικανότητα του IoT να ενεργοποιεί την ανάδραση σε πραγματικό χρόνο είναι κρίσιμη για τα προσαρμοστικά συστήματα μάθησης, καθώς άλλες τεχνολογίες δεν επιτρέπουν πραγματικά αυτόν τον προηγμένο τύπο AI/αναλυτικών στοιχείων. Επομένως και οι δύο τεχνολογίες χρειάζονται η μία την άλλη.

Σήμερα πάρα πολλές επιχειρήσεις και οργανισμοί έχουν υιοθετήσει λύσεις IoT και AI για να αυξήσουν την παραγωγικότητά τους και να βελτιώσουν την παροχή υπηρεσιών τους. Ο συνδυασμός των δύο αυτών μεγάλων τεχνολογιών προσφέρει μεγάλο ανταγωνιστικό πλεονέκτημα που μεταφράζεται σε βελτιωμένες και καινοτόμες υπηρεσίες, ιδιαίτερα αν λάβει κανείς υπόψιν του τα κάτωθι:

- Στο AIoT, η τεχνητή νοημοσύνη είναι ικανή να εντοπίζει ανάμεσα στον τεράστιο όγκο των δεδομένων που συλλέγει το IoT, εκείνα τα στοιχεία που με την τροποποίησή τους θα εξασφαλιστούν τα ιδανικά αποτελέσματα. Δηλαδή, μπορεί να διακρίνει ποια διαδικασία είναι περιττή και χρονοβόρα, αλλά και ποια εργασία μπορεί να βελτιστοποιηθεί για να ενισχύσει τη λειτουργική αποτελεσματικότητα. Ένα τέτοιο παράδειγμα εφαρμογής AIoT λύσης είναι στα Google Data Centers, όπου με την υιοθέτηση της τεχνητής νοημοσύνης των πραγμάτων, κατάφεραν να μειώσουν το κόστος ψύξης τους κατά ποσοστό 40%, το οποίο ισοδυναμεί με 15% μείωση των συνολικών εξόδων ενέργειας (PUE - Power usage effectiveness)[150].
- Το AIoT αυξάνει την επεκτασιμότητα του IoT. Αυτό πρακτικά σημαίνει ότι δυνάμει της εφαρμογής διαδικασίας ανάλυσης και επιλογής των δεδομένων

[150] "DeepMind AI Reduces Google Data Centre Cooling Bill by 40%», Διαθέσιμο: https://www.deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

που είναι απαραίτητα, μειώνει τον όγκο των δεδομένων που μοιράζεται το IoT με άλλες συσκευές, σε τέτοιο επίπεδο, που επιτρέπει τη σύνδεση μεγαλύτερου αριθμού συσκευών χωρίς την παραμικρή καθυστέρηση.

- Στο AIoT είναι δυνατή η πρόβλεψη ποικιλόμορφων κινδύνων (οικονομικές απώλειες, απειλές στον κυβερνοχώρο κα.), που επιτρέπει στις επιχειρήσεις να αυτοματοποιηθούν για την άμεση απόκριση και την αποφυγή δυσάρεστων επιπτώσεων. Όπως η εκ των προτέρων πρόβλεψη αστοχιών εξοπλισμού, μέσω της εφαρμογής προγνωστικών συντηρήσεων σε μια υπεράκτια βιομηχανία πετρελαίου και φυσικού αερίου, που θα εξαλείψει τυχόν δαπανηρές απρογραμμάτιστες διακοπές λειτουργίας. Ένα αντίστοιχο πραγματικό παράδειγμα είναι η εταιρία TITAN Τσιμέντα, η οποία εγκατέστησε πληθώρα αισθητήρων σε εργοστάσιό της στην περιοχή των Βαλκανίων, και στη συνέχεια χρησιμοποιώντας αλγόριθμους τεχνητής νοημοσύνης ανίχνευσε ανωμαλίες στα εν λόγω μηχανήματα, ειδοποιώντας σχετικά με τον εξοπλισμό που θα χρειαζόταν σύντομα συντήρηση. Η TITAN αντιμετώπισε προληπτικά αυτά τα ζητήματα, αποφεύγοντας τους υψηλούς λογαριασμούς επισκευών. Με βάση αυτά τα πολλά υποσχόμενα αποτελέσματα, η εταιρεία σχεδιάζει να κλιμακώσει το πιλοτικό πρόγραμμα σε πολλά άλλα εργοστάσια[151].

Μάλιστα το AIoT είναι η τεχνολογία που επέτρεψε στο λεγόμενο «**Digital Twin**»[152] να αναπτυχθεί και να χρησιμοποιείται σήμερα κυρίως σε τομείς όπως η ιατρική, η βιομηχανία και οι έξυπνες πόλεις. Ουσιαστικά το «ψηφιακό δίδυμο» καθιστά δυνατή την πρόβλεψη σφαλμάτων· παραδείγματος χάρη, στη βιομηχανία προσφέρει αξιόπιστη πρόβλεψη επιφανειακών ζημιών στο περιβάλλον παραγωγής. Οι αλγόριθμοι τεχνητής νοημοσύνης που συνδέονται με Digital Twins έχουν τη δυνατότητα για μεγαλύτερη

[151] https://web-assets.bcg.com/93/be/5ac6b7ff4d698947da09681332db/harnessing-the-power-web-final.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[152] Ο καθηγητής του Πανεπιστημίου του Αιγαίου Νικήτας Νικητάκος αναφέρει ότι το Digital Twin είναι «*μια δυναμική εικονική αναπαράσταση ενός φυσικού αντικειμένου ή συστήματος σε όλο τον κύκλο ζωής του, χρησιμοποιώντας δεδομένα σε πραγματικό χρόνο, για να καταστεί δυνατή η κατανόηση, η μάθηση και ο συλλογισμός», καθώς και τα μοντέλα που χρησιμοποιούνται για την υποστήριξη αποφάσεων, καθ' όλη τη διάρκεια του κύκλου ζωής του εν λόγω περιουσιακού στοιχείου. Η δύναμη των ψηφιακών διδύμων έγκειται στην ικανότητα να εκτελούν «πειράματα» σε έναν υπολογιστή και όχι στο πεδίο, επειδή είναι πολύ φθηνότερο, ασφαλέστερο και ταχύτερο να γίνει αυτό σε μια ψηφιακή πλατφόρμα, παρά στο πεδίο*. Διαθέσιμο: https://www.isalos.net/2022/07/psifiaka-didyma-digital-twins-sti-naftilia/?fbclid=IwAR0ZivXtIS1OtlS0JKphBFohQuQb2tZHgv1BAaeVWk_T2EavqXPx9hZBjOc [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

ακρίβεια, καθώς το μηχάνημα μπορεί να κρατήσει μεγάλο όγκο δεδομένων, που απαιτούνται για ανάλυση απόδοσης και πρόβλεψης[153]. Με αυτήν την τεχνογνωσία, μπορούν να προσαρμοστούν οι ρυθμίσεις του συστήματος σε πραγματικό χρόνο, αποφεύγοντας την οποιαδήποτε βλάβη.

4.3.1 Έξυπνη πόλη και Drone Traffic Monitoring

Η χρήση του AIoT στις έξυπνες πόλεις για την παρακολούθηση της οδικής κυκλοφορίας με drones, μπορεί να οδηγήσει σε εντυπωσιακή μείωση της κυκλοφοριακής συμφόρησης. Αυτό συμβαίνει διότι με το AIoT μπορούμε πλέον σε πραγματικό χρόνο να κάνουμε σε προσαρμογές στη ροή της κυκλοφορίας, στα όρια ταχύτητας και το χρονοδιάγραμμα των φωτεινών σηματοδοτών χωρίς ανθρώπινη συμμετοχή[154]. Τέτοιου είδους drones χρησιμοποιεί ήδη από το 2017 το Ντουμπάι, όπως επίσης και η Λυών στη Γαλλία[155].

4.3.2 ET City Brain

Η ET City Brain της Alibaba Cloud είναι ένα έξυπνο σύστημα AIoT που χρησιμοποιεί υπολογιστές μεγάλων δεδομένων και βαθιά νευρωνικά δίκτυα για την επεξεργασία μαζικών αρχείων καταγραφής, βίντεο και ροών δεδομένων από συστήματα και αισθητήρες σε ένα αστικό κέντρο. Αυτό το σύστημα μπορεί να ανιχνεύσει παράνομη στάθμευση, τροχαία ατυχήματα, να αλλάξει φανάρια για να βοηθήσει τα ασθενοφόρα να φτάνουν σε ασθενείς που χρειάζονται βοήθεια γρηγορότερα και πολλά άλλα[156].

---

[153] Fuller A., Z. Fan, C. Day and C. Barlow, «*Digital Twin: Enabling Technologies, Challenges and Open Research*», 2020, doi: 10.1109/ACCESS.2020.2998358. Διαθέσιμο:
https://ieeexplore.ieee.org/document/9103025 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[154] Bisio, Igor & Garibotto, Chiara & Haleem, Halar & Lavagetto, Fabio & Sciarrone, Andrea. (2022). *«A Systematic Review of Drone Based Road Traffic Monitoring System»*. Διαθέσιμο: https://www.researchgate.net/publication/363627429_A_Systematic_Review_of_Drone_Based_Road_Traffic_Monitoring_System [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[155] Navid Ali Khan, N.Z. Jhanjhi, Sarfraz Nawaz Brohi, Raja Sher Afgun Usmani, Anand Nayyar, «*Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs* https://doi.org/10.1016/j.comcom.2020.04.049. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S0140366420300189 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[156] Zhang, Jianfeng & Hua, Xian-Sheng & Huang, Jianqiang & Shen, Xu & Chen, Jingyuan & Zhou, Qin & Fu, Zhihang & Zhao, Yiru. (2019). «*The City Brain: Practice of Large-Scale Artificial Intelligence in the Real World. IET Smart Cities»*. Διαθέσιμο:

4.3.3 Αυτόνομα οχήματα

Το AIoT όπως ήδη ειπώθηκε, χρησιμοποιείται στη διαχείριση και παρακολούθηση των οχημάτων ενός δρόμου, στη μείωση του κόστους καυσίμων, στην παρακολούθηση της συντήρησης του οχήματος και στον εντοπισμό της μη ασφαλούς συμπεριφοράς του οδηγού. Μέσω συσκευών IoT, δηλαδή GPS και άλλων αισθητήρων και ενός συστήματος τεχνητής νοημοσύνης, οι εταιρίες μπορούν να διαχειρίζονται καλύτερα τον στόλο τους χάρη στο AIoT. Η τεχνολογία AIoT χρησιμοποιείται επίσης σήμερα στα αυτόνομα οχήματα. Παραδείγματος χάρη, το σύστημα αυτόματου πιλότου της Tesla χρησιμοποιεί GPS, σόναρ, ραντάρ και κάμερες για τη συλλογή δεδομένων σχετικά με τις συνθήκες οδήγησης. Στη συνέχεια, η TN λαμβάνει αποφάσεις σχετικά με τα δεδομένα που συγκλίνουν οι συσκευές IoT. Με τη δύναμη της τεχνητής νοημοσύνης, τα αυτοοδηγούμενα αυτοκίνητα της Tesla προβλέπουν τη συμπεριφορά των πεζών και των αυτοκινήτων σε διάφορες περιστάσεις, π.χ. Μπορούν να καθορίσουν τις συνθήκες του δρόμου, τη βέλτιστη ταχύτητα, τον καιρό, να αποφύγουν τα εμπόδια και να γίνουν πιο έξυπνα με κάθε ταξίδι[157].

4.3.4 Amazon GO (USA) και Amazon Fresh (UK) stores

Ένα εξαιρετικό παράδειγμα AIoT είναι τα concept stores της Amazon (Amazon Go στην Αμερική και Amazon Fresh στο Ηνωμένο Βασίλειο), τα οποία έχουν φέρει επανάσταση στη βιομηχανία λιανικής, διευκολύνοντας τις αγορές. Τα εν λόγω καταστήματα είναι εξοπλισμένα με κάμερες, αισθητήρες, RFID αναγνώστες, ενώ εφαρμόζεται και η αναγνώριση προσώπου του χρήστη για την ταυτοποίησή του. Με τον τρόπο αυτό, ο καταναλωτής αφού εισέλθει στο κατάστημα, στο οποίο δεν υπάρχουν ταμεία, σκανάρει την εφαρμογή από το κινητό του και πλέον είναι έτοιμος να διαλέξει το προϊόν που θέλει να αγοράσει. Όταν περάσει την έξοδο, το σύστημα AI θα έχει εντοπίσει

https://www.researchgate.net/publication/333456538_The_City_Brain_Practice_of_Large-Scale_Artificial_Intelligence_in_the_Real_World [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[157] Khayyam, Hamid & Javadi, Bahman & Jalili, Mahdi & Jazar, Reza. (2020). «*Artificial Intelligence and Internet of Things for Autonomous Vehicles*». Διαθέσιμο: https://www.researchgate.net/publication/335021813_Artificial_Intelligence_and_Internet_of_Things_for_Autonomous_Vehicles [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

τα είδη που αγόρασε και θα χρεωθεί αυτόματα το ηλεκτρονικό του πορτοφόλι μέσω του λογαριασμού του Amazon[158].

4.3.5 Boston Dynamics' Spot Robot

Με την εμφάνιση του AIoT τα ρομπότ έχουν γίνει πλέον πιο έξυπνα και ευαίσθητα σε διάφορες διαδικασίες. Το ρομπότ Spot με τη χρήση ΤΝ μπορεί να περπατά, να ανεβαίνει σκάλες, να αποφεύγει εμπόδια, να διασχίζει δύσκολο έδαφος και να ακολουθεί αυτόνομα προκαθορισμένες διαδρομές με ελάχιστη ή καθόλου συνεισφορά από τους χρήστες. Δεδομένου ότι το Spot είναι ένα ρομπότ γενικής χρήσης, έχει ευρείες εφαρμογές, συμπεριλαμβανομένων πιθανών στρατιωτικών χρήσεων που θα μπορούσαν να περιλαμβάνουν απομακρυσμένη επιθεώρηση επικίνδυνων περιβαλλόντων, επιχειρήσεις διάσωσης ή επιχειρήσεις υλικοτεχνικής υποστήριξης.

Η αστυνομία και η πυροσβεστική χρησιμοποιούν το Spot για να έχουν εξ αποστάσεως ορατότητα σε δυνητικά επικίνδυνες καταστάσεις. Με την εξ αποστάσεως αξιολόγηση μιας σκηνής πριν αναλάβει δράση, η αστυνομία μπορεί να λάβει πιο ενημερωμένες αποφάσεις που μειώνουν τον κίνδυνο, βελτιώνουν την ασφάλεια και αποκλιμακώνουν τις συγκρούσεις. Συγκεκριμένα, τα αστυνομικά τμήματα χρησιμοποιούν το Spot για να επιθεωρήσουν ύποπτα πακέτα και περιβάλλοντα για επικίνδυνα υλικά ή εκρηκτικά, να αξιολογήσουν εχθρικές απειλές από απόσταση και να αναζητήσουν δομικά επικίνδυνα περιβάλλοντα σε σενάρια αντιμετώπισης έκτακτης ανάγκης, κρατώντας έτσι τους πρώτους ανταποκριτές και το κοινό ασφαλή[159].

5 / Η προστασία των προσωπικών δεδομένων στην Ελλάδα και την Ευρωπαϊκή Ένωση

5.1 Εισαγωγή

Όπως ήδη ειπώθηκε, οι τεχνολογίες AI και IOT κατά τη χρήση τους επεξεργάζονται τεράστιο όγκο δεδομένων. Τα δεδομένα πια έχουν χαρακτηριστεί «*το νέο*

[158] Maggie Tillman, «*Amazon Go and Amazon Fresh: How the 'Just walk out' tech work*» Διαθέσιμο: https://www.pocket-lint.com/gadgets/news/amazon/139650-what-is-amazon-go-where-is-it-and-how-does-it-work/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[159] https://www.bostondynamics.com/about [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

πετρέλαιο» της οικονομίας για την τόνωση της καινοτομίας και της δημιουργικότητας[160]. Και αυτό διότι με την ραγδαία εξέλιξη των τεχνολογιών αυτών, πολλές εταιρίες έχουν οικοδομήσει εύρωστα επιχειρηματικά πρότυπα γύρω από την επεξεργασία δεδομένων, και η εν λόγω επεξεργασία συχνά περιλαμβάνει δεδομένα προσωπικού χαρακτήρα. Αυτή η αύξηση της ζήτησης των προσωπικών δεδομένων από τις επιχειρήσεις για εμπορικούς σκοπούς, οδήγησε στην ανάγκη θέσπισης κανόνων για την προστασία τους.

Αρχικά, η προστασία δεδομένων αφορά την προστασία κάθε πληροφορίας που σχετιζόμενης με ταυτοποιημένο ή αναγνωρίσιμο φυσικό εν ζωή πρόσωπο, μεταξύ των οποίων ονόματα, ημερομηνίες γέννησης, φωτογραφίες, βίντεο, διευθύνσεις email και αριθμοί τηλεφώνου. Προσωπικά δεδομένα ωστόσο, θεωρούνται επίσης και άλλες πληροφορίες, όπως διευθύνσεις IP και περιεχόμενο επικοινωνίας - που σχετίζονται ή παρέχονται από τελικούς χρήστες υπηρεσιών επικοινωνιών.

Η έννοια της προστασίας δεδομένων πηγάζει από το δικαίωμα στην ιδιωτική ζωή και αμφότερα είναι καθοριστικά για τη διατήρηση και την προώθηση θεμελιωδών αξιών και δικαιωμάτων. Μάλιστα, η προστασία δεδομένων, έχει ακριβείς στόχους για τη διασφάλιση της δίκαιης επεξεργασίας (συλλογή, χρήση, αποθήκευση) προσωπικών δεδομένων τόσο από τον δημόσιο όσο και από τον ιδιωτικό τομέα.

Από το 1950 που διακηρύχθηκε και υπογράφηκε από το Συμβούλιο της Ευρώπης η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου[161], έχει ασκήσει αναμφίβολα σημαντική επιρροή στο εσωτερικό δίκαιο των χωρών μελών του Συμβουλίου της Ευρώπης και θεωρείται ευρέως ως η πιο αποτελεσματική διεθνής συνθήκη για την προστασία των ανθρωπίνων δικαιωμάτων. Όλα τα δικαιώματα της ΕΣΔΑ περιλαμβάνονται στον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΧΘΔΕΕ)[162] που διακηρύχθηκε από την Ευρωπαϊκή Συνέλευση και τέθηκε σε ισχύ ως μέρος της Συνθήκης της Λισσαβώνας[163] την 1-12-2009. Ο Χάρτης αντιμετωπίζει ορισμένα

---

[160] Financial Times (2016), «Data is the new oil… who's going to own it?», Διαθέσιμο: https://www.ft.com/content/e548deac-856a-11e6-8897-2359a58ac7a5 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[161] Η Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου είναι μια διεθνής συνθήκη για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών στην Ευρώπη. Στη Σύμβαση αυτή συμμετέχουν και οι 47 χώρες του Συμβουλίου της Ευρώπης, 27 από τις οποίες είναι μέλη της ΕΕ. Διαθέσιμο: https://www.echr.coe.int/documents/convention_ell.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[162] Ο Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ, Διαθέσιμο: https://www.europarl.europa.eu/charter/pdf/text_el.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[163] Η συνθήκη της Λισσαβώνας μεταρρυθμίζει τον τρόπο λειτουργίας των θεσμικών οργάνων της Ευρωπαϊκής Ένωσης (ΕΕ) και τους τρόπους λήψης αποφάσεων, ώστε οι αποφάσεις αυτές να είναι κατάλληλες για μια ΕΕ η οποία αύξησε τον αριθμό των μελών της σε 28 μετά τις διαδοχικές διευρύνσεις. Επιπλέον, μεταρρυθμίζει την εσωτερική και εξωτερική πολιτική της ΕΕ και, με την εκχώρηση περισσότερων

σύγχρονα ζητήματα που δεν περιλαμβάνονται στην ΕΣΔΑ, όπως την ανθρώπινη κλωνοποίηση, την προστασία δεδομένων (άρθρο 8) κ.α. Γενικότερα όμως, στο πλαίσιο του δικαίου της ΕΕ, η προστασία δεδομένων ρυθμίστηκε για πρώτη φορά με την Οδηγία για την Προστασία Δεδομένων το 1995 (95/46/ΕΚ).

Αναφορικά με την προστασία των προσωπικών δεδομένων, το άρθρο 8 του Χάρτη ορίζει ότι: «*1.Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν»* και «*2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο*…».

Το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα προβλέπεται επίσης και από το άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ)[164].

Σε εθνικό επίπεδο, συναντάμε στο άρθρο 9Α του Συντάγματος την προστασία των προσωπικών δεδομένων, το οποίο προστέθηκε με την αναθεώρηση του ελληνικού Συντάγματος το 2001. Σύμφωνα με αυτό: «*Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει..»*. Σχετική είναι και η διάταξη του άρθρου 5Α ως προς το δικαίωμα της πληροφόρησης και του δικαιώματος συμμετοχής στην κοινωνία της πληροφορίας.

Από την άλλη, σε διεθνές επίπεδο η Σύμβαση 108 ήταν, και παραμένει, η μόνη νομικά δεσμευτική πράξη στον τομέα της προστασίας δεδομένων[165].

νομοθετικών εξουσιών στο Ευρωπαϊκό Κοινοβούλιο, ενισχύει τη δημοκρατία στη διαδικασία λήψης αποφάσεων της ΕΕ. Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:ai0033 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[164] Η Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης είναι μία από τις 2 ιδρυτικές συνθήκες της ΕΕ, μαζί με τη Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ). Αποτελεί τη λεπτομερή βάση του δικαίου της ΕΕ ορίζοντας τις αρχές και τους σκοπούς της ΕΕ, καθώς και το πεδίο εφαρμογής των δράσεων στους τομείς πολιτικής της. Καθορίζει επίσης οργανωτικά και λειτουργικά χαρακτηριστικά των θεσμικών κοινοτικών οργάνων. Διαθέσιμο: https://eur-lex.europa.eu/EL/legal-content/summary/treaty-on-the-functioning-of-the-european-union.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[165] «*Με την ανάδυση της τεχνολογίας των πληροφοριών στη δεκαετία του 1960, υπήρχε η αυξανόμενη ανάγκη για λεπτομερέστερους κανόνες προστασίας των φυσικών προσώπων μέσω της προστασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Το 1981 άνοιξε προς υπογραφή η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (CETS αριθ. 108, 1981). Η Σύμβαση 108 εφαρμόζεται σε κάθε επεξεργασία δεδομένων η οποία εκτελείται τόσο από τον ιδιωτικό, όσο και από τον δημόσιο τομέα, συμπεριλαμβανομένης της επεξεργασίας δεδομένων από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου. Προστατεύει τα πρόσωπα από τις καταχρήσεις οι οποίες ενδέχεται να συνοδεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και αποσκοπεί, ταυτόχρονα, στη ρύθμιση των διασυνοριακών ροών αυτών των δεδομένων. Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι προβλεπόμενες στη Σύμβαση αρχές αφορούν, ιδίως, τη δίκαιη και νόμιμη συλλογή και αυτοματοποιημένη επεξεργασία, για συγκεκριμένους, θεμιτούς σκοπούς. Αυτό σημαίνει ότι τα δεδομένα δεν θα*

Κατά τα ανωτέρω, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μέσω της ανάλυσης μαζικών δεδομένων, εμπίπτουν στο πεδίο εφαρμογής της νομοθεσίας της ΕΕ και του Συμβουλίου της Ευρώπης.

Ωστόσο, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, δεν είναι απόλυτο· μπορεί να περιοριστεί όταν πρόκειται για στόχους γενικού συμφέροντος ή για την προστασία των δικαιωμάτων και των ελευθεριών των τρίτων. Οι προϋποθέσεις περιορισμού των δικαιωμάτων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα απαριθμούνται στο άρθρο 8 παρ. 2 της ΕΣΔΑ, σύμφωνα με το οποίο «*Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.»*, αλλά και στο άρθρο 52 παρ.1 του ΧΘΔΕΕ, σύμφωνα με το οποίο «*Κάθε περιορισμός στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον παρόντα Χάρτη πρέπει να προβλέπεται από το νόμο και να σέβεται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων και ελευθεριών. Τηρουμένης της αρχής της αναλογικότητας, περιορισμοί επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού ενδιαφέροντος που αναγνωρίζει η Ένωση ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.».*

Στον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ), που αναλύεται αμέσως παρακάτω, στο άρθρο 23, προβλέπονται 10 λόγοι περιορισμού του δικαιώματος προστασίας προσωπικών δεδομένων που αφορούν τη διασφάλιση της ασφάλειας του κράτους, της εθνικής άμυνας, της δημόσιας ασφάλειας, της πρόληψης/διερεύνησης/ ανίχνευσης/δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, άλλων σημαντικών στόχων γενικού δημόσιου συμφέροντος της Ένωσης ή κράτους μέλους, της προστασίας της ανεξαρτησίας της δικαιοσύνης και των δικαστικών διαδικασιών, της πρόληψης/διερεύνησης/ανίχνευσης/δίωξης παραβάσεων δεοντολογίας σε νομοθετικά

πρέπει να χρησιμοποιούνται για την επιδίωξη στόχων οι οποίοι δεν συνάδουν με τους σκοπούς αυτούς και δεν θα πρέπει να διατηρούνται για διάστημα μεγαλύτερο από το αναγκαίο. Οι αρχές αφορούν επίσης την ποιότητα των δεδομένων και ιδίως την ανάγκη να είναι κατάλληλα, συναφή και όχι υπερβολικά (αναλογικότητα), καθώς και ακριβή.». - Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων Έκδοση 2018, Διαθέσιμο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

κατοχυρωμένα επαγγέλματα, της παρακολούθησης, επιθεώρησης, κανονιστικής λειτουργίας που συνδέεται, έστω περιστασιακά, με την άσκηση δημόσιας εξουσίας στις περιπτώσεις που αναφέρονται στα παραπάνω, της προστασίας του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων, και της εκτέλεσης αστικών αξιώσεων.

5.2 Ο Γενικός Κανονισμός Προστασίας Δεδομένων GDPR 2016/679

Η πιο ολοκληρωμένη και προοδευτική προσπάθεια θέσπισης κοινών -σε ευρωπαϊκό επίπεδο-ρυθμίσεων για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, έγινε από την Ευρωπαϊκή Ένωση στις 27 Απριλίου 2016 με την ψήφιση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων GDPR 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου με έναρξη ισχύος την 25η Μαΐου 2018, ο οποίος κατήργησε και την Οδηγία 95/46/ΕΚ[166].

Σκοπός της εφαρμογής είναι η άρση των νομικών ασαφειών και της ανασφάλειας που δημιουργούσε το προηγούμενο νομικό πλαίσιο, η αντιμετώπιση των επιπτώσεων της ψηφιακής εποχής, η ενδυνάμωση θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων καθώς και η ομοιομορφία του νομικού πλαισίου σε όλα τα κράτη-μέλη.

Γενικά ο ΓΚΠΔ εφαρμόζεται και αφορά όλα τα φυσικά και νομικά πρόσωπα, που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών ή σχετίζονται με οποιουδήποτε είδους υπηρεσίες και αγαθά προς Ευρωπαίους πολίτες, είτε η έδρα τους βρίσκεται εντός Ευρωπαϊκής Ένωσης, είτε εκτός.

Στα πλαίσια συμμόρφωσης με τον ΓΚΠΔ, ο οποίος ερείδεται στο άρθρο 16 ΣΛΕΕ, αλλά και στο αντίστοιχο άρθρο 8 του ΧΘΔΕΕ, το είδος και ο όγκος των δεδομένων προσωπικού χαρακτήρα που μπορεί να επεξεργάζεται μια εταιρία ή ένας οργανισμός, εξαρτάται από τον λόγο της επεξεργασίας και από τη σκοπούμενη χρήση.

Στο άρθρο 5 ΓΚΠΔ περιέχονται οι βασικές αρχές του ευρωπαϊκού δικαίου για την προστασία των προσωπικών δεδομένων. Ειδικότερα, σύμφωνα με αυτές, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία με νόμιμο και

[166] Η οδηγία 95/46/ΕΚ ήταν το πρώτο μεγάλο βήμα της Ευρωπαϊκής Ένωσης (Ε.Ε) προς το σκοπό της προστασίας των προσωπικών δεδομένων, η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 2472/1997. Εξαιτίας των διαφορετικών επιπέδων προστασίας στο εθνικό δίκαιο κάθε κράτους μέλους, είχε προκαλέσει τον κατακερματισμό της εφαρμογής της προστασίας των προσωπικών δεδομένων και, ως εκ τούτου, ανασφάλεια δικαίου εντός της Ένωσης.

διαφανή τρόπο, διασφαλίζοντας την αντικειμενικότητα προς τα άτομα των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία («*νομιμότητα, αντικειμενικότητα και διαφάνεια*» - άρθρο 5 παρ. 1α΄). Επίσης, σύμφωνα με την αρχή του «*περιορισμού του σκοπού*» που προβλέπεται στο άρθρο 5 παρ. 1β΄, θα πρέπει να υπάρχει συγκεκριμένος σκοπός για την επεξεργασία των δεδομένων, ο οποίος να υποδεικνύεται στο υποκείμενο του οποίου τα προσωπικά δεδομένα συλλέγονται, καθώς δεν επιτρέπεται η συλλογή δεδομένων προσωπικού χαρακτήρα για απροσδιόριστους σκοπούς, ούτε και η επεξεργασία τους για άλλους σκοπούς που δεν είναι συμβατοί με τον αρχικό για τον οποίο δόθηκαν. Μια ακόμη βασική αρχή είναι η αρχή της «*ελαχιστοποίησης των δεδομένων*» του άρθρου 5 παρ. 1γ΄, βάσει της οποίας θα πρέπει να συλλέγονται και να επεξεργάζονται μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για την επίτευξη του εν λόγω σκοπού. Τα εν λόγω δεδομένα σύμφωνα με την αρχή «*ακριβείας*» του άρθρου 5 παρ. 1δ΄, οφείλουν να είναι ακριβή και ενημερωμένα, λαμβάνοντας υπόψη τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, άλλως να διορθώνονται. Ταυτόχρονα, θα πρέπει να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποθηκεύονται για διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για τους σκοπούς για τα οποία συλλέχθηκαν σύμφωνα με την αρχή του «*περιορισμού της περιόδου αποθήκευσης*» - (άρθρο 5 παρ. 1ε΄). Τέλος, σύμφωνα με την περίπτωση στ' της παραγράφου 1 του άρθρου 5 ΓΚΠΔ θα πρέπει με τις κατάλληλες τεχνικές και οργανωτικές εγγυήσεις να εξασφαλίζεται η ασφάλεια των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά, χρησιμοποιώντας κατάλληλη τεχνολογία («*ακεραιότητα και εμπιστευτικότητα*» - άρθρο 5 παρ. 1στ΄)[167].

Εν συνεχεία, και προκειμένου οι πληροφορίες που συνιστούν απλά προσωπικά δεδομένα να μπορούν να υπόκεινται σε επεξεργασία, θα πρέπει σύμφωνα με το άρθρο 6 ΓΚΠΔ να συντρέχει μία από τις έξι νόμιμες βάσεις επεξεργασίας. Αυτές επιγραμματικά είναι: συγκατάθεση του υποκειμένου, ανάγκη εκτέλεσης σύμβασης, ανάγκη συμμόρφωσης με έννομη υποχρέωση του υπευθύνου επεξεργασίας, ανάγκη διαφύλαξης

[167] Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018 σελ. 149-176 Διαθέσιμο: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

ζωτικού συμφέροντος, ανάγκη εκπλήρωσης καθήκοντος υπέρ του δημοσίου και ανάγκη άσκησης των σκοπών των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου.

Στο αμέσως επόμενο άρθρο 7, απαριθμούνται οι προϋποθέσεις συγκατάθεσης προκειμένου η τελευταία να αποτελεί νόμιμη βάση επεξεργασίας. Ορίζεται, μεταξύ άλλων, ότι ο υπεύθυνος επεξεργασίας φέρει το βάρος της αποδείξεως όσον αφορά την παροχή της συγκατάθεσης του προσώπου, του οποίου τα δεδομένα προσωπικού χαρακτήρα αποτελούν το αντικείμενο προστασίας. Η δήλωση συγκατάθεσης του χρήστη για την επεξεργασία των προσωπικών του δεδομένων πρέπει να είναι διατυπωμένη εκ των προτέρων από τον υπεύθυνο επεξεργασίας σε γλώσσα απλή και κατανοητή, χωρίς καταχρηστικές ρήτρες. Η συγκατάθεση θεωρείται ότι δε δόθηκε ελεύθερα εάν υπήρχε ανισότητα μεταξύ του υπεύθυνου επεξεργασίας και του χρήστη, εάν δεν υπάρχει αληθινή επιλογή ή ο χρήστης δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεση του χωρίς επακόλουθη ζημία. Οι υπεύθυνοι επεξεργασίας οφείλουν να παρέχουν τη δυνατότητα στο υποκείμενο της επεξεργασίας να ανακαλέσει την συγκατάθεσή του οποτεδήποτε.

Στο άρθρο 9 ΓΚΠΔ και στην παράγραφο 1 αυτού, προβλέπεται καταρχήν η απαγόρευση επεξεργασίας δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Στην παράγραφο 2 του ίδιου άρθρου περιλαμβάνονται οι δέκα νόμιμες βάσεις επεξεργασίας των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ήτοι: α) συγκατάθεση, β) η ανάγκη εκτέλεσης υποχρεώσεων και άσκησης δικαιωμάτων του Πανεπιστημίου στους τομείς του εργατικού δικαίου, του δικαίου κοινωνικής ασφάλισης και του δικαίου κοινωνικής προστασίας, (γ) η ανάγκη διαφύλαξης ζωτικού συμφέροντος φυσικού προσώπου, (δ) η επεξεργασία στο πλαίσιο δραστηριοτήτων ιδρύματος κλπ με στόχο πολιτικό, φιλοσοφικά κ.α. (υπό τους όρους της διάταξης), (ε) η προηγούμενη δημοσιοποίηση των δεδομένων από το υποκείμενό τους, (στ) η άσκηση νομικών αξιώσεων (ζ) λόγοι ουσιαστικού δημοσίου συμφέροντος ανάλογου προς τον επιδιωκόμενο σκοπό (υπό τους όρους της διάταξης), (η) η ανάγκη εξυπηρέτησης συγκεκριμένων ιατρικών σκοπών, (θ) λόγοι δημοσίου συμφέροντος στον τομέας της δημόσιας υγείας (υπό τους

όρους της διάταξης) και (ι) σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, σκοποί επιστημονικής και ιστορικής έρευνας και σκοποί στατιστικοί.

Περαιτέρω, σύμφωνα με τα άρθρα άρθρα 12-14 του ΓΚΠΔ, στο πλαίσιο τήρησης των αρχών της διαφανούς επεξεργασίας των προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει, να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία, όπως ενημέρωση για το γεγονός της επεξεργασίας των προσωπικών του δεδομένων, την έκταση και τους σκοπούς της, πριν ή κατά την έναρξη της επεξεργασίας και πιο συγκεκριμένα κατά τη συλλογή των δεδομένων ή εντός εύλογου χρονικού διαστήματος, όταν τα δεδομένα δεν έχουν συλλεγεί από το ίδιο το υποκείμενο. Η ενημέρωση πρέπει να είναι σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή και να χρησιμοποιείται σαφής και απλή διατύπωση. Επίσης, σε περίπτωση που ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί τα δεδομένα προσωπικού χαρακτήρα για σκοπό άλλο από εκείνον για τον οποίο συλλέχθηκαν, θα πρέπει να παρέχει στο υποκείμενο των δεδομένων, πριν από την εν λόγω περαιτέρω επεξεργασία, πληροφορίες για τον σκοπό αυτόν και όλες τις αναγκαίες πληροφορίες (άρθρο 13 παρ.3).

Παρακάτω στο άρθρο 15 ΓΚΠΔ συναντάμε το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων, τη δυνατότητα δηλαδή να πληροφορηθεί εάν τα δεδομένα του επεξεργάζονται καθώς και σχετικές πληροφορίες. Επίσης, στο υποκείμενο των δεδομένων παρέχεται βάσει του άρθρου 16 ΓΚΠΔ, το δικαίωμα διόρθωσης των δεδομένων αυτών σε περίπτωση ύπαρξης ανακριβειών.

Το άρθρο 17 ΓΚΠΔ αφορά το δικαίωμα διαγραφής ή «δικαίωμα στη λήθη», σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει χωρίς καθυστέρηση δεδομένα προσωπικού χαρακτήρα στην περίπτωση που δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή ανακλήθηκε η συγκατάθεση του υποκειμένου που συνιστούσε νομική βάση για την επεξεργασία κ.α.

Σύμφωνα με το άρθρο 18 ΓΚΠΔ και το δικαίωμα περιορισμού της επεξεργασίας, η επεξεργασία των δεδομένων του υποκειμένου δύναται να περιοριστεί, όταν αμφισβητείται η ακρίβεια τους ή η επεξεργασία είναι παράνομη, αλλά και στην περίπτωση που αυτά δεν είναι πλέον απαραίτητα στον υπεύθυνο επεξεργασίας ή το υποκείμενο έχει αντιρρήσεις για την επεξεργασία τους σύμφωνα με το άρθρο 21 παρ. 1 ΓΚΠΔ.

Στο άρθρο 20 του Κανονισμού προβλέπεται επίσης το δικαίωμα φορητότητας των δεδομένων, ήτοι το δικαίωμα μεταφοράς των δεδομένων από έναν υπεύθυνο επεξεργασίας σε έναν άλλο.

Ακολούθως το άρθρο 21 ρυθμίζει το δικαίωμα εναντίωσης του υποκειμένου των δεδομένων στην επεξεργασία, και το άρθρο 22 ορίζει ότι «*το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο*.». Η αυτοματοποιημένη επεξεργασία και κατάρτιση προφίλ είναι, όπως προαναφέρθηκε σε προηγούμενο κεφάλαιο, δυνατότητα που προσφέρει η τεχνολογία της τεχνητής νοημοσύνης.

Στη συνέχεια στο άρθρο 25 συναντάμε τη ρύθμιση για την προστασία των δεδομένων από τον σχεδιασμό και εξ ορισμού (privacy by design), σύμφωνα με την οποία: *«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.».*

Το αμέσως προηγούμενο άρθρο μπορούμε να πούμε ότι αλληλοσυμπληρώνει το άρθρο 32 για την ασφάλεια της επεξεργασίας των δεδομένων, σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα, της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού

συμβάντος, και διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

Ολοκληρώνοντας την επισκόπηση του ΓΚΠΔ από την σκοπιά των σημαντικότερων ρυθμίσεων για τα προσωπικά δεδομένα, θα πρέπει να σημειωθεί ότι στα πλαίσια των προστατευτικών μέτρων με βάση τον Κανονισμό καθορίζεται στα άρθρα 33-35 ΓΚΠΔ η γνωστοποίηση σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή εντός 72 ωρών από την γνώση του συμβάντος, καθώς επίσης και στο υποκείμενο των δεδομένων, ενώ ρυθμίζεται και η υποχρέωση του υπεύθυνου επεξεργασίας στη σύνταξη «Εκτίμησης Αντίκτυπου» για την περίπτωση που η συλλογή και η επεξεργασία προσωπικών δεδομένων ενδέχεται να επιφέρει υψηλό κίνδυνο για τις ελευθερίες και τα δικαιώματα των χρηστών.

5.2.1 Τεχνητή Νοημοσύνη και ΓΚΠΔ

Όπως είδαμε σε προηγούμενο κεφάλαιο η τεχνητή νοημοσύνη, εξαιτίας της αυξημένης χρήσης δεδομένων που απαιτεί για να λειτουργήσει, εγείρει ανησυχίες σχετικά με το απόρρητο και την προστασία τους. Λόγω της φύσης της, είναι πράγματι εκ προοιμίου ασυμβίβαστη με τις σημαντικότερες αρχές του ΓΚΠΔ, ιδιαίτερα όσον αφορά τη διαφάνεια, τον περιορισμό του σκοπού, τη νόμιμη βάση επεξεργασίας όταν αυτή είναι η συγκατάθεση, τη λογοδοσία κ.α.

Αρχικά, η ΤΝ βασίζεται σε τεράστιο όγκο δεδομένων από τα οποία «μαθαίνει» και λαμβάνει αποφάσεις, τα οποία πολλές φορές συλλέγονται εν αγνοία του υποκειμένου, δηλαδή άνευ χορήγησης της συγκατάθεσής του προς επεξεργασία. Αυτό έρχεται σε αντίθεση με την αρχή της ελαχιστοποίησης των δεδομένων του άρθρου 5 ΓΚΠΔ, διότι η τεχνητή νοημοσύνη επεξεργάζεται όλα τα διαθέσιμα δεδομένα και όχι μόνο τα απαραίτητα, όπως επίσης και με το άρθρο 6 του Κανονισμού περί νόμιμης βάσης επεξεργασίας. Όταν η βάση επεξεργασίας είναι η συγκατάθεση του υποκειμένου και η προσήκουσα συγκατάθεση, ήτοι η σαφής, ελεύθερη, συγκεκριμένη και εν πλήρει επιγνώσει, απουσιάζει, τότε η επεξεργασία των δεδομένων είναι παράνομη και αντίθετη στον GDPR. Από την άλλη, η αρχή του περιορισμού του σκοπού επιβάλλει η επεξεργασία των δεδομένων να γίνεται μόνο για το σκοπό τον οποίο αυτά συλλέχθηκαν, ωστόσο η ΤΝ με τους διάφορους αλγόριθμους χρησιμοποιείται για να δημιουργεί προφίλ και μοτίβα, τα

οποία εν συνεχεία αναλύουν για την εξαγωγή συμπερασμάτων, χωρίς να είναι σαφές αν είναι ο νέος σκοπός είναι συμβατός με τον αρχικό. Οι αλγόριθμοι τεχνητής νοημοσύνης είναι επίσης συχνά περίπλοκοι και δύσκολοι στην κατανόηση, καθιστώντας δύσκολο για τα άτομα να γνωρίζουν πώς χρησιμοποιούνται τα δεδομένα τους και πώς λαμβάνονται οι αποφάσεις. Αυτή η αδιαφάνεια που μπορεί να οδηγήσει σε έλλειψη εμπιστοσύνης στα συστήματα τεχνητής νοημοσύνης, είναι και αντίθετη στην αρχή διαφάνειας του ΓΚΠΔ. Περαιτέρω και με δεδομένο ότι τα συστήματα ΤΝ τρέφονται με τεράστιο όγκο δεδομένων, παρατηρείται αδυναμία ευθυγράμμισης με την αρχή της ακρίβειας, και ανάγκη αντικατάστασης των δεδομένων με αντίστοιχα υψηλότερης ποιότητας από διαφορετικές πηγές. Τέλος, τα δεδομένα προσωπικού χαρακτήρα οφείλουν να μην αποθηκεύονται για διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για τους σκοπούς για τα οποία συλλέχθηκαν όπως επιτάσσει η αρχή του περιορισμού της περιόδου αποθήκευσης, ωστόσο ουκ ολίγες φορές αυτό δεν τηρείται και τα δεδομένα αποθηκεύονται για πολύ μεγαλύτερο χρονικό διάστημα, ενάντια στην αρχή αυτή.

Συμπερασματικά, λαμβάνοντας υπόψη κάποιος την ανάγκη της ΤΝ για δεδομένα, καθώς και τους περιορισμούς που θέτει ο ΓΚΠΔ, αντιλαμβάνεται ότι υφίσταται μια σύγκρουση μεταξύ τους. Μάλιστα, η Katyal το 2019 σε άρθρο της στο UCLA Law Review διερεύνησε πιθανές στρατηγικές για την αντιμετώπιση της σύγκρουσης μεταξύ ΤΝ και συμμόρφωσης με τον ΓΚΠΔ. Πρότεινε δε ως πιο αποτελεσματική προσέγγιση τον σχεδιασμό συστημάτων ΤΝ που ενσωματώνουν τις βασικές αρχές του ΓΚΠΔ. Επιπλέον, η Katyal συνιστά στους οργανισμούς να χρησιμοποιούν διαδικασίες ειδικές για την τεχνητή νοημοσύνη που είναι προσαρμοσμένες στη συμμόρφωση με τον ΓΚΠΔ, όπως η χρήση μοντέλων ΤΝ για τη διασφάλιση της ακρίβειας και της ακεραιότητας των δεδομένων. Από την άλλη, οι οργανισμοί θα πρέπει να δημιουργούν συστήματα τεχνητής νοημοσύνης που είναι διαφανή και ελεγχόμενα, καθώς και να παρέχουν συστήματα τεχνητής νοημοσύνης που είναι συμβατά με τις αρχές περιορισμού σκοπού, ελαχιστοποίησης δεδομένων και προφίλ του ΓΚΠΔ. Χρησιμοποιώντας τέτοιες στρατηγικές, θα μπορεί να διασφαλιστεί ότι τα συστήματα τεχνητής νοημοσύνης συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ (Katyal, 2019)[168].

[168] SK Katyal. "Private accountability in the age of artificial intelligence. Διαθέσιμο: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/uclalr66&section=6 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Συνοψίζοντας, για την συμμόρφωση των συστημάτων ΤΝ με τον ΓΚΠΔ απαιτείται ο εκάστοτε χρήστης να μπορεί να διασφαλίσει τα εξής:

α) νομική βάση για τη συλλογή και επεξεργασία των δεδομένων,

β) συλλογή και επεξεργασία των δεδομένων με βάση την αρχή της διαφάνειας,

γ) ενημέρωση των υποκειμένων των δεδομένων για τη συλλογή και επεξεργασία τους,

δ) ασφάλεια των δεδομένων με τη λήψη κατάλληλων μέτρων προστασίας από μη εξουσιοδοτημένη πρόσβαση ή χρήση όπως η κρυπτογράφηση,

ε) προστασία του απορρήτου των δεδομένων από το σχεδιασμό των συστημάτων, συμπεριλαμβανομένης της εφαρμογής της αρχής περιορισμού του σκοπού, της μη χρήσης τους για άλλο σκοπό χωρίς συγκατάθεση του υποκειμένου και για λήψη αποφάσεων που έχουν σημαντικό αντίκτυπο στο υποκείμενο των δεδομένων

στ) τήρηση διαδικασιών ενημέρωσης των υποκειμένων και ανταπόκρισης σε αιτήματα πρόσβασης ή διαγραφής των δεδομένων τους, αλλά και αντιμετώπισης τυχόν περιστατικών παραβιάσεων με τη διενέργεια σχετικής εκτίμησης αντικτύπου.

Κατ' αυτό τον τρόπο και τα δικαιώματα των υποκειμένων των δεδομένων γίνονται σεβαστά, και τα συστήματα ΤΝ συμμορφώνονται με τις επιταγές των ΕΣΔΑ,ΧΘΔΕΕ, ΓΚΠΔ, ΣΥΝΤΑΓΜΑΤΟΣ κτλ.

5.3 Ο Κανονισμός ΕΕ 2018/1725 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών

Στις 23 Οκτωβρίου 2018, ψηφίστηκε ο Κανονισμός ΕΕ 2018/1725[169] από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της ΕΕ σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των

[169] Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018R1725 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

δεδομένων προσωπικού χαρακτήρα μεταξύ των εν λόγω οργάνων και οργανισμών ή προς άλλους αποδέκτες εγκατεστημένους στην Ένωση. Ο Κανονισμός καταργεί τον προηγούμενο Κανονισμό 45/2001 και την απόφαση 1247/2002/ΕΚ περί του καθεστώτος και των γενικών όρων άσκησης των καθηκόντων του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, με ισχύ από 11 Δεκεμβρίου 2018.

Ο νέος κανονισμός λειτουργεί παράλληλα με τον GDPR, επιδιώκοντας να διασφαλίσει ότι οι κανόνες προστασίας δεδομένων που εφαρμόζονται από τα θεσμικά όργανα και άλλους φορείς και οργανισμούς της Ένωσης είναι σύμφωνοι με τους κανόνες προστασίας δεδομένων που εφαρμόζει ο δημόσιος τομέας των κρατών μελών. Αυτό βοηθά στη δημιουργία μιας ενιαίας προσέγγισης για την προστασία των προσωπικών δεδομένων σε ολόκληρη την Ένωση, καθώς και στη διευκόλυνση της ελεύθερης ροής προσωπικών δεδομένων εντός της Ένωσης.

Έτσι οι διατάξεις του παρόντος κανονισμού ακολουθούν τις ίδιες αρχές με τις διατάξεις του ΓΚΠΔ, όπως αυτές προβλέπονται στο άρθρο 5 του ΓΚΠΔ και υιοθετούνται στο ακέραιο από το άρθρο 4 του παρόντος Κανονισμού. Προβλέπονται επίσης για τη νομιμότητα της επεξεργασίας των δεδομένων, οι νόμιμες βάσεις στις οποίες πρέπει να στηρίζεται η επεξεργασία (άρθρο 5), αναφέρονται τα δικαιώματα του υποκειμένου των δεδομένων και δίνεται ιδιαίτερη βαρύτητα στο απόρρητο των ηλεκτρονικών υπηρεσιών (άρθρο 36). Σε περίπτωση δε, παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας οφείλει να γνωστοποιεί αμελλητί εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (άρθρο 34), ο οποίος επιβλέπει την εφαρμογή του παρόντος κανονισμού σε κάθε πράξη επεξεργασίας δεδομένων που πραγματοποιείται από όργανο ή οργανισμό της Ένωσης (άρθρο 1 παρ.3).

5.4 Ο Νόμος 4624/2019

Ο Νόμος 4624/2019 που ψηφίστηκε στις 26 Αυγούστου 2019 και δημοσιεύτηκε τρεις ημέρες αργότερα στο ΦΕΚ Α’ 137/Α/29-08-2019, θεσπίζει συμπληρωματικά μέτρα εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων και ενσωματώνει στην ελληνική έννομη τάξη την Οδηγία (ΕΕ) 2016/680 για την επεξεργασία δεδομένων από τις από δημόσιες αρχές αρμόδιες για την πρόληψη, διερεύνηση, ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων.

Η ψήφιση του νόμου έλαβε χώρα με τη διαδικασία του κατεπείγοντος, λόγω του ότι η Χώρα μας κινδύνευε να καταδικαστεί με μεγαλύτερο πρόστιμο εξαιτίας της καθυστέρησης ενσωμάτωσης στο εθνικό δίκαιο της προαναφερθείσης Οδηγίας[170].

Σύμφωνα με την έκθεση αξιολόγησης ρυθμίσεων του νόμου[171], οι διατάξεις του εφαρμόζονται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη που πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης από δημόσιους ή ιδιωτικούς φορείς.

Όπως προαναφέρθηκε, ο ΓΚΠΔ ως Κανονισμός Ε.Ε, δεσμεύει άμεσα τα κρατικά όργανα, τις δημόσιες αρχές και τα δικαστήρια, καθώς και όλα τα πρόσωπα, φυσικά και νομικά, που εμπίπτουν στο πεδίο εφαρμογής του, δίχως να απαιτείται έκδοση ιδιαίτερης νομικής πράξης εφαρμογής από τα κράτη μέλη · ωστόσο περιέχει τις λεγόμενες «*ρήτρες ανοίγματος»* και *«ρήτρες ευελιξίας*», τις οποίες ο νέος νόμος εξειδικεύει και αίρει με αυτό τον τρόπο, την νομική αβεβαιότητα σχετικά με την καθυστερημένη συμπλήρωση του Κανονισμού και την μέχρι πρότινος παράλληλη ισχύ του Ν. 2472/1997, «*περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*».

Ειδικότερα, ο νόμος απαρτίζεται από 87 άρθρα[172], το σύνολο των οποίων, με εξαίρεση το άρθρο 86, αφορούν στην προστασία των προσωπικών δεδομένων. Το Κεφάλαιο Α', δηλαδή άρθρα 1-8, περιλαμβάνει γενικές διατάξεις, το σκοπό του νόμου, το πεδίο εφαρμογής του και ορισμούς. Το Κεφάλαιο Β', ήτοι τα άρθρα 9-20, περιλαμβάνει ρυθμίσεις σχετικά με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

---

[170] Απόσμασμα της απόφασης: «*Η Ευρωπαϊκή Επιτροπή αποφάσισε σήμερα να παραπέμψει την Ελλάδα και την Ισπανία στο Δικαστήριο της ΕΕ, επειδή δεν εφάρμοσαν τους ενωσιακούς κανόνες σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα [οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου — οδηγία (ΕΕ) 2016/680]. Τον Απρίλιο του 2016, το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο συμφώνησαν να μεταφερθεί η οδηγία στο εθνικό δίκαιο έως τις 6 Μαΐου 2018. Στην περίπτωση της Ελλάδας, η Επιτροπή καλεί το Δικαστήριο της ΕΕ να επιβάλει οικονομικές κυρώσεις με τη μορφή κατ' αποκοπή ποσού ύψους 5.287,50 ευρώ ημερησίως μεταξύ, αφενός, της επόμενης ημέρας μετά τη λήξη της προθεσμίας για τη μεταφορά της οδηγίας στο εθνικό δίκαιο, όπως αυτή ορίζεται στην οδηγία, και, αφετέρου, είτε της συμμόρφωσης της Ελλάδας είτε της ημερομηνίας δημοσίευσης της απόφασης, δυνάμει του άρθρου 260 παράγραφος 3 της ΣΛΕΕ, με κατώτατο κατ' αποκοπή ποσό ύψους 1.310.000,00 ευρώ και ημερήσια χρηματική ποινή 22.169,70 ευρώ από την ημέρα της πρώτης απόφασης μέχρι την πλήρη συμμόρφωση ή μέχρι την έκδοση δεύτερης δικαστικής απόφασης. ... Η Επιτροπή κίνησε τη διαδικασία επί παραβάσει αποστέλλοντας προειδοποιητική επιστολή στις εθνικές αρχές των οικείων κρατών μελών τον Ιούλιο του 2018 και τις αντίστοιχες αιτιολογημένες γνώμες τον Ιανουάριο του 2019.» Διαθέσιμο:* https://ec.europa.eu/commission/presscorner/detail/EL/INF_19_4251 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[171]Τσιάνακας Χ. Έκθεση αξιολόγησης συνεπειών ρυθμίσεων, Αιτιολογική έκθεση Ν. 4624/2019, Διαθέσιμο: https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/ODHGIA.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[172] Ο νόμος 4624/2019 https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

(ΑΠΔΠΧ), η οποία ορίζεται ως εποπτική Αρχή των ρυθμίσεων του παρόντος νόμου και του ΓΚΠΔ. Το Κεφάλαιο Γ' εκτείνεται στα άρθρα 21-42, και περιέχει ρυθμίσεις που θεσπίστηκαν κατ' εξουσιοδότηση των διατάξεων του ΓΚΠΔ, κάνοντας χρήση των εξαιρέσεων και ρητρών «ευελιξίας». Σο Κεφάλαιο Δ' (άρθρα 43-82) ενσωματώνεται η Οδηγία 2016/680, με τις ρυθμίσεις της οποίας, μεταξύ άλλων, προβλέπεται πλέον η δυνατότητα επεξεργασίας των δεδομένων προσωπικού χαρακτήρα είτε για σκοπό διαφορετικό από εκείνον για τον οποίο έχουν συλλεχθεί είτε για σκοπούς επιστημονικής ή ιστορικής έρευνας (άρθρα 46-52). Στο ίδιο κεφάλαιο περιλαμβάνονται τα δικαιώματα του υποκειμένου των δεδομένων. Τέλος στο Κεφάλαιο Ε΄ και στα άρθρα 83-87, περιέχονται μεταβατικές διατάξεις, καταργείται ο νόμος 2472/1997 για λόγους ασφάλειας δικαίου και συνεκτικότητας των ρυθμίσεων του νέου νόμου, πλην ελαχίστων εξαιρέσεων του άρθρου 84 και ορίζεται ως χρόνος έναρξης ισχύος του νόμου η 1-9-2019.

Στην παρούσα εργασία θα εξετάσουμε συνοπτικά τα άρθρα του νόμου, τα οποία λειτουργούν συμπληρωματικά προς τον ΓΚΠΔ, αναφορικά με την προστασία προσωπικών δεδομένων, ήτοι διατάξεις των άρθρων 21-42 του Κεφαλαίου Γ'.

Αρχικά, στο άρθρο 21 του νόμου, ορίζεται ότι κατά την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών, η συγκατάθεση ανηλίκου είναι έγκυρη, μόνο εφόσον ο τελευταίος έχει συμπληρώσει το 15ο έτος της ηλικίας του, άλλως μόνο μετά την παροχή συγκατάθεσης του νόμιμου αντιπροσώπου του.

Στο άρθρο 22 ρυθμίζεται ο τρόπος επεξεργασίας από δημόσιους και ιδιωτικούς φορείς των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα (των πρώην «ευαίσθητων» [173] του ήδη καταργηθέντος νόμου 2472/1997) κατά παρέκκλιση του άρθρου 9 παρ.1 ΓΚΠΔ. Ειδικότερα προβλέπεται το σύννομο της επεξεργασίας τους, μόνο εφόσον η επεξεργασία είναι απαραίτητη για την άσκηση δικαιωμάτων και υποχρεώσεων κοινωνικής ασφάλισης, για λόγους προληπτικής ιατρικής, ιατρικών διαγνώσεων, εκτίμησης ικανότητας προς εργασία και παροχής κοινωνικής περίθαλψης, καθώς και για λόγους δημοσίου συμφέροντος.

Μάλιστα σύμφωνα με την παρ. 3 του ίδιου άρθρου, οι φορείς που επεξεργάζονται τα δεδομένα, οφείλουν να λαμβάνουν κατάλληλα και ειδικά μέτρα για τη διαφύλαξη των

[173] Σύμφωνα με το άρθρο 9 παρ. 1 ΓΚΠΔ, το , άρθρο 10 της Οδηγίας 2016/680 και το άρθρο 44 περίπτωση ιδ΄ Ν. 4624/2019 με τον όρο «ευαίσθητα» προσωπικά δεδομένα εννοούνται δεδομένα που αποκαλύπτουν «*φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό*».

συμφερόντων του υποκειμένου των δεδομένων, λαμβάνοντας υπόψη την κατάσταση της τεχνολογίας, το κόστος εφαρμογής και τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που θέτει η επεξεργασία στα δικαιώματα και στις ελευθερίες των φυσικών προσώπων.

Στα μέτρα αυτά περιλαμβάνονται ιδίως: α) τεχνικά και οργανωτικά μέτρα που διασφαλίζουν ότι η επεξεργασία είναι σύμφωνη με τον ΓΚΠΔ· β) μέτρα για να διασφαλιστεί ότι είναι δυνατή η εκ των υστέρων επαλήθευση και ο προσδιορισμός του εάν και από ποιον έχουν εισαχθεί, τροποποιηθεί ή αφαιρεθεί τα προσωπικά δεδομένα· γ) μέτρα για την ενδυνάμωση της ευαισθητοποίησης του προσωπικού που ασχολείται με την επεξεργασία· δ) περιορισμοί πρόσβασης από τους υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία· ε) η ψευδωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα· στ) η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα· ζ) μέτρα για τη διασφάλιση της ικανότητας, της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της ανθεκτικότητας των συστημάτων και υπηρεσιών επεξεργασίας που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της δυνατότητας ταχείας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε περίπτωση φυσικού ή τεχνικού συμβάντος· η) διαδικασίες για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας·, θ) ειδικοί κανόνες διασφάλισης της συμμόρφωσης με τον παρόντα νόμο και τον ΓΚΠΔ σε περίπτωση διαβίβασης ή επεξεργασίας για άλλους σκοπούς·, ι) ο ορισμός ΥΠΔ.

Ένα παράδειγμα εφαρμογής ρήτρας ευελιξίας του άρθρου 9 παρ.4 ΓΚΠΔ στον παρόντα νόμο συναντάμε στο άρθρο 23, σύμφωνα με το οποίο απαγορεύεται ρητά η επεξεργασία γενετικών δεδομένων[174] για σκοπούς ασφάλισης υγείας και ζωής. Η απαγόρευση αυτή, βάσει της αιτιολογικής έκθεσης του νόμου, είναι σύμφωνη με την αρχή, η οποία διακηρύσσεται στο άρθρο 12 παρ. 1 της Σύμβασης του Συμβουλίου της Ευρώπης για την προστασία των ανθρωπίνων δικαιωμάτων και της αξιοπρέπειας του ατόμου σε σχέση με τις εφαρμογές της βιολογίας και της ιατρικής «Σύμβαση για τα Ανθρώπινα Δικαιώματα και τη Βιοϊατρική»[175], όπως επίσης και με τη Σύσταση του Συμβουλίου της

[174] Σύμφωνα με το άρθρο 4 εδ. 13 ΓΚΠΔ, γενετικά δεδομένα νοούνται «*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 την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου*».

[175] Η «Σύμβαση για τα ανθρώπινα δικαιώματα και τη Βιοϊατρική» ή αλλιώς Σύμβαση Oviedo, υπογράφηκε στις 4-4-1997 στο Oviedo της Ισπανίας, και κυρώθηκε με το νόμο 2619/1998 (ΦΕΚ Α' 132/19-06-1998)

Ευρώπης CM/Rec (2016)[176], η οποία δεν επιτρέπει να γίνεται διάκριση των ασφαλισμένων βάσει γενετικών χαρακτηριστικών, αλλά τελεί σε συμφωνία και με το πνεύμα του άρθρου 5 της Οικουμενικής Διακήρυξης για τα Γενετικά Δεδομένα του Ανθρώπου της UNESCO[177]. Ουσιαστικά η διάταξη συνεπάγεται την αδυναμία του ασφαλιστικού φορέα να λάβει γνώση των γενετικών δεδομένων καθ' οιονδήποτε τρόπο, προκειμένου να μην παραβιάζεται η διάταξη.

Εντούτοις και παρά την ανωτέρω ρύθμιση για την επεξεργασία των γενετικών δεδομένων, και ενώ θα περίμενε κανείς να εφαρμοστεί αντίστοιχη προστασία για τα βιομετρικά δεδομένα[178], αυτά εξαιρούνται αυτής, γεγονός που συνεπάγεται υποχρέωση του λήπτη της ασφάλισης να τα δηλώνει στον ασφαλιστικό φορέα, προκειμένου να μην κατηγορηθεί για απόκρυψη και του αρνηθεί ο ασφαλιστικός φορέας τυχόν καταβολή ασφαλιστικής αποζημίωσης.

Σύμφωνα με το άρθρο 12 παρ. 1 της εν λόγω Σύμβασης διακηρύσσεται ότι: «*Εξετάσεις που προβλέπουν την εμφάνιση γενετικών νόσων ή που χρησιμοποιούνται είτε για την αναγνώριση του υποκειμένου ως φορέα γονιδίου υπεύθυνου για νόσο είτε για την ανίχνευση γενετικής προδιάθεσης ή δεκτικότητας για νόσο, επιτρέπεται να διενεργούνται μόνο για λόγους υγείας ή για επιστημονική έρευνα που σχετίζεται με λόγους υγείας, και υπό την προϋπόθεση της κατάλληλης γενετικής συμβουλευτικής*».. Διαθέσιμο: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[176] Recommendation Rec(2016) 8 of the Committee of Ministers to the member States on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests Διαθέσιμο: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168093b26e [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[177] Σύμφωνα με το άρθρο 5 της Οικουμενικής Διακήρυξης για τα γενετικά δεδομένα του ανθρώπου της UNESCO, *«α) Η έρευνα, η θεραπεία ή η διάγνωση που αφορούν στο γονιδίωμα ενός ατόμου πραγματοποιούνται μόνο αφού προηγουμένως αξιολογηθούν αυστηρά οι ενδεχόμενοι κίνδυνοι και τα ενδεχόμενα οφέλη και σύμφωνα με τις απαιτήσεις της εθνικής νομοθεσίας. β) Σε όλες τις περιπτώσεις, πρέπει να λαμβάνεται η ελεύθερη και συνειδητή συναίνεση του ενδιαφερόμενου ατόμου. Αν το ενδιαφερόμενο άτομο δεν είναι σε θέση να συναινέσει, πρέπει να λαμβάνεται έγκριση ή εξουσιοδότηση όπως ορίζεται από τη νομοθεσία, με γνώμονα το συμφέρον του ατόμου... ε) Αν σύμφωνα με το νόμο το άτονο δεν είναι ικανό να συναινέσει, η έρευνα που αφορά το γονιδίωμά του δεν μπορεί να διεξάγεται παρά μόνο προς άμεσο όφελος της υγείας του, σύμφωνα με την εξουσιοδότηση και τις προστατευτικές διατάξεις που ορίζει η νομοθεσία. Έρευνα που δεν αναμένεται να έχει άμεσο όφελος για την υγεία μπορεί να επιχειρείται μόνο κατ' εξαίρεσιν, με τη μεγαλύτερη συγκράτηση, αφού ληφθεί μέριμνα να εκτεθεί το άτομο στον ελάχιστο κίνδυνο και καταναγκασμό και μόνο αν η έρευνα πραγματοποιείται προς όφελος της υγείας άλλων ατόμων που ανήκουν στην ίδια ηλικιακή ομάδα ή βρίσκονται στην ίδια γενετική κατάσταση, σύμφωνα με τις διατάξεις που ορίζονται από τη νομοθεσία και με την προϋπόθεση ότι αυτή η έρευνα συμβαδίζει με την προστασία των ανθρωπίνων δικαιωμάτων του ατόμου.»* Διαθέσιμο: https://bioethics.gr/api/files/download/2198/UNESCO_Declaration_on_human_genome.pdf?attachment=false [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[178]Σύμφωνα με το άρθρο 4 εδ. 14 του ΓΚΠΔ, βιομετρικά δεδομένα είναι «*τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα*».

Στη συνέχεια και στα άρθρα 24-26 του νόμου προβλέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από αυτούς για τους οποίους είχαν συλλεχθεί αρχικά και διακρίνει επίσης ανάμεσα σε δημόσιους και ιδιωτικούς φορείς.

Γενικά, σύμφωνα με την αρχή του περιορισμού του σκοπού (άρθρο 5 παρ. 1 β' ΓΚΠΔ), τα δεδομένα προσωπικού χαρακτήρα «*συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς*». Ωστόσο, βάσει της ρύθμισης του άρθρου 6 παρ. 4 του ΓΚΠΔ, είναι δυνατή η επεξεργασία των προσωπικών δεδομένων για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί, όταν αυτή βασίζεται σε διάταξη του εθνικού δικαίου κράτους-μέλους, και αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών δημοσίου συμφέροντος που προβλέπονται στο άρθρο 23 του ΓΚΠΔ.

Συγκεκριμένα σύμφωνα με το άρθρο 24 παρ. 1 τέτοιου είδους επεξεργασία επιτρέπεται από τους δημόσιους φορείς όταν είναι αναγκαία για την εκπλήρωση των καθηκόντων που τους έχουν ανατεθεί και εφόσον είναι α) απαραίτητο να ελεγχθούν οι πληροφορίες που παρέχονται από το υποκείμενο των δεδομένων, διότι υπάρχουν βάσιμες ενδείξεις ότι οι πληροφορίες αυτές είναι εσφαλμένες· β) αναγκαία για την αποτροπή κινδύνων για την εθνική ασφάλεια, εθνική άμυνα ή δημόσια ασφάλεια ή για τη διασφάλιση φορολογικών και τελωνειακών εσόδων· γ) αναγκαία για τη δίωξη ποινικών αδικημάτων· δ) αναγκαία για την αποτροπή σοβαρής βλάβης στα δικαιώματα άλλου προσώπου· ε) απαραίτητη για την παραγωγή των επίσημων στατιστικών.

Αναφορικά με τους ιδιωτικούς φορείς (α.25 παρ.1), η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί, επιτρέπεται, εφόσον είναι απαραίτητη α) για την αποτροπή απειλών κατά της εθνικής ασφάλειας ή της δημόσιας ασφάλειας κατόπιν αιτήματος δημόσιου φορέα· ή β) για τη δίωξη ποινικών αδικημάτων· ή γ) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, εκτός και εάν υπερτερεί το συμφέρον του υποκειμένου των δεδομένων να μην τύχουν επεξεργασίας τα δεδομένα αυτά.

Στο άρθρο 26 καθορίζονται οι προϋποθέσεις που απαιτούνται για τη σύννομη διαβίβαση προσωπικών δεδομένων από δημόσιο σε δημόσιο φορέα, σύμφωνα με το οποίο: «*Οι δημόσιοι φορείς επιτρέπεται να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα σε ιδιωτικούς φορείς εφόσον: α) η διαβίβαση είναι απαραίτητη για την εκτέλεση των καθηκόντων του φορέα που διαβιβάζει και πληρούνται περαιτέρω και οι προϋποθέσεις του*

άρθρου 24· β) ο τρίτος στον οποίο διαβιβάζονται έχει έννομο συμφέρον να είναι σε γνώση της διαβίβασης και το υποκείμενο των δεδομένων δεν έχει έννομο συμφέρον να μην διαβιβασθούν τα δεδομένα που το αφορούν· ή γ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων και ο τρίτος δεσμεύθηκε έναντι του δημόσιου φορέα που του διαβίβασε τα δεδομένα ότι θα τα επεξεργαστεί μόνο για τον σκοπό για τον οποίο διαβιβάσθηκαν. Η επεξεργασία για άλλους σκοπούς επιτρέπεται, εάν επιτρέπεται η διαβίβαση σύμφωνα με την παράγραφο 1 και ο φορέας διαβίβασης έχει παράσχει τη συγκατάθεσή του για τη διαβίβαση.».

Παρακάτω στο άρθρο 27 του νόμου[179], σε συνέχεια των κατευθυντήριων γραμμών της Ομάδας Εργασίας του Άρθρου 29 για τη συγκατάθεση (WP 259 rev.01[180]) αλλά και της Απόφασης 26/2019 της ΑΠΔΠΧ[181], ρυθμίζεται για πρώτη φορά σε επίπεδο νομοθεσίας η νόμιμη βάση επεξεργασίας των προσωπικών δεδομένων στο πλαίσιο των εργασιακών σχέσεων. Ειδικότερα στην παράγραφο 1 του άρθρου προβλέπεται ότι: «*Δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβάλλονται σε επεξεργασία για σκοπούς της σύμβασης εργασίας, εφόσον είναι απολύτως απαραίτητο για την απόφαση σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της*.», ενώ στην παρ. 2 γίνεται αναφορά στην περίπτωση συγκατάθεσης του εργαζομένου στην επεξεργασία.

Με τη διάταξη αυτή περιορίζονται οι σκοποί επεξεργασίας των δεδομένων των εργαζομένων, ωστόσο σύμφωνα με τον Καρκατζούνη[182] «*χρήζει ιδιαίτερης προσοχής και θα πρέπει να ερμηνεύεται στενά, υπό το πρίσμα των αποφάσεων όχι μόνο της ελληνικής Αρχής, αλλά και των κατευθύνσεων των ευρωπαϊκών οργάνων, αφού διαφαίνεται αρκετά πιθανό να οδηγήσει σε ευρεία χρήση της δυνατότητας αυτής, με αποτέλεσμα να οδηγηθούμε σε μία de facto εναντίωση με το πνεύμα του Κανονισμού, αλλά και την παγιωμένη νομολογία σχετικά*».

---

[179] Το άρθρο θεσπίστηκε δυνάμει σχετικής δυνατότητας που παρέχεται με τη «ρήτρα ανοίγματος» του άρθρου 88 παρ.1 ΓΚΠΔ, αιτιολογική σκέψη 155 ΓΚΠΔ.

[180] Guidelines on Consent under Regulation 2016/679 (wp259rev.01) Διαθέσιμο: https://ec.europa.eu/newsroom/article29/items/623051 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[181] Απόφαση 26/2019 ΑΠΔΠΧ, Διαθέσιμο: https://www.dpa.gr/sites/default/files/2020-05/26_2019anonym.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[182] Καρκατζούνης Β., «Οι νέες διατάξεις για την προστασία προσωπικών δεδομένων των εργαζομένων (Νόμος 4624/2019)» Διαθέσιμο: https://www.lawspot.gr/nomika-blogs/vasilis_karkatzoynis/oi-nees-diataxeis-gia-tin-prostasia-prosopikon-dedomenon-ton#footnote2_zk8oftb [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Αξιοσημείωτη επίσης είναι η ρύθμιση του άρθρου 28, με την οποία θεσπίζεται ένα προβάδισμα της ελευθερίας του Τύπου, υπό τη μορφή της μη εφαρμογής των δικαιωμάτων των υποκειμένων, λ.χ. του δικαιώματος διαγραφής, έναντι της αρχικής επιλογής του νομοθέτη στον ήδη καταργηθέντα νόμο 2472/1997 που έδινε προβάδισμα υπέρ της προστασίας δεδομένων προσωπικού χαρακτήρα, αλλά και της ουδετερότητας του Συντάγματος, από το οποίο δεν προκύπτει επικράτηση του ενός ατομικού δικαιώματος επί του άλλου.

Ειδικότερα, το δικαίωμα για την προστασία της ιδιωτικής ζωής (άρθρο 9 παρ. 1 του Συντάγματος) αλλά και των προσωπικών δεδομένων (άρθρο 9Α του Συντάγματος) συχνά συγκρούεται με την ελευθερία της εκφράσεως και του Τύπου για την ενημέρωση του κοινού (άρθρο 14 παρ. 1 του Συντάγματος), καθώς και με το δικαίωμα στην πληροφόρηση (άρθρο 5Α του Συντάγματος)[183]. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων υποχρεώνει τα κράτη μέλη να συμβιβάζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία έκφρασης και πληροφόρησης στη διάταξη του άρθρου 85 ΓΚΠΔ. Ειδικότερα, εξαιρέσεις και παρεκκλίσεις από συγκεκριμένα κεφάλαια του ΓΚΠΔ προβλέπονται για δημοσιογραφικούς σκοπούς ή για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, στο μέτρο που είναι αναγκαίες για τον συμβιβασμό του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία της έκφρασης και πληροφόρησης.

Το δικαίωμα της ελευθερίας της έκφρασης κατοχυρώνεται επίσης στο άρθρο 11 του ΧΘΔΕΕ και περιλαμβάνει την «*ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων*». Σύμφωνα τόσο με το άρθρο 11 του ΧΘΔΕΕ όσο και με το άρθρο 10 της ΕΣΔΑ, η ελευθερία πληροφόρησης προστατεύει το δικαίωμα όχι μόνο της μετάδοσης αλλά και της λήψης πληροφοριών.

Δεδομένων των ανωτέρω, θα πρέπει να εφαρμόζεται η αρχή της αναλογικότητας που προβλέπει το άρθρο 25 παρ. 1 του Συντάγματος με τέτοιον τρόπο, ώστε τα προστατευόμενα αγαθά (ελευθερία του τύπου, δικαίωμα των πολιτών στην πληροφόρηση και δικαίωμα στην προστασία της ιδιωτικής ζωής του ατόμου και στον πληροφοριακό

[183] ΑΠΔΠΧ, Αποφάσεις 26/2007, 43/2007, 58/2007, 36/2012, 165/2012, 16/2015, 17/2015, 52/2015

αυτοκαθορισμό) να διατηρήσουν την κανονιστική τους εμβέλεια (Παναγοπούλου, 2016)[184].

Στο άρθρο 31 του νόμου βλέπουμε ότι η υποχρέωση του υπευθύνου επεξεργασίας να ενημερώνει το υποκείμενο των δεδομένων περιορίζεται, σε αντίθεση με το άρθρο 13 ΓΚΠΔ, όταν «*α) αφορά μια περαιτέρω επεξεργασία αποθηκευμένων σε γραπτή μορφή δεδομένων, στην οποία ο υπεύθυνος επεξεργασίας απευθύνεται άμεσα στο υποκείμενο των δεδομένων, ο σκοπός είναι συμβατός με τον αρχικό σκοπό συλλογής σύμφωνα με το ΓΚΠΔ, η επικοινωνία με το υποκείμενο των δεδομένων δεν γίνεται σε ψηφιακή μορφή και το ενδιαφέρον του υποκειμένου των δεδομένων για την παροχή πληροφοριών κατά τις περιστάσεις της συγκεκριμένης περίπτωσης, ιδίως όσον αφορά το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα θεωρείται ότι δεν είναι υψηλό· β) στην περίπτωση του δημόσιου φορέα, θα έθετε σε κίνδυνο την ορθή εκτέλεση των καθηκόντων του υπεύθυνου επεξεργασίας με την έννοια του άρθρου 23 παράγραφος 1 στοιχεία α) έως ε) του ΓΚΠΔ, και το συμφέρον του υπεύθυνου επεξεργασίας να μην παράσχει τις πληροφορίες, υπερτερεί του συμφέροντος του υποκειμένου των δεδομένων· γ) θα έθετε σε κίνδυνο την εθνική ή τη δημόσια ασφάλεια και το συμφέρον του υπεύθυνου επεξεργασίας να μην παράσχει τις πληροφορίες υπερτερεί του συμφέροντος του υποκειμένου των δεδομένων· δ) θα παρεμπόδιζε τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων και το συμφέρον του υπεύθυνου επεξεργασίας να μην παράσχει πληροφορίες υπερτερεί του συμφέροντος του υποκειμένου των δεδομένων· ε) θα έθετε σε κίνδυνο την εμπιστευτική διαβίβαση δεδομένων σε δημόσιους φορείς.*»

Τέλος ιδιαίτερη αναφορά θα πρέπει μεταξύ άλλων, να γίνει στο άρθρο 10 παρ. 5 ν. 4624/2019, καθώς εξαιρεί την ΑΠΔΠΧ από τον έλεγχο των δικαστικών και εισαγγελικών αρχών στο πλαίσιο της δικαστικής λειτουργίας και των δικαστικών καθηκόντων, χωρίς να ορίζει εποπτική αρχή αποτελούμενη από δικαστές που θα είναι αρμόδιες για τα δικαστήρια. Αυτό έρχεται σε ευθεία αντίθεση με το άρθρο 8 παρ. 3 του Χάρτη των Θεμελιωδών Δικαιωμάτων, που ορίζει ότι ο σεβασμός των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα υπόκειται σε ανεξάρτητη αρχή, χωρίς να αναγνωρίζονται εξαιρέσεις για ορισμένες εξουσίες, όπως οι δικαστικές εξουσίες. Ο GDPR έχει επεκτείνει το πεδίο εφαρμογής του στις δικαστικές και εισαγγελικές αρχές, ωστόσο, δεν καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοσία τους, προκειμένου να διασφαλιστεί η ανεξαρτησία των

[184] Παναγοπούλου Φ., Προσωπικά Δεδομένα, 2016, σελ. 5

δικαστικών λειτουργών κατά την άσκηση των δικαστικών τους καθηκόντων. συμπεριλαμβανομένης της λήψης αποφάσεων (άρθρο 55 παρ. 3 και αιτιολογική σκέψη 20 ΓΚΠΔ)[185]. Ωστόσο αυτή η εξαίρεση της ΑΠΔΠΧ από τον έλεγχο των δικαστικών και εισαγγελικών αρχών είναι ανησυχητική καθώς θα μπορούσε να οδηγήσει σε έλλειψη λογοδοσίας και διαφάνειας στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Είναι σημαντικό να γίνεται σεβαστός ο GDPR και να τηρείται ο Χάρτης των Θεμελιωδών Δικαιωμάτων, προκειμένου να διασφαλιστεί ότι τα προσωπικά δεδομένα προστατεύονται και ότι τα άτομα έχουν το δικαίωμα στην ιδιωτική ζωή.

Σύμφωνα με τα ανωτέρω λοιπόν, δεν υπάρχει αμφιβολία ότι και ο νέος αυτός νόμος δεν είναι άριστα καταρτισμένος ούτε οι ρυθμίσεις του είναι πλήρεις στο σύνολό τους, καθώς περιέχει νομοθετικές αστοχίες, νομοτεχνικά παροράματα, αντιθέσεις προς το ευρωπαϊκό δίκαιο και εσωτερικές αντιφάσεις (Γριβοκωστόπουλος, 2021)[186]. Ωστόσο δεδομένης της ανάγκης διορθωτικών ρυθμίσεων, αναμένεται ότι θα βελτιωθεί η ισορροπία μεταξύ του δικαιώματος ενός ατόμου στην πληροφοριακή αυτοδιάθεση και της ανάγκης της αγοράς να προσφέρει καλύτερης ποιότητας και πιο εξατομικευμένα προϊόντα και υπηρεσίες. Ο απώτερος στόχος είναι να διατηρηθεί αυτή η ισορροπία, επιτρέποντας και στα δύο μέρη να επωφεληθούν.

6 / Το νομοθετικό πλαίσιο των τεχνολογιών AI και IOT σε ευρωπαϊκό και εθνικό επίπεδο

6.1 Εισαγωγή

Καίτοι τεχνητή νοημοσύνη και διαδίκτυο των πραγμάτων υπάρχουν εδώ και χρόνια στις ζωές μας, ανέκαθεν το νομοθετικό πλαίσιο των τεχνολογιών αυτών ήταν ελλιπές.

Υπάρχουν πλείστα νομοθετήματα που αφορούν την ΤΝ και το IoT, μερικά εκ των οποίων καταργήθηκαν, ενώ άλλα εξακολουθούν και βρίσκονται σε ισχύ.

[185] Παναγοπούλου Φ., «Νόμος 4624/2019 και Εφαρμογή GDPR: Πολλά υποσχόμενος, αλλά παράλληλα καθυστερημένος» Διαθέσιμο: https://www.syntagmawatch.gr/trending-issues/nomos-4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[186] Γριβοκωστόπουλος Ι., «Κριτική ανάλυση του Ν. 4624/2019», Επιθεώρηση Δικαίου Πληροφορικής Τ.1 (2021), Διαθέσιμο: https://ejournals.lib.auth.gr/infolawj/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Επιγραμματικά, όσον αφορά το **Διαδίκτυο των Πραγμάτων**, η συνολική σχετική νομοθεσία που έχει εφαρμοστεί είναι η ακόλουθη:

- **Οδηγία 95/46/ΕΚ,** η οποία **καταργήθηκε** από τον ΓΚΠΔ 2016/679
- **Ν. 2472/1997,** ο οποίος **καταργήθηκε** με τον Ν. 4624/2019 με εξαίρεση των διατάξεων που αναφέρονται στο άρθρο 84 του νέου νόμου
- **Οδηγία 2002/58/ΕΚ** (e-Privacy Directive or Cookie Law) - τροποποιήθηκε με την Οδηγία **2009/136/ΕΚ** και οδεύει ***προς κατάργηση***[187]
- **Ν.3471/2006** για τις ηλεκτρονικές επικοινωνίες, **ισχύει**
- **Οδηγία 2006/24/ΕΚ και Ν. 3917/2011, ισχύουν**
- **Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) 2016/679, ισχύει**
- **Ν. 4624/2019, ισχύει**
- **Ν.4961/2022, ισχύει**
- **Γνωμοδοτικό πλαίσιο - (Γνώμες της Ομάδας Εργασίας του άρθρου 29)**[188] **- ισχύουν:**

- **Γνώμη 5/2010** η οποία ***αντικαταστάθηκε*** από την **9/2011**: Αφορά τις εφαρμογές αναγνώρισης ραδιοσυχνοτήτων (RFID/Radio-frequency identification) και συγκεκριμένα την αναθεωρημένη πρόταση της βιομηχανίας για ένα πλαίσιο αξιολόγησης αντικτύπου και προστασίας δεδομένων για εφαρμογές RFID, κατά την οποία θα πρέπει να εφαρμόζεται μια φάση πρότερης αξιολόγησης που ταξινομεί μια εφαρμογή RFID σύμφωνα με μια κλίμακα τεσσάρων επιπέδων και με βάση ένα δέντρο απόφασης (decision tree). Θα πρέπει, δηλαδή, να υπάρχει μια φάση προ-αξιολόγησης με συγκεκριμένη διαδικασία πέραν της υποχρεωτικής αξιολόγησης κινδύνου (risk assessment) που εφαρμόζεται για την προστασία των δεδομένων RFID και αναλύεται σε τέσσερα επίπεδα.
- **Γνώμη 13/2011:** Σχετίζεται με τον γεωεντοπισμό (υπηρεσίες εντοπισμού γεωγραφικής θέσης) και συγκεκριμένα τη χρήση δεδομένων γεωγραφικής θέσεως από τις λεγόμενες «έξυπνες» κινητές συσκευές, τα οποία συνιστούν δεδομένα προσωπικού χαρακτήρα. Η γνώμη 13/2011 θεσπίζει τους θεμιτούς λόγους επεξεργασίας που

[187] Πρόταση Κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το σεβασμό της ιδιωτικής ζωής και την προστασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/εκ (κανονισμός για το απόρρητο και τις ηλεκτρονικές επικοινωνίες) Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[188] Η ομάδα εργασίας του άρθρου 29 είναι η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ.

βασίζονται στην έγκυρη συγκατάθεση, η οποία συγκατάθεση αφορά συγκεκριμένο σκοπό επεξεργασίας δεδομένων από τον υπεύθυνο της επεξεργασίας (για παράδειγμα την κατάρτιση προφίλ). Επίσης η γνώμη υπογραμμίζει ότι οι υπηρεσίες εντοπισμού θέσεως, κατά την αγορά της συσκευής, πρέπει να μην είναι ενεργοποιημένες.

- **Γνώμη 02/2013:** Αφορά εφαρμογές έξυπνων συσκευών, η οποία θέτει πολλές υποχρεώσεις στους σχεδιαστές των συσκευών όπως: α) να γνωρίζουν και να συμμορφώνονται με τις υποχρεώσεις που υπέχουν ως υπεύθυνοι επεξεργασίας, όταν επεξεργάζονται δεδομένα που έχουν λάβει από ή που αφορούν τους τελικούς χρήστες και όταν συνεργάζονται με εκτελούντες επεξεργασία δεδομένων, β) να ζητούν συγκατάθεση προτού η εφαρμογή αρχίσει να ανακτά ή να τοποθετεί πληροφορίες στη συσκευή για κάθε κατηγορία δεδομένων, γ)να έχουν επίγνωση του ότι η συγκατάθεση δεν νομιμοποιεί την υπερβολική ή δυσανάλογη επεξεργασία δεδομένων, δ) να γνωστοποιούν κατά τρόπο συγκεκριμένο και κατανοητό τους σκοπούς της επεξεργασίας δεδομένων πριν από την εγκατάσταση της εφαρμογής και να μην τροποποιούν αυτούς τους σκοπούς χωρίς ανανέωση της συγκατάθεσης, ε) να επιτρέπουν στους χρήστες να ανακαλούν τη συγκατάθεσή τους και να απεγκαθιστούν την εφαρμογή και να διαγράφουν τα δεδομένα, εφόσον απαιτείται, στ) να τηρούν την αρχή της ελαχιστοποιήσεως δεδομένων και να συλλέγουν μόνο τα δεδομένα που είναι απολύτως απαραίτητα για την εκτέλεση της επιθυμητής λειτουργικής δυνατότητας, ζ) να λαμβάνουν τα αναγκαία οργανωτικά και τεχνικά μέτρα προκειμένου να εξασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα που επεξεργάζονται σε όλα τα στάδια του σχεδιασμού και της εκτέλεσης της εφαρμογής, η) να παρέχουν ευανάγνωστη, κατανοητή και ευχερώς προσπελάσιμη πολιτική προστασίας της ιδιωτικής ζωής, θ) να επιτρέπουν στους χρήστες εφαρμογών να ασκούν τα δικαιώματα προσβάσεως, διορθώσεως, διαγραφής, καθώς και το δικαίωμα ενστάσεως στην επεξεργασία των δεδομένων τους και να τους ενημερώνουν για την ύπαρξη των αντίστοιχων μηχανισμών, και ι) να καθορίζουν εύλογη περίοδο διατηρήσεως για τα δεδομένα που συλλέγονται με την εφαρμογή και να προκαθορίζουν περίοδο αδράνειας, μετά την οποία ο λογαριασμός θεωρείται ότι έχει λήξει.
- **Γνώμη 04/2013:** για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων αναφορικά με τα ευφυή δίκτυα και ευφυή συστήματα μέτρησης - «υπόδειγμα ΕΕΠΔ», σύμφωνα με την οποία θα πρέπει να υπάρχει σαφής καθοδήγηση σχετικά με το τι μπορεί να γίνει χωρίς συγκατάθεση του χρήστη και το τι απαιτεί συγκατάθεση του χρήστη.

- **Γνώμη 8/2014**[189]**:** Η σημαντικότερη γνωμοδότηση της ομάδας εργασίας του άρθρου 29 για το IoT και την προστασία της ιδιωτικής ζωής και των δεδομένων, που παρουσιάζει τους κυριότερους κινδύνους που απειλούν την προστασία των δεδομένων του οικοσυστήματος IoT, εστιάζοντας σε τρεις τομείς που είναι πιο κοντά στην καθημερινότητα του μέσου ανθρώπου, ήτοι: τις wearable συσκευές όπως έξυπνα ρολόγια ή γυαλιά κ.α, τις quantified self ή ποσοτικοποιημένου εαυτού, που καταγράφουν πληροφορίες σχετικά με τις συνήθειες και τον τρόπο ζωής των χρηστών (αυτοπαρακολούθηση), με σκοπό μετέπειτα εξάγουν πληροφορίες, καθώς και του οικιακού αυτοματισμού/domotics, όπως θερμοστάτες, ψυγεία κτλ.

Αναφορικά με την **Τεχνητή Νοημοσύνη**, σε ευρωπαϊκό επίπεδο συναντάμε τα εξής σημαντικά κείμενα:

Με αφετηρία την 20η Ιανουαρίου 2015 οπότε η Επιτροπή JURI αποφάσισε τη σύσταση Ομάδας Εργασίας (WG) για νομικά ζητήματα που σχετίζονται με την ανάπτυξη της Ρομποτικής και της Τεχνητής Νοημοσύνης (AI) στην Ευρωπαϊκή Ένωση, το Μάιο του 2016, η Mady Delvaux, εισηγήτρια της επιτροπής νομικών θεμάτων του Ευρωπαϊκού Κοινοβουλίου παρουσίασε μια πρόχειρη έκθεση με συστάσεις προς την Επιτροπή σχετικά με τους κανόνες του αστικού δικαίου για τη ρομποτική (2015/2103(INL))[190], μετά από την οποία ακολούθησε το **Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 16ης Φεβρουαρίου 2017**, (2018/C 252/25)[191]. Το Ψήφισμα περιλαμβάνει τις γενικές και ηθικές αρχές σχετικά με την ανάπτυξη της ρομποτικής και της τεχνητής νοημοσύνης και καλεί την Επιτροπή να προτείνει ένα κοινό ευρωπαϊκό ορισμό των έξυπνων αυτόνομων ρομπότ και των υποκατηγοριών τους λαμβάνοντας υπόψη τα διάφορα χαρακτηριστικά τους. Ταυτόχρονα ζητά τη δημιουργία ενός Ευρωπαϊκού Οργανισμού για τη ρομποτική και την τεχνητή νοημοσύνη προκειμένου να παρέχει την τεχνική, ηθική και κανονιστική εμπειρογνωμοσύνη που απαιτείται.

Εν συνεχεία τον Απρίλιο του 2018 μεσολάβησε η ανακοίνωση της Ευρωπαϊκής Στρατηγικής για την ΤΝ «**Τεχνητή Νοημοσύνη για την Ευρώπη**»[192], σύμφωνα με την

[189]Διαθέσιμο:https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[190]Διαθέσιμο: https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_EN.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[191] «European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics» (2018/C 252/25) Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&rid=9 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
[192] Τεχνητή νοημοσύνη για την Ευρώπη, COM/2018/237 final, Διαθέσιμο:

οποία «*Η προσέγγιση της τεχνητής νοημοσύνης που περιγράφεται στο παρόν έγγραφο καταδεικνύει την πορεία που πρέπει να ακολουθηθεί στο μέλλον και τονίζει την ανάγκη συνένωσης των δυνάμεων σε ευρωπαϊκό επίπεδο, προκειμένου να διασφαλιστεί ότι όλοι οι Ευρωπαίοι συμμετέχουν στον ψηφιακό μετασχηματισμό, ότι διατίθενται επαρκείς πόροι στην τεχνητή νοημοσύνη και ότι οι αξίες και τα θεμελιώδη δικαιώματα της Ένωσης βρίσκονται στην πρώτη γραμμή του κλάδου της τεχνητής νοημοσύνης*».

Επόμενο βήμα ήταν η σύσταση της «Ομάδας εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη» τον Ιούνιο του 2018, αποτελούμενη από 52 εμπειρογνώμονες του ακαδημαϊκού κόσμου, των επιχειρήσεων και της κοινωνίας των πολιτών[193], η οποία τον Απρίλιο του 2019 εξέδωσε τις « **Κατευθυντήριες γραμμές δεοντολογίας για αξιόπιστη τεχνητή νοημοσύνη**»[194], θέτοντας τις βάσεις και τις απαιτήσεις για αξιόπιστη ΤΝ. Στόχος των κατευθυντήριων γραμμών είναι η προαγωγή της αξιοπιστίας της τεχνητής νοημοσύνης (ΤΝ). Η αξιόπιστη ΤΝ έχει τρεις συνιστώσες, οι οποίες θα πρέπει να πληρούνται σε ολόκληρο τον κύκλο ζωής του συστήματος: α) θα πρέπει να είναι **σύννομη**, ήτοι να τηρεί όλες τις εφαρμοστέες νομοθετικές και κανονιστικές διατάξεις, β) θα πρέπει να είναι **δεοντολογική**, ήτοι να διασφαλίζει τη συμμόρφωση με δεοντολογικές αρχές και αξίες και γ) θα πρέπει να είναι **στιβαρή**, τόσο από τεχνικής όσο και από κοινωνικής άποψης, διότι, ακόμη κι όταν υπάρχει καλή πρόθεση, τα συστήματα ΤΝ μπορούν να προκαλέσουν ακούσια βλάβη.

Τον Φεβρουάριο του 2020 η Ευρωπαϊκή Επιτροπή δημοσίευσε τη «**Λευκή Βίβλο για την Τεχνητή Νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης**»[195], συνοδευόμενη από την «**Έκθεση σχετικά με τις επιπτώσεις της τεχνητής νοημοσύνης, του διαδικτύου των πραγμάτων και της ρομποτικής στην ασφάλεια και την ευθύνη**»**[196],** όπου παρουσιάζει επιλογές πολιτικής που θα επιτρέψουν

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=COM%3A2018%3A237%3AFIN [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[193] «*Commission appoints expert group on AI and launches the European AI Alliance*» Διαθέσιμο: https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[194] *«Ethics guidelines for trustworthy AI»* Διαθέσιμο: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[195] «Λευκή Βίβλος για την τεχνητή νοημοσύνη», Διαθέσιμο: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligencefeb2020_el_1.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[196] https://eur-lex.europa.eu/legal-content/EL/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

την αξιόπιστη και ασφαλή ανάπτυξη της ΤΝ στην Ευρώπη, με πλήρη σεβασμό στις αξίες και τα δικαιώματα των πολιτών της ΕΕ. Ειδικότερα, όρισε ποιες εφαρμογές ΤΝ είναι υψηλού κινδύνου[197] και έθεσε το κανονιστικό τους πλαίσιο :

- ασφαλή **δεδομένα εκπαίδευσης** κατά την τυχόν μεταγενέστερη χρήση των προϊόντων ή υπηρεσιών ΤΝ ώστε να μην οδηγήσει σε αποτελέσματα που συνεπάγονται απαγορευμένη διάκριση, και να αποσκοπούν στη διασφάλιση της επαρκούς προστασίας της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα.
- **τήρηση αρχείων** του συνόλου των δεδομένων που χρησιμοποιήθηκε για την εκπαίδευση και τη δοκιμή των συστημάτων ΤΝ για εύλογο χρονικό διάστημα.
- Διασφάλιση της **παροχής σαφών αντικειμενικών, συνοπτικών και εύληπτων πληροφοριών** σχετικά με τις ικανότητες και τους περιορισμούς του συστήματος ΤΝ.
- **στιβαρά και ακριβή** συστήματα ΤΝ που αντιμετωπίζουν επαρκώς τα σφάλματα ή τις ανακολουθίες και τις επιθέσεις σε δεδομένα και αλγορίθμους σε όλες τις φάσεις του κύκλου ζωής.
- **ανθρώπινη εποπτεία** για διασφάλιση μη υπονόμευσης της ανθρώπινης αυτονομίας.
- Η χρήση της ΤΝ για την **εξ αποστάσεως βιομετρική ταυτοποίηση** επιτρέπεται μόνο όταν είναι δεόντως αιτιολογημένη, αναλογική και υπόκειται σε επαρκείς εγγυήσεις.

Η πρώτη παγκόσμια απόπειρα ρύθμισης με κανόνες οριζόντιας εφαρμογής των συστημάτων ΤΝ ήρθε τον Απρίλιο του 2021, όταν η Επιτροπή, στα πλαίσια της πολιτικής υπόσχεσης της Προέδρου της Ursula von der Leyen περί θεσμοθέτησης νομοθεσίας, ικανής να αντιμετωπίσει τις ηθικές συνέπειες της ΤΝ για τον άνθρωπο, ανακοίνωσε την «**Πρόταση – Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση Εναρμονισμένων Κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για**

[197] Για παράδειγμα όταν η εφαρμογή ΤΝ χρησιμοποιείται σε έναν τομέα στον οποίο, δεδομένων των χαρακτηριστικών των δραστηριοτήτων που αναλαμβάνονται συνήθως, αναμένεται ότι θα εκδηλωθούν σημαντικοί κίνδυνοι, όπως πχ. υγειονομική περίθαλψη· μεταφορές· ενέργεια και τμήματα του δημόσιου τομέα και όταν η εφαρμογή ΤΝ στον εν λόγω τομέα χρησιμοποιείται, επιπλέον, με τρόπο που μπορεί να συνεπάγεται σημαντικούς κινδύνους.

την Τεχνητή Νοημοσύνη) και για την Τροποποίηση Ορισμένων Νομοθετικών Πράξεων της Ένωσης»[198] με τους ακόλουθους ειδικούς στόχους:

- να διασφαλιστεί ότι τα συστήματα ΤΝ που διατίθενται στην αγορά και χρησιμοποιούνται είναι ασφαλή και τηρούν την ισχύουσα νομοθεσία για τα θεμελιώδη δικαιώματα και τις αξίες της Ένωσης·
- να διασφαλιστεί ασφάλεια δικαίου για τη διευκόλυνση των επενδύσεων και της καινοτομίας στον τομέα της ΤΝ·
- να ενισχυθεί η διακυβέρνηση και η αποτελεσματική επιβολή της ισχύουσας νομοθεσίας για τα θεμελιώδη δικαιώματα και τις απαιτήσεις ασφάλειας που εφαρμόζονται στα συστήματα ΤΝ·
- να διευκολυνθεί η ανάπτυξη ενιαίας αγοράς για νόμιμα, ασφαλή και αξιόπιστα συστήματα ΤΝ και να προληφθεί ο κατακερματισμός της αγοράς.

Ακολούθως, τον Σεπτέμβριο του 2022 η Ευρωπαϊκή Επιτροπή δημοσίευσε την «**Πρόταση οδηγίας για την προσαρμογή των κανόνων εξωσυμβατικής αστικής ευθύνης στην τεχνητή νοημοσύνη**»[199]**,** η οποία στοχεύει να αντιμετωπίσει τη νομική αβεβαιότητα και το νομικό κατακερματισμό που εμποδίζουν την ανάπτυξη της εσωτερικής αγοράς και, ως εκ τούτου, αποτελούν σημαντικά εμπόδια στο διασυνοριακό εμπόριο προϊόντων και υπηρεσιών με δυνατότητα τεχνητής νοημοσύνης.

Τέλος, μόλις στις 25 Νοεμβρίου 2022 το Συμβούλιο της ΕΕ ανακοίνωσε την «**Πρόταση – Κανονισμό του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση Εναρμονισμένων Κανόνων σχετικά με την Τεχνητή Νοημοσύνη (Πράξη για την Τεχνητή Νοημοσύνη) και για την Τροποποίηση Ορισμένων Νομοθετικών Πράξεων της Ένωσης – Γενική Προσέγγιση**»[200], στην οποία ακολουθείται μια προσέγγιση βάσει κινδύνου και θεσπίζεται ένα ενιαίο, οριζόντιο νομικό πλαίσιο για την ΤΝ, το οποίο αποσκοπεί να εξασφαλίσει ασφάλεια δικαίου. Προωθούνται οι επενδύσεις και η καινοτομία στην ΤΝ, ενισχύεται η διακυβέρνηση και η αποτελεσματική επιβολή της ισχύουσας νομοθεσίας για τα θεμελιώδη δικαιώματα και την ασφάλεια και

---

[198] Διαθέσιμο: https://eurlex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[199] «Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)» Διαθέσιμο: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[200] https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/el/pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

διευκολύνεται η ανάπτυξη ενιαίας αγοράς για τις εφαρμογές ΤΝ. Η πρόταση συνδέεται με άλλες πρωτοβουλίες, όπως το συντονισμένο σχέδιο για την τεχνητή νοημοσύνη το οποίο αποσκοπεί στην επιτάχυνση των επενδύσεων στην ΤΝ στην Ευρώπη[201].

6.2 Ο Νόμος 4577/2018 - ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Στις 3 Δεκεμβρίου 2018, δημοσιεύθηκε στο ΦΕΚ Α' 199/3-12-2018 ο Νόμος 4577/2018[202], με τις διατάξεις του οποίου ενσωματώνεται στην εθνική μας έννομη τάξη η **Οδηγία (ΕΕ) 2016/1148**[203] ("**NIS Directive**"). Με την εν λόγω Ευρωπαϊκή Οδηγία Ασφάλειας Δικτύου και Πληροφοριών (EU NIS Directive) της 6ης Ιουλίου 2016 (ΕΕ L 194) από την Ευρωπαϊκή Επιτροπή, θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών, ως μέρος της γενικότερης ευρωπαϊκής στρατηγικής για την κυβερνοασφάλεια. Είναι ο πρώτος κανονισμός κυβερνοασφάλειας σε ευρωπαϊκό επίπεδο και στόχο έχει την ενίσχυση της κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση.

Στα πλαίσια εφαρμογής των ανωτέρω, εκδόθηκε η υπ'αρ. 1027 Υπουργική Απόφαση, η οποία δημοσιεύτηκε στο ΦΕΚ Β' 3739/8-10-2019 με σκοπό τον καθορισμό των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών, της διαδικασίας παροχής πληροφοριών κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές, της μεθοδολογίας προσδιορισμού των Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) και της μεθοδολογίας αξιολόγησης και ελέγχου.

Για σκοπούς παρακολούθησης και εφαρμογής του νόμου ορίζεται η «Εθνική Αρχή Κυβερνοασφάλειας», ήτοι η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης (άρθρα 6 και 7), η οποία θα λειτουργεί και ως «Ενιαίο Κέντρο Επαφής»

---

[201] Μαμμόνας Δημοσθένης, «Πράξη για την τεχνητή νοημοσύνη: Το Συμβούλιο ζητεί την προώθηση ασφαλών συστημάτων ΤΝ που σέβονται τα θεμελιώδη δικαιώματα», Διαθέσιμο: https://www.consilium.europa.eu/el/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/ [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[202] Νόμος 4577/2018 Διαθέσιμο: https://www.kodiko.gr/nomothesia/document/474449/nomos-4577-2018 και Αιτιολογική έκθεση στο σχέδιο νόμου «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση» Διαθέσιμο: https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/e-endik-eis-olo.pdf [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

[203] Οδηγία 2016/1148/ΕΕ https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EN [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

(ΕΚΕ) για τη διευκόλυνση της διασυνοριακής συνεργασίας και θα έχει συντονιστικό ρόλο επί όλων των σχετικών θεμάτων.

Παράλληλα, στο άρθρο 8 ορίζεται και η Αρμόδια Ομάδα Απόκρισης σε Συμβάντα («Computer Security Incident Response Team — CSIRT» ή και «Computer Emergency Response Team - CERT»), η οποία και θα λαμβάνει άμεσα την κοινοποίησή τους, θα φροντίζει για την αντιμετώπισή τους και θα ενημερώνει σχετικά και όποτε απαιτείται το ΕΚΕ. Το ΕΚΕ υποβάλλει τακτική συνοπτική και ανωνυμοποιημένη (για λόγους επιχειρηματικού απορρήτου ή και προσωπικών δεδομένων) έκθεση, στο αρμόδιο ευρωπαϊκό όργανο («Ομάδα Συνεργασίας - Cooperation Group»), η οποία περιλαμβάνει στοιχεία για το πλήθος των παραβιάσεων, το είδος και τη σοβαρότητά τους.

Ο νόμος λειτουργεί συμπληρωματικά και επικουρικά σε ό,τι έχει ήδη ρυθμιστεί ειδικά ή τομεακά. Εντούτοις περιέχει διατάξεις σύμφωνα με τις οποίες, οργανισμοί σχετικοί με τους παρακάτω τομείς θα πρέπει να προχωρήσουν άμεσα σε πλάνο συμμόρφωσης με την Οδηγία και το εθνικό πλαίσιο εφαρμογής της: 1) Ενέργειας, 2) Πόσιμου νερού, 3) Μεταφορών, 4) Υγείας, 5) Τράπεζες, 6) Ψηφιακών Υποδομών.

Οι Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (ΦΕΒΥ) έχουν υποχρέωση:

- Να ορίσουν Υπεύθυνο Ασφαλείας Πληροφοριών και Δικτύων και να κοινοποιηθούν τα στοιχεία του στην Εθνική Αρχή Κυβερνοασφάλειας
- Να ορίσουν ενιαία πολιτική ασφαλείας
- Να συντάξουν εγχειρίδιο ασφάλειας πληροφοριών.
- Να πραγματοποιήσουν αποτίμηση κινδύνων
- Να συντάξουν αναφορά αυτοαξιολόγησης και να κοινοποιηθεί στην ΕΑΚ, εντός 6 μηνών από την ημερομηνία έκδοσης του Οδηγού Αυτοαξιολόγησης από την Εθνική Αρχή Κυβερνοασφάλειας
- Να κοινοποιούν σε ετήσια βάση τα αποτελέσματα αυτοαξιολόγησης στην Εθνική Αρχή Κυβερνοασφάλειας
- Να ακολουθήσουν κατάλληλα τα 3 στάδια εφαρμογής (Αναγνώριση – Προστασία – Αντιμετώπιση)
- Να επικαιροποιήσουν συμβάσεις με προμηθευτές (SLA)

6.3 Ο Νόμος 4961/2022

Υπό το πρίσμα των ανωτέρω διατάξεων και συμπληρωματικά στα προαναφερόμενα νομοθετήματα, μόλις στις 27 Ιουλίου 2022 δημοσιεύθηκε στο ΦΕΚ 146/Α/27-07-2022 ο Ν. 4961/2022 σχετικά με τις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, την ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.

Ο νέος νόμος, μεταξύ άλλων, θεσπίζει ένα συνεκτικό νομοθετικό πλαίσιο για την τεχνητή νοημοσύνη με ισχύ από 1.1.2023, αλλά και για το διαδίκτυο των πραγμάτων με ισχύ από 1.3.2023. Αντικείμενό του σύμφωνα με το άρθρο 2 του νόμου είναι «*η θέσπιση ρυθμίσεων για τη διαμόρφωση των κατάλληλων εγγυήσεων για τη διασφάλιση των δικαιωμάτων των φυσικών και των νομικών προσώπων και την ενίσχυση της λογοδοσίας και της διαφάνειας κατά τη χρήση συστημάτων τεχνητής νοημοσύνης και τη συμπλήρωση του υφιστάμενου θεσμικού πλαισίου για την κυβερνοασφάλεια*».

Παρακάτω ακολουθεί σύντομη επισκόπηση των ρυθμίσεων του νόμου που αφορούν το θέμα της παρούσας διπλωματικής εργασίας:

6.3.1 Οι ρυθμίσεις σχετικά με την τεχνητή νοημοσύνη

Σε αναμονή της υιοθέτησης της Πράξης για την Τεχνητή Νοημοσύνη από την ΕΕ, ο νέος αυτός νόμος εισάγει ένα εθνικό πλαίσιο για τη ρύθμιση της χρήσης τεχνολογιών ΤΝ στον δημόσιο και ιδιωτικό τομέα. Το εθνικό αυτό νομικό πλαίσιο προβλέπει τις ακόλουθες υποχρεώσεις ανά κατηγορία υπόχρεων φορέων:

- **Για τους φορείς του Δημοσίου Τομέα**:

- το άρθρο 4 παρ. 1 του νόμου ορίζει ότι, η χρήση συστημάτων ΤΝ για τη διαδικασία λήψης ή την υποστήριξη της διαδικασίας λήψης μιας απόφασης ή την έκδοση πράξης, οι οποίες επηρεάζουν τα δικαιώματα ενός φυσικού ή νομικού προσώπου, επιτρέπεται μόνο αν προβλέπεται ρητά σε ειδική διάταξη νόμου που περιλαμβάνει κατάλληλες εγγυήσεις για την προστασία των δικαιωμάτων αυτών.
- το άρθρο 5 του νόμου απαιτεί προ της έναρξης λειτουργίας συστήματος ΤΝ, πέρα από την εκτέλεση εκτίμησης αντικτύπου του άρθρου 35 του Γενικού Κανονισμού Προστασίας Δεδομένων GDPR 2016/679 και την εκπόνηση αλγοριθμικής εκτίμησης αντικτύπου για την αξιολόγηση των κινδύνων που ενδέχεται να προκύπτουν για τα δικαιώματα, τις ελευθερίες και τα έννομα συμφέροντα των προσώπων, που επηρεάζονται από το σύστημα αυτό.

- το άρθρο 6 προβλέπει την υποχρεωτική διαφάνεια λειτουργίας, όπου κάθε φορέας υποχρεούται να παρέχει δημόσια πληροφορίες, μεταξύ άλλων, για τον χρόνο έναρξης και τις παραμέτρους λειτουργίας του συστήματος ΤΝ καθώς και για τις αποφάσεις που λαμβάνονται ή υποστηρίζονται μέσω αυτού. Τυχόν καταγγελίες για παραβιάσεις των υποχρεώσεων διαφάνειας εξετάζονται από την Εθνική Αρχή Διαφάνειας.
- Το άρθρο 8 αναφέρει την υποχρέωση του φορέα στην τήρηση μητρώου συστημάτων ΤΝ που χρησιμοποιεί.

- **Για τους φορείς του Ιδιωτικού Τομέα:**

- Το άρθρο 9 του νόμου προβλέπει ότι πριν από την πρώτη χρήση συστήματος ΤΝ, που επηρεάζει τη διαδικασία λήψης αποφάσεων σχετικά με τους εργαζομένους ή τους υποψήφιους εργαζομένους και έχει αντίκτυπο στις συνθήκες εργασίας, την επιλογή, την πρόσληψη ή την αξιολόγησή τους, κάθε επιχείρηση οφείλει να παρέχει σχετική πληροφόρηση στον εργαζόμενο.

- Το άρθρο 10 παρ. 1 του νόμου ορίζει ότι κάθε μεσαία ή μεγάλη οντότητα του ιδιωτικού τομέα κατά την έννοια του άρθρου 2 του Ν. 4308/2014 τηρεί μητρώο των συστημάτων ΤΝ, που χρησιμοποιεί αλλά και να υιοθετεί πολιτική δεοντολογικής χρήσης δεδομένων, η οποία περιλαμβάνει πληροφορίες σχετικά με τα μέτρα, τις ενέργειες και τις διαδικασίες που εφαρμόζει σε θέματα δεοντολογίας δεδομένων κατά τη χρήση συστημάτων τεχνητής νοημοσύνης (α.10 παρ.2).

Με τον νέο Νόμο συστήνεται, αφενός, Συντονιστική Επιτροπή για την ΤΝ με αρμοδιότητες την κατάρτιση της Εθνικής Στρατηγικής για την ΤΝ και, γενικότερα, την χάραξη πολιτικής γύρω από την ΤΝ (άρθρο 12), και, αφετέρου, Επιτροπή για την εποπτεία της στρατηγικής, που μεριμνά για την υλοποίηση, τον συντονισμό των αρμοδίων φορέων και την μέριμνα για την εφαρμογή της (άρθρο 13). Για την επιτέλεση του έργου τους οι δύο επιτροπές τροφοδοτούνται με στοιχεία από το Παρατηρητήριο ΤΝ, που παρακολουθεί και αποτυπώνει σε εκθέσεις τις τεχνολογικές εξελίξεις και τις πολιτικές γύρω από την ΤΝ στην χώρα και σε διεθνές επίπεδο (άρθρο 14).

6.3.2 Οι ρυθμίσεις σχετικά με το Διαδίκτυο των Πραγμάτων

Σύμφωνα με το άρθρο 32 παρ. 1 του νόμου 4961/2022 θεσπίζεται υποχρέωση των κατασκευαστών, ώστε οι συσκευές τεχνολογίας ΔτΠ να σχεδιάζονται και αναπτύσσονται κατά τρόπο, ώστε να επιτυγχάνεται κατάλληλο επίπεδο κυβερνοασφάλειας καθ' όλη τη διάρκεια του κύκλου ζωής τους και να αποτρέπονται απόπειρες μη εξουσιοδοτημένων τρίτων να αλλοιώσουν τη χρήση ή τις επιδόσεις τους, ενώ υποχρεούνται να συνοδεύουν τέτοιες συσκευές με δήλωση συμμόρφωσης με τις τεχνικές προδιαγραφές ασφαλείας, που προβλέπονται στον νόμο, καθώς και οδηγίες χρήσης και πληροφορίες ασφάλειας (άρθρο 33).

Επίσης στην παράγραφο 2 του άρθρου 32 προβλέπεται η κατά περίπτωση, ενσωμάτωση μέτρων διασφάλισης κατάλληλου επιπέδου κυβερνοασφάλειας στις συσκευές τεχνολογίας ΔτΠ, όπως: α) η χρήση ασφαλών κωδικών πρόσβασης στις συσκευές τεχνολογίας ΔτΠ, β) η έγκαιρη ενημέρωση λογισμικού από αξιόπιστες πηγές, γ) η κρυπτογράφηση κατά τη μεταφορά κρίσιμων δεδομένων ασφαλείας, συμπεριλαμβανομένων των δεδομένων ελέγχου και διαχείρισης της απομακρυσμένης πρόσβασης, δ) ο προσδιορισμός από τον φορέα εκμετάλλευσης ΔτΠ ενός δημόσιου σημείου επαφής, στο οποίο μπορούν οι χρήστες να γνωστοποιούν περιστατικά ασφάλειας των συσκευών και ε) η πρόβλεψη πολιτικής ή διαδικασίας γνωστοποίησης περιστατικών ευπάθειας ή ασφάλειας.

Με το άρθρο 35 θεσπίζονται οι υποχρεώσεις των φορέων εκμετάλλευσης ΔτΠ σχετικά με τις τεχνικές προδιαγραφές ασφαλείας κάθε συσκευής και τον ορισμό Υπευθύνου Ασφαλείας ΔτΠ για την παρακολούθηση των μέτρων ασφαλείας των συσκευών τεχνολογίας ΔτΠ, που προβλέπονται στον νόμο.

Ανάμεσα στις λοιπές υποχρεώσεις των φορέων είναι η τήρηση μητρώου συσκευών τεχνολογίας ΔτΠ που χρησιμοποιεί ο φορέας, το οποίο επικαιροποιεί σε ετήσια βάση και, σε κάθε περίπτωση, όταν θέτει σε λειτουργία νέα συσκευή τεχνολογίας ΔτΠ (άρθρο 38), καθώς και η εκτίμηση αντικτύπου.

Εν κατακλείδι, λόγω του ότι η ΤΝ είναι ένας τεχνολογικός τομέας σε «νηπιακή ηλικία» (Fuller et al., 2020), καθότι μόλις τα τελευταία χρόνια αναπτύχθηκε και συνεχίζει να αναπτύσσεται με γοργό ρυθμό, δεν υπήρχε νομοθεσία ικανή να την πλαισιώσει. Η προσπάθεια της ΕΕ αλλά και της Ελλάδας να θέσουν ένα γενικό κανονιστικό πλαίσιο για τις νέες αναδυόμενες ψηφιακές τεχνολογίες, είναι ένα πρώτο βήμα, προκειμένου να μπορέσει απρόσκοπτα και η ίδια η ΤΝ να εξελιχθεί, αλλά πάντα έως το βαθμό που αυτή η

εξέλιξη δεν θα αποτελεί απειλή για τα θεμελιώδη δικαιώματα των ανθρώπων, καθώς και την ανθρωπότητα γενικότερα.

7 / Αντί επιλόγου

Το διαδίκτυο των πραγμάτων είναι πλέον πρωταγωνιστής στη ζωή των σύγχρονων ανθρώπων, ωστόσο η χρήση του και κατ' επέκταση η χρήση των διασυνδεδεμένων συσκευών εγκυμονεί πολλαπλούς κινδύνους για την ασφάλεια των προσωπικών δεδομένων και όχι μόνο. Η βασική προϋπόθεση για την ορθή χρήση και την επιτυχία του IoT είναι η σαφής και πλήρη ενημέρωσή των χρηστών για τους πιθανούς κινδύνους και η εφαρμογή μέτρων ασφαλείας, που συνδέονται αναπόφευκτα με την υποχρέωση των κατασκευαστών για την προστασία από το σχεδιασμό, καθώς και μεταξύ άλλων την τακτική ενημέρωση/αναβάθμιση των λογισμικών ασφαλείας των συσκευών.

Η τεχνητή νοημοσύνη αποτελεί τον κρίσιμο παράγοντα για να μπορούν οι συσκευές IoT να μάθουν από προηγούμενες αποφάσεις, να προβλέψουν μελλοντικές δραστηριότητες και να βελτιώνουν συνεχώς την απόδοση και τις δυνατότητες λήψης αποφάσεων σε πραγματικό χρόνο, χωρίς τις καθυστερήσεις και τη συμφόρηση που προκύπτουν από τις μεταφορές του τεράστιου όγκου δεδομένων. Πλέον συναντάμε τις εφαρμογές της παντού γύρω μας, είτε πρόκειται για την υγειονομική περίθαλψη, την κατασκευή, τη ρομποτική, τα αυτόνομα συστήματα, τις έξυπνες πόλεις κ.α.

Η σύγκλιση των ανωτέρω τεχνολογιών αναμφισβήτητα πια σηματοδοτεί μια νέα εποχή δυνατοτήτων σε όλους τους τομείς εφαρμογής της. Αφενός μεν διότι η τεχνητή νοημοσύνη ενισχύει το Διαδίκτυο των Πραγμάτων μέσω της έξυπνης λήψης αποφάσεων, αφετέρου διότι το Διαδίκτυο το Πραγμάτων με τη σειρά του, διευκολύνει την απόδοση και αυξάνει τις δυνατότητες της τεχνητής νοημοσύνης μέσω της ανταλλαγής δεδομένων που λαμβάνουν χώρα μεταξύ των διασυνδεδεμένων συσκευών σε πραγματικό χρόνο. Όλα τα ανωτέρω την καθιστούν μια στρατηγική τεχνολογία που θα ηγηθεί στο μέλλον, η ανάπτυξη της οποίας θεωρείται παγκοσμίως απαραίτητη για την ενίσχυση της εθνικής ανταγωνιστικότητας και την προστασία της εθνικής ασφάλειας.

Στα πλαίσια όμως της αδιάκοπης ανάπτυξης των τεχνολογιών IoT και AI αναδύονται με γοργό ρυθμό και αρκετά ζητήματα, μερικά εκ των οποίων παρουσιάστηκαν με την παρούσα εργασία, όπως της ασφάλειας συστημάτων, δεδομένων και δικτύων κ.α. Οι τεράστιες ποσότητες ψηφιακών δεδομένων που αντλεί η ΤΝ από το IoT, η αύξηση της

υπολογιστικής ισχύος και της αποθηκευτικής ικανότητας συντέλεσαν στην τωρινή εξέλιξή της. Η τάση «εμπορευματοποίησης» των προσωπικών δεδομένων που επικρατεί σήμερα για προσπορισμό κερδών ή για την πρόκληση ηθικής βλάβης του θύματος και τρίτων, είναι αποτέλεσμα και αιτία της διαρκώς ογκούμενης επεξεργασίας τους. Επιχειρήσεις στοχεύουν στην απόκτησή τους, ούτως ώστε με την κατάλληλη επεξεργασία να αποκομίσουν όσο το δυνατό μεγαλύτερο όφελος από αυτά, γεγονός που οδηγεί στην ανάγκη εξισορρόπησης των συμφερόντων των επιχειρήσεων και των υποκειμένων των δεδομένων.

Κατά την άποψη της γράφουσας, είναι υψίστης σημασίας η εκτίμηση των ηθικών επιπτώσεων που επιφέρει η ανάπτυξη και εφαρμογή της τεχνολογίας της ΤΝ. Και αυτό διότι τα συστήματα ΤΝ, όπως προναφέρθηκε, χρησιμοποιούνται όλο και πιο πολύ σε επιχειρήσεις, στην υγειονομική περίθαλψη αλλά και σε άλλους τομείς, έχοντας έτσι τη δυνατότητα άμεσου αντικτύπου στις ανθρώπινες ζωές. Ως εκ τούτου, είναι σημαντικό να διασφαλιστεί ότι τα εν λόγω συστήματα κατασκευάζονται με πρωτόκολλα ασφαλείας για την προστασία των χρηστών από πιθανή κακή χρήση ή βλάβη. Επιπλέον κρίνεται απαραίτητο να δημιουργηθούν διαφανείς πολιτικές που να καθορίζουν σαφείς κατευθυντήριες γραμμές για τη συλλογή και επεξεργασία δεδομένων από συστήματα ΤΝ. Μόνο εάν ληφθούν υπόψιν τα εν λόγω ηθικά ζητήματα, θα διασφαλιστεί ότι η τεχνολογία της ΤΝ αναπτύσσεται υπεύθυνα και χωρίς να διακυβεύεται το απόρρητο και η ασφάλεια των χρηστών.

Εντούτοις, το νομοθετικό πλαίσιο που υπάρχει σήμερα για να αντιμετωπίσει τις προκλήσεις που συνοδεύουν τις τεχνολογίες AI και IoT, είτε αυτές έχουν να κάνουν με την παραβίαση της ιδιωτικότητας, του απορρήτου και των δεδομένων, είτε με την αδιαφάνεια και την ασφάλεια γενικότερα, είναι ακόμα στα θεμέλια. Ο ΓΚΠΔ όπως είδαμε, έδωσε τις βάσεις για στηριχθούν τα επόμενα νομοθετήματα που θα εφαρμοστούν είτε σε εθνικό είτε σε ευρωπαϊκό επίπεδο, θεσπίζοντας τις βασικές αρχές και σκοπούς για το σύννομο της επεξεργασίας τους και λειτουργώντας κατ' αυτό τον τρόπο ως μηχανισμός εξισορρόπησης. Στο έργο αυτό βοήθησαν πολύ οι Γνωμοδοτήσεις της Ομάδας Εργασίας του άρθρου 29, οι οποίες εξειδίκευσαν κατά περίπτωση τα ζητήματα που άπτονται της ασφάλειας των δεδομένων, των συσκευών κ..α. στο οικοσύστημα των AI και IoT. Μάλιστα μία από τις μεγαλύτερες προκλήσεις που πρέπει να αντιμετωπιστούν, είναι το γεγονός ότι, ενώ ο ΓΚΠΔ θέτει περιορισμούς στην επεξεργασία προσωπικών δεδομένων, η ΤΝ για να λειτουργήσει, απαιτεί μεγάλες ποσότητες δεδομένων για ακριβή και αξιόπιστα

αποτελέσματα. Ωστόσο το πεδίο ρύθμισης AI και IoT είναι απροσδιόριστο, διότι η συνεχώς μεταβαλλόμενη και εξελισσόμενη ΤΝ δημιουργεί όλο και περισσότερα ζητήματα που θα πρέπει να ρυθμιστούν.

Σε εθνικό επίπεδο ήδη παρατηρούμε την ενσωμάτωση των σχετικών ρυθμίσεων και Οδηγιών σε επιμέρους νομοθετήματα, όπως στο Ν. 4577/2018 για την Κυβερνοασφάλεια, ο οποίος εξειδικεύθηκε με την υπ'αρ. 1027/8-10-2019 Υπουργική Απόφαση. Με τις σχετικές διατάξεις δίδεται προτεραιότητα στην ασφάλεια συστημάτων και υπηρεσιών δικτύων, υπηρεσιών δηλαδή που διαδραματίζουν σημαντικό ρόλο στην κοινωνία, καθώς μέσω των κυβερνοεπιθέσεων δεν θίγεται μόνο ο δημόσιος και ο ιδιωτικός τομέας, διαταράσσεται η εύρυθμη λειτουργία της οικονομίας και θίγεται ο πυρήνας της κοινωνικής ζωής. Τα ανωτέρω συμπληρώνει ο Ν. 4961/2022 σχετικά με τις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ο οποίος καθορίζει ποια είναι τα μέτρα διασφάλισης κατάλληλου επιπέδου κυβερνοασφάλειας στις IoT συσκευές και προβλέπει υποχρεώσεις και περιορισμούς των δημόσιων και ιδιωτικών φορέων αναφορικά με τη χρήση της ΤΝ.

Έτσι, παρά το γεγονός ότι καταβάλλεται σημαντική προσπάθεια θεσμοθέτησης κανόνων γύρω από αυτά, πάντοτε θα προκύπτει και κάτι νέο που δεν είχε προβλεφθεί στις αρχικές ρυθμίσεις, είτε γιατί δεν υπάρχει κατά τη στιγμή της ψήφισης ενός νόμου, είτε γιατί προέκυψε αργότερα από την ικανότητα της ΤΝ να μιμείται την ανθρώπινη ευφυία. Προς το σκοπό αυτό κρίνεται απαραίτητη η τροποποίηση/μεταρρύθμιση των σχετικών νομοθετημάτων ανά τακτά χρονικά διαστήματα για να συμβαδίζει με τον γρήγορο ρυθμό της τεχνολογικής προόδου, έτσι ώστε να εξασφαλίζεται η όσο το δυνατόν μεγαλύτερη ασφάλεια και εμπιστοσύνη γύρω από αυτές τις τεχνολογίες του μέλλοντος και ταυτόχρονα η ελαχιστοποίηση των κινδύνων τους (πχ. παραβίαση), στο οποίο θα βοηθήσουν επίσης οι συχνές ενημερώσεις των λογισμικών των συστημάτων ΤΝ.

Βιβλιογραφία - [τελευταία ανάκτηση 15 Ιανουαρίου 2023]

Α.1 Ξένη ηλεκτρονική και έντυπη

- **Acemoglu, Daron, and Pascual Restrepo**. 2018. «*Artificial intelligence, automation, and work*». In *The Economics of Artificial Intelligence: An Agenda*. Edited by Ajay Agrawal, Joshua Gans and Avi Goldfarb. Chicago: University of Chicago Press, pp. 197–236. Διαθέσιμο: https://www.nber.org/system/files/chapters/c14027/c14027.pdf
- **Aizenberg, E., & van den Hoven, J**. (2020). «*Designing for human rights in AI.»* Big Data & Society, *7*(2). https://doi.org/10.1177/2053951720949566 Διαθέσιμο: https://journals.sagepub.com/doi/10.1177/2053951720949566
- **Al-Shargabi, Bassam & Abuarqoub, Simak**. (2020). «*IoT-Enabled Healthcare: Benefits, Issues and Challenges», 10.1145/3440749.3442596.* Διαθέσιμο: https://www.researchgate.net/publication/351391253_IoT-Enabled_Healthcare_Benefits_Issues_and_Challenges
- **Assael, Y., Sommerschield, T., Shillingford, B. et al.,** «*Restoring and attributing ancient texts using deep neural networks*», (2022). Διαθέσιμο: https://doi.org/10.1038/s41586-022-04448-z
- **Ashton Kevin**, «*That 'Internet of Things' Thing*» 2009, Διαθέσιμο: http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf
- **Babu, P. & Bhaskari, Lalitha & CH.Satyanarayana,.** (2011). «*A Comprehensive Analysis of Spoofing». 10.14569/IJACSA.2010.010623.* Διαθέσιμο: https://www.researchgate.net/publication/49597043_A_Comprehensive_Analysis_of_Spoofing
- **Bastos, Daniel & Giubilo, Fabio & Shackleton, Mark & El-Mousa, Fadi**. (2018). «*GDPR Privacy Implications for the Internet of Things».* Διαθέσιμο: https://www.researchgate.net/publication/331991225_GDPR_Privacy_Implications_for_the_Internet_of_Things
- **Bisio, Igor & Garibotto, Chiara & Haleem, Halar & Lavagetto, Fabio & Sciarrone, Andrea.** (2022). *«A Systematic Review of Drone Based Road Traffic Monitoring System*», IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3207282.

Διαθέσιμο:https://www.researchgate.net/publication/363627429_A_Systematic_Review_of_Drone_Based_Road_Traffic_Monitoring_System

- **Boucher, Philip & Bentley, Peter**. «*Should we fear artificial intelligence? – In depth analysis*», European Parliament, European Parliamentary research service, STOA, March 2018, σελ. 5-6 Διαθέσιμο: https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/614547/EPRS_IDA%282018%29614547_EN.pdf
- **Chehri A., G. Jeon, F. Rivest and H. T. Mouftah,** "*Evolution and Trends in Artificial Intelligence of Things Security: When Good Enough is Not Good Enough!*," 2022, doi: 10.1109/IOTM.001.2100130. διαθέσιμο: https://ieeexplore.ieee.org/document/9945852
- **CHETAN SHARMA**, *«CORRECTING THE IOT HISTORY», 2016, http://www.chetansharma.com/correcting-the-iot-history/*
- **Chodorek, Agnieszka, Robert Ryszard Chodorek, and Alexander Yastrebov**. 2022. «*The Prototype Monitoring System for Pollution Sensing and Online Visualization with the Use of a UAV and a WebRTC-Based Platform*», Sensors (Basel). 2022 Feb 17;22(4):1578. doi: 10.3390/s22041578. PMID: 35214478; PMCID: PMC8877218. Διαθέσιμο: https://pubmed.ncbi.nlm.nih.gov/35214478/
- **Crevier, Daniel** (1993). «*AI: The Tumultuous History of the Search for Artificial Intelligence*», σελ. 100-144 Διαθέσιμο online: https://www.researchgate.net/publication/233820788_AI_The_Tumultuous_History_of_the_Search_for_Artificial_Intelligence
- **Davenport, T. & Ronanki, R**. (2018). «*Artificial Intelligence for the real world. Harvard Business Review»* Διαθέσιμο: https://www.bizjournals.com/boston/news/2018/01/09/hbr-artificial-intelligence-for-the-real-world.html
- **Dilmaghani S., M. R. Brust, G. Danoy, N. Cassagnes, J. Pecero and P. Bouvry**, «*Privacy and Security of Big Data in AI Systems: A Research and Standards Perspective*,» *2019 IEEE International Conference on Big Data (Big Data)*, Los Angeles, CA, USA, 2019, pp. 5737-5743, doi:10.1109/BigData47090.2019.9006283, Διαθέσιμο: https://ieeexplore.ieee.org/document/9006283

- **Dressel J, Farid H**. «*The accuracy, fairness, and limits of predicting recidivism*», 2018, Science Advances, Vol 4, Issue 1, DOI: 10.1126/sciadv.aao5580, Διαθέσιμο: https://www.science.org/doi/10.1126/sciadv.aao5580
- **Dugan Steven** - UNESCO, «*Ai in Education, Change at the speed of learning*», Διαθέσιμο:https://iite.unesco.org/wp-content/uploads/2020/11/Steven_Duggan_AI-in-Education_2020.pdf
- **Durand-Richard, MJ.** (2022). «*Boole's Symbolized Laws of Thought Facing Empiricism*». In: Béziau, JY., Desclés, JP., Moktefi, A., Pascu, A.C. (eds) Logic in Question. Studies in Universal Logic. Birkhäuser, Cham. https://doi.org/10.1007/978-3-030-94452-0_6 Διαθέσιμο: https://link.springer.com/chapter/10.1007/978-3-030-94452-0_6
- **Evans, Dave**, 2011, «The Internet of Things How the Next Evolution of the Internet Is Changing Everything», Cisco white paper, Διαθέσιμο: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
- **Fuller A., Z. Fan, C. Day and C. Barlow**, «*Digital Twin: Enabling Technologies, Challenges and Open Research*», 2020, doi: 10.1109/ACCESS.2020.2998358. Διαθέσιμο: https://ieeexplore.ieee.org/document/9103025
- **Geest, Maarten & Tekinerdogan, Bedir & Catal, Cagatay**. (2021). «*Smart Warehouses: Rationale, Challenges and Solution Directions*», Applied Sciences. 12. 219. 10.3390/app12010219. Διαθέσιμο: https://www.researchgate.net/publication/357372387_Smart_Warehouses_Rationale_Challenges_and_Solution_Directions
- **Gherhes, Vasile**. (2018). «*Why Are We Afraid of Artificial Intelligence (Ai)?. European Review Of Applied Sociology*», European Review Of Applied Sociology. 11. 6-15. 10.1515/eras-2018-0006. Διαθέσιμο: https://www.researchgate.net/publication/330678764_Why_Are_We_Afraid_of_Artificial_Intelligence_Ai
- **Ghosh, A., Chakraborty, D. and Law, A.** (2018), *«Artificial intelligence in Internet of things*». CAAI Trans. Intell. Technol., 3: 208-218. https://doi.org/10.1049/trit.2018.1008 Διαθέσιμο: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/trit.2018.1008

- **Goundar, Sam & Bhardwaj, Akashdeep & Nur, Safiya & Kumar, Shonal & Harish, Rajneet.** (2021). «*Industrial Internet of Things: Benefit, Applications, and Challenges*», Industrial Internet of Things: Benefit, Applications, and Challenges. 10.4018/978-1-7998-3375-8.ch010. Διαθέσιμο: https://www.researchgate.net/publication/348132641_Industrial_Internet_of_Things_Benefit_Applications_and_Challenges
- **Jackson, Brandon W.,** «*Cybersecurity, Privacy, and Artificial Intelligence: An Examination of Legal Issues Surrounding the European Union General Data Protection Regulation and Autonomous Network Defense»* 21 MINN. J.L. SCI. & TECH. 169 (2019). Available at: https://scholarship.law.umn.edu/mjlst/vol21/iss1/6
- **Jackson Philip,** *Introduction to Artificial Intelligence: Third Edition*, 2019
- **Jiang, Y., Li, X., Luo, H. *et al***. «*Quo vadis artificial intelligence*?». *Discov Artif Intell* **2**, 4 (2022). https://doi.org/10.1007/s44163-022-00022-8
- **Kavounides Chryssos, Markos Giakoumelos, Evdokia Kaffe**, «*Harnessing the Power of AI in Greece. Embarking on the path to value*» Διαθέσιμο: https://web-assets.bcg.com/93/be/5ac6b7ff4d698947da09681332db/harnessing-the-power-web-final.pdf
- **Khalid Elgazzar et al**., *«Revisiting the internet of things: New trends, opportunities and grand challenges*», 2022 | https://doi.org/10.3389/friot.2022.1073780, Διαθέσιμο: https://www.frontiersin.org/articles/10.3389/friot.2022.1073780/full?&utm_source=Email_to_authors_&utm_medium=Email&utm_content=T1_11.5e1_author&utm_campaign=Email_publication&field=&journalName=Frontiers_in_the_Internet_of_Things&id=1073780
- **Khayyam, Hamid & Javadi, Bahman & Jalili, Mahdi & Jazar, Reza**. (2020). «*Artificial Intelligence and Internet of Things for Autonomous Vehicles*». 10.1007/978-3-030-18963-1_2. Διαθέσιμο: https://www.researchgate.net/publication/335021813_Artificial_Intelligence_and_Internet_of_Things_for_Autonomous_Vehicles
- **Kim, H.** (2022). «*Historical Sketch of Artificial Intelligence. In: Artificial Intelligence for 6G».* Springer, Cham., pp 3–14 https://doi.org/10.1007/978-3-030-95041-5_1

- **Kotha, Harika & Gupta, V..** (2018). «*IoT Application, A Survey*», International Journal of Engineering & Technology. 7. 891. 10.14419/ijet.v7i2.7.11089. Διαθέσιμο: https://www.researchgate.net/publication/325116647_IoT_Application_A_Survey
- **Kott, Alexander & Swami, Ananthram & West, Bruce.** (2016). «*The Internet of Battle Things*», Computer. 49. 70-75. 10.1109/MC.2016.355. Διαθέσιμο: https://www.researchgate.net/publication/311215660_The_Internet_of_Battle_Things
- **Kuzlu, M., Fair, C. & Guler, O.** «*Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity*», (2021). Discov Internet Things 1, 7 (2021). https://doi.org/10.1007/s43926-020-00001-4 Διαθέσιμο: https://link.springer.com/article/10.1007/s43926-020-00001-4
- **Lindsay RK, Buchanan BG, Feigenbaum EA, Lederberg J.** «*DENDRAL: a case study of the first expert system for scientific hypothesis formation*». Artif Intell. 1993;61(2):209–61. Διαθέσιμο: https://www.sciencedirect.com/science/article/abs/pii/000437029390068M
- **Look, Brandon C.,** «*Gottfried Wilhelm Leibniz", The Stanford Encyclopedia of Philosophy»* (Spring 2020 Edition), Edward N. Zalta (ed.), Διαθέσιμο: https://plato.stanford.edu/archives/spr2020/entries/leibniz/
- **Lu Y. and L. D. Xu,** *«Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics*» 2019, doi: 10.1109/JIOT.2018.2869847. Διαθέσιμο: https://ieeexplore.ieee.org/abstract/document/8462745 [τελευταία ανάκτηση 15 Ιανουαρίου 2023]
- **Marr, Bernard.** «*Understanding the 4 types of Artificial Intelligence*» Διαθέσιμο: https://bernardmarr.com/understanding-the-4-types-of-artificial-intelligence/
- **Mashrur Chowdhury, Adel W. Sadek** «*Advantages and Limitations of Artificial Intelligence*», CIRCULAR [online] Νοέμβριος 2012, διαθέσιμο: https://onlinepubs.trb.org/onlinepubs/circulars/ec168.pdf
- **Mattern F. and C. Floerkemeier**, «*From the Internet of Computers to the Internet of Things*» In: Sachs, K., Petrov, I., Guerrero, P. (eds) From Active Data Management to Event-Based Systems and More. Lecture Notes in Computer Science, vol 6462. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-

642-17226-7_15 Διαθέσιμο: https://link.springer.com/chapter/10.1007/978-3-642-17226-7_15

- **Memos V. A., G. Minopoulos, C. Stergiou, K. E. Psannis, Y. Ishibashi**, «*A Revolutionary Interactive Smart Classroom (RISC) with the Use of Emerging Technologies*» in Proceedings of 2nd International Conference on Computer Communication and the Internet (ICCCI 2020), 26-28 June 2020, Nagoya Institute of Technology, Japan. DOI: 10.1109/ICCCI49374.2020.9145987, Διαθέσιμο: https://www.researchgate.net/publication/339933375_A_Revolutionary_Interactive_Smart_Classroom_RISC_with_the_Use_of_Emerging_Technologies
- **Minopoulos GM, Memos VA, Stergiou CL, Stergiou KD, Plageras AP, Koidou MP, Psannis KE.** «*Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System*». *Applied Sciences*. 2022; 12(12):5859. https://doi.org/10.3390/app12125859 Διαθέσιμο: https://www.mdpi.com/2076-3417/12/12/5859
- **Mitrou, Lilian, «***Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?»* SSRN Electronic Journal. 10.2139/ssrn.3386914**.** 2018
- **McCarthy, J.** *"What is AI? / Basic Questions, Professor John McCarthy / Stanford».* Διαθέσιμο: http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html.
- **Mcclure, S., Scambray, J. & Kurtz, G.** «*Ασφάλεια Δικτύων*.», 2009
- **McCulloch, W.S., Pitts, W.** «*A logical calculus of the ideas immanent in nervous activity*», Bulletin of Mathematical Biophysics 5, 115–133 (1943), Διαθέσιμο: https://link.springer.com/article/10.1007/BF02478259
- **Naik Nithesh, et.al**, «*Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility*?», 2022 Διαθέσιμο: https://www.frontiersin.org/articles/10.3389/fsurg.2022.862322
- **Navid Ali Khan, N.Z. Jhanjhi, Sarfraz Nawaz Brohi, Raja Sher Afgun Usmani, Anand Nayyar**, «*Smart traffic monitoring system using Unmanned Aerial Vehicles (UAVs* Computer Communications, Volume 157, 2020, Pages 434-443, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2020.04.049. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S0140366420300189

- **Neelam Tyagi,** «*6 Major Branches of Artificial Intelligence (AI)»,* Διαθέσιμο: https://www.analyticssteps.com/blogs/6-major-branches-artificial-intelligence-ai
- **Nižetić S, Šolić P, López-de-Ipiña González-de-Artaza D, Patrono L.** «*Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future*.» doi: 10.1016/j.jclepro.2020.122877, 2020 Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S095965262032922X?via%3Dihub
- **Olinder, Nina, Konstantin Fedyakin, Elena Korneeva** «*Personal Data Protection in the Internet of Things », 10.2991/aebmr.k.210318.037.* Διαθέσιμο: https://www.researchgate.net/publication/350375595_Personal_Data_Protection_in_the_Internet_of_Things
- **Papatsimouli Maria, Lazaros Lazaridis, Dimitris Ziouzios, Minas Dasygenis, George Fragulis** « *Internet Of Things (IoT) awareness in Greece*», SHS Web Conf., 139 (2022) 03013 DOI: https://doi.org/10.1051/shsconf/202213903013 Διαθέσιμο: https://www.shs-conferences.org/articles/shsconf/abs/2022/09/shsconf_etltc2022_03013/shsconf_etltc2022_03013.html
- **Pradhan, Bikash & Bhattacharyya, Saugat & Pal, Kunal.** (2021). «*IoT-Based Applications in Healthcare Devices.»*, Journal of Healthcare Engineering. 2021. 1-18. 10.1155/2021/6632599. διαθέσιμο: https://www.researchgate.net/publication/350206154_IoT-Based_Applications_in_Healthcare_Devices
- **Raji, R.S.** (1994). *"Smart networks for control*, IEEE Spectrum, volume 31, pp 49-55 Διαθέσιμο: *https://www.semanticscholar.org/paper/Smart-networks-for-control-Raji/f7b3654bc95a8a4c490d9d41c1ec63cf4cb37730*
- **Räz, T.** «*COMPAS: zu einer wegweisenden Debatte über algorithmische Risikobeurteilung.*» *Forens Psychiatr Psychol Kriminol* **16**, 300–306 (2022). https://doi.org/10.1007/s11757-022-00741-9 Διαθέσιμο: https://link.springer.com/article/10.1007/s11757-022-00741-9
- **Roberts, H., Cowls, J., Morley, J. *et al***. «*The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*». *AI & Soc* **36**, 59–77 (2021). https://doi.org/10.1007/s00146-020-00992-2 Διαθέσιμο: https://link.springer.com/article/10.1007/s00146-020-00992-2

- **Rodrigues Rowena** *«Legal and human rights issues of AI: Gaps, challenges and vulnerabilities.» Journal of Responsible Technology. 4. 100005. 10.1016/j.jrt.2020.100005.* Διαθέσιμο: https://www.researchgate.net/publication/346305027_Legal_and_human_rights_issues_of_AI_Gaps_challenges_and_vulnerabilities
- **Russell, Stuart J .; Norvig, Peter** (2010), «*Artificial Intelligence: A Modern Approach»* (3rd Edition), σελ 21-22. Διαθέσιμο online: http://repo.darmajaya.ac.id/3800/1/Artificial%20Intelligence%20A%20Modern%20Approach%20%283rd%20Edition%29.pdf%20%28%20PDFDrive%20%29.pdf
- **Sai dyuti Vaishnavi Vaddiparthi**, «*ADVANTAGES OF AI IN THE MODERN WORLD*», 5. 95-98. (2021), διαθέσιμο: https://www.researchgate.net/publication/348687836_ADVANTAGES_OF_AI_IN_THE_MODERN_WORLD
- **Sindermann, C., Sha, P., Zhou, M. *et al.*** «*Assessing the Attitude Towards Artificial Intelligence: Introduction of a Short Measure in German, Chinese, and English Language*», *Künstl Intell* **35**, 109–118 (2021). https://doi.org/10.1007/s13218-020-00689-0 Διαθέσιμο:
- **Stahl, Bernd.** (2021). «*Ethical Issues of AI*», Διαθέσιμο: https://www.researchgate.net/publication/350145020_Ethical_Issues_of_AI
- **Stergiou, C., Psannis, K. E., Kim, B.-G. & Gupta, B**., 2016 «*Secure integration of IoT and Cloud Computing»,* Διαθέσιμο: https://ruomo.lib.uom.gr/bitstream/7000/79/1/1-s2.0-S0167739X1630694X-main%281%29.pdf
- **Stergiou, K.D., G. M. Minopoulos, V. A. Memos, C. L. Stergiou, M. P. Koidou, K. E. Psannis**, «*A Machine Learning-based Model for Epidemic Forecasting and Faster Drug Discovery»*, MDPI, Applied Sciences, vol. 12, issue: 21, October 2022. [DOI: 10.3390/app122110766] Διαθέσιμο: https://www.mdpi.com/2076-3417/12/21/10766
- **Stergiou C. L., E. Bompoli, K. E. Psannis,** «*Security & privacy issues in IoT-based Big Data Cloud systems in a Digital Twin scenario*», MDPI, Applied Sciences, vol. 13, issue: 2, January 2023. [DOI: 10.3390/app13020758] Διαθέσιμο: https://www.mdpi.com/2076-3417/13/2/758

- **Schmidt, J. et al.** «*Recent advances and applications of machine learning in solid-state materials science*», *npj Comput Mater* **5**, 83 (2019). https://doi:10.1038/s41524-019-0221-0, 2019
- **Simon, Herbert** (1965), «*The Shape of Automation for Men and Management*»
- **Srinivasan, C.R. & Bodduna, Rajesh & Saikalyan, P. & Premsagar, K. & Yadav, Eadala Sarath**. (2019). «*A review on the different types of internet of things (IoT)», Journal of Advanced Research in Dynamical and Control Systems. 11. 154-158.* Διαθέσιμο: https://www.researchgate.net/publication/332153657_A_review_on_the_different_types_of_internet_of_things_IoT
- **Sriranga Narasimha Gandhi Aryavalli, Hemantha Kumar, «***Top 12 layer-wise security challenges and a secure architectural solution for Internet of Things*», Computers and Electrical Engineering, Volume 105, 2023, 108487, ISSN 0045-7906, https://doi.org/10.1016/j.compeleceng.2022.108487. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S0045790622007029
- **Tanha Talaviya, Dhara Shah, Nivedita Patel, Hiteshri Yagnik, Manan Shah**, «*Implementation of artificial intelligence in agriculture for optimisation of irrigation and application of pesticides and herbicides*», Artificial Intelligence in Agriculture, Volume 4, 2020, Pages 58-73, ISSN 2589-7217, https://doi.org/10.1016/j.aiia.2020.04.002. Διαθέσιμο: https://www.sciencedirect.com/science/article/pii/S258972172030012X
- **Thiel, C**. (2022). «*Gottlob Frege: Die Abstraktion*». In *Fregeana*. Leiden, The Netherlands: Brill | mentis. doi: https://doi.org/10.30965/9783969752654_009 Διαθέσιμο: https://brill.com/edcollchap/book/9783969752654/BP000009.xml
- **Tillman, Maggie.** «*Amazon Go and Amazon Fresh: How the 'Just walk out' tech work*» Διαθέσιμο: https://www.pocket-lint.com/gadgets/news/amazon/139650-what-is-amazon-go-where-is-it-and-how-does-it-work/
- **Tripathi, Nikhil & Mehtre, Babu.** (2013). «*DoS and DDoS Attacks: Impact, Analysis and Countermeasures», 1-6.* Διαθέσιμο: https://www.researchgate.net/publication/259941506_DoS_and_DDoS_Attacks_Impact_Analysis_and_Countermeasures

- **Tsantikidou K. and N. Sklavos**, "*Flexible Security and Privacy, System Architecture for IoT, in Healthcare*," *2022 IFIP/IEEE 30th International Conference on Very Large Scale Integration (VLSI-SoC)*, Patras, Greece, 2022, pp. 1-6, doi: 10.1109/VLSI-SoC54400.2022.9939659. Διαθέσιμο: https://ieeexplore.ieee.org/document/9939659
- **Tsantikidou K. and N. Sklavos**, "*Vulnerabilities of Internet of Things, for Healthcare Devices and Applications*," *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, Hanoi, Vietnam, 2021, pp. 498-503, doi: 10.1109/NICS54270.2021.9701497.Διαθέσιμο: https://ieeexplore.ieee.org/document/9701497
- **Verdouw, Cor & Wolfert, Sjaak & Tekinerdogan, Bedir**. (2016). «*Internet of Things in agriculture*», CAB Reviews. 11. 1-12. 10.1079/PAVSNNR201611035. Διαθέσιμο: https://www.researchgate.net/publication/312164156_Internet_of_Things_in_agriculture
- **Wang C. -X., M. D. Renzo, S. Stanczak, S. Wang and E. G. Larsson**, *«Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges»,* 2020, doi: 10.1109/MWC.001.1900292. Διαθέσιμο: https://ieeexplore.ieee.org/abstract/document/9023918
- **Weiser, Mark** (1991). *«The Computer for the 21st Century»*, Διαθέσιμο: https://web.archive.org/web/20150311220327/http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf
- **William Stallings,** «*Cryptography and Network Security Principles and Practice*», 6 th edition, Chapter 21-24
- **Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi**, 2014, «*Internet of Things for Smart Cities*», in *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328. Διαθέσιμο: https://ieeexplore.ieee.org/document/6740844
- **Zhang, Jianfeng & Hua, Xian-Sheng & Huang, Jianqiang & Shen, Xu & Chen, Jingyuan & Zhou, Qin & Fu, Zhihang & Zhao, Yiru**. (2019). «*The City Brain: Practice of Large-Scale Artificial Intelligence in the Real World. IET Smart Cities»*. IET Smart Cities. 1. 10.1049/iet-smc.2019.0034. Διαθέσιμο:

https://www.researchgate.net/publication/333456538_The_City_Brain_Practice_of_Large-Scale_Artificial_Intelligence_in_the_Real_World

Α.2 Ελληνική ηλεκτρονική και έντυπη

- **Αλεξανδροπούλου - Αιγυπτιάδου Ευγενία**, «*Προσωπικά Δεδομένα*», Εκδόσεις Νομική Βιβλιοθήκη, Θεσσαλονίκη, 2016
- **Βόρρας Α.,Μήτρου Λ.,** «*Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679*», ΔικΜΕΕ, τ.4, 2018
- **Γεωργούλη Κ.** *«Τεχνητή Νοημοσύνη – Μια εισαγωγική προσέγγιση»* 2015
- **Γριβοκωστόπουλος Ιωάννης,** «*Κριτική ανάλυση του Ν. 4624/2019*», Επιθεώρηση Δικαίου Πληροφορικής Τ.1 (2021), Διαθέσιμο: https://ejournals.lib.auth.gr/infolawj/
- **Ζέκος Γ.,** «*Διαδίκτυο & τεχνητή νοημοσύνη στο Ελληνικό δίκαιο*», 2022
- **Ιγγλεζάκης Δ. Ιωάννης**, «*Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679)*», εκδ. Interactive Books, (γ΄ εκδ.) 2020
- **Καρκατζούνης Β.,** «*Οι νέες διατάξεις για την προστασία προσωπικών δεδομένων των εργαζομένων (Νόμος 4624/2019*)» Διαθέσιμο: https://www.lawspot.gr/nomika-blogs/vasilis_karkatzoynis/oi-nees-diataxeis-gia-tin-prostasia-prosopikon-dedomenon-ton#footnote2_zk8oftb
- **Καρύδα Σπυριδούλα**, «*ΓΚΠΔ και ν. 4624/2019. Μία ιστορική μεταρρύθμιση του εθνικού νομοθετικού πλαισίου για την προστασία του θεμελιώδους δικαιώματος της προστασίας των δεδομένων προσωπικού χαρακτήρα του ατόμου. Νέες προκλήσεις στη σύγχρονη ψηφιακή εποχή. Διάλογος μεταξύ ενωσιακού και εθνικού νομοθέτη*»
- **Κιρίκος Ε.** «Γενική Τεχνητή Νοημοσύνη, Τι είναι», Διαθέσιμο: https://www.athinodromio.gr/γενική-τεχνητή-νοημοσύνη-τι-είναι/
- **Μαμμόνας Δημοσθένης**, «*Πράξη για την τεχνητή νοημοσύνη: Το Συμβούλιο ζητεί την προώθηση ασφαλών συστημάτων ΤΝ που σέβονται τα θεμελιώδη δικαιώματα*», Διαθέσιμο**:** https://www.consilium.europa.eu/el/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/

- **Μήτρου Λίλιαν**, «*Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων. Νέο δίκαιο – νέες υποχρεώσεις – νέα δικαιώματα*», εκδ. Σάκκουλα, 2017
- **Μπακόλας Ευάγγελος**, «*Η τεχνητή νοημοσύνη για το κοινό καλό: Τάσεις-Προκλήσεις-Προοπτικές»,* 2018
- **Μπούσγου Βασιλική**, «*Η τεχνητή νοημοσύνη ως κινητήριος δύναμη της σύγχρονης ευρωπαϊκής ψηφιακής αγοράς προσωπικών δεδομένων : προκλήσεις στην εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) με έμφαση στην προστασία των προσωπικών δεδομένων των καταναλωτών*», 2022
- **Μυλώση, Μ.:** *«Τα 'έξυπνα γυαλιά' στην εποχή της επαυξημένης πραγματικότητας. Προστατεύοντας τα προσωπικά δεδομένα ως 'κόρην οφθαλμού'»*. International Conference «NEW TECHNOLOGIES IN HEALTH: MEDICAL, LEGAL AND ETHICAL ISSUES", Θεσσαλονίκη 20-21 Νοεμβρίου 2019, Εργαστήριο μελέτης ιατρικού δικαίου και βιοηθικής, ΑΠΘ, ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ (2021) σελ. 255-265
- **Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπη**, *«Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων»* 2018, Διαθέσιμο online: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
- **Παναγοπούλου-Κουτνατζή Φερενίκη**, «Προσωπικά Δεδομένα», 2016
- **Παναγοπούλου-Κουτνατζή Φερενίκη**, «*Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση, Μελέτες, Απόψεις*», ΕφημΔΔ-1/2017
- **Παναγοπούλου-Κουτνατζή Φερενίκη,** «*Νόμος 4624/2019 και Εφαρμογή GDPR: Πολλά υποσχόμενος, αλλά παράλληλα καθυστερημένος*» Διαθέσιμο: https://www.syntagmawatch.gr/trending-issues/nomos-4624-2019-kai-efarmogi-gdpr-polla-yposchomenos-alla-parallila-kathysterimenos/
- **Πράσσος Παναγιώτης**, «*Κυβερνοασφάλεια και συστήματα τεχνητής νοημοσύνης*», 2022
- **Σπυρόπουλος Φώτιος**, *«Χωρίς δικαίωμα πρόσβασης σε ηλεκτρονικά δεδομένα (hacking): ποινική και εγκληματολογική προσέγγιση: αξιολόγηση της ελληνικής ποινικής νομοθεσίας: έρευνα σε δείγμα νομικών, επιστημόνων πληροφορικής και hackers», 2015*

- **Τζιούφα Παρασκευή, «***INTERNET OF THINGS-RFID και προσωπικά δεδομένα: θέματα ασφάλειας και απορρήτου στο διαδίκτυο των πραγμάτων (IoT)»,* 2019
- **Τσουραμάνης, Χ.**, «*Ψηφιακή Εγκληματικότητα. Η α(να)σφαλής όψη του διαδικτύου».* 2005
- **Χατζηβασιλείου Χρυσή**, «*Προσωπικά δεδομένα, Τεχνητή Νοημοσύνη, Υπολογιστική Νέφους και Διαδίκτυο των πραγμάτων στον τομέα της υγείας*», 2020

Α.2.1 Ανέκδοτες Πηγές (Εργασίες / Διατριβές)

- **Γαλάνη Ελένη, Ζιώγου Αφροδίτη** «*Διαδίκτυο των πραγμάτων (IoT) και προσωπικά δεδομένα*», Φεβρουάριος 2021
- **Ζιώγου Αφροδίτη**, «*Οι συμπεριφορές πρόσβασης σε συστήματα πληροφοριών ή δεδομένα και προγράμματα χωρίς δικαίωμα. Η παράνομη διείσδυση σε δεδομένα (hacking). Οι διατάξεις των άρθρων 370Β και 370Γ του ΠΚ για την παραβίαση απορρήτων*», Φεβρουάριος 2021

Α.3 Ιστοσελίδες

- https://www.theatlantic.com/technology/archive/2017/03/aristotle-computer/518697/
- http://users.sch.gr/jenyk/index.php/robotics/robotics-historicalreview/37-talos
- http://www.mikrosapoplous.gr/iliada/BIBLIO_18_323_467.htm
- http://www.alanturing.net/turing_archive/pages/Reference%20Articles/The%20Turing-Church%20Thesis.html
- https://www.turing.org.uk/scrapbook/test.html
- https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341
- https://www.oed.com/viewdictionaryentry/Entry/271625
- https://www.britannica.com/technology/artificial-intelligence
- https://commission.europa.eu/system/files/2020-03/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf
- https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=716dee29233e
- https://www.javatpoint.com/types-of-artificial-intelligence

- https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/
- https://ithaca.deepmind.com/
- https://www.ibm.com/topics/artificial-intelligence-medicine
- https://www.turing.com/kb/an-introduction-to-naive-bayes-algorithm-for-beginners
- https://news.tulane.edu/pr/tulane-university-study-uses-artificial-intelligence-detect-colorectal-cancer
- https://www.maastrichtuniversity.nl/news/world%E2%80%99s-first-super-microsurgery-operation-%E2%80%98robot-hands%E2%80%99
- https://www.maastrichtuniversity.nl/news/artificial-intelligence-chooses-best-treatment-option-breast-cancer
- http://caressesrobot.org/en/project/
- www.myhealthavatar.eu
- https://orelit.com/benefits-of-artificial-intelligence-in-automotive-industry/
- https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai
- https://openai.com/
- https://www.aldebaran.com/en/pepper
- https://www.hansonrobotics.com/sophia/
- https://www.engineeredarts.co.uk/robot/ameca/
- https://www.bbc.com/news/technology-63100636
- https://www.africa.com/africas-first-humanoid-robot-omeife-unveiled-at-gitex/
- https://www.javatpoint.com/advantages-and-disadvantages-of-artificial-intelligence
- https://www.photo.gr/blogs/eidiki-nomothesia-apo-evropaiki-enosi-gia-tin-techniti-noimosyni/
- https://www.iefimerida.gr/kosmos/deepfakes-psifiako-mellon-paraplirofor isis
- https://www.procon.org/headlines/artificial-intelligence-ai-top-3-pros-and-cons/
- https://focusbari.gr/wp-content/uploads/2022/02/GREEKS-AND-ARTIFICIAL-INTELLIGENCE_EN.pdf
- http://fi.china-embassy.gov.cn/eng/kxjs/201710/P020210628714286134479.pdf

- https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
- https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5
- https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
- https://www.oracle.com/internet-of-things/what-is-iot/
- https://aws.amazon.com/what-is/iot/?nc1=h_ls
- https://www.statista.com/statistics/1194709/iot-revenue-worldwide/
- https://www.cloudcredential.org/blog/knowledge-byte-the-different-types-of-iot/
- https://syntegra.net/internet-of-things-the-five-types-of-iot/
- https://www.jardcs.org/abstract.php?id=20
- https://www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf
- https://about.meta.com/metaverse/#smart-glasses
- https://neuralink.com/approach/
- https://www.aboutamazon.com/news/transportation/amazon-prime-air-prepares-for-drone-deliveries
- https://arstechnica.com/gadgets/2022/12/amazon-begins-drone-deliveries-in-california-and-texas/
- https://www.dailymail.co.uk/sciencetech/article-11453187/US-Army-tests-DRONES-deliver-blood-medical-supplies-dangerous-battlefield-situations.html
- https://www.smartfarmsensing.com/
- https://www.precedenceresearch.com/iot-in-agriculture-market
- https://www.geeksforgeeks.org/advantages-and-disadvantages-of-iot/
- https://www.linkedin.com/pulse/advantages-disadvantages-internet-things-iot-tommy-quek
- https://techvidvan.com/tutorials/advantages-and-disadvantages-of-iot/
- https://www.onstar.com/
- https://rm.coe.int/16806ebe7a
- https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf
- https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/magazine/internet-threats

- https://light-it.net/blog/9-prominent-benefits-of-iot-for-business/
- https://usa.kaspersky.com/resource-center/threats/spyware
- https://www.kaspersky.com/resource-center/definitions/keylogger
- https://cyberalert.gr/ransomware/
- https://www.kaspersky.com/resource-center/definitions/dns
- https://www.kaspersky.com/resource-center/threats/ip-spoofing
- https://www.gartner.com/en/newsroom/press-releases/2018-12-06-gartner-data-shows-87-percent-of-organizations-have-low-bi-and-analytics-maturity
- https://www.hitechnectar.com/blogs/future-of-aiot-technologies/
- https://www.deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40
- https://web-assets.bcg.com/93/be/5ac6b7ff4d698947da09681332db/harnessing-the-power-web-final.pdf
- https://www.isalos.net/2022/07/psifiaka-didyma-digital-twins-sti-naftilia/?fbclid=IwAR0ZivXtIS1OtlS0JKphBFohQuQb2tZHgv1BAaeVWk_T2EavqXPx9hZBjOc
- https://www.bostondynamics.com/about
- https://www.ft.com/content/e548deac-856a-11e6-8897-2359a58ac7a5
- https://www.echr.coe.int/documents/convention_ell.pdf
- https://www.europarl.europa.eu/charter/pdf/text_el.pdf
- https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=LEGISSUM:ai0033
- https://eur-lex.europa.eu/EL/legal-content/summary/treaty-on-the-functioning-of-the-european-union.html
- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf
- https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/uclalr66&section=6
- https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32018R1725
- https://ec.europa.eu/commission/presscorner/detail/EL/INF_19_4251
- https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/ODHGIA.pdf

- https://www.e-nomothesia.gr/kat-dedomena-prosopikou-kharaktera/nomos-4624-2019-phek-137a-29-8-2019.html
- https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=164
- https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168093b26e
- https://bioethics.gr/api/files/download/2198/UNESCO_Declaration_on_human_genome.pdf?attachment=false
- https://ec.europa.eu/newsroom/article29/items/623051
- https://www.dpa.gr/sites/default/files/2020-05/26_2019anonym.pdf
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010
- https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_el.pdf
- https://www.europarl.europa.eu/doceo/document/JURI-PR-582443_EN.pdf
- https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0051&rid=9
- https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=COM%3A2018%3A237%3AFIN
- https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance
- https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligencefeb2020_el_1.pdf
- https://eur-lex.europa.eu/legal-content/EL/TXT/?qid=1593079180383&uri=CELEX%3A52020DC0064
- https://eurlex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0009.02/DOC_1&format=PDF
- https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf
- https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/el/pdf
- https://www.kodiko.gr/nomothesia/document/474449/nomos-4577-2018

- https://www.hellenicparliament.gr/UserFiles/2f026f42-950c-4efc-b950-340c4fb76a24/e-endik-eis-olo.pdf
- https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L1148&from=EN
- https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf
- https://www.europarl.europa.eu/news/en/press-room/20170210IPR61808/robots-and-artificial-intelligence-meps-call-for-eu-wide-liability-rules