ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2023-2024

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Άντζελας Ράσα (Α.Μ.: 2238)

«ΠΑΡΑΓΩΓΙΚΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ / ΓΛΩΣΣΙΚΑ ΜΟΝΤΕΛΑ (ChatGPT κ.α.) ΚΑΙ ΠΡΟΣΤΑΣΤΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»

«GENERATIVE AI / LANGUAGE MODELS (ChatGPT etc.) AND DATA PROTECTION»

<u>Επιβλέπουσα:</u>

κ. Λίλιαν Μήτρου

Πειραιάς, Ιανουάριος 2024

Περιεχόμενα

Συντομογραφίες

ΤΝ: Τεχνητή Νοημοσύνη

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

AI: Artificial Intelligence

LLM: Large Language Model

κ.α.: και άλλα

κ.λπ.: και λοιπά

αρθρ.: άρθρο

Ε.Ε.: Ευρωπαϊκή Ένωση

π.χ.: παραδείγματος χάρη

σελ.: σελίδα

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Περίληψη

Το παρόν πόνημα έχει ως στόχο να εξετάσει την ιδιάζουσα σχέση μεταξύ των σύγχρονων τεχνολογιών τεχνητής νοημοσύνης, όπως είναι η παραγωγική τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα και της προστασίας προσωπικών δεδομένων. Αν και η παραγωγική τεχνητή νοημοσύνη έχει φέρει σημαντικές καινοτομίες και διευκολύνσεις στην ανθρώπινη επικοινωνία και τις επιχειρηματικές πρακτικές, η εκτενής χρήση δεδομένων, μεταξύ των οποίων και προσωπικών δεδομένων, εγείρει σημαντικά νομικά και ηθικά ζητήματα σχετικά με τη συμμόρφωση με το ισχύον νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων και τους ηθικούς κανόνες της κοινωνίας.

Η διπλωματική εργασία εκκινεί με μια ιστορική αναδρομή της εμφάνισης της τεχνητής νοημοσύνης, μια προσπάθεια ορισμού της έννοιας της τεχνητής νοημοσύνης και μια ανάλυση των τεχνικών και προσεγγίσεων της τεχνητής νοημοσύνης. Αναγκαιότητα για την κατανόηση της παραγωγικής τεχνητής νοημοσύνης δεν αποτελεί μόνο η προγενέστερη κατανόηση της παραδοσιακής τεχνητής νοημοσύνης αλλά και η κατανόηση των δεδομένων μεγάλης κλίμακας (Big Data). Ακολούθως, εξετάζεται η παραγωγική τεχνητή νοημοσύνη μέσω της δομής και του τρόπου λειτουργίας των μεγάλων γλωσσικών μοντέλων, όπως το ChatGPT. Στο δεύτερο κεφάλαιο της παρούσας, εξετάζεται το νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων και συγκεκριμένα ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) και η εφαρμογή του στα γλωσσικά μοντέλα. Παρατίθενται τα συγκρουσιακά του σημεία σε σχέση με την πρακτική λειτουργία των μεγάλων γλωσσικών μοντέλων και προτείνονται σχετικοί τρόποι συμμόρφωσης της τεχνητής νοημοσύνης με το ισχύον νομοθετικό πλαίσιο πλαίσιο. Στη συνέχεια, αναφέρεται το νομοθετικό πλαίσιο για την τεχνητή νοημοσύνη με έμφαση στο νέο Κανονισμό για τη ρύθμιση της τεχνητής νοημοσύνης (AI ACT) και της σχέσης του με τον ΓΚΠΔ. Τέλος, μνημονεύονται και τα ηθικά ζητήματα χρήσης της τεχνητής νοημοσύνης αλλά και κάποιες αποφάσεις ορόσημο του ΔΕΕ, οι οποίες ελλείψει νομολογίας για την παραγωγική τεχνητή νοημοσύνη, τυγχάνουν αναλογικής εφαρμογής.

Λέξεις – Κλειδιά: Παραγωγική Τεχνητή Νοημοσύνη, Μεγάλα Γλωσσικά Μοντέλα, Προσωπικά Δεδομένα, Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ), Κανονισμός για τη ρύθμιση της τεχνητής νοημοσύνης (AI ACT)

Abstract

This paper aims to examine the peculiar relationship between modern artificial intelligence technologies (AI), such as generative AI and large language models, and privacy protection. While generative AI has introduced significant innovations and conveniences in human communication and business practices, its extensive use of data, including personal data, raises important legal and ethical issues concerning compliance with existing data protection laws and societal ethical standards.

The thesis starts with a historical overview of the development of AI, an attempt to define the concept of AI and an analysis of AI techniques and approaches. A necessity for understanding productive AI is not only the prior understanding of traditional AI but also the understanding of Big Data. Next, productive AI is examined through the structure and mode of operation of big language models such as ChatGPT. In the second chapter of this paper, the legal framework for data protection, specifically the General Data Protection Regulation (GDPR) and its application to language models is discussed. Its conflicts with respect to the practical operation of large language models are listed and relevant ways for AI to comply with the current legislative framework are suggested. Then, the legislative framework for AI is mentioned, with emphasis on newly published AI ACT and its relation to the GDPR. Finally, the ethical issues of the use of AI are mentioned, as well as some landmark decisions of the Court of Justice of the European Union (CJEU), which, in the absence of case law on productive AI, which can be applied analogously to generative AI.

Key words: Generative AI, Large Language Models, Personal Data, Big Data, General Data Protection Regulation, AI ACT

Εισαγωγή

Πριν από μερικές δεκαετίες όταν ο Alan Turing μας μιλούσε για την τεχνητή νοημοσύνη και για την ευφυΐα των μηχανών φαινόταν να αναφέρεται σε ένα ουτοπικό όραμα χωρίς εφαρμογή. Σήμερα, η ραγδαία εξέλιξη της τεχνολογίας έχει μεταμορφώσει τον σύγχρονο κόσμο και οι «έξυπνες μηχανές» φαίνεται να έχουν εισχωρήσει στην καθημερινή ζωή, προκαλώντας ανησυχία για το εάν έχουν εισχωρήσει σε υπέρμετρο βαθμό. Εύλογα παρατηρώντας κανείς την κυριαρχία της τεχνητής νοημοσύνης αναρωτιέται εάν θα μπορέσει άραγε η μηχανή να αντικαταστήσει εξ ολοκλήρου τον άνθρωπο κατά τέτοιον τρόπο ώστε να μην είναι πλέον απαραίτητη ούτε η συμβολή του;

Τα τελευταία χρόνια έκανε την εμφάνιση της η παραγωγική τεχνητή νοημοσύνη μέσω των μεγάλων γλωσσικών μοντέλων (“Large Language Models”) που έχουν την δυνατότητα να επεξεργάζονται δεδομένα και κείμενα σε φυσική γλώσσα και να εξαγάγουν δεδομένα ομοίως σε φυσική γλώσσα. Το χαρακτηριστικότερο παράδειγμα από αυτά τα μοντέλα είναι το δημοφιλές ChatGPT που παράγει κείμενο βάσει των ερεθισμάτων (ερωτήσεων) που λαμβάνει από τον χρήστη και φαίνεται πως μπορεί να αντικαταστήσει τον άνθρωπο και να γίνει συνομιλητής του χρήστη με απόλυτα φυσικό τρόπο. Το ChatGPT έχει γίνει συχνό θέμα έρευνας και συζήτησης του επιστημονικού κόσμου τόσο για τον πρωτότυπο τρόπο ανάπτυξης και λειτουργίας του όσο και για τις προκλήσεις που θέτει στην σφαίρα του ιδιωτικού βίου και της προστασίας των προσωπικών δεδομένων. Η τεχνητή νοημοσύνη αποτελεί μέρος της 4ης βιομηχανικής επανάστασης και η ειδοποιός διαφορά που παρουσιάζει η σύγχρονη τεχνητή νοημοσύνη σε σχέση με το παρελθόν είναι η δυνατότητα της να αξιοποιεί έναν τεράστιο όγκο δεδομένων, μεταξύ αυτών και προσωπικά δεδομένα, αποσκοπώντας στην αδιάλειπτη εκπαίδευση και βελτίωση τους και την εξαγωγή όλο και καλύτερων αποτελεσμάτων από άποψη γνώσεων και αξιοπιστίας.

Αδιαμφισβήτητα τα πλεονεκτήματά της τεχνολογικής εξέλιξης και δη της τεχνητής νοημοσύνης στις εφαρμογές της είναι πολλά και σημαντικά συμβάλλοντας θετικά στην οικονομία, τις κοινωνικές σχέσεις, την εκπαίδευση, την υγεία κ.α., όμως, όπως κάθε νόμισμα έχει δύο πλευρές έτσι και η τεχνητή νοημοσύνη μας φέρνει αντιμέτωπους τόσο με κινδύνους που δύνανται να βάλλουν τα θεμελιώδη ανθρώπινα δικαιώματα όσο και με ηθικά

διλήμματα. Αξίζει μόνο να σημειωθεί ότι Stephen Hawking έχει υπάρξει από τους πιο σκληρούς επικριτές της προσπάθειας για ανάπτυξη συστημάτων τεχνητής νοημοσύνης κατανοώντας τα τεράστια πλεονεκτήματα που μπορούν να φέρουν επισημαίνοντας όμως και τους κινδύνους όπως την πιθανότητα η τεχνητή νοημοσύνη να αναπτύξει ακόμη και δική της βούληση που θα έρχεται σε αντίθεση με την ανθρώπινη βούληση που την έθεσε σε λειτουργία. Παραταύτα ο ίδιος ο Stephen Hawking χρησιμοποιούσε τεχνητή νοημοσύνη για να μπορέσει να επικοινωνήσει. Ένας ακόμη επικριτής της Τεχνητής Νοημόσυνης είναι ο Elon Musk, ο οποίος προειδοποιεί ότι η τεχνητή νοημοσύνη μπορεί να αποτελέσει «βασικό κίνδυνο για την ύπαρξη του ανθρώπινου πολιτισμού» και θεωρεί ότι η τεχνητή νοημοσύνη θα είναι πιθανότατα η αιτία του Τρίτου Παγκοσμίου Πολέμου. Ο ίδιος, όμως, ο Elon Musk δημιούργησε την xAI μια εταιρεία Τεχνητής Νοημοσύνης (C. Daffy, 2024), η οποία πρόσφατα κυκλοφόρησε μια εφαρμογή παραγωγικής τεχνητής νοημοσύνης και συγκεκριμένα ένα chatbox για την δημιουργία εικόνων βασισμένων σε κείμενο που μπορούν να δημοσιεύονται στο μέσο κοινωνικής δικτύωσης X του Elon Musk.

Τα νέα γλωσσικά μοντέλα παραγωγικής τεχνητής νοημοσύνης εγείρουν έντονους προβληματισμούς για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, κυρίως λόγω των μεγάλων δεδομένων που χρειάζονται για να εκπαιδευτούν και της αδιαφάνειας που τα χαρακτηρίζει ως προς τον μετέπειτα τρόπο λειτουργίας τους. Τα παραπάνω οδηγούν σε σύγκρουση του ChatGPT και άλλων παρόμοιων μοντέλων με τις διατάξεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων που θεσπίστηκε το 2018 στην Ευρωπαϊκή Ένωση με στόχο την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Η Ευρωπαϊκή Ένωση επιλέγει να μην παραμένει αμμέτοχη ενώπιον της ραγδαίας τεχνολογικής εξέλιξης που παρακολουθεί, αντιθέτως καταβάλει συνεχείς αξιόλογες προσπάθειες δημιουργίας ενός περιβάλλοντος αξιοπιστίας, φιλικού προς την ανάπτυξη της καινοτομίας και παράλληλα ασφαλούς για την προστασία των θεμελιωδών ανθρωπίνων δικαιωμάτων. Για την επίτευξη των παραπάνω προέβη αρχικά στην δημιουργία μη δεσμευτικών κειμένων που παρουσίαζαν το όραμα μιας ασφαλούς τεχνητής νοημοσύνης,

όπως οι κατευθυντήριες γραμμές δεοντολογίας και η Λευκή Βίβλος. Έπειτα έθεσε σε εφαρμογή τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων επιδιώκοντας την ενιαία προστασία των προσωπικών δεδομένων στον χώρο της ένωσης και τέλος δημοσίευσε πρόσφατα, μετά από μακροχρόνιες διαβουλεύσεις, τον Κανονισμό για την θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη θέτοντας ως στόχο την δημιουργία ενός περιβάλλοντος αξιοπιστίας και επενδύσεων για την τεχνητή νοημοσύνη. Η ΕΕ καθίσταται πρωτοπόρος στην ρύθμιση των τεχνολογιών και θέση σε προτεραιότητα του κοινωνικού συνόλου.

Η παρούσα εργασία πραγματεύεται την σχέση της παραγωγικής τεχνητής νοημοσύνης και των μεγάλων γλωσσικών μοντέλων, όπως το Chat GPT, με το νομοθετικό πλαίσιο περί προστασίας των προσωπικών δεδομένων του ανθρώπου. Μέσα από μια ιστορική αναδρομή της τεχνητής νοημοσύνης θα γίνει κατανοητή η προέλευση και η εξέλιξη της ανά τα χρόνια. Ακολούθως, θα πραγματοποιηθεί μια ανάλυση της έννοιας της τεχνητής νοημοσύνης με ρητή αναφορά στα είδη και τις τεχνικές προσεγγίσεις που χρησιμοποιεί, οδηγούμενοι στο κύριο ζήτημα της παρούσας, την παραγωγική τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα που έχουν προσελκύσει ιδιαίτερο ενδιαφέρον με τις δυνατότητες τους. Με σκοπό να καταστεί κατανοητό τι ακριβώς είναι η τεχνητή νοημοσύνη και πως είναι χρήσιμη, θα αναφέρουμε παραδείγματα καθημερινών εφαρμογών της σε ποικίλους τομείς. Το ευρωπαϊκό νομοθετικό πλαίσιο τόσο για την τεχνική νοημοσύνη όσο και για την προστασία των προσωπικών δεδομένων αλλά και η γενικότερη προσπάθεια που καταβάλει η ένωση τα τελευταία χρόνια για την θεσμοθέτηση κανόνων γύρω από την εξέλιξη της τεχνολογίας, θα αποτελέσει αντικείμενο της παρούσας. Οι ιδιότητες των γλωσσικών μοντέλων παραγωγικής τεχνητής νοημοσύνης θα εξεταστούν υπό το πρίσμα του ΓΚΠΔ και θα παρατεθούν οι συγκρούσεις που αναδύονται μέσα από την σχέση τους, εξετάζοντας μάλιστα και συγκεκριμένα παραδείγματα της ενωσιακής νομολογίας που εξετάζεται η παραβίαση των θεμελιωδών ανθρωπίνων δικαιωμάτων από την τεχνητή νοημοσύνη. Τέλος, θα προταθούν τρόποι αντιμετώπισης των εν λόγω συγκρούσεων και μετριασμού των κινδύνων που προκύπτουν μέσα από την χρήση των μεγάλων γλωσσικών μοντέλων (π.χ. ChatGPT).

Η τάχιστη εξέλιξη της τεχνολογίας είναι γεγονός και η εμφάνιση καινοτομιών όπως τα μεγάλα γλωσσικά μοντέλα τεχνητής νοημοσύνης αναπόφευκτη. Το ερώτημα που τίθεται είναι σε τι κίνδυνο θέτουν αυτές οι τεχνολογίες τα θεμελιώδη ανθρώπινα δικαιώματα, όπως η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, και με ποιον τρόπο μπορούν να αντιμετωπιστούν; Είναι το ισχύον νομοθετικό πλαίσιο επαρκές ή απαιτείται η υιοθέτηση νέων ρυθμίσεων, ίσως στοχευμένων στην παραγωγική τεχνητή νοημοσύνη;

1. Γενικά περί Τεχνητής Νοημοσύνης

1.1. Ιστορική Αναδρομή

Αναζητώντας τις απαρχές της Τεχνητής Νοημοσύνης θα μπορούσε κανείς να οδηγηθεί στην Αριστοτέλεια συλλογιστική, ήτοι στους συλλογισμούς του Αριστοτέλη που παρείχαν πρότυπα εκφράσεων και έδιναν σωστά συμπεράσματα προερχόμενα από σωστές υποθέσεις. Τα πρώτα σημάδια δημιουργίας μηχανών – συστημάτων τεχνητής νοημοσύνης λέγεται πως συναντώνται στην αρχαία Ελλάδα˙ ειδικότερα, χαρακτηριστικό παράδειγμα των πρώτων μηχανών αποτελεί ο μηχανισμός των αντικυθήρων, γνωστός και ως ο πρώτος αναλογικός υπολογιστής με σκοπό την πρόβλεψη αστρονομικών θέσεων και εκλείψεων.

Η τεχνητή νοημοσύνη εμφανίσθηκε για πρώτη φορά ως όρος το 1950 από τον λεγόμενο πατέρα της, τον Allan Turing, με την δημοσίευση του άρθρου του "Computing Machinery and Intelligence", μέσα από το οποίο εισήγαγε μια διαδικασία που φιλοδοξούσε να εξακριβώσει, εάν μία μηχανή διαθέτει ευφυΐα, το γνωστό ως Turing Test. Συγκεκριμένα, εάν μια μηχανή κατάφερνε να ξεγελάσει τον άνθρωπο παριστάνοντας και η ίδια τον άνθρωπο, τότε θα λαμβάνεται ως δεδομένο ότι είναι εξίσου έξυπνη με αυτόν (Λ. Μήτρου, Α. Βόρρας, 2018).

Λίγα χρόνια αργότερα, ο John McCarthy ορίζει την τεχνητή νοημοσύνη ως την επιστήμη και τη μηχανική της κατασκευής ευφυών μηχανών (C. Stryker, E. Kavlakoglu, 2024). Έπειτα, ακολούθησαν οι αλγόριθμοι, οποίοι αρχικά αποσκοπούσαν στην λήψη απλών αποφάσεων, όμως, εξελίχθηκαν σε αλγόριθμους ικανούς να μιμηθούν την ανθρώπινη συλλογιστική ακολουθώντας συγκεκριμένα μοτίβα. Κατά την δεκαετία του 1990, λόγω της αύξησης διαθεσιμότητας των ψηφιακών δεδομένων και της προόδου της υπολογιστικής ισχύος, επικράτησε η μηχανική εκμάθηση και εμφανίσθηκαν τα «νευρωνικά δίκτυα» για την

μίμηση πολυπλοκότερων μοτίβων με καλύτερη απόδοση και προσαρμοστικότητα (prefer.gr, 20.08.2023), ενώ το τελευταίο στάδιο εξέλιξης που παρατηρείται να κυριαρχεί είναι οι αλγόριθμοι βαθιάς εκμάθησης, οι οποίοι είναι και αυτοί που χρησιμοποιούνται σε όλες τις εφαρμογές παραγωγικής τεχνητής νοημοσύνης (Christofer Rigano, 2018).

Η τάχιστη εξέλιξη της τεχνητής νοημοσύνης από τις αρχές της εμφάνισης της έως και σήμερα έχει φέρει την επανάσταση και έχει εισχωρήσει με μη αναστρέψιμο τρόπο στην οικονομία, την κοινωνία, την πολιτική καθώς και στην καθημερινότητα του μέσου ανθρώπου φέροντας μαζί με τα πλεονεκτήματα και τα αντίστοιχα διλήμματα, όπως θα συζητηθούν στη συνέχεια της παρούσας.

1.2. Έννοια Τεχνητής Νοημοσύνης

Παρά την ευρεία χρήση και κυριαρχία της τεχνητής νοημοσύνης στη σύγχρονη εποχή, λόγω της ρευστότητας της έννοιας της υπάρχει δυσκολία εύρεσης ενός ενιαίου καθολικού στενού ορισμού που να υιοθετείται από το σύνολο του επιστημονικού κόσμου. Όπως και ο ίδιος ο όρος προδίδει, τεχνητή νοημοσύνη είναι η νοημοσύνη που επιτυγχάνεται με τεχνικά μέσα. Με άλλα λόγια, πρόκειται για τη δυνατότητα πραγματοποίησης εργασιών που κάνουν οι άνθρωποι με τεχνικά μέσα από υπολογιστές, οι οποίοι «μαθαίνοντας» μέσω δεδομένων, αποκτούν νοημοσύνη (Λ. Κανέλλος, 2021) (M. Negnevitsky, 2020). Η δυσκολία ορισμού οφείλεται κατά κύριο λόγο στον όρο της νοημοσύνης, ο οποίος μέχρι την ανάδυση των σχετικών τεχνολογιών συνδεόταν αποκλειστικά με τον ανθρώπινο νου. Ο προβληματισμός του τι ακριβώς αποτελεί νοημοσύνη έχει απασχολήσει ιδιαίτερα τόσο φιλόσοφους όσο και επιστήμονες και συνεχίζει να προβληματίζει, καθώς φαίνεται να μην μπορεί να αποτυπωθεί με σαφήνεια η λειτουργία της νοημοσύνης.

Η τεχνητή νοημοσύνη είναι ένα σύνολο τεχνολογιών που μπορεί να αποφέρει ευρείας κλίμακας οικονομικά και κοινωνικά οφέλη σε όλο το φάσμα των κλάδων και των κοινωνικών δραστηριοτήτων (Μ. Δεληγιάννη, 2021). Η ανυπαρξία ενός και μοναδικού ορισμού προκύπτει και από τις διαβουλεύσεις για την οριστικοποίηση του περιεχομένου του Κανονισμού σχετικά με την ρύθμιση της τεχνητής νοημοσύνης, κατά την διάρκεια των οποίων τα ενδιαφερόμενα μέρη ζήτησαν ένα στενό, σαφή και ακριβή ορισμό της.

Η επικρατέστερη εννοιολογική προσέγγιση της τεχνητής νοημοσύνης έως σήμερα είναι αυτή των Barr και Feigenbaum, σύμφωνα με την οποία «*η Τεχνητή Νοημοσύνη αποτελεί τομέα της επιστήμης των υπολογιστών, που αποσκοπεί στη σχεδίαση και υλοποίηση προγραμμάτων, τα οποία είναι ικανά να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες, εμφανίζοντας έτσι χαρακτηριστικά που αποδίδουμε συνήθως σε ανθρώπινη συμπεριφορά, όπως η επίλυση προβλημάτων, η αντίληψη μέσω της όρασης, η μάθηση, η εξαγωγή συμπερασμάτων, η κατανόηση φυσικής γλώσσας κ.λπ.*» (A. Barr, E. Feigenbaum, 1981) (Α. Βόρρας, Λ. Μήτρου, 2018). Ο Marvin Minsky προσπάθησε να ορίσει την τεχνητή νοημοσύνη με έναν απλούστερο και περιεκτικό τρόπο ως την τεχνολογία που επιτρέπει στους υπολογιστές να κάνουν πράγματα τα οποία απαιτούν νοημοσύνη όταν γίνονται από ανθρώπους. Με τον ορισμό του M. Minsky, όμως, είναι αδύνατον να γίνει πλήρως αντιληπτή η πολυπλοκότητα της τεχνητής νοημοσύνης, η οποία είναι μεν μια τεχνολογία, της οποίας τα τεχνικά χαρακτηριστικά την κάνουν να διαφέρει ουσιωδώς από τις παραδοσιακές τεχνολογίες και να παρουσιάζει ιδιαίτερο ενδιαφέρον (C. Lexcellent, 2019).

Ένας λεπτομερέστερος ορισμός δόθηκε από την Ομάδα Εμπειρογνωμόνων Υψηλού Επιπέδου για την Τεχνητή Νοημοσύνη (AI HLEG, 2019), που συστάθηκε από την Επιτροπή της ΕΕ, σύμφωνα με τον οποία «*τα συστήματα τεχνητής νοημοσύνης είναι συστήματα λογισμικού (ή ενδεχομένως και υλισμικού) σχεδιασμένα από ανθρώπους που, βάσει ενός δεδομένου σύνθετου στόχου, ενεργούν στην υλική ή ψηφιακή διάσταση με το να αντιλαμβάνονται το περιβάλλον τους μέσω της απόκτησης δεδομένων, να ερμηνεύουν τα δομημένα ή αδόμητα δεδομένα που έχουν συλλεχθεί, να προβαίνουν σε συλλογισμούς με βάση τις γνώσεις ή να επεξεργάζονται τις πληροφορίες, που εξάγονται από αυτά τα δεδομένα, και να αποφασίζουν ποια είναι η βέλτιστη ενέργεια (ή οι βέλτιστες ενέργειες) που θα πρέπει να εκτελέσουν για να επιτύχουν τον δεδομένο στόχο. Τα συστήματα ΤΝ μπορεί είτε να χρησιμοποιούν συμβολικούς κανόνες είτε να μαθαίνουν ένα αριθμητικό μοντέλο, και μπορεί επίσης να προσαρμόζουν τη συμπεριφορά τους με το να αναλύουν πώς επηρεάζεται το περιβάλλον από τις προηγούμενες ενέργειές τους*».

Ενδιαφέρον παρουσιάζει η δημόσια κατανόηση της τεχνητής νοημοσύνης που παρέχει η Wikipedia και την οποία επισήμαναν στο έγγραφό τους σχετικά με την τεχνητή νοημοσύνη,

τη ρομποτική, την ιδιωτική ζωή και την προστασία των δεδομένων οι Επίτροποι Προστασίας Δεδομένων και Προστασίας Προσωπικών Δεδομένων. Ειδικότερα, παρατηρείται το ρευστό υποκειμενικό όριο γύρω από το τι συνιστά τεχνητή νοημοσύνη. Το σύνολο των τεχνολογιών που θεωρείται τεχνητή νοημοσύνη από τον μέσο άνθρωπο τείνει να συρρικνώνεται με την πάροδο του χρόνου, καθώς ορισμένες δυνατότητες (όπως η οπτική αναγνώριση χαρακτήρων, τα βιομετρικά δεδομένα για την χρήση των κινητών συσκευών κ.α.) που αποτελούν τεχνητή νοημοσύνη δεν θεωρούνται πλέον τεχνητή νοημοσύνη από τους περισσότερους, καθώς μετατρέπονται σε "μια τετριμμένη τεχνολογία ρουτίνας", μια συνήθης λειτουργία των «έξυπνων» συσκευών η οποία δεν φαντάζει στα μάτια του μέσου ανθρώπου τόσο περίπλοκη όσο ένα σύστημα τεχνητής νοημοσύνης. Το φαινόμενο αυτό χαρακτηρίζεται ως AI Effect(Επίτροποι Προστασίας Δεδομένων και Προστασίας Προσωπικών Δεδομένων) (Λ. Μήτρου, Σ. Τάσσης, Η. Κωστή, Α. Βόρρας, Β. Καρκατζούνης, 2023).

Παρατηρώντας μια τάση κατακερματισμού της έννοιας της τεχνητής νοημοσύνης, νοείται ως επιτακτική η ανάγκη να οριστεί καθολικά με σαφήνεια η έννοια τόσο για λόγους ασφάλειας δικαίου όσο και για να διασφαλιστεί, παράλληλα, ευελιξία για την προσαρμογή στις μελλοντικές τεχνολογικές εξελίξεις. Ο ορισμός του συστήματος τεχνητής δεν θα πρέπει σε καμία περίπτωση να είναι ιδιαίτερα περιοριστικός και δεσμευτικός θέτοντας κατ' αυτό τον τρόπο εκτός αυτού νέες πιθανές αναδυόμενες τεχνολογίες. Άλλος ένας σημαντικός ορισμός της τεχνητής νοημοσύνης δόθηκε από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ)και είναι ο εξής: *«Ένα σύστημα τεχνητής νοημοσύνης είναι ένα σύστημα που βασίζεται σε μηχανές που, για ρητούς ή άρρητους στόχους, συμπεραίνει, από τα δεδομένα που λαμβάνει, τον τρόπο δημιουργίας αποτελεσμάτων όπως προβλέψεις, περιεχόμενο, προτάσεις ή αποφάσεις που μπορούν να επηρεάσουν φυσικά ή εικονικά περιβάλλοντα. Τα διαφορετικά συστήματα AI διαφέρουν ως προς τα επίπεδα αυτονομίας και προσαρμοστικότητας μετά την ανάπτυξη»*. Λαμβάνοντας υπόψη τα παραπάνω, ανάμεσα στους ορισμούς του Κανονισμού για την τεχνητή νοημοσύνη συγκαταλέγεται και το σύστημα τεχνητής νοημοσύνης, βασιζόμενος σε βασικά χαρακτηριστικά που το διακρίνουν από απλούστερα παραδοσιακά συστήματα λογισμικού ή προσεγγίσεις προγραμματισμού (αιτιολογική σκέψη 12 AI Act) και άμεσα επηρεασμένο από τον ορισμό που υιοθετεί ο ΟΟΣΑ,

ορίζεται ως «*μηχανικό σύστημα που έχει σχεδιαστεί για να λειτουργεί με διαφορετικά επίπεδα αυτονομίας και μπορεί να παρουσιάζει προσαρμοστικότητα μετά την εφαρμογή του και το οποίο, για ρητούς ή σιωπηρούς στόχους, συνάγει, από τα στοιχεία εισόδου που λαμβάνει, πώς να παράγει στοιχεία εξόδου, όπως προβλέψεις, περιεχόμενο, συστάσεις ή αποφάσεις που μπορούν να επηρεάσουν υλικά ή εικονικά περιβάλλοντα*».

1.3. Είδη, Τεχνικές και προσεγγίσεις Τεχνητής Νοημοσύνης

Η τεχνητή νοημοσύνη διακρίνεται βάσει των δυνατοτήτων της σε δύο ευρύτερες κατηγορίες, την στενή (narrow / weak) και την γενική ή ισχυρή (general). Τα συστήματα τεχνητής νοημοσύνης υπό στενή μορφή τροφοδοτούνται από τον άνθρωπο με συγκεκριμένα δεδομένα και προγραμματίζονται για την επίτευξη ενός μεμονωμένου αποτελέσματος, το οποίο επιτυγχάνεται συχνά με ταχύτητα μεγαλύτερη και από τον ίδιο τον άνθρωπο (Λ. Κανέλλος, 2021). Σε αντιδιαστολή με την στενή τεχνητή νοημοσύνη, η γενική τεχνητή νοημοσύνη έχει στόχο την λειτουργία της σαν άνθρωπος, ήτοι την διενέργεια κάθε είδους νοητικής εργασίας που διενεργεί ο άνθρωπος χωρίς περιορισμούς, κάτι που δεν έχει επιτευχθεί ακόμη. Υποστηρίζεται μέρος της κοινότητας του επιστημονικού κόσμου πως στο σύντομο μέλλον θα δημιουργηθούν συστήματα τεχνητής νοημοσύνης γενικής μορφής, δηλαδή μηχανές πιο «έξυπνες» από τον άνθρωπο, ικανές να τον αντικαταστήσουν. Η επικρατέστερη παρόλα αυτά άποψη της επιστημονικής κοινότητας είναι πως η τεχνολογία βρίσκεται ακόμη σε σημείο μακριά από την επίτευξη της γενικής τεχνητής νοημοσύνης. Μη αναμενόμενη υπήρξε και η νίκη στο παραδοσιακό κινέζικο παιχνίδι σκέψης και στρατηγικής Go επί του παγκόσμιου πρωταθλητή Lee Sedol από τον υπερυπολογιστή της Google τον Μάρτιο του 2016 στο πλαίσιο του προγράμματος DeepMind και τα προγράμματα μηχανής AlphaZero και AlphaGo, αποτέλεσαν μία ιστορική στιγμή, καθώς ένα μηχάνημα έδειξε σημάδια για αυτό που αναφέρουν οι ερευνητές ως δημιουργικότητα (Σ. Τάσσης, 2018). Το ως άνω παράδειγμα καταδεικνύει και τον απρόβλεπτο παράγοντα για την εξέλιξη της τεχνητής νοημοσύνης, με αποτέλεσμα οποιαδήποτε πρόβλεψη για το μέλλον της να μην μπορεί να χαρακτηρισθεί από βεβαιότητα. Συνεπώς, ακόμη και αν στην πλειονότητα η επίτευξη της γενικής τεχνητής νοημοσύνης στο εγγύτερο μέλλον φαντάζει αδύνατη, δεν μπορεί να αποκλειστεί δια βεβαιότητας.

Οι τεχνικές και οι προσεγγίσεις της τεχνητής νοημοσύνης που αναφέρονται και στον ίδιο τον Κανονισμό για την τεχνητή νοημοσύνη είναι αυτή της μηχανικής μάθησης (συμπεριλαμβανομένων της επιβλεπόμενης, της μη επιβλεπόμενης και της ενισχυτικής μάθησης, με τη χρήση ευρέος φάσματος μεθόδων, συμπεριλαμβανομένης της βαθιάς μάθησης), της βασισμένης στη λογική και στις γνώσεις (συμπεριλαμβανομένων της αναπαράστασης γνώσεων, του επαγωγικού (λογικού) προγραμματισμού, των βάσεων γνώσεων, των μηχανών εξαγωγής συμπερασμάτων και παραγωγικών συλλογισμών, των συστημάτων (συμβολικής) συλλογιστικής και των συστημάτων εμπειρογνωμόνων) και των στατιστικών προσεγγίσεων, εκτίμησης κατά Bayes, μεθόδων αναζήτησης και βελτιστοποίησης.

Ο αλγόριθμος, ο οποίος αποτελεί ένα από τα βασικότερα εργαλεία της τεχνητής νοημοσύνης, είναι η περιγραφή μιας πεπερασμένης και αδιαμφισβήτητης ακολουθίας βημάτων (ή οδηγιών) για την παραγωγή αποτελεσμάτων (εξόδου) από αρχικά δεδομένα (εισόδου). Η Γαλλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (CNIL) αναφέρει για την καλύτερη κατανόηση του αλγορίθμου ότι πρόκειται για «μια συνταγή [ως παράδειγμα] αλγορίθμου...., καθώς ένα πιάτο μπορεί να παρασκευαστεί από τα συστατικά του». Υπάρχουν οι κλασσικοί αλγόριθμοι που βασίζονται στον ανθρώπινο προγραμματισμό και δρουν περιορισμένα και οι αλγόριθμοι μηχανικής εκμάθησης που βασίζονται στα δεδομένα που λαμβάνουν από οποιαδήποτε πηγή, κυρίως στα μεγάλα δεδομένα (Big Data) που θα αναλυθούν κατωτέρω, και στην εμπειρία που δημιουργείται από την παρατήρηση επαναλαμβανόμενων μοτίβων για την εξαγωγή των ζητούμενων αποτελεσμάτων. Επιπλέον, οι αλγόριθμοι διαχωρίζονται σε περιγραφικούς ή αλγορίθμους λευκού κουτιού (white – box algorithms) και σε αλγορίθμους μαύρου κουτιού (black box algorithms), ανάλογα με το εάν υπάρχει ή όχι δυνατότητα ερμηνείας της αλγοριθμικής λειτουργίας και επενέργειας του ανθρώπου σε αυτή [Α. Μικρουλέα]. Η παραγωγική τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα που θα πραγματευτεί η παρούσα υπάγεται στο φαινόμενο του «μαύρου κουτιού», όπως θα αναλυθεί και στην συνέχεια.

Συχνά, φαίνεται οι όροι της μηχανικής εκμάθησης ή της βαθιάς μάθησης να συμπίπτουν με τον ευρύτερο όρο της τεχνητής νοημοσύνης. Στην πραγματικότητα, όμως, η μηχανική

εκμάθηση αποτελεί ένα σύνολο τεχνικών και εργαλείων, βασισμένοι στο οποίο οι υπολογιστές «σκέφτονται» δημιουργώντας μαθηματικούς αλγορίθμους σύμφωνα με τα δεδομένα, με τα οποία τροφοδοτούνται. Η μηχανική εκμάθηση αποτελεί μια από τις αναπτυσσόμενες προσεγγίσεις με τις οποίες επιτυγχάνεται η τεχνητή νοημοσύνη και λειτουργεί με βάση την εμπειρία που αποκτά αναλύοντας τα δεδομένα που λαμβάνει και παρατηρώντας τα μοτίβα και την επανάληψη γύρω από αυτά, ώστε να είναι σε θέση με την εισαγωγή νέων δεδομένων να τα κατηγοριοποιήσει σύμφωνα με την έως τότε εμπειρία της (Norwegian Data Protection Authority, 2018). Τα δεδομένα που εισάγονται σε ένα σύστημα μηχανικής εκμάθησης μπορούν να είναι κατηγοριοποιημένα βάσει ενός χαρακτηριστικού τους (π.χ. να φέρουν τον χαρακτηρισμό του σχήματος του ή του χρώματος τους) είτε να εισάγονται χωρίς κάποιον χαρακτηρισμό και να πρέπει το ίδιο το σύστημα να τον ανακαλύψει (αντίστοιχα επιβλεπόμενη και μη επιβλεπόμενη μηχανική εκμάθηση). Η ενισχυτική μάθηση βασίζεται στην αλληλεπίδραση του συστήματος με το περιβάλλον, «μαθαίνοντας» με διαδραστικό τρόπο, αφού παρατηρεί την επίδραση των ενεργειών του στο περιβάλλον (θετική ή αρνητική) και προχωρά σε ανατροφοδότηση των νέων ενεργειών που ακολουθούν.

Η βαθιά μάθηση (deep learning), όπως και η μηχανική εκμάθηση, είναι μεν υποπεδία της τεχνητής νοημοσύνης, η βαθιά μάθηση είναι παράλληλα ένα είδος - υποσύνολο της μηχανικής εκμάθησης, μια πολυεπίπεδη δομή αλγορίθμων που επιτρέπει στη μηχανή να «μαθαίνει» και να λαμβάνει αποφάσεις αυτόνομα, ενώ προσιδιάζει ιδιαίτερα στα «νευρωνικά δίκτυα», καθώς βασίζεται σε γνωστά δεδομένα που της παρέχονται και ακολουθεί την μέθοδο της αυτό-μάθησης για την παραγωγή αποτελεσμάτων (Σ. Τάσσης, 2018). Η βαθιά μάθηση δύναται να λειτουργήσει και με μη γνωστά σύνολα δεδομένων, προσδιορίζοντας μόνη της βάσει της έως τότε εμπειρίας της τα χαρακτηριστικά των εκάστοτε δεδομένων και χωρίζοντας τα σε κατηγορίες (C. Stryker - E. Kavlakoglu, 2024), λειτουργεί δηλαδή όπως λειτουργεί και η εμπειρία για την εξέλιξη και την πρόοδο του κάθε ανθρώπου. Η βαθιά εκμάθηση συνιστά μηχανική μάθηση μαύρου κουτιού, καθώς από την στιγμή που θα τεθεί σε λειτουργία δεν υπάρχει η δυνατότητα εποπτείας και ερμηνείας της δραστηριότητας της βήμα - βήμα.

Τα «νευρωνικά δίκτυα» συνιστούν τύπο αλγορίθμου μηχανικής μάθησης και επεξεργάζονται τα δεδομένα με αρχιτεκτονική εμπνευσμένη από τη δομή και την λειτουργία του ανθρώπινου εγκεφάλου, προσομοιάζουν δηλαδή στα νευρικά συστήματα του εγκεφάλου των εμβίων όντων. Τα «νευρωνικά δίκτυα» αποτελούνται από στρώματα τεχνητών νευρώνων που επεξεργάζονται σταδιακά τα δεδομένα με τα οποία τροφοδοτούνται και εξάγουν στο τελικό στρώμα ένα αποτέλεσμα (Big Blue Data Academy, 2023). Βασικό πλεονέκτημα των νευρωνικών δικτύων αποτελεί η δυνατότητα τους να επεξεργάζονται μεγάλο όγκο δεδομένων και να οδηγούν σε καλύτερα αποτελέσματα χωρίς ανθρώπινη παρέμβαση. Τα μεγάλα γλωσσικά μοντέλα, όπως το ChatGPT, για το οποίο θα μιλήσουμε ακολούθως αποτελούν ένα μοντέλο μηχανικής εκμάθησης που χρησιμοποιεί νευρωνικά δίκτυα.

1.4. Δεδομένα Μεγάλης Κλίμακας (Big Data)

Βασική προϋπόθεση λειτουργίας όλων των συστημάτων τεχνητής νοημοσύνης που υφίστανται, σε αλλά περισσότερο και σε άλλα λιγότερο, είναι τα δεδομένα. Μεταξύ των αλγορίθμων τεχνητής νοημοσύνης και των δεδομένων παρατηρείται μια σχέση αλληλεξάρτησης, ζωτικής σημασίας θα έλεγε κανείς. Με την ταχύτατη εξέλιξη του ψηφιακού κόσμου σημειώθηκε ραγδαία αύξηση των δεδομένων αλλά και της αξίας τους.

Σε μια προσπάθεια ορισμού τα Big Data είναι «*τεράστια σύνολα δεδομένων που έχουν μια πιο μεγάλη, πιο ποικίλη και πολύπλοκη δομή, που δημιουργεί δυσκολίες στην αποθήκευση, την ανάλυση και την οπτικοποίηση τους ώστε να είναι εκμεταλλεύσιμα για περαιτέρω διαδικασίες σε μια επιχείρηση*», ενώ για την επεξεργασία τους απαιτείται αυξημένη υπολογιστική ισχύς (Ι. Πολυμένης, 2017). Τα μεγάλα δεδομένα έχουν πέντε βασικά χαρακτηριστικά (γνωστά ως 5 V's), τον όγκο (volume) -ήτοι, τεράστια ποσότητα δεδομένων-, την ποικιλία (variety) -ήτοι, δεδομένα διαφορετικών μορφών-, την ταχύτητα (velocity) – ήτοι, εξαιρετικά υψηλή ταχύτητα παραγωγής, διανομής και επεξεργασίας των δεδομένων-, την αξία (value) αλλά και την ακρίβεια (veracity) των δεδομένων. τα οποία τα καθιστούν κατάλληλα για τα γλωσσικά μοντέλα τεχνητής νοημοσύνης (Ι. Ιγγλεζάκης, 2020).

Τα εν λόγω τεράστια σύνολα δεδομένων, αν και φαινομενικά είναι ασύνδετες μεταξύ τους πληροφορίες, στην πραγματικότητα δύναται να περιλαμβάνουν προσωπικά δεδομένα

και υποκείμενα σε επεξεργασία από συστήματα τεχνητής νοημοσύνης να αποκαλύπτουν μοτίβα και συμπεριφορές που μπορούν να οδηγήσουν έως και την κατάρτιση προφίλ ενός χρήστη (G. Mazurek, K. Małagocka, 2019). Βασική προϋπόθεση λειτουργίας των γλωσσικών μοντέλων παραγωγικής τεχνητής νοημοσύνης αποτελεί η ύπαρξη big data που αντλούν από δημόσια προσβάσιμες πηγές δεδομένων, όπως το διαδίκτυο.

1.5. Παραγωγική Τεχνητή Νοημοσύνη / Γλωσσικά Μοντέλα (ChatGPT)

Η τεχνητή νοημοσύνη, όπως ορίσθηκε παραπάνω, απασχολεί τον επιστημονικό κόσμο εδώ και αρκετές δεκαετίες. Η ανάπτυξη, όμως, νέων τεχνολογιών οδήγησε στην εμφάνιση της παραγωγικής τεχνητής νοημοσύνης, η οποία προκάλεσε ισχυρή αίσθηση για τις ικανότητες της και έγινε γνωστή μέσω της πασίγνωστης πλέον εφαρμογής γλωσσικού μοντέλου ChatGPT που δημιούργησε η OpenAI, προκαλώντας παράλληλα αναστάτωση και ανησυχία στην επιστημονική κοινότητα σχετικά με τον τρόπο λειτουργίας της και τον κίνδυνο που θέτει για την προστασία των προσωπικών δεδομένων των χρηστών της, καθώς τίθεται υπό αμφισβήτηση το εάν μπορούν να τηρηθούν οι βασικές αρχές προστασίας των προσωπικών δεδομένων, όπως προβλέπονται στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ), μεταξύ άλλων της διαφάνειας, της λογοδοσίας αλλά και της ελαχιστοποίησης των δεδομένων (CEDPO, 2023).

Η παραγωγική τεχνητή νοημοσύνη αποτελεί προηγμένο είδος τεχνητής νοημοσύνης, που βάσει των ερεθισμάτων (inputs) που λαμβάνει και μέσω της εκμάθησης μοτίβων που προκύπτουν από τα ήδη υπάρχοντα δεδομένα με τα οποία την έχει εφοδιάσει ο άνθρωπος (CRS REPORT, 2023), παράγει νέο περιεχόμενο (outputs), το οποίο ποικίλει ανά την εκάστοτε εφαρμογή (π.χ. κείμενο, εικόνα, ήχο, βίντεο). Οι εν λόγω εφαρμογές εκπαιδεύονται μέσω της μεθόδου βαθιάς μάθησης σε έναν εξωπραγματικό όγκο δεδομένων (big data) και δύνανται να απαντούν σε φυσική γλώσσα, παράγοντας ένα αποτέλεσμα που θα μπορούσε να έχει παραχθεί από τον άνθρωπο με την διαφορά, όμως, ότι ο χρόνος που θα χρειαζόταν ο άνθρωπος θα ήταν σαφώς περισσότερος. Μια βασική διαφορά μεταξύ της παραγωγικής τεχνητής νοημοσύνης και της παραδοσιακής τεχνητής νοημοσύνης είναι ότι η πρώτη λαμβάνοντας ως βάση τη γνώση που έχει αποκτήσει με τα δεδομένα που της έχουν παρασχεθεί τα αξιοποιεί και μέσω της κατάλληλης επεξεργασίας, δεν δημιουργεί

προβλέψεις αλλά νέα δεδομένα, όπως νέα κείμενα, εικόνες, ήχους κ.λπ. Ακριβώς, αυτά τα νέα δεδομένα μπορεί να τα λάβει και να τα χρησιμοποιήσει ο μέσος άνθρωπος με κοινές γνώσεις, γεγονός που οδηγεί σε άλλη μια ειδοποιό διαφορά της παραγωγικής τεχνητής νοημοσύνης σε σχέση με αυτή που γνωρίζαμε έως σήμερα. Τα προσωπικά δεδομένα και η παραγωγική τεχνητή νοημοσύνη έχουν μια σχέση διπλής κατεύθυνσης καθώς τα προσωπικά δεδομένα τροφοδοτούν και εκπαιδεύουν το εκάστοτε γλωσσικό μοντέλο και αυτό με την σειρά του παράγει νέα δεδομένα. Πλέον, η χρήση των εφαρμογών παραγωγικής τεχνητής νοημοσύνης είναι ευρεία, καθώς δύναται να τις χρησιμοποιεί ο καθένας χωρίς να απαιτείται η ύπαρξη εξειδικευμένων τεχνολογικών γνώσεων προγραμματισμού. Για παράδειγμα, ακόμη και ένας ανήλικος μαθητής μπορεί να κάνει χρήση του ChatGPT μέσω του εύχρηστου chatbox που παρέχει για να αναζητήσει λύσεις των εργασιών του.

Το ChatGPT, όπως προελέχθη, είναι ένα προηγμένο μοντέλο γλώσσας τεχνητής νοημοσύνης δομημένο από νευρωνικό δίκτυο και επεξεργάζεται με την μέθοδο της βαθιάς μάθησης τα δεδομένα που έχει στην διάθεση του, εντοπίζει σε αυτά μοτίβα -κοινά σημεία- και είναι μετέπειτα σε θέση να προβεί σε «παραγωγή» βασιζόμενη πάντοτε στις γνώσεις του. Το GPT (Generative Pre-trained Transformer) παρουσιάστηκε για πρώτη φορά το 2018 από την OpenAI, το 2019 προχώρησε στην αναβαθμισμένη έκδοση GPT-2 και το 2020 δημιούργησε το GPT-3, ικανό να δημιουργεί πολύπλοκα κείμενα με ακρίβεια και συνέπεια. Τον Νοέμβριο του 2022 τέθηκε σε ευρεία κυκλοφορία το ChatGPT με την χρήση του GPT-3, σχεδιασμένο για την δημιουργία διαλόγων και η εξάπλωση του ήταν ραγδαία αν αναλογιστούμε ότι μέσα σε πέντε μέρες απέκτησε ένα εκατομμύριο χρήστες και μέσα σε δύο μήνες εκατό εκατομμύρια χρήστες (Ahfaz Ahmed, 2024).

Ένα σημαντικό ερώτημα που ανακύπτει παρατηρώντας τα μεγάλα γλωσσικά μοντέλα που έχουν κατακλύσει τον τεχνολογικό και μη κόσμο (π.χ. το ChatGPT) είναι η προέλευση των δεδομένων που τα βοηθούν να εκπαιδευτούν και να εξελιχθούν σε συνδυασμό με το γεγονός ότι ο όγκος των δεδομένων που χρειάζονται για να παράγουν το επιθυμητό αποτέλεσμα είναι ασύλληπτος. Αρκεί μόνο να αναλογιστεί κανείς ότι η έκδοση GPT-3,5 έχει εκπαιδευτεί με 300 δισεκατομμύρια λέξεις ή αλλιώς με 570 GB δεδομένων (A. Hughes, 2023). Η πλειοψηφία των δεδομένων (big data) συλλέγεται από δημόσια προσβάσιμες πηγές όπως

ιστοσελίδες, αρθρογραφία, ηλεκτρονικά βιβλία ακόμη και από τα μέσα κοινωνικής δικτύωσης αλλά και από τα προσωπικά δεδομένα που παρέχουν οι χρήστες τόσο κατά την εγγραφή (ονοματεπώνυμο, στοιχεία επικοινωνίας, στοιχεία κάρτας πληρωμής κ.α.) όσο και με την μεταφόρτωση δεδομένων για την πραγματοποίηση του διαλόγου (δεδομένα που εκμαιεύει από τις ερωτήσεις που τίθεντα, εικόνες κ.α.). Εκτός των προσωπικών δεδομένων που οι ίδιοι οι χρήστες αποκαλύπτουν στο ChatGPT, ανάμεσα στα big data που αντλεί το μοντέλο συγκαταλέγονται και προσωπικά δεδομένα υποκειμένων, όχι απαραίτητα χρηστών του.

Οι προβληματισμοί που αναδύονται από την χρήση του ChatGPT και ηθικοί αλλά και σε σχέση με τα θεμελιώδη ανθρώπινα δικαιώματα απασχολούν ιδιαιτέρως τον επιστημονικό κόσμο αλλά και τον Ευρωπαίο νομοθέτη. Κατά κύριο λόγο το μεγαλύτερο πλήγμα το έχει δεχτεί το δικαίωμα στον ιδιωτικό βίο και την προστασία των προσωπικών δεδομένων ένεκα του μεγάλου όγκου δεδομένων που απαιτεί το ChatGPT για την εκπαίδευση του. Το ChatGPT οφείλει να συμμορφώνεται με το ισχύον νομοθετικό πλαίσιο για την προστασία των προσωπικών δεδομένων και κατά βάση με τον ΓΚΠΔ, αλλά τα βασικά του τεχνικά χαρακτηριστικά το φέρνουν συχνά σε σύγκρουση με τις διατάξεις του, όπως θα αναλύσουμε και στα επόμενα κεφάλαια.

Ενδεικτικά, η ανησυχία της Ευρωπαϊκής Ένωσης για το ChatGPT εμφαίνεται από το γεγονός ότι το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) δημιούργησε μια ειδική υπό-ομάδα για την αντιμετώπιση των ζητημάτων που προκύπτουν σχετικά με το ChatGPT. Τον Μάϊο του 2024 δημοσίευσε την πρώτη της έκθεση σχετικά με τα ζητήματα της λειτουργίας του ChatGPT που γεννώνται σε σχέση με το ισχύον νομοθετικό πλαίσιο γύρω από την προστασία των προσωπικών δεδομένων, δίνοντας παράλληλα στους προγραμματιστές μεγάλων γλωσσικών μοντέλων (LLMs) κατευθυντήριες οδηγίες σχεδίασης και λειτουργίας. Τόνισε κατά κύριο λόγο τέσσερεις προβληματικές για την σχέση του ChatGPT με την προστασία των προσωπικών δεδομένων: τη νόμιμη βάση επεξεργασίας προσωπικών δεδομένων που συλλέγονται από δημόσιες πηγές του διαδικτύου, την πλήρωση της αρχής της νομιμότητας και της διαφάνειας της επεξεργασίας, καθώς και την ακρίβεια των δεδομένων που επεξεργάζεται.

Ενδιαφέρον παρουσιάζει η διαφορετική αντιμετώπιση του ChatGPT σε διαφορετικά κράτη του κόσμου, γεγονός που δείχνει και την αμηχανία που προκάλεσε η κυκλοφορία του. Η Ιταλική Αρχή Προστασίας Προσωπικών Δεδομένων, μια εκ των Αρχών της Ευρωπαϊκής Ένωσης, όταν διέρρευσαν πληροφορίες σχετικά με τις συζητήσεις και τα στοιχεία πληρωμών των συνδρομητών του ChatGPT, απαγόρευσε την χρήση του στην Ιταλία. Η Αρχή επεσήμανε ότι το ChatGPT συλλέγει δεδομένα από τα υποκείμενα χωρίς να πληρείται η απαραίτητη νόμιμη βάση και χωρίς να τηρείται η αρχή της ακρίβειας των δεδομένων, αφού δεν έδειχναν την δέουσα επιμέλεια για την ενημέρωση τους. Έθεσε προθεσμία συμμόρφωσης στην OpenAI για την ενίσχυση της προστασίας των δεδομένων και την παροχή μεγαλύτερης διαφάνειας διαφορετικά προειδοποίησε για την επιβολή προστίμου (GPDP, 2023). Η OpenAI μετά την προειδοποίηση της Ιταλικής Αρχής παρείχε στους χρήστες της το δικαίωμα να ζητούν την διαγραφή των δεδομένων τους από την βάση δεδομένων του και μεταξύ και άλλων μέτρων προστασίας δεδομένων που έλαβε, κατάφερε να συνεχίσει την λειτουργία της στην Ιταλία.

Μετά την απόφαση της Ιταλικής Αρχής, χώρες όπως η Ισπανία και η Γαλλία θορυβήθηκαν και άρχισαν να εξετάζουν ενδελεχώς το ChatGPT σε σχέση με την προστασία των προσωπικών δεδομένων εκφράζοντας τις ανησυχίες τους για την δέουσα και προσήκουσα επεξεργασία των προσωπικών δεδομένων. Εκ διαμέτρου αντίθετη είναι αντιμετώπιση του ChatGPT από χώρες όπως η Κίνα, η Ρωσία, η Βόρεια Κορέα και το Ιράν. Στις δύο τελευταίες η απαγόρευση φαίνεται εύλογη λόγω των ιδιαίτερα αυστηρών περιορισμών που εφαρμόζουν αυτές οι χώρες αναφορικά με την πρόσβαση στο διαδίκτυο, ενώ οι δύο πρώτες προβάλουν ως δικαιολογία τον κίνδυνο περί ασφάλειας πληροφοριών. Η Κίνα ως πρωτοπόρος στον χώρο της τεχνολογίας προσπαθεί με ιδία μέσα να δημιουργήσει μια παρεμφερή εφαρμογή με σκοπό την τήρηση της ασφάλειας των δεδομένων αλλά και της τεχνολογικής της ανεξαρτησίας. Την ελαστικότερη αντιμετώπιση εφαρμόζουν οι ΗΠΑ που θέτουν σε προτεραιότητα την τεχνολογική ανάπτυξη και όχι την προστασία των προσωπικών δεδομένων, αφήνοντας τους τεχνολογικούς κολοσσούς που έχουν την έδρα τους στις ΗΠΑ να δρουν και να αναπτύσσονται ελεύθερα χωρίς περιορισμούς (Ο. Κοργιαλά, 2023).

Το ChatGPT μπορεί να είναι το διασημότερο στην κατηγορία των γλωσσικών μοντέλων δεν είναι, όμως, ούτε το μοναδικό αλλά ούτε και το πρώτο που δημιουργήθηκε. Το πρώτο γλωσσικό μοντέλο παρουσιάστηκε στο ευρύ κοινό το 1966 από τον Joseph Weizenbaum και ονομάστηκε Eliza ενσαρκώνοντας τον ρόλο του ψυχοθεραπευτή. Η Eliza «άκουγε» τα προβλήματα του χρήστη και ακολουθώντας συγκεκριμένα μοτίβα με τα οποία είχε εκπαιδευτεί τον έκανε να νιώθει πως συνομιλεί με έναν συνάνθρωπο του που τον «συμπονά» (B. Tarnoff, 2023). Ακολούθησαν και άλλα γλωσσικά μοντέλα περιορισμένων δυνατοτήτων έως την σύγχρονη εποχή που την εμφάνιση του έκανε το ChatGPT, το οποίο ξεχωρίζει για την φυσικότητα του λόγου του και τον τεράστιο όγκο δεδομένων που χρησιμοποιεί με αποτέλεσμα πλέον να μιλάμε για Μεγάλα Γλωσσικά Μοντέλα (Large Language Models). Άλλα χαρακτηριστικά παραδείγματα των μεγάλων γλωσσικών μοντέλων είναι οι εφαρμογές ανάλυσης συναισθήματος πίσω από κάποιο κείμενο όπως η Google Cloud Natural Language API, οι εφαρμογές μετάφρασης κειμένων όπως το Google Translate, το Microsoft Translator, το DeepL κ.α., οι εφαρμογές αναγνώρισης ομιλίας και μεταγραφής σε κείμενο όπως το Google speech-to-text και τέλος οι συνομιλίες μέσω chatbox που ακολούθησαν το ChatGPT όπως το Google Bard και το Microsoft Bing Chat.

Όσο πρωτοποριακές και αν είναι οι προαναφερθείσες εφαρμογές θα πρέπει να εξεταστεί εάν το ισχύον νομοθετικό πλαίσιο αρκεί για την εξασφάλιση της ορθής λειτουργίας τους και τη δέουσα προστασία των χρηστών της ή εάν οι κίνδυνοι παραβίασης τους είναι υπέρμετροι και απαιτείται η υιοθέτηση αυστηρότερου, ίσως πιο εξειδικευμένου, νομοθετικού πλαισίου.

1.6. Εφαρμογές Τεχνητής Νοημοσύνης

Η αδιαμφισβήτητη εισβολή της τεχνητής νοημοσύνης στην καθημερινή ζωή βαίνει ολοένα και αυξανόμενη καθιστώντας ίσως την χρήση της τετριμμένη και απαλοίφωντας σταδιακά από την συνείδηση όλων το γεγονός ότι η εκάστοτε τεχνολογία που τους διευκολύνει αποτελεί συνάμα εφαρμογή τεχνητής νοημοσύνης. Προς επίρρωση του παραπάνω, κατόπιν έρευνας που πραγματοποιήθηκε το 2017, το 88 % των ερωτηθέντων Ευρωπαίων απάντησε ότι οι τεχνολογίες τεχνητής νοημοσύνης απαιτούν προσεκτική διαχείριση (Special Eurobarometer, 2017). Το ερώτημα είναι εάν διαχειρίζονται στην πραγματικότητα αυτές τις τεχνολογίες προσεκτικά ή εάν η ευρεία χρήση τους κάνει να

ξεχνάνε πως πρόκειται για τεχνολογίες τεχνητής νοημοσύνης και να μην επιδεικνύουν την δέουσα προσοχή;

Εφαρμογές όπως η Siri της Apple και η Alexa της Android είναι μέρος της καθημερινότητας όλων των χρηστών καθώς αποτελούν την προσωπική τους γραμματέα («προσωπικοί ψηφιακοί βοηθοί»). Εκτελούν εντολές των χρηστών για τις οποίες, όμως, απαιτούν απεριόριστη πρόσβαση σε όλα τα αποθηκευμένα δεδομένα των χρηστών γεννώντας προβληματισμούς για τους οποίους θα μιλήσουμε στη συνέχεια της παρούσας. Βασικό χαρακτηριστικό της τεχνητής νοημοσύνης που εφαρμόζει η Alexa και η Siri και οι λοιπές παρόμοιες εφαρμογές είναι η βελτίωση των αποτελεσμάτων μέσω της καθημερινής εξάσκησης. Κατ' αυτόν τον τρόπο και οι εν λόγω εφαρμογές με τον καιρό βελτιώνονται και απαντούν σε εντολές με λιγότερες λεπτομέρειες καθώς έχουν εξατομικευθεί στις ανάγκες του «αφεντικού» τους με δυνατότητα πρόβλεψης τους.

Μια περαιτέρω έκφανση της τεχνητής νοημοσύνης στην καθημερινή ζωή είναι τα νέας τεχνολογίας αυτοκίνητα με αισθητήρες και δυνατότητα αντίδρασης πριν τον οδηγό τους και σκοπό την προστασία αυτού. Για παράδειγμα, με τους ενσωματωμένους αισθητήρες το αυτοκίνητο είναι σε θέση να αντιληφθεί τον κίνδυνο και να επιβραδύνει χωρίς να δεχτεί την αντίστοιχη εντολή από τον οδηγό. Τα νέα αυτοκίνητα είναι σε θέση να σκέφτονται πριν σκεφτεί ο ίδιος ο οδηγός τους.

Η τεχνητή νοημοσύνη είναι βασικό εργαλείο της κυβερνοασφάλειας και χρησιμοποιείται από τους μεγαλύτερους τεχνολογικούς κολοσσούς, όπως η Microsoft, στις εφαρμογές τους. Χαρακτηριστικότερο παράδειγμα που οι περισσότεροι έχουν συναντήσει ίσως δίχως να αντιληφθούν ότι πρόκειται για τεχνητή νοημοσύνη είναι ο διαχωρισμός των μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να μπορούν να βλάψουν τον υπολογιστή με ιούς (spam emails) και η αρχειοθέτηση τους σε διαφορετικό φάκελο ώστε να προστατέψουν τον χρήστη από το άνοιγμα τους.

Στον τομέα της υγείας, η κατασκευή μηχανημάτων σε σχήμα βραχιολιού που αντιλαμβάνονται μέσω τεχνητής νοημοσύνης καταστάσεις κινδύνου των ανθρώπων που τα φοράνε – ασθενών είναι άλλη μια θετική όψη της.

Τέλος, η τεχνητή νοημοσύνη «κρύβεται» πίσω και από τα λεγόμενα chatboxes που έχουν εγκαταστήσει σχεδόν όλοι οι πάροχοι υπηρεσιών στις ιστοσελίδες τους για την άμεση εξυπηρέτηση των πελατών τους αποφεύγοντας και οι ίδιοι λειτουργικά κόστη όπως η πρόσληψη περισσότερων εργαζομένων. Τα εν λόγω chatboxes επικοινωνούν με τους πελάτες και τους εξυπηρετούν για εύκολα ζητήματα μέσα σε λίγα λεπτά βάσει λέξεων κλειδί και με τα δεδομένα που τους έχουν δοθεί.

Τα παραπάνω είναι λίγα μόνο παραδείγματα εφαρμογής τεχνητής νοημοσύνης στη σημερινή εποχή, τα οποία εκ πρώτης όψεως μόνο θετική επίδραση φαίνονται να έχουν. Η πρώτη εντύπωση δεν αντικατοπτρίζει, όμως, πάντοτε την πραγματικότητα και στη συγκεκριμένη περίπτωση οι κίνδυνοι που ελλοχεύουν για τους χρήστες είναι πολλαπλοί και σοβαροί και ως εκ τούτου χρήζουν ιδιαίτερης προσοχής και οριοθέτησης, όπως θα αναλυθεί ακολούθως.

2. Προστασία προσωπικών δεδομένων και γλωσσικά μοντέλα (ChatGPT κ.α.)

2.1. Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η ραγδαία ανάπτυξη της τεχνολογίας, μέρος της οποίας αποτελεί και η τεχνητή νοημοσύνη, σε συνδυασμό με τον ασύλληπτο όγκο δεδομένων που χρησιμοποιούν και επεξεργάζονται οι νέες τεχνολογίες έκανε επιτακτική την ανάγκη θεσμοθέτησης ενός ενιαίου πλαισίου προστασίας προσωπικών δεδομένων βασιζόμενο στα θεμελιώδη δικαιώματα του ΧΘΔΕΕ και συγκεκριμένα στο άρθρο 7 περί σεβασμού της ιδιωτικής ζωής αλλά και στο άρθρο 8 περί προστασίας των δεδομένων προσωπικού χαρακτήρα. Το 2018, δύο χρόνια μετά τη δημοσίευση του, τέθηκε σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (General Data Protection Regulation – GDPR) με κύριο αντικείμενο την οριοθέτηση της επεξεργασίας προσωπικών δεδομένων φυσικών προσώπων και την προστασία τους.

Ως *«δεδομένα προσωπικού χαρακτήρα»* ο ΓΚΠΔ ορίζει *«κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί,*

άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου». Το άρθρο 9 του ΓΚΠΔ προβλέπει την ειδική κατηγορία προσωπικών δεδομένων,τα ευαίσθητα προσωπικά δεδομένα 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»*, τα οποία υπόκεινται σε επεξεργασία μόνο υπό συγκεκριμένες προϋποθέσεις. Εξαίρεση από το πεδίο εφαρμογής του ΓΚΠΔ αποτελούν τα δεδομένα που δεν αφορούν φυσικά πρόσωπα, όπως τα δεδομένα νομικών προσώπων, καθώς και τα ανώνυμα δεδομένα μέσω των οποίων δεν είναι δυνατή η αντιστοίχιση αυτών των δεδομένων με τα φυσικά πρόσωπα στα οποία ανήκουν.

Το εδαφικό πεδίο εφαρμογής του ΓΚΠΔ παρουσιάζει ομοιότητα με το πεδίο εφαρμογής του Κανονισμού για την τεχνητή νοημοσύνη (βλ. επόμενο κεφάλαιο), καθώς δεν περιορίζεται από τον τόπο εγκατάστασης του παρόχου εντός της ΕΕ αλλά εφαρμόζεται και σε περιπτώσεις που ο πάροχος ή αντίστοιχα ο υπεύθυνος / εκτελών την επεξεργασία έχει την εγκατάσταση του σε τρίτη χώρα, αρκεί το υποκείμενο του οποίου τα δεδομένα επεξεργάζονται να βρίσκεται εντός της ένωσης[1].

Με δεδομένο ότι η τεχνητή νοημοσύνη και περισσότερο τα σύγχρονα γλωσσικά μοντέλα όπως το ChatGPT χρειάζονται μεγάλο όγκο δεδομένων (Big Data) (Α. Βόρρας – Λ. Μήτρου, 2018), κατά κύριο λόγο προσωπικών δεδομένων, για να εκπαιδευτούν και να προβούν στην παραγωγή νέων δεδομένων. Η σχέση προσωπικών δεδομένων και τεχνητής νοημοσύνης είναι αμφίδρομη, η τεχνητή νοημοσύνη «τρέφεται» με δεδομένα και «γεννά» νέα δεδομένα (L. Mitrou, 2018). Ο ΓΚΠΔ βρίσκει εφαρμογή στα συστήματα τεχνητής νοημοσύνης και

[1] Άρθρο 3 ΓΚΠΔ

μάλιστα μέχρι την θέση σε ισχύ του Κανονισμού για την τεχνητή νοημοσύνη, ήταν και το μόνο κανονιστικό νομοθέτημα που επέβαλε περιορισμούς, έστω και εμμέσως, στα εν λόγω συστήματα. Η συμμόρφωση με τον ΓΚΠΔ είναι ιδιαίτερα κρίσιμη για τη διασφάλιση της διαφάνειας, της ασφάλειας και της δικαιοσύνης στις διαδικασίες που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων.

Ο ΓΚΠΔ αποτελεί ένα νομοθετικό κείμενο τεχνολογικά ουδέτερο, ώστε η εφαρμογή του να μην επηρεάζεται από την συνεχή και ταχύτατη εξέλιξη της τεχνολογίας, ενώ εφαρμόζεται τόσο στην αυτοματοποιημένη επεξεργασία των προσωπικών δεδομένων όσο και στην μη αυτοματοποιημένη επεξεργασία. Επιπλέον, σκοπός του είναι η προστασία των δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων, χωρίς να εκφράζει σύμφωνη ή αντίθετη γνώμη για την εφαρμογή αυτών των νέων τεχνολογιών. Η ουδετερότητα του ΓΚΠΔ σημαίνει πως μέσα στο κείμενο του δεν εντοπίζεται κάποια ειδική ρύθμιση για την επεξεργασία των προσωπικών δεδομένων από συστήματα τεχνητής νοημοσύνης και δη παραγωγικής τεχνητής νοημοσύνης.

Ο ουδέτερος χαρακτήρας του εν λόγω νομοθετήματος είναι που το καθιστά εφαρμόσιμο ακόμη και στα νέα γλωσσικά μοντέλα τεχνητής νοημοσύνης, οι πάροχοι των οποίων υποχρεούνται να συμμορφώνονται με τις βασικές αρχές ΓΚΠΔ επεξεργασίας προσωπικών δεδομένων, όπως αυτές προβλέπονται στο άρθρο 5 αυτού και κυρίως με τις υποχρεώσεις για διαφάνεια, περιορισμό του σκοπού, ελαχιστοποίηση των δεδομένων καθώς και για λογοδοσία.

Ειδικότερα οι βασικές αρχές του άρθρου 5 του ΓΚΠΔ με τις οποίες πρέπει να συμμορφώνονται τα γλωσσικά μοντέλα είναι οι εξής:

i. Αρχή νομιμότητας επεξεργασίας / νόμιμη βάση επεξεργασίας

Τα προσωπικά δεδομένα θα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία. Για να επιτευχθεί η νόμιμη επεξεργασία είναι ιδιαιτέρως σημαντικό να επιλέγεται η κατάλληλη νομική βάση της επεξεργασίας. Οι προβλεπόμενες νομικές βάσεις επεξεργασίας απαριθμούνται εξαντλητικώς στο άρθρο 6 του ΓΚΠΔ και είναι η συγκατάθεση, η ύπαρξη

συμβατικής υποχρέωσης, η ύπαρξη υποχρέωσης για τον Υπεύθυνο Επεξεργασίας [2] απορρέουσα εκ του νόμου, η ύπαρξη ζωτικού συμφέροντος του υποκειμένου που επιτρέπει την επεξεργασία των δεδομένων του, η ύπαρξη δημοσίου ή εννόμου συμφέροντος.

Η κυριότερη βάση επεξεργασίας που θα μας απασχολήσει και παρακάτω και η οποία τυγχάνει συχνότερα εφαρμογής και κατά την επεξεργασία προσωπικών δεδομένων από το ChatGPT και από άλλα αντίστοιχα μεγάλα γλωσσικά μοντέλα τεχνητής νοημοσύνης είναι η συγκατάθεση, η οποία για να θεωρηθεί έγκυρη θα πρέπει να φέρει συγκεκριμένες προϋποθέσεις[3]. Η συγκατάθεση θα πρέπει να είναι ελεύθερη, να μην εκμαιεύεται με τρόπο που επηρεάζει / παραπλανά την ελεύθερη βούληση του υποκειμένου, θα πρέπει να έχει δοθεί σε απλή και κατανοητή γλώσσα, να είναι συγκεκριμένη, αδιαμφισβήτητη, ενώ θα πρέπει να παρέχεται η δυνατότητα ανάκλησης της ανά πάσα ώρα και στιγμή. Για να είναι εφικτή η ελεύθερη συγκατάθεση απαιτείται το υποκείμενο να λάβει πλήρη και σαφή ενημέρωση για το ποια δεδομένα θα επεξεργαστούν, ποιος θα κάνει την επεξεργασία και για ποιον σκοπό, αλλά και ποια δικαιώματα έχει, πότε και πως μπορεί να τα ασκήσει. Οι παραπάνω προϋποθέσεις για την έγκυρη συγκατάθεση ισχύουν σωρευτικώς διαφορετικά μιλάμε για άκυρη συγκατάθεση και κατ' αποτέλεσμα για παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τέλος, ο Υπεύθυνος Επεξεργασίας υποχρεούται να μπορεί να αποδείξει και εκ των υστέρων την λήψη έγκυρης συγκατάθεσης από το υποκείμενο των δεδομένων που επεξεργάζεται.

ii. Αρχή διαφάνειας

Σε άμεση συνάφεια με την ορθή ενημέρωση του υποκειμένου που απαιτείται για έγκυρη συγκατάθεση, σύμφωνα με όσα αναφέρθηκαν παραπάνω, έρχεται η αρχή της διαφάνειας, η οποία αποτελεί θεμελιώδη και βασική αρχή του ΓΚΠΔ. Η αρχή της διαφάνειας προβλέπει ότι η ενημέρωση του υποκειμένου οφείλει να είναι συνοπτική, διαφανής, κατανοητή, εύκολα

[2] Άρθρο 4 παρ. 7 ΓΚΠΔ: «Υπεύθυνος Επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,

[3] Άρθρο 7 ΓΚΠΔ

προσβάσιμη και διατυπωμένη σε απλή και σαφή γλώσσα. Παραταύτα, από διαφάνεια δεν οφείλει να χαρακτηρίζεται μόνο η προγενέστερη της συγκατάθεσης ενημέρωση αλλά και όλη η δραστηριότητα επεξεργασίας των προσωπικών δεδομένων μέχρι την εξαγωγή του τελικού αποτελέσματος. Με άλλα λόγια, οι ενέργειες του υπευθύνου επεξεργασίας κατά την διάρκεια της επεξεργασίας πρέπει να μπορούν να διακριθούν και να επεξηγηθούν ακόμη και όταν έχει επέλθει το αποτέλεσμα της επεξεργασίας. Κατ' αυτόν τον τρόπο, το υποκείμενο θα έχει την δυνατότητα να δει ποια δεδομένα του επεξεργάστηκαν, εάν υπήρξε υπέρβαση του σκοπού που είχε αρχικώς οριστεί, καθώς και για τις επιπτώσεις που έχει η εκάστοτε επεξεργασία.

iii. Αρχή περιορισμού του σκοπού

Με σκοπό να είναι σύννομη μια επεξεργασία προσωπικών δεδομένων θα πρέπει να οριστεί εξαρχής ο ακριβής σκοπός επεξεργασίας για τα δεδομένα που συλλέγονται και τα εν λόγω δεδομένα να μην υποβάλλονται σε περαιτέρω επεξεργασία για σκοπούς που υπερβαίνουν τον αρχικώς ορισθέντα σκοπό. Εξαίρεση από τον περιορισμό του σκοπού αποτελεί η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης λόγω δημοσίου συμφέροντος ή για σκοπούς έρευνας ή για στατιστικούς σκοπούς. Σε περίπτωση που για οποιονδήποτε λόγο υπάρξει διαφοροποίηση του σκοπού, η νομική βάση που είχε επιλεχθεί για την επεξεργασία, βασιζόμενη στον αρχικό σκοπό, δεν θα έχει πλέον ισχύ και εκ του αποτελέσματος η επεξεργασία των δεδομένων προς εκπλήρωση του νέου σκοπού θα καθίσταται αυτομάτως παράνομη.

iv. Αρχή ελαχιστοποίησης δεδομένων

Μια περαιτέρω, ζωτικής σημασίας για τα δεδομένα, αρχή είναι η αρχή της ελαχιστοποίησης των δεδομένων ή διαφορετικά η αρχή της αναλογικότητας, σύμφωνα με την οποία τα δεδομένα που συλλέγονται θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για την εκπλήρωση του επιδιωκόμενου σκοπού (Ι. Ιγγλεζάκης, 2020). Κάθε δεδομένο που συλλέγει ο υπεύθυνος επεξεργασίας οφείλει να έχει την δυνατότητα να αιτιολογεί τον λόγο για τον οποίο το χρειάζεται και πως το συγκεκριμένο δεδομένο θα τον βοηθήσει στην εκπλήρωση του σκοπού του. Η αρχή ελαχιστοποίησης των δεδομένων συνδέεται άρρηκτα με την αρχή της ακρίβειας των δεδομένων, τα οποία θα πρέπει να

επικαιροποιούνται και να είναι ακριβή, καθώς δεδομένα που δεν είναι ακριβή είτε θα πρέπει να διορθώνονται είτε θα πρέπει να διαγράφονται καθώς δεν χρησιμεύουν πλέον αλλά αντιθέτως μπορούν να οδηγήσουν σε βλάβη του υποκειμένου.

v. Λογοδοσία

Η αρχή της λογοδοσίας φέρει αντιμέτωπο με τις ευθύνες του τον υπεύθυνο επεξεργασίας, ο οποίος θα πρέπει να έχει την ικανότητα οποτεδήποτε να «λογοδοτεί», δηλαδή να αποδεικνύει την συμμόρφωση του με τις υποχρεώσεις που τίθενται από τον ΓΚΠΔ, με αποτέλεσμα να μετατοπίζεται το βάρος της απόδειξης σε εκείνον. Ο υπεύθυνος επεξεργασίας θα πρέπει τόσο κατά τον σχεδιασμό (by design) να εξασφαλίζει ότι η επεξεργασία είναι σύμφωνη με τις νομοθετικές επιταγές και ειδικότερα με τις διατάξεις του ΓΚΠΔ, όσο και κατά την διάρκεια της επεξεργασίας να μην παρεκκλίνει από αυτές, και να διατηρεί έγγραφες αποδείξεις για τα παραπάνω ώστε να μπορέσει να συμμορφωθεί και με την οριζόμενη αρχή της λογοδοσίας.

vi. Αρχή περιορισμού αποθήκευσης

Η αποθήκευση των προσωπικών δεδομένων αποτελεί μορφή επεξεργασίας τους και θα ήταν εξαιρετικά καταχρηστικό για το υποκείμενο να παραμένουν τα δεδομένα του αποθηκευμένα εσαεί. Συνεπώς, ο υπεύθυνος επεξεργασίας οφείλει να μην διατηρήσει αποθηκευμένα τα δεδομένα για μεγαλύτερο χρονικό διάστημα από το απαιτούμενο για την εκπλήρωση του σκοπού της επεξεργασίας.

vii. Αρχή ακεραιότητας και εμπιστευτικότητας

Σύμφωνα με την αρχή ακεραιότητας και εμπιστευτικότητας, τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία με τρόπο που να διασφαλίζει την κατάλληλη ασφάλεια, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά, με χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων.

Η συνεχής τροφοδότηση των εφαρμογών όπως το ChatGPT αλλά και η δημιουργία νέων δεδομένων και προβλέψεων για το υποκείμενο από την εν λόγω τροφοδότηση περιλαμβάνει και επεξεργασία προσωπικών δεδομένων σύμφωνα με τον ΓΚΠΔ (Conrad Sebastian, 2017) και ως εκ τούτου είναι η υποχρεωτική η εφαρμογή των διατάξεων του και η συμμόρφωση με

τις αρχές του, όπως παρατέθηκαν παραπάνω. Παρόλα αυτά, κατά την δημιουργία και λειτουργία αυτών των εφαρμογών τεχνητής νοημοσύνης σημειώνεται η δημιουργία συγκρούσεων με τις διατάξεις για την προστασία των προσωπικών δεδομένων, οι οποίες θα συζητηθούν περαιτέρω στο επόμενο κεφάλαιο.

Ο ΓΚΠΔ προβλέπει μια σειρά δικαιωμάτων που μπορεί να ασκήσει το υποκείμενο των δεδομένων, το δικαίωμα στην ενημέρωση (διαφάνεια)[4], το δικαίωμα πρόσβασης στα δεδομένα[5], το δικαίωμα διόρθωσης[6], το δικαίωμα διαγραφής («δικαίωμα στη λήθη»)[7], το δικαίωμα περιορισμού της επεξεργασίας[8], το δικαίωμα στη φορητότητα των δεδομένων[9], το δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων[10] και τέλος το δικαίωμα στην μη αυτοματοποιημένη ατομική λήψη αποφάσεων (συμπεριλαμβανομένου της κατάρτισης προφίλ)[11]. Αυτά τα δικαιώματα ενισχύουν την προστασία των προσωπικών δεδομένων και επιτρέπουν στα άτομα να έχουν μεγαλύτερο έλεγχο επί των προσωπικών τους δεδομένων, ενώ η δυνατότητα άσκησης τους θα πρέπει να δίνεται κατά την λειτουργία των γλωσσικών μοντέλων τεχνητής νοημοσύνης.

Οι νέες τεχνολογίες που έρχονται στην επιφάνεια θα πρέπει να συμμορφώνονται πλήρως με το ισχύον νομοθετικό πλαίσιο, συνεπώς ο νόμος προϋπάρχει χωρίς όμως να είναι εξειδικευμένος σε κάθε καινοτομία καθώς δεν δύναται να την προβλέψει προτού δημιουργηθεί. Ο νομοθέτης προσπαθεί με γενικούς νόμους πλαίσια να διασφαλίσει τα δικαιώματα των πολιτών σε κάθε περίσταση, προβλέψιμη ή μη, και εκ των υστέρων όταν πλέον είναι αποδεκτό ότι απαιτούνται πρόσθετες νομοθετικές ρυθμίσεις που θα εστιάζουν στις νέες τεχνολογίες αφού προηγουμένως έχουν τεθεί σε λειτουργία και έχουν εντοπιστεί ζητήματα που χρειάζονται ρύθμιση.

[4] Άρθρα 12-14 ΓΚΠΔ
[5] Άρθρο 15 ΓΚΠΔ
[6] Άρθρο 16 ΓΚΠΔ
[7] Άρθρο 17 ΓΚΠΔ
[8] Άρθρο 18 ΓΚΠΔ
[9] Άρθρο 20 ΓΚΠΔ
[10] Άρθρο 21 ΓΚΠΔ
[11] Άρθρο 22 ΓΚΠΔ

Οι ΗΠΑ ως ο τόπος εγκαθίδρυσης των μεγαλύτερων τεχνολογικών κολοσσών του κόσμου εφαρμόζουν και το ευνοϊκότερο και λιγότερο περιοριστικό ρυθμιστικό πλαίσιο θέτοντας σε προτεραιότητα την τεχνολογική ανάπτυξη έναντι της προστασίας των προσωπικών δεδομένων. Αντιθέτως, σε ενωσιακό επίπεδο, το οποίο θα μας απασχολήσει και στην παρούσα, το Κοινοβούλιο της Ε.Ε. είναι από τα πρωτοπόρα θεσμικά όργανα που έχει απασχοληθεί ιδιαιτέρως με την τεχνολογία και ειδικότερα με την Τεχνητή Νοημοσύνη δημιουργώντας το λεγόμενο Brussels effect. Με άλλα λόγια, ως Brussels Effect, σύμφωνα με την Anu Bradford, νοείται η επιρροή της ΕΕ στο διεθνές επιχειρηματικό περιβάλλον μέσω των κανονισμών που υιοθετεί, η διαμόρφωση παγκόσμιων πολιτικών σε νέα καίρια νομοθετικά κενά, ιδίως όσον αφορά ζητήματα βαθιτεχνολογίας και προσωπικών δεδομένων και ο γενικότερος παγκόσμιος εξευρωπαϊσμός (A. Bradfort, 2019). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων διαδραματίζει καταλυτικό ρόλο για την λειτουργία της Τεχνητής Νοημοσύνης, με του οποίου τις διατάξεις οφείλουν οι εφαρμογές όπως το ChatGPT να συμμορφώνονται αλλά παράλληλα παρουσιάζουν τα περισσότερα συγκρουσιακά σημεία.

2.2. Γλωσσικά μοντέλα τεχνητής νοημοσύνης και προστασία δεδομένων

Το ChatGPT για να εκπαιδευτεί και να αναπτύξει τις δυνατότητες του χρειάζεται «μεγάλα δεδομένα», ήτοι τεράστιο όγκο δεδομένων από οποιαδήποτε πηγή έχει πρόσβαση έχοντας τα κατάλληλα εργαλεία και μεθόδους επεξεργασίας τους, όπως την βαθιά μάθηση. Μεταξύ των μεγάλων δεδομένων που χρησιμοποιεί το ChatGPT βρίσκονται και προσωπικά δεδομένα που συνοδεύονται από σειρά υποχρεώσεων και θεμελιωδών αρχών προστασίας τους.

Επιπλέον, το ChatGPT αποκτά πρόσβαση σε προσωπικά δεδομένα και μέσω της αλληλεπίδρασης με τους χρήστες του. Συγκεκριμένα, θέτοντας ερωτήσεις μέσω του chatbox αποκαλύπτει ο χρήσης πληροφορίες για τον ίδιο του τον εαυτό. Για παράδειγμα, μέσω της των ερωτήσεων το ChatGPT είναι συχνά σε θέση να εντοπίσει το φύλο και την ηλικία του «συνομιλούντος» του, ακόμη και το μορφωτικό του επίπεδο μέσα από ορθογραφικά λάθη ή μέσα από ερωτήσεις για εργασίες που του έχουν ανατεθεί. Μέσω της εν λόγω αλληλεπίδρασης, υπάρχει κίνδυνος αποκάλυψης ακόμη και ευαίσθητων προσωπικών

δεδομένων, όπως για παράδειγμα δεδομένων υγείας. Εάν ένας χρήστης ρωτά για τα συμπτώματα μιας εγκυμοσύνης ή μιας ασθένειας, τότε υπάρχει πιθανότητα να αποκαλυφθεί πως είναι έγκυος ή ασθενής. Η ίδια η OpenAI αναφέρει στην πολιτική απορρήτου της ότι λαμβάνουν αυτόματα δεδομένα των χρηστών από την χρήση που κάνουν μέσω του ChatGPT (Suarez, 2023).

Σημαντικό για την κατανόηση εφαρμογής του ΓΚΠΔ και της αναζήτησης της ευθύνης στα συστήματα τεχνητής νοημοσύνης και δη στα μεγάλα γλωσσικά μοντέλα είναι να δούμε ποιος είναι ο εκάστοτε υπεύθυνος επεξεργασίας των δεδομένων. Σύμφωνα με τον ΓΚΠΔ, υπεύθυνος επεξεργασίας δεδομένων είναι ο οργανισμός ή η νομική οντότητα που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων. Στην περίπτωση του ChatGPT υπεύθυνος επεξεργασίας των δεδομένων είναι η εταιρεία OpenAI που αναπτύσσει και λειτουργεί το μοντέλο και φέρει και την ευθύνη συμμόρφωση με τις διατάξεις του ΓΚΠΔ. Αντίστοιχα, σε κάθε άλλο γλωσσικό μοντέλο τεχνητής νοημοσύνης υπεύθυνος επεξεργασίας ορίζεται η εταιρεία που βρίσκεται πίσω από την ανάπτυξη και λειτουργία του ορίζοντας τον σκοπό επεξεργασίας των δεδομένων.

Στο προηγούμενο κεφάλαιο αναλύθηκε ο βασικός κορμός του ΓΚΠΔ συμπεριλαμβανομένων των θεμελιωδών αρχών επεξεργασίας δεδομένων και των δικαιωμάτων των υποκειμένων. Στο παρόν κεφάλαιο θα λάβει χώρα μια προσπάθεια κατανόησης του τρόπου λειτουργίας των συστημάτων παραγωγικής τεχνητής νοημοσύνης σε συνάρτηση με τον ΓΚΠΔ και τις συγκρούσεις που αναδύονται μέσα από αυτή την σχέση. Το ChatGPT και οι παρόμοιες τεχνολογίες τεχνητής νοημοσύνης εγείρουν σοβαρά ζητήματα σχετικά με την ιδιωτικότητα και την προστασία προσωπικών δεδομένων.

Σύμφωνα με την αρχής της νομιμότητας, με σκοπό να είναι σύννομη θα πρέπει να υπάρχει μια νόμιμη βάση επεξεργασίας των δεδομένων από τον εξαντλητικό κατάλογο που προβλέπει ο ΓΚΠΔ και παρατέθηκε ανωτέρω. Η νόμιμη βάση εξαρτάται από τον σκοπό για τον οποίο χρησιμοποιείται το ChatGPT ή το εκάστοτε γλωσσικό μοντέλο καθώς και από το ποιος το χρησιμοποιεί. Σύμφωνα με την OpenAI, την εταιρεία που κυκλοφόρησε το ChatGPT, η νομική βάση επεξεργασίας που επικαλείται για τα δεδομένα που επεξεργάζεται είναι το έννομο συμφέρον για την τεχνολογική ανάπτυξη της εφαρμογής.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων κατόπιν σχετικού αιτήματος της Ιρλανδικής Αρχής Προστασίας Δεδομένων δημοσίευσε στις 18 Δεκεμβρίου του 2024 την υπ' αριθμό 28 γνώμη αναφορικά με ορισμένες πτυχές της προστασίας δεδομένων που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο μοντέλων ΤΝ. Μεταξύ άλλων ζητήθηκε γνώμη για το πως μπορεί ο Υπεύθυνος Επεξεργασίας Προσωπικών Δεδομένων να αποδείξει την καταλληλόλητα του εννόμου συμφέροντος ως νόμιμη βάση επεξεργασίας τόσο κατά το στάδιο της ανάπτυξης του μοντέλου όσο και το στάδιο λειτουργίας του.

Με δεδομένο ότι ο Υπεύθυνος Επεξεργασίας μπορεί να επιλέξει οποιαδήποτε νόμιμη βάση του άρθρου 6 του ΓΚΠΔ, χωρίς να απαιτείται να ακολουθήσει κάποια προβλεπόμενη ιεραρχία, το έννομο συμφέρον θα μπορούσε να αποτελέσει τη νόμιμη βάση επεξεργασίας για μοντέλα τεχνητής νοημοσύνης, όπως και του Chat GPT, αρκεί να πληρούνται ορισμένες προϋποθέσεις. Για να διαπιστωθεί το έννομο συμφέρον μπορεί να τεκμηριωθεί κατάλληλα ως νόμιμη βάση, θα πρέπει να διενεργηθεί ένα τεστ τριών βημάτων, το οποίο υπενθυμίζει το Συμβούλιο στην εν λόγω γνώμη. Θα πρέπει να διαπιστωθεί εάν πληρούνται οι εξής τρείς σωρευτικές προϋποθέσεις: α) η επιδίωξη έννομου συμφέροντος από τον υπεύθυνο επεξεργασίας ή από τρίτο, β) η επεξεργασία να είναι απαραίτητη για την επιδίωξη του έννομου συμφέροντος και γ) το έννομο συμφέρον δεν υπερισχύει των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων (Γνώμη 28/2024). Η εξέταση των παραπάνω κριτηρίων θα πρέπει να εφαρμόζεται ανά περίπτωση χωρίς να υπάρχει δυνατότητα να βασιστούμε σε μια εξαντλητική κατηγοριοποίηση επεξεργασιών που μπορούν να πραγματοποιηθούν βάσει εννόμου συμφέροντος.

Βάσει των κατευθυντήριων γραμμών σε σχέση με το έννομο συμφέρον (Κατευθυντήριες 1/2024), το έννομο συμφέρον θα πρέπει να είναι νόμιμο, να διατυπώνεται με σαφήνεια και ακρίβεια και να είναι πραγματικό και υπάρχον – όχι υποθετικό-. Εφόσον διαπιστωθούν τα εν λόγω χαρακτηριστικά του εννόμου συμφέροντος, θα πρέπει να διενεργηθεί ένα τεστ αναγκαιότητας ("necessity test") και να εξετασθεί εάν υφίσταται ηπιότερος τρόπος επίτευξης του σκοπού που επιδιώκεται. Εάν για παράδειγμα ο σκοπός θα μπορούσε να επιτευχθεί και από άλλο μοντέλο ΤΝ που δεν προβαίνει σε επεξεργασία προσωπικών

δεδομένων, το τεστ αναγκαιότητας θα ήταν αποτυχημένο. Τελευταίο βήμα στην εξέταση του εννόμου συμφέροντος ως κατάλληλη νόμιμη βάση αποτελεί η αξιολόγηση του υπό το πρίσμα της αρχής της αναλογικότητας. Ειδικότερα, θα πρέπει να εξετασθεί εάν το έννομο συμφέρον υπερισχύει των συμφερόντων και των θεμελιωδών δικαιωμάτων των υποκειμένων των δεδομένων ("balancing test"). Για να αξιολογηθεί με ακρίβεια τι υπερισχύει, θα πρέπει να εξετασθεί ανά περίπτωση ποιες είναι οι επιπτώσεις της επεξεργασίας στα υποκείμενα, είτε πρόκειται για θετικές είτε για αρνητικές επιπτώσεις.

Μεταξύ άλλων, τα σημαντικότερα θεμελιώδη δικαιώματα, τα οποία κινδυνεύουν με παραβίαση κατά την επεξεργασία προσωπικών δεδομένων από μοντέλα ΤΝ, είναι το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής (αρ. 7 ΧΘΔΕΕ) αλλά και το δικαίωμα στην προστασία των προσωπικών δεδομένων (αρ. 8 ΧΘΔΕΕ), δεδομένου ότι τα προσωπικά δεδομένα μπορούν να αντληθούν χωρίς την γνώση και συναίνεση του υποκειμένου (είτε κατά την ανάπτυξη από δημόσιες πηγές όπως το διαδίκτυο είτε κατά την λειτουργία του μοντέλου μέσω παροχής πληροφοριών από το υποκείμενο για άλλο σκοπό π.χ. την συνδρομή του).

Επιπλέον, θα πρέπει οι εύλογες προσδοκίες των υποκειμένων των δεδομένων από την επεξεργασία να εξετάζονται ανά περίπτωση, κάτι που λόγω της πολυπλοκότητας λειτουργίας των μοντέλων ΤΝ φαίνεται δύσκολο να επιτευχθεί. Θα πρέπει να λαμβάνεται υπ' όψιν η φύση των προσωπικών δεδομένων, το πως και από που αντλήθηκαν, η ευρύτερη διαθεσιμότητα τους στο κοινό κ.λπ. Κατά την λειτουργία του μοντέλου, για παράδειγμα του ChatGPT, θα πρέπει ίσως για παράδειγμα να θεωρείται εύλογη προσδοκία του χρήστη ότι τα δεδομένα του θα επεξεργασθούν όταν ο ίδιος τα παρέχει για να λάβει ένα πιο εξειδικευμένο αποτέλεσμα.

Τέλος, ακόμη και σε περίπτωση που θεωρηθεί ότι τα συμφέροντα των υποκειμένων υπερτερούν του εννόμου συμφέροντος, μπορεί ο Υπεύθυνος Επεξεργασίας να υιοθετήσει κατάλληλα τεχνικά και οργανωτικά μέτρα με σκοπό τον μετριασμό του κινδύνου και σε περίπτωση που αυτός μειωθεί στο επίπεδο του αποδεκτού, τότε μπορεί να επικαλεστεί το έννομο συμφέρον ως νόμιμη βάση της επεξεργασίας που διενεργεί.

Αξίζει δε να σημειωθεί ότι το ΔΕΕ έχει κρίνει πως το εμπορικό συμφέρον του Υπευθύνου Επεξεργασίας μπορεί να συνιστά έννομο συμφέρον, εφόσον δεν αντιβαίνει στον νόμο και εναπόκειται στην κρίση του εκάστοτε δικαστηρίου να αποφανθεί εάν υπάρχει έννομο συμφέρον (ΔΕΕ, C-621/22).

Κατά την επικρατούσα γνώμη, εκ των ως άνω νομικών βάσεων η μόνη που βρίσκει έρεισμα γλωσσικό μοντέλο και μπορεί να χρησιμοποιήσει είναι η συγκατάθεση του υποκειμένου. Για την εγκυρότητα της συγκατάθεσης θα πρέπει το υποκείμενο να είναι πλήρως ενημερωμένο για τα δεδομένα που συλλέγονται, τον σκοπό της επεξεργασίας τους και τον υπεύθυνο επεξεργασίας προτού ξεκινήσει η επεξεργασία (Η. Κωστή, 2023). Για την καλύτερη κατανόηση μας θα χρησιμοποιήσουμε ως παράδειγμα γλωσσικού μοντέλου τεχνητής νοημοσύνης το ChatGPT. Το ChatGPT λαμβάνει δεδομένα από ποικίλες πηγές κυρίως δημόσιες χωρίς να ενημερώνεται το ίδιο το υποκείμενο ότι τα δεδομένα του θα χρησιμοποιηθούν για την εκπαίδευση της εφαρμογής. Ακολούθως, το ChatGPT επεξεργάζεται αδιαλείπτως τα δεδομένα που έχει συλλέξει, δημιουργώντας «αόρατους», μη επεξηγήσιμους συσχετισμούς μεταξύ των δεδομένων και επανακαθορίζοντας έκαστη φορά τον σκοπό επεξεργασίας ανάλογα με την εντολή που έχει λάβει και παραβιάζοντας την αρχή περιορισμού του σκοπού (ICO, version 2.2.).

Το δικαίωμα ενημέρωσης φαίνεται να είναι δυσανάλογο στα πλαίσια λειτουργίας του ChatGPT, δεδομένου του όγκου των δεδομένων και της ταχύτητας επεξεργασίας τους, καθώς θα λειτουργούσε ως τροχοπέδη στην λειτουργία του με αποτέλεσμα να είναι δυσχερής ίσως και αδύνατη η λήψη έγκυρης συγκατάθεσης από το υποκείμενο. Δεδομένου ότι τα περισσότερα δεδομένα που λαμβάνει το ChatGPT προέρχονται από δημόσια διαθέσιμες πηγές και κυρίως από το διαδίκτυο πρέπει να αποσαφηνιστεί ότι ακόμα τα ανοικτά μεγάλα δεδομένα (open big data) μπορούν να προκύψουν προσωπικά δεδομένα, τα οποία προστατεύονται από τις διατάξεις του ΓΚΠΔ με αποτέλεσμα την υποχρεωτική τήρηση όλων των προϋποθέσεων για την νόμιμη επεξεργασία τους, μεταξύ άλλων και της έγκυρης συγκατάθεσης. Κάθε ακριβής πληροφορία για ένα πρόσωπο που δημοσιοποιείται επηρεάζει αναγκαστικά το δικαίωμα πληροφοριακής αυτοδιάθεσης και άρα οφείλει να τηρεί το ισχύον νομοθετικό πλαίσιο διαφορετικά υπάρχει κίνδυνος παραβίασης της ιδιωτικότητας των

υποκειμένων. Μια προτεινόμενη λύση για την λήψη συγκατάθεσης στο ψηφιακό περιβάλλον είναι η χρήση της τεχνητής νοημοσύνης για να προβλεφθεί σε ποιες πρακτικές επεξεργασίας θα συναινούσε το υποκείμενο και τα αποτελέσματα αυτής της πρόβλεψης να κοινοποιούνται σε εφαρμογές όπως το ChatGPT, ώστε να οριοθετείται αντίστοιχα η εκάστοτε επεξεργασία(M. Jones, E. Kaufman, E. Edenberg, 2018).

Υποστηρίζεται ότι η επεξεργασία προσωπικών δεδομένων από το ChatGPT δύναται να βασιστεί στην εξαίρεση που θέτει το άρθρο 89 του ΓΚΠΔ για σκοπούς επιστημονικής έρευνας και να μην απαιτείται συγκατάθεση του υποκειμένου, υπό την προϋπόθεση θέσπισης τεχνικών και οργανωτικών μέτρων. Η εφαρμογή όμως του άρθρου 89 του ΓΚΠΔ αμφισβητείται σύμφωνα με τον εμπορικό χαρακτήρα που έχουν αποκτήσει εφαρμογές όπως το ChatGPT. Αρχικώς, μπορούσε να θεωρηθεί πως η επεξεργασία των δεδομένων συμβάλει στην έρευνα και ανάπτυξη της τεχνολογίας, πλέον όμως υφίστανται συνδρομές για την χρήση προηγμένων ειδών του ChatGPT χωρίς περιορισμούς. Επιπλέον, άλλος ένας δυνατός τρόπος επεξεργασίας προσωπικών δεδομένων από το ChatGPT είναι η πλήρης ανωνυμοποίηση των δεδομένων λαμβάνοντας υπόψη ότι τα ανώνυμα δεδομένα δεν υπόκεινται στο πεδίο εφαρμογής του ΓΚΠΔ. Πόσο εύκολή είναι, όμως, η ανωνυμοποίηση των δεδομένων με στόχο να μη μπορούν να ταυτοποιηθούν τα υποκείμενα; Ο καθηγητής Matt Blaze, ο οποίος ειδικεύεται στον τομέα της κρυπτογραφίας και της προστασίας των δεδομένων, έγραψε επιγραμματικά: «κάτι που φαίνεται ανώνυμο, τις περισσότερες φορές, δεν είναι ανώνυμο, ακόμα κι αν έχει σχεδιαστεί με τις καλύτερες προθέσεις.». Στην πράξη, για την ανωνυμοποίηση απαιτείται η αφαίρεση, όχι μόνο των αναγνωρίσιμων στοιχείων των υποκειμένων, αλλά και των πληροφοριών που μπορούν να ταυτοποιήσουν ένα φυσικό πρόσωπο, όταν συνδυαστούν με άλλες γνωστές πληροφορίες για αυτό (Γ. Θεοδωρίδου, 2024).

Το υποκείμενο των δεδομένων που έχει συναινέσει στην επεξεργασία των προσωπικών του δεδομένων έχει οποτεδήποτε δικαίωμα ανάκλησης της συγκατάθεσης και διαγραφής δεδομένων του. Στην πράξη η διαγραφή δεδομένων αποτελεί κίνδυνο για την ανάπτυξη της τεχνητής νοημοσύνης και την λειτουργία εφαρμογών όπως το ChatGPT, καθώς θα πρέπει να διασφαλίζεται ότι η διαγραφή των δεδομένων δεν επηρεάζει την αντιπροσωπευτικότητα του συνόλου. Η πλήρης διαγραφή δεδομένων από το ChatGPT φαίνεται να είναι αδύνατη,

καθώς έχει ήδη κατά την ανάπτυξη και εκπαίδευση του χρησιμοποιήσει τα εν λόγω δεδομένα και δεν μπορεί να τα «ξεχάσει». Η τεχνητή νοημοσύνη λειτουργεί κατά τον ίδιο τρόπο με την ανθρώπινη νοημοσύνη, με άλλα λόγια όπως δεν είναι δυνατόν να διαγράψουμε κατ' αίτημα από την μνήμη ενός ανθρώπου κάτι που γνωρίζει, έτσι δεν είναι δυνατόν να διαγράψουμε από την βάση δεδομένων του ChatGPT γνωστά σε εκείνο δεδομένα. Η OpenAI εισήγαγε στο ChatGPT ένα χαρακτηριστικό ικανό κατ' εκείνη να μετριάσει τον κίνδυνο παραβίασης του δικαιώματος της διαγραφής δεδομένων των υποκειμένων. Δίνεται η δυνατότητα στο χρήστη να απενεργοποιεί το ιστορικό της συνομιλίας του ώστε να μην μπορεί το ChatGPT να αποθηκεύει και να επεξεργάζεται σε δεύτερο χρόνο για την εκπαίδευση του τα προσωπικά δεδομένα που προκύπτουν από την συνομιλία.

Η αρχή της αντικειμενικότητας δύναται να παραβιαστεί εάν αναλογιστεί κανείς ότι τα δεδομένα με τα οποία εκπαιδεύεται το ChatGPT προέρχονται από τα ανοικτά δεδομένα που υπάρχουν σε δημόσιες πηγές, όπου υπάρχουν εγγενείς προκαταλήψεις και στερεότυπα. Αυτές οι προκαταλήψεις μπορούν να εισαχθούν και στα αποτελέσματα που παράγει το γλωσσικό μοντέλο, με αποτέλεσμα την ενίσχυση στερεοτύπων και διακρίσεων σε διάφορα κοινωνικά θέματα, όπως το φύλο, η φυλή, η θρησκεία, και ο σεξουαλικός προσανατολισμός . Αυτή η έλλειψη αντικειμενικότητας μπορεί να οδηγήσει σε μεροληπτικές, μη ακριβείς αποφάσεις που επηρεάζουν πραγματικά άτομα και κοινότητες. Συναφής είναι και η αρχή της ακρίβειας των δεδομένων, η οποία εφαρμόζεται όχι μόνο στα εισαγόμενα στο ChatGPT δεδομένα αλλά και στα δεδομένα που δημιουργεί, διασφαλίζοντας πως και τα δύο είναι ακριβή και ανταποκρίνονται στην πραγματικότητα. Με την γέννηση του ChatGPT πολλοί έσπευσαν να επωφεληθούν από αυτό, μεταξύ των οποίων και πολλοί επαγγελματίες για να διευκολύνουν τις εργασίες τους. Ανάμεσα τους συγκαταλέγεται ένας δικηγόρος στις ΗΠΑ, ο οποίος στα πλαίσια κατάθεσης αγωγής κατά αεροπορικής εταιρείας ζήτησε την συνδρομή του ChatGPT για την εύρεση αντίστοιχης νομολογίας που υποστηρίζει το αιτητικό του και το πρώτο με ευκολία απαρίθμησε έξι σχετικές υποθέσεις με όλες τις αναγκαίες λεπτομέρειες. Η μόνη επαλήθευση στην οποία προέβη ο δικηγόρος ήταν να ρωτήσει το ίδιο το ChatGPT αν οι δικαστικές αποφάσεις που ανέφερε ήταν ψεύτικές με αποτέλεσμα εκείνο να τον διαβεβαιώσει πως είναι πραγματικές και μπορεί να τις βρει σε μεγάλες βάσεις νομολογίας.

Κατά την ακρόαση, όμως, της υπόθεσης προέκυψε ότι η εν λόγω νομολογία ήταν δημιούργημα του ChatGPT με αποτέλεσμα η αγωγή του να απορριφθεί ως αβάσιμη και να αντιμετωπίσει ακόμη και δεοντολογικές κυρώσεις.

Η αρχή της διαφάνειας αποτελεί έναν από τους θεμελιώδεις πυλώνες του ΓΚΠΔ, η οποία υποχρεώνει τους υπευθύνους επεξεργασίας δεδομένων να ενημερώνουν σαφώς και επαρκώς τα υποκείμενα των δεδομένων για το πώς τα προσωπικά τους δεδομένα συλλέγονται, επεξεργάζονται, και χρησιμοποιούνται. Η εφαρμογή αυτής της αρχής στην εποχή της τεχνητής νοημοσύνης και των μεγάλων γλωσσικών μοντέλων, όπως το ChatGPT, εγείρει σοβαρές προκλήσεις, λόγω του άγνωστου «παρασκηνιακού» τρόπου λειτουργίας που εφαρμόζουν. Το λεγόμενο φαινόμενο του «μαύρου κουτιού» (“black box”) περιγράφει την αδιαφάνεια και την έλλειψη κατανόησης γύρω από τον τρόπο με τον οποίο λειτουργούν οι περίπλοκοι αλγόριθμοι τεχνητής νοημοσύνης, οδηγώντας σε δυσκολίες στην ερμηνεία και την εξήγηση των αποτελεσμάτων τους. Ο όρος "μαύρο κουτί" χρησιμοποιείται για να περιγράψει τα περίπλοκα, μη διαφανή συστήματα, όπως οι αλγόριθμοι μηχανικής μάθησης, τα οποία παράγουν αποτελέσματα χωρίς να είναι σαφές το πώς ακριβώς φτάνουν σε αυτά τα αποτελέσματα. Στην περίπτωση των γλωσσικών μοντέλων, όπως το ChatGPT, το μοντέλο εκπαιδεύεται σε τεράστια σύνολα δεδομένων και αναπτύσσει πολύπλοκες σχέσεις μεταξύ των δεδομένων αυτών, ενώ αναπτύσσει με την πορεία της εκπαίδευσης του μια αυτόνομη συμπεριφορά, καθιστώντας τη διαδικασία παραγωγής των απαντήσεών του σχεδόν ακατανόητη ακόμα και για τους ίδιους τους προγραμματιστές του. Αυτή η έλλειψη διαφάνειας οδηγεί αδιαμφισβήτητα στην παραβίαση των διατάξεων του ΓΚΠΔ και της ιδιωτικότητας του υποκειμένου, καθώς δεν μπορούν να γνωρίζουν με ακρίβεια πώς χρησιμοποιούνται τα δεδομένα τους ή πώς λαμβάνονται οι αποφάσεις που επηρεάζουν τις ζωές τους. Η αρχή της διαφάνειας αλλά και η υποχρέωση λογοδοσίας απαιτεί από τους υπεύθυνους επεξεργασίας να παρέχουν σαφείς και κατανοητές πληροφορίες στα υποκείμενα των δεδομένων σχετικά με τη φύση και τους σκοπούς της επεξεργασίας των προσωπικών τους δεδομένων. Ωστόσο, στην περίπτωση των γλωσσικών μοντέλων, αυτή η απαίτηση μπορεί να είναι δύσκολα εφαρμόσιμη, καθώς οι πολύπλοκοι αλγόριθμοι είναι δύσκολο να εξηγηθούν με απλούς όρους. Οι υπεύθυνοι επεξεργασίας μπορεί να

δυσκολευτούν να εκπληρώσουν τις υποχρεώσεις τους, όπως η παροχή ενημέρωσης σχετικά με τη λογική που ακολουθείται στην επεξεργασία των δεδομένων και η διασφάλιση ότι οι πληροφορίες είναι εύκολα προσβάσιμες και κατανοητές.

Η αρχή της ελαχιστοποίησης των δεδομένων φαίνεται να είναι έννοια εντελώς αντίθετη από το ChatGPT και τα παρόμοια του μοντέλα. Εξ ορισμού με όσα περισσότερα δεδομένα τροφοδοτείται το ChatGPT τόσο καλύτερο γίνεται και τόσο βελτιώνονται τα αποτελέσματα του. Είναι πρακτικά αδύνατο ένα γλωσσικό μοντέλο τεχνητής νοημοσύνης να συλλέγει μόνο τα ακριβή, συναφή και αναγκαία προσωπικά δεδομένα που θα επαρκούν για την επίτευξη του επιδιωκόμενου σκοπού (Butterworth, 2018).

Η αρχή του περιορισμού του χρόνου αποθήκευσης των δεδομένων σχετίζεται άμεσα με τον σκοπό για τον οποίο συλλέγονται και επεξεργάζονται τα δεδομένα. Τα προσωπικά δεδομένα θα πρέπει να αποθηκεύονται για συγκεκριμένο χρονικό διάστημα και δη για όσο απαιτείται για την ολοκλήρωση του σκοπού. Το παραπάνω έρχεται σε αντίθεση με τον τρόπο λειτουργίας του ChatGPT, το οποίο όχι μόνο διατηρεί τα δεδομένα αποθηκευμένα για μεγάλο χρονικό διάστημα θέτοντας τα στο παρασκήνιο με την απόκτηση ακόμη νεότερων δεδομένων χωρίς να τα διαγράφει, αλλά τα χρησιμοποιεί εκ νέου όποτε τα χρειάζεται επανακαθορίζοντας τον σκοπό επεξεργασίας.

2.3. Τρόποι συμμόρφωσης της τεχνητής νοημοσύνης με το πλαίσιο προστασίας των προσωπικών δεδομένων και μετρίασης των κινδύνων

Κύριο σημείο του ΓΚΠΔ και βασική υποχρέωση που επιβάλλεται στον εκάστοτε υπεύθυνο επεξεργασίας είναι η δημιουργία προϊόντων με γνώμονα τις διατάξεις περί προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων, ήτοι τα λεγόμενα «Privacy by design» και «Privacy by default». Με το privacy by design (προστασία δεδομένων εκ του σχεδιασμού) υποστηρίζεται η ενσωμάτωση χαρακτηριστικών προστασίας της ιδιωτικής ζωής και των προσωπικών δεδομένων από τον σχεδιασμό και την ανάπτυξη ενός συστήματος που επεξεργάζονται δεδομένα. Με αυτόν τον τρόπο τονίζεται η σημασία της πρόληψης με στόχο την πρόβλεψη τυχόν ζητημάτων παραβίασης του ΓΚΠΔ και άλλων διατάξεων προστασίας

της ιδιωτικής ζωής και την ανεύρεση εκ των προτέρων τρόπων αντιμετώπισης των ανακυπτόντων προβλημάτων έναντι της εκ των υστέρων ξαφνικής αντιμετώπισης τους. Η εφαρμογή της προσέγγισης αυτής στα συστήματα παραγωγικής τεχνητής νοημοσύνης και δη στα γλωσσικά μοντέλα που απασχολούν ιδιαιτέρως τον νομικό κόσμο διασφαλίζει ότι η προστασία των θεμελιωδών δικαιωμάτων του ανθρώπου, μεταξύ των οποίων η προστασία των προσωπικών δεδομένων, ενσωματώνεται στην εφαρμογή από τον σχεδιασμό και την υλοποίηση του, διευκολύνοντας την αυτόματη και με φυσικό τρόπο συμμόρφωση με το ισχύον νομοθετικό πλαίσιο καθ' όλη τη διάρκεια του κύκλου ζωής της εκάστοτε εφαρμογής τεχνητής νοημοσύνης/γλωσσικού μοντέλου. Τρόποι υλοποίησης της προστασία ήδη από τον σχεδιασμό («by design») θα μπορούσε να είναι η ανωνυμοποίηση ή ψευδωνυμοποίηση των προσωπικών δεδομένων ή κρυπτογράφηση τους, ώστε να μην είναι δυνατή η διαρροή τους και η προσβολή της ιδιωτικότητας ενός υποκειμένου.

Συναφής έννοια είναι το «privacy by default» (προστασία δεδομένων εξ ορισμού), η οποία σχετίζεται με την εγκατάσταση οργανωτικών και τεχνικών ρυθμίσεων στα σχετικά προϊόντα επεξεργασίας προσωπικών δεδομένων, όπως το ChatGPT, που συμμορφώνονται πλήρως με το ισχύον νομοθετικό πλαίσιο. Τα οργανωτικά και τεχνολογικά μέτρα προστασίας των προσωπικών δεδομένων οφείλουν να ενσωματώνονται από τον σχεδιασμό του αντίστοιχου προϊόντος / συστήματος με αποτέλεσμα αυτό να λειτουργεί εξ ορισμού σύννομα χωρίς την ανάγκη ανθρώπινης παρέμβασης.

Για παράδειγμα, οι ρυθμίσεις του ChatGPT θα πρέπει να διαμορφώνονται με τρόπο που διασφαλίζει την τήρηση των θεμελιωδών αρχών του ΓΚΠΔ και την προστασία του υποκειμένου των δεδομένων. Όταν ολοκληρώνεται ο σκοπός για τον οποίο υποβλήθηκαν σε επεξεργασία σειρά δεδομένων τότε το ChatGPT ή κάθε άλλο προϊόν επεξεργασίας προσωπικών δεδομένων θα πρέπει να διαγράφει τα εν λόγω δεδομένα, τηρουμένων των όσων ορίζει η αρχή της ελαχιστοποίησης των δεδομένων και η αρχή περιορισμού του σκοπού. Η λήθη των δεδομένων που χρησιμοποιήθηκαν προτείνεται ως μια λύση αλλά παράλληλα προβληματίζει το πως θα μπορέσει μια επεξεργασία να αιτιολογηθεί εκ των υστέρων, εάν αυτό απαιτηθεί (Mantelero, 2018).

Ένας περαιτέρω τρόπος αποτροπής κινδύνων κατά την χρήση συστημάτων παραγωγικής τεχνητής νοημοσύνης είναι η αυτόματη ψευδωνυμοποίηση ή ακόμη και ανωνυμοποίηση των δεδομένων από το σύστημα προτού προχωρήσει στην περαιτέρω επεξεργασία τους αποσκοπώντας στην μη ταυτοποίηση των υποκειμένων και την προστασία της ιδιωτικότητας τους.

Επιπλέον, ανάμεσα στα τεχνικά και οργανωτικά μέτρα που πρέπει να εγκατασταθούν σε γλωσσικά μοντέλα μαζικής επεξεργασίας προσωπικών δεδομένων είναι μέτρα κυβερνοασφάλειας για την αποφυγή παραβίασης δεδομένων, ήτοι συμβάντος ασφαλείας που έχει ως αποτέλεσμα την παραβίαση του απορρήτου και την προσβολή της ιδιωτικής ζωής του υποκειμένου.

Το νομοθετικό πλαίσιο γύρω από την τεχνητή νοημοσύνη και τα προσωπικά δεδομένα παροτρύνει τους ιδιώτες και κυρίως τους παρόχους εφαρμογών τεχνητής νοημοσύνης, όπως είναι η OpenAI να υιοθετούν κείμενα, πολιτικές και κανόνες δεοντολογίας που προαγάγουν την προστασία των προσωπικών δεδομένων. Μέσα από την περιγραφή του αρχικού σχεδιασμού τους, των ρυθμίσεων, της λειτουργίας και των αρχών που τηρούν τα συστήματα τεχνητής νοημοσύνης προκύπτει η ορθή και σύννομη συλλογή, επεξεργασία και χρήση των προσωπικών δεδομένων που συμβάλλουν στην εκπαίδευση τους. Στα εν λόγω κείμενα θα πρέπει να ορίζεται ο σκοπός επεξεργασίας των δεδομένων, ο τρόπος συλλογής τους, ο υπεύθυνος επεξεργασίας τους, η περίοδος διατήρησης τους, καθώς και κάθε άλλη σημαντική πληροφορία στην οποία πρέπει να έχει πρόσβαση ο χρήστης του συστήματος και δυνητικό υποκείμενο δεδομένων. Μέσω των ως άνω κειμένων ενισχύεται και η διαφάνεια του αλγορίθμου, δεδομένου ότι το υποκείμενο ανατρέχοντας σε αυτά θα είναι σε θέση να αντιληφθεί ολόκληρη την διαδικασία επεξεργασίας των προσωπικών τους δεδομένων ενώ ο αλγόριθμος θα πρέπει να είναι σε θέση να αιτιολογεί την απόφαση του βάσει των ως άνω διαδικασιών που προβλέπει. Επιπροσθέτως, με τον σαφή ορισμό του υπευθύνου επεξεργασίας το υποκείμενο μπορεί να αισθανθεί την απαιτούμενη ασφάλεια έναντι της τεχνητής νοημοσύνης, καθώς γνωρίζει που μπορεί να απευθυνθεί για την ικανοποίηση των δικαιωμάτων του.

Η OpenAI και οι αντίστοιχες με αυτή εταιρείες οφείλουν να αναπτύσσουν και να θέτουν σε λειτουργία συστήματα αυτόματου εντοπισμού κινδύνων με την βοήθεια και πάλι της τεχνητής νοημοσύνης. Ο αλγόριθμος θα πρέπει να εκπαιδευτεί να εντοπίζει ψευδή ή παραπλανητικά δεδομένα και να τα εκτοπίζει. Ο τρόπος με τον οποίο αυτό μπορεί να γίνει είναι η τροφοδότηση του ChatGPT με ψευδή, παραπλανητικά, ρατσιστικά κ.α. δεδομένα αποσκοπώντας στην αναγνώριση του μοτίβου και την εκπαίδευση του να αντιμετωπίζει αντίστοιχα μοτίβα στα δεδομένα που λαμβάνει και να μην τα χρησιμοποιεί. Έτσι, επιτυγχάνεται ένα υψηλό επίπεδο ακρίβειας και ακεραιότητας των δεδομένων με τα οποία εκπαιδεύεται ο αλγόριθμος.

Αξίζει να σημειωθεί πως για μια ασφαλή τεχνητή νοημοσύνη θα πρέπει να αποφεύγονται οι διαδικασίες εξ ολοκλήρου αυτοματοποιημένης λήψης αποφάσεων και να διασφαλίζεται η ανθρώπινη παρέμβαση, όπως αυτή προβλέπεται τόσο στον Κανονισμό για την τεχνητή νοημοσύνη όσο και στον ΓΚΠΔ. Σκοπός της ανθρώπινης εποπτείας είναι η πρόληψη και ελαχιστοποίηση των κινδύνων για την ασφάλεια και τα θεμελιώδη ανθρώπινα δικαιώματα και η επέμβαση σε όποιο σημείο θεωρεί ότι η τεχνητή νοημοσύνη οδεύει προς την παραβίαση αυτών.

Ένα επιπλέον εργαλείο μετριασμού των κινδύνων που δημιουργεί η τεχνητή νοημοσύνη είναι η Μελέτη Εκτίμησης Αντικτύπου για την προστασία των προσωπικών δεδομένων («ΕΑΠΔ», «Data Processing Impact Assessment (DPIA)"), η οποία θα πρέπει, σύμφωνα με το άρθρο 35 του ΓΚΠΔ, να διενεργείται όταν πραγματοποιούνται πράξεις επεξεργασίας που έχουν ως αποτέλεσμα υψηλό κίνδυνο. Η διενέργεια της ΕΑΠΔ διασφαλίζει την πλήρωση της αρχής της λογοδοσίας αποδεικνύοντας την λήψη των μέτρων που προέβλεψε ο υπεύθυνος επεξεργασίας για την συμμόρφωση της πράξης επεξεργασίας με τον ΓΚΠΔ. Με την Απόφαση 65/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) δημοσιεύθηκε ο ενδεικτικός κατάλογος με είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργειας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων. Ανάμεσα στις εν λόγω πράξεις συγκαταλέγονται οι εφαρμογές τεχνητής νοημοσύνης (Ν. Θεογνώστου, 2023). Οι πάροχοι εφαρμογών τεχνητής νοημοσύνης, όπως η OpenAI, οφείλουν να διενεργούν ΕΑΠΔ για τις εν λόγω εφαρμογές που θέτουν σε σοβαρό κίνδυνο τα

δικαιώματα και τις ελευθερίες των ατόμων με στόχο εντοπισμό και τον μετριασμό των πιθανών κινδύνων για την προστασία των δεδομένων πριν από την ανάπτυξη συστημάτων και θέση σε λειτουργία αυτών. Κάθε φορά, λοιπόν, που αναπτύσσεται μια εφαρμογή τεχνητής νοημοσύνης ή ένα γλωσσικό μοντέλο, ο δημιουργός του οφείλει να διορίζει έναν υπεύθυνο προστασίας δεδομένων (Data Protection Officer – DPO), ο οποίος μέσω της μεθοδολογίας που θα επιλέξει, θα αποφανθεί για την αξιολόγηση των πιθανών κινδύνων που προκύπτει από την χρήση τους για την ιδιωτική ζωή και τα προσωπικά δεδομένα, θα προτείνει τα απαραίτητα μέτρα για την μείωση του κινδύνου στο επίπεδο του αποδεκτού στην ΕΑΠΔ.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η αναδυόμενη αλγοριθμική εκτίμηση αντικτύπου, η οποία δεν έχει προβλεφθεί σε κάποιο ενωσιακό νομοθέτημα, παρόλα αυτά έχει προβλεφθεί στην εθνική μας νομοθεσία και συγκεκριμένα στο άρθρο 5 του νόμου 4961/2022 ως υποχρέωση για τους φορείς του δημοσίου τομέα που χρησιμοποιούν συστήματα τεχνητής νοημοσύνης (Lawspot, 27.07.20222). Προσδιορίζεται ο σκοπός συλλογής δεδομένων, οι κατηγορίες των δεδομένων, οι δυνατότητες και τα τεχνικά χαρακτηριστικά του αλγορίθμου, οι κίνδυνοι που γεννώνται αλλά και το προσδοκώμενο όφελος. Παρότι η αλγοριθμική εκτίμηση αντικτύπου παραπέμπει στην ΕΑΠΔ του ΓΚΠΔ πρόκειται για δύο διαφορετικές έννοιες με την πρώτη να βρίσκεται ακόμη υπό διαμόρφωση και να εστιάζει στην πολυπλοκότητα ενός αλγορίθμου ενώ εξετάζει το σύνολο του αντικτύπου του σε κάθε τομέα της ζωής χωρίς να ασχολείται αποκλειστικά με την προστασία των δεδομένων.

Σε γενικότερο πλαίσιο, ένα επιπλέον εργαλείο μετριασμού των κινδύνων που προέρχονται από την τεχνητή νοημοσύνη είναι η Εκτίμηση Αντικτύπου στα Θεμελιώδη Δικαιώματα (Fundamental Rights Impact Assessment / "FRIA"), η οποία προβλέπεται στη Κατευθυντήριες Αρχές του Οργανισμού των Ηνωμένων Εθνών για τις Επιχειρήσεις και τα Ανθρώπινα Δικαιώματα. Η ΕΑΠΔ που αναφέρθηκε παραπάνω και προβλέπεται και από τον ΓΚΠΔ εστιάζει εξ ολοκλήρου στο δικαίωμα της προστασίας των δεδομένων, ενώ από την άλλη η FRIA εξετάζει και αξιολογεί καθολικά τους κινδύνους για τα θεμελιώδη δικαιώματα, μεταξύ των οποίων και την ιδιωτικότητα αλλά όχι αποκλειστικά αυτή.

Όσα αναφέρθηκαν στο παρόν κεφάλαιο αποδεικνύουν ότι η τεχνολογική ανάπτυξη μπορεί να βρει απροετοίμαστο τον νομοθέτη και το ισχύον νομοθετικό πλαίσιο αλλά δεν μπορεί να αναπτυχθεί και να λειτουργήσει άνευ ετέρου, καθώς υπάρχουν τεχνολογικά ουδέτερες διατάξεις που εφαρμόζονται σε κάθε περίπτωση και υποχρεώνουν τεχνολογίες όπως το ChatGPT να συμμορφώνεται και να σέβεται την προστασία των προσωπικών δεδομένων.

3. Νομοθετικό πλαίσιο τεχνητής νοημοσύνης

Η προσπάθεια ρύθμισης της τεχνητής νοημοσύνης από την ΕΕ εκκίνησε το 2018 με την δημοσίευση κατευθυντήριων γραμμών για αξιόπιστη τεχνητή νοημοσύνη, έπειτα το 2020 δημοσιεύθηκε η Λευκή Βίβλος με στόχο ένα σύστημα αριστείας και εμπιστοσύνης για την Τεχνητή Νοημοσύνη και κατέληξε στην πρόσφατη δημοσίευση του Κανονισμού για την Τεχνητή Νοημοσύνη με αριθμό 2024/1689 (AI ACT) με την οποία επιδιώκεται η ανάπτυξη και η υιοθέτηση ασφαλούς και αξιόπιστης τεχνητής νοημοσύνης σε ολόκληρη την ενιαία αγορά της ΕΕ τόσο από ιδιωτικούς όσο και από δημόσιους φορείς.

3.1. Κατευθυντήριες Γραμμές Δεοντολογίας για Αξιόπιστη Τεχνητή Νοημοσύνη

Αμέσως μετά την δημοσίευση της Ευρωπαϊκής στρατηγικής για την Τεχνητή Νοημοσύνη, η Ευρωπαϊκή Επιτροπή τον Ιούνιο του 2018 διόρισε μια ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη (HLEG), η οποία σκοπό είχε την δημοσίευση κατευθυντήριων δεοντολογιών για την ανάπτυξη και την χρήση τεχνητής νοημοσύνης. Οι «κατευθυντήριες γραμμές δεοντολογίας για την αξιόπιστη τεχνητή νοημοσύνη» δημοσιεύθηκαν οριστικά μετά από ένα έτος, το 2019, με στόχο την προαγωγή της αξιοπιστίας στην τεχνητή νοημοσύνη και βασικό γνώμονα την επίτευξη της συμμόρφωσης της τεχνητής νοημοσύνης με τα θεμελιώδη ανθρώπινα δικαιώματα, όπως αυτά θεσπίζονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ (Χάρτης της ΕΕ) και στο συναφές διεθνές δίκαιο των ανθρωπίνων δικαιωμάτων. Οι κατευθυντήριες γραμμές δεν αποτελούν νομικά δεσμευτικό κείμενο αλλά αποσκοπούν στη δημιουργία μιας οριζόντιας βάσης ρυθμίσεων για τους

προγραμματιστές της τεχνητής νοημοσύνης. Η ομάδα υποστήριξε πως τα συστήματα τεχνητής νοημοσύνης για να μπορέσουν να λειτουργήσουν με τρόπο ευνοϊκό προς το σύνολο θα πρέπει να είναι ανθρωποκεντρικά, να τίθενται δηλαδή στη διάθεση της ανθρωπότητας και του κοινού λαού με στόχο τη βελτίωση της ευημερίας του και της ελευθερίας του (Κατευθυντήριες Γραμμές, σελ 5).

Η αξιοπιστία της τεχνητής νοημοσύνης βασίζεται σε τρεις συνιστώσες, οι οποίες θα πρέπει να πληρούνται από τα συστήματα τεχνητής νοημοσύνης καθ' όλη τη διάρκεια της ζωής τους από τον σχεδιασμό έως την χρήση τους ταυτόχρονα και οι τρεις, καθώς η μια συμπληρώνει την άλλη και σε περίπτωση που δεν συνυπάρχουν δεν επιτυγχάνεται η αξιοπιστία (Φ. Παναγοπούλου Κουτνατζή, 2023). Συγκεκριμένα, κατά τους εμπειρογνώμονες η τεχνητή νοημοσύνη θα πρέπει να είναι σύννομη, δεοντολογική και στιβαρή.

Ως «σύννομη» θεωρείται η συμμόρφωση της τεχνητής νοημοσύνης με το σύνολο του ισχύοντος νομοθετικού πλαισίου. Τα συστήματα τεχνητής νοημοσύνης θα πρέπει να τηρούν κάθε δεσμευτικό κανόνα σε εθνικό, ευρωπαϊκό και διεθνές επίπεδο που σχετίζεται με την λειτουργία τους. Ενδεικτικά ως δεσμευτικοί κανόνες νοούνται το πρωτογενές δίκαιο της ΕΕ (οι συνθήκες της Ευρωπαϊκής Ένωσης και ο Χάρτης Θεμελιωδών Δικαιωμάτων της), το παράγωγο δίκαιο της ΕΕ (όπως ο γενικός κανονισμός για την προστασία δεδομένων, οι οδηγίες κατά των διακρίσεων, η οδηγία για τα μηχανήματα, η οδηγία για την ευθύνη λόγω ελαττωματικών προϊόντων, ο κανονισμός για την ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα, το δίκαιο σε θέματα προστασίας των καταναλωτών και οι οδηγίες για την ασφάλεια και την υγεία κατά την εργασία), αλλά και οι συνθήκες του ΟΗΕ για τα ανθρώπινα δικαιώματα και οι συμβάσεις του Συμβουλίου της Ευρώπης (όπως η Ευρωπαϊκή Σύμβαση ανθρωπίνων δικαιωμάτων) και πολυάριθμοι νόμοι των κρατών μελών της ΕΕ (Κατευθυντήριες Γραμμές, σελ. 8).

Ακολούθως, η τεχνητή νοημοσύνη, σύμφωνα με τη δεύτερη συνιστώσα αξιοπιστίας που προβλέπουν οι Κατευθυντήριες γραμμές, θα πρέπει να είναι δεοντολογική, ήτοι να συμμορφώνεται με δεοντολογικές αρχές και αξίες. Δεν αρκεί επομένως η συμμόρφωση με τα νομοθετικά κείμενα αλλά απαιτείται η τεχνητή νοημοσύνη να συμβαδίζει και με τις

ηθικές αρχές και τους κώδικες δεοντολογίας που εφαρμόζονται βάσει τοπικής αρμοδιότητας. Τέσσερις βασικές δεοντολογικές αρχές που πρέπει να εφαρμόζονται και αναφέρονται αυτούσιες στις κατευθυντήριες είναι η αρχή του σεβασμού της ανθρώπινης αυτονομίας, η αρχή της πρόληψης της βλάβης, η αρχή της δικαιοσύνης και η αρχής της επεξηγησιμότητας.

Τέλος, όσον αφορά την τρίτη συνιστώσα αξιοπιστίας, η τεχνητή νοημοσύνη θα πρέπει να είναι στιβαρή τόσο από τεχνικής πλευράς όσο και από κοινωνικής. Θα πρέπει, δηλαδή, να προσδίδουν την βεβαιότητα στους χρήστες τους ότι έχουν ληφθεί τα κατάλληλα τεχνικά και οργανωτικά μέτρα και έχουν εφαρμοσθεί οι απαραίτητες ασφαλιστικές δικλείδες για την αποφυγή, την πρόληψη αλλά και την αντιμετώπιση κάθε βλάβης στον άνθρωπο από το σύστημα τεχνητής νοημοσύνης, ακόμη και ακούσιας.

Η διασφάλιση της αξιοπιστίας εξαρτάται από τους προγραμματιστές, οι οποίοι είναι υπεύθυνοι για τον σχεδιασμό του συστήματος, από τους εγκαταστάτες οι οποίοι πρέπει να διασφαλίζουν ότι πληρούνται οι απαιτήσεις για την αξιοπιστία τους συστήματος, αλλά και οι τελικοί χρήστες του συστήματος, οι οποίοι μπορούν να εντοπίσουν κατά την λειτουργία του (του συστήματος) ελλείψεις και συνακόλουθα να ζητούν την τήρηση των απαιτήσεων, ενώ θα πρέπει να το χρησιμοποιούν νόμιμα και ηθικά βάσει του συνιστώμενου τρόπου χρήσης. Στο τέλος των κατευθυντηρίων η ομάδα εμπειρογνωμόνων προς διευκόλυνση των επαγγελματιών της τεχνητής νοημοσύνης έχει δημιουργήσει και παραθέτει έναν μη εξαντλητικό κατάλογο αξιολόγησης της αξιοπιστίας της τεχνητής νοημοσύνης, ο οποίος μπορεί να λειτουργήσει συμπληρωματικά στις ήδη υπάρχουσες διαδικασίες αξιολόγησης και να δώσει επιπλέον κατευθύνσεις για την επιχειρησιακή υλοποίηση της αξιοπιστίας.

3.2. Λευκή Βίβλος

Η Ευρωπαϊκή Επιτροπή δημοσίευσε το 19 Φεβρουαρίου 2020 τη Λευκή Βίβλο με τίτλο «Τεχνητή Νοημοσύνη – Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης» με στόχο τη δημιουργία ενός αξιόπιστου και ανθρωποκεντρικού πλαισίου για την ανάπτυξη της τεχνητής νοημοσύνης[12] και την ανάδειξη της Ευρωπαϊκής Ένωσης ως ηγέτιδα δύναμη.

[12] Η Λευκή Βίβλος ορίζει την τεχνητή νοημοσύνη ως ένα σύνολο τεχνολογιών που συνδυάζουν δεδομένα, αλγορίθμους και υπολογιστική ισχύ.

Η Λευκή Βίβλος για την Τεχνητή Νοημοσύνη προτείνει μια στρατηγική για τη δημιουργία ενός «οικοσυστήματος αριστείας και εμπιστοσύνης», στο οποίο η τεχνητή νοημοσύνη θα μπορούσε να αναπτυχθεί με ασφάλεια και διαφάνεια, ενός περιβάλλοντος που η ύπαρξη ρυθμιστικού πλαισίου θα προστατεύει επαρκώς τα θεμελιώδη ανθρώπινα δικαιώματα χωρίς παράλληλα να αποτρέπει τις επενδύσεις για την ανάπτυξη της. Η Λευκή Βίβλος επικεντρώνεται σε δύο κύριους τομείς: την προώθηση της τεχνητής νοημοσύνης και την αντιμετώπιση των κινδύνων που γεννώνται από την λειτουργία της, επιλέγοντας με αυτόν τον τρόπο μια προσέγγιση βάσει κινδύνου (risk-based approach), δηλαδή την κατηγοριοποίηση των κινδύνων και την ρύθμιση της τεχνητής νοημοσύνης σε συνάρτηση με τους κινδύνους που έκαστη εφαρμογή παρουσιάζει (B. Thomas, 2021).

Η Λευκή Βίβλος αναγνωρίζει τη σημασία της τεχνητής νοημοσύνης για την οικονομική ανάπτυξη και την καινοτομία και ξεκινά μάλιστα αναφέροντας πως «θα αλλάξει τη ζωή μας» απαριθμώντας τρόπους με τους οποίους θα την βελτιώσει. Για τον λόγο αυτό, επιδιώκει την ενίσχυση της έρευνας και της ανάπτυξης στον τομέα αυτό, ώστε να μπορεί η τεχνητή νοημοσύνη να καταστεί ωφέλιμη για τους πολίτες, για τις επιχειρήσεις (ακόμη και για τις μικρομεσαίες επιχειρήσεις) αλλά και για το δημόσιο συμφέρον. Παράλληλα, η Λευκή Βίβλος προτείνει τη δημιουργία μια κοινής ευρωπαϊκής προσέγγισης, ώστε να ενισχυθεί η συνεργασία σε ενωσιακό επίπεδο και να αποφευχθεί ο κατακερματισμός της αγοράς.

Παράλληλα, όμως, αναγνωρίζεται η ανάγκη για αυστηρό νομοθετικό πλαίσιο, με έμφαση στην προστασία των θεμελιωδών δικαιωμάτων, όπως η ιδιωτικότητα, η προστασία των δεδομένων, και η ισότητα κ.α. διασφαλίζοντας την ορθή και ασφαλή χρήση της τεχνητής νοημοσύνης. Βασικά εργαλεία για την επίτευξη των παραπάνω, σύμφωνα με όσα ορίζονται στη Λευκή Βίβλο είναι η ενίσχυση της έρευνας και καινοτομίας, η δημιουργία ενός ενιαίου πλαισίου αξιολόγησης κινδύνου, η ενίσχυση της διαφάνειας και η διασφάλιση της ύπαρξης ανθρώπινης εποπτείας κυρίως κατά την λήψη τελικών κρίσιμων αποφάσεων.

Η Λευκή Βίβλος για την τεχνητή νοημοσύνη αποτελεί ένα κρίσιμο έγγραφο καθώς καθόρισε τις βασικές κατευθυντήριες γραμμές για την ανάπτυξη και τη ρύθμιση της τεχνητής νοημοσύνης σε επίπεδο ΕΕ και επεδίωξε να συνδράμει, όπως και έγινε, στην υιοθέτηση ενός δεσμευτικού κανονιστικού συστήματος. Χωρίς ένα σαφές και αυστηρό

ρυθμιστικό πλαίσιο, υπάρχει κίνδυνος η τεχνητή νοημοσύνη να χρησιμοποιηθεί με τρόπους που παραβιάζουν τα δικαιώματα των πολιτών ή να οδηγήσει σε ανεπιθύμητες κοινωνικές συνέπειες.

Στην πράξη, όμως, όπως και για κάθε προσπάθεια ρύθμισης και περιορισμού της τεχνητής νοημοσύνης, έτσι και για την Λευκή Βίβλο μία από τις κύριες προκλήσεις που αναφέρονται είναι η δυσκολία στην εφαρμογή των προτάσεων της λόγω του αποτρεπτικού για την ανάπτυξη χαρακτήρα των ρυθμίσεων που θα επιφέρουν πρόσθετη επιβάρυνση σε πιθανούς επενδυτές. Επιπλέον, η Λευκή Βίβλος προκάλεσε ανησυχίες σχετικά με το αν το πλαίσιο που προτάθηκε ήταν αρκετά ευέλικτο για να προσαρμόζεται στις ταχέως μεταβαλλόμενες τεχνολογικές εξελίξεις.

Η Λευκή Βίβλος για την Τεχνητή Νοημοσύνη αποτέλεσε ένα σημαντικό βήμα προς τη δημιουργία ενός αξιόπιστου και ηθικού πλαισίου για την ανάπτυξη της τεχνητής νοημοσύνης στην Ευρώπη και οδήγησε στην υιοθέτηση της πρόσφατης πράξης για την τεχνητή νοημοσύνη δημιουργώντας και αμφιβολίες για το εάν η ΕΕ στην προσπάθεια της να διασφαλίσει τη νομιμότητα, αποκρούει την ανάπτυξη της τεχνητής νοημοσύνης και τοποθετείται σε μειονεκτική θέση έναντι άλλων δικαιοδοσιών, όπως των ΗΠΑ, που χαρακτηρίζονται από ιδιαίτερη ευελιξία και ανεκτικότητα.

3.3. Κανονισμός για την Τεχνητή Νοημοσύνη

Στις 12 Ιουλίου του 2024, έπειτα από μακροχρόνιες διαβουλεύσεις και σωρεία αλλαγών, δημοσιεύθηκε ο Κανονισμός για την θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη, ο οποίος στα αγγλικά αποδίδεται ως AI ACT, στο επίσημο φύλλο της ΕΕ. Το κείμενο της Πρότασης για την Πράξη ρύθμισης της τεχνητής νοημοσύνης δημοσιεύθηκε τον Απρίλιο του 2021 για τα επόμενα τρία έτη οι διαβουλεύσεις ήταν συνεχείς, επιφέροντας σωρεία αλλαγών στο κείμενο που τελικώς υιοθετήθηκε και θα τεθεί σε σταδιακή εφαρμογή.

Η πρόταση αυτή αποτελεί την πρώτη προσπάθεια της Ευρωπαϊκής Ένωσης με την οποία επιχειρείται μια ισορροπημένη και αναλογική οριζόντια κανονιστική προσέγγιση για την τεχνητή νοημοσύνη, η οποία αναφέροντας τις ελάχιστες απαιτήσεις για την αντιμετώπιση των κινδύνων και των προβλημάτων που συνδέονται με αυτή, προσπαθεί παράλληλα να

μην περιορίζει ούτε και να παρεμποδίζει αδικαιολόγητα την τεχνητή ανάπτυξη και να αυξάνεται το κόστος διάθεσης λύσεων τεχνητής νοημοσύνης στην αγορά. Η επιλογή του Κανονισμού ως μέσου ρύθμισης της τεχνητής νοημοσύνης καταδεικνύει την ανάγκη θέσπισης ενιαίου κανονιστικού πλαισίου και δημιουργίας ενός κοινού μετώπου αντιμετώπισης της τεχνητής νοημοσύνης απ' όλα τα κράτη μέλη. Ο Κανονισμός λαμβάνοντας υπόψη ότι η συντριπτική πλειοψηφία των παρόχων εφαρμογών τεχνητής νοημοσύνης βρίσκεται εκτός των γεωγραφικών ορίων της ΕΕ όρισε ένα ευρύτερο πεδίο εφαρμογής ώστε να καταλαμβάνει κάθε σύστημα τεχνητής νοημοσύνης που επιδρά με οποιονδήποτε τρόπο εντός της ΕΕ, ακόμη και αν η εγκατάσταση του δεν είναι εντός ΕΕ (Μ. Δεληγιάννη, 2021). Ειδικότερα, ο Κανονισμός εφαρμόζεται για κάθε εφαρμογή τεχνητής νοημοσύνης που τίθεται σε λειτουργία και παρέχεται σε χρήστες εντός ΕΕ ή τα στοιχεία εξόδου της χρησιμοποιούνται εντός ΕΕ ανεξαρτήτως της εγκατάστασης του παρόχου της[13]. Εξαιρούνται από το πεδίο εφαρμογής του Κανονισμού τα συστήματα τεχνητής νοημοσύνης που χρησιμοποιούνται για στρατιωτικούς, αμυντικούς και ερευνητικούς σκοπούς.

Ο Κανονισμός θέτει «κανόνες» στην χρήση της τεχνητής νοημοσύνης με γνώμονα την ανθρωποκεντρική προσέγγιση τάσσοντας την χρήση της τεχνητής νοημοσύνης στην διάθεση της κοινής ευημερίας, όπως και ο ίδιος αναφέρει στο προοίμιο του.

Επιπλέον, το κείμενο του Κανονισμού διαμορφώθηκε σύμφωνα με τον προπομπό του, την Λευκή Βίβλο, υιοθετώντας την προσέγγιση βάσει κινδύνου (risk-based approach) που δημιουργούν για τα θεμελιώδη ανθρώπινα δικαιώματα και την κατηγοριοποίηση των συστημάτων τεχνητής νοημοσύνης σε τέσσερις κατηγορίες κινδύνου, τον ελάχιστο, τον περιορισμένο, τον υψηλό και τον μη αποδεκτό κίνδυνο. Οι ρυθμίσεις που θεσμοθετεί για κάθε κατηγορία κινδύνου είναι διαφορετικές, εστιάζοντας την προσοχή του στην κατηγορία υψηλού κινδύνου καθώς τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου είναι αυτά που είναι πιθανότερο να παραβιάσουν τα ανθρώπινα δικαιώματα και ιδίως την προστασία δεδομένων προσωπικού χαρακτήρα (The EAPIL blog, 2021).

[13] Άρθρο 2 Κανονισμού (ΕΕ) 2024/1689

Όπως γίνεται κατανοητό και από την ορολογία του, τα συστήματα μη αποδεκτού κινδύνου δημιουργούν τόσο σημαντικό κίνδυνο για τα θεμελιώδη ανθρώπινα δικαιώματα ώστε η χρήση τους να θεωρείται απαράδεκτη. Το άρθρο 5 του Κανονισμού ορίζει ως απαγορευμένες τεχνικές της τεχνητής νοημοσύνης μεταξύ άλλων τεχνικές που απευθύνονται στο ανθρώπινο υποσυνείδητο, τεχνικές παραπλανητικές για την λήψη αποφάσεων, τεχνικές που εκμεταλλεύονται τις ανθρώπινες αδυναμίες, όπως μια αναπηρία καθώς και τεχνικές διάκρισης και ταξινόμησης ανθρώπων βάσει χαρακτηριστικών τους (π.χ. φύλο, καταγωγή κ.λπ.) που οδηγούν σε άνιση μεταχείριση ή κοινωνική βαθμολόγηση.

Δεδομένου ότι η πρώτη κατηγορία του μη αποδεκτού κινδύνου δεν είναι εφαρμόσιμη υπό καμία προϋπόθεση, ο Κανονισμός πραγματεύεται στο μεγαλύτερο του μέρος τα συστήματα υψηλού κινδύνου για τα οποία θεσμοθετεί και την πλειοψηφία των ρυθμίσεων. Για τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου, η διάθεση και χρήση τους είναι επιτρεπτή μόνο υπό την υποχρεωτική εφαρμογή των διατάξεων του κανονισμού ώστε να διασφαλίζεται ότι ο κίνδυνος παραμένει υψηλός και δεν μεταπηδά στην κατηγορία του μη αποδεκτού.

Για να κριθεί ένα σύστημα τεχνητής νοημοσύνης υψηλού κινδύνου θα πρέπει, σύμφωνα με το άρθρο 6 του κανονισμού, σωρευτικά το σύστημα α) να προορίζεται να χρησιμοποιηθεί ως κατασκευαστικό στοιχείο ασφάλειας ενός προϊόντος ή το σύστημα ΤΝ είναι το ίδιο προϊόν που καλύπτεται από την ενωσιακή νομοθεσία εναρμόνισης που παρατίθεται στο παράρτημα Ι· β) το προϊόν του οποίου κατασκευαστικό στοιχείο ασφάλειας σύμφωνα με το στοιχείο α) είναι το σύστημα ΤΝ ή το ίδιο το σύστημα ΤΝ ως προϊόν απαιτείται να υποβληθεί σε αξιολόγηση της συμμόρφωσης από τρίτο μέρος με σκοπό τη διάθεση του εν λόγω προϊόντος στην αγορά ή τη θέση του σε λειτουργία, δυνάμει της ενωσιακής νομοθεσίας εναρμόνισης που παρατίθεται στο παράρτημα Ι του Κανονισμού. Στο παράρτημα ΙΙΙ του Κανονισμού παρατίθεται κατάλογος με συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου μεταξύ των οποίων συγκαταλέγονται συστήματα που χρησιμοποιούνται είτε για επιτρεπτή επεξεργασία βιομετρικών ή σε υποδομές ζωτικής σημασίας ή για σκοπούς εκπαίδευσης και επαγγελματικής κατάρτισης.

Τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου θα πρέπει να συμμορφώνονται με μια σειρά από απαιτήσεις που θεσπίζονται στο κεφάλαιο ΙΙ του Κανονισμού τόσο για τους παρόχους όσο και για τους διανομείς τους ώστε να είναι σύννομη και επιτρεπτή η λειτουργία τους. Στο άρθρο 9 του Κανονισμού προβλέπεται ένα σύστημα διαχείρισης κινδύνου που υποχρεούται να υιοθετήσει ο πάροχος και θα πρέπει να τηρείται καθ' όλη τη διάρκεια ζωής και επανεξετάζεται / επικαιροποιείται ανά τακτά χρονικά διαστήματα. Σύμφωνα με το εν λόγω σύστημα διαχείρισης ο κίνδυνος προσδιορίζεται, αναλύεται, γίνεται μια εκτίμηση και αξιολόγηση του κινδύνου και την θέσπιση των απαραίτητων κατάλληλων μέτρων διαχείρισης για την αντιμετώπιση του. Κατ' αυτόν τον τρόπο ο κίνδυνος είτε αντιμετωπίζεται πλήρως και αποτελεσματικά είτε ελαττώνεται στο σημείο του αποδεκτού και τίθεται σε λειτουργία υπό την προϋπόθεση ότι ο υπολειπόμενος κίνδυνος γνωστοποιείται στον χρήστη του (Ι. Ιγγλεζάκης, 2022, σ.185). Τα απαραίτητα μέτρα / προϋποθέσεις που πρέπει να πληρούνται για να είναι αποδεκτός ο κίνδυνος θα πρέπει να διασφαλίζεται ότι τα δεδομένα με τα οποία εκπαιδεύεται το σύστημα τεχνητής νοημοσύνης είναι υψηλής ποιότητας[14], ο πάροχος θα πρέπει να υποβάλει τεχνικό φάκελο στην αρμόδια οριζόμενη αρχή από τον οποίο θα προκύπτουν τα αποτελέσματα της πραγματοποιηθείσας αξιολόγησης[15] και θα πρέπει να τηρούνται τα αρχεία καταγραφής ώστε να επιτυγχάνεται η ιχνηλασιμότητα της λειτουργίας του συστήματος ("logs")[16]. Επιπροσθέτως, είναι αναγκαίο να τηρείται η αρχή της διαφάνειας και της πληροφόρησης των χρηστών[17], να υπάρχει ανθρώπινη εποπτεία ικανή να παρέμβει ανά πάσα στιγμή και όχι πλήρης αυτόνομη λειτουργία ενός συστήματος τεχνητής νοημοσύνης[18], ενώ τέλος θα πρέπει να επιτυγχάνεται το κατάλληλο επίπεδο ακρίβειας, στιβαρότητας και κυβερνοσφάλειας[19].

Με σκοπό να πραγματοποιηθούν τα παραπάνω, ο Κανονισμός επιβάλει σειρά υποχρεώσεων από τους παρόχους έως και τους τελικούς χρήστες δημιουργώντας έτσι

[14] Άρθρο 10 Κανονισμού για την ΤΝ
[15] Άρθρο 11 Κανονισμού για την ΤΝ
[16] Άρθρο 12 Κανονισμού για την ΤΝ
[17] Άρθρο 13 Κανονισμού για την ΤΝ
[18] Άρθρο 14 Κανονισμού για την ΤΝ
[19] Άρθρο 15 Κανονισμού για την ΤΝ

«στρώματα» ασφαλείας για την επαλήθευση της εφαρμογής των ως άνω προϋποθέσεων[20]. Τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου καταχωρούνται από τον πάροχο τους σε μια βάση δεδομένων της ΕΕ[21], η οποία δημιουργείται από την Ευρωπαϊκή Επιτροπή σε συνεργασία με τα κράτη μέλη και θα πρέπει να φέρουν τη σήμανση CE, ώστε να δηλώνεται η συμμόρφωσή τους με τον παρόντα κανονισμό και να μπορούν να κυκλοφορούν ελεύθερα εντός της εσωτερικής αγοράς[22].

Η πρόσφατη κυκλοφορία των συστημάτων παραγωγικής τεχνητής νοημοσύνης και δη των γλωσσικών μοντέλων, όπως το ChatGPT, και η άμεση δημοφιλία που απέκτησαν βρήκε απροετοίμαστη την Επιτροπή και ως εκ τούτου ήταν αναγκαία η προσαρμογή του έως τότε σχεδίου του Κανονισμού. Παρόλο που τα εν λόγω συστήματα τεχνητής νοημοσύνης δεν υπήρχαν κατά τον χρόνο της πρότασης πράξης για την ΤΝ, δημιούργησαν ένα νέο τεχνολογικό παράδειγμα όπου η προσέγγιση βάσει κινδύνου δεν είναι εφαρμόσιμη (T. Kellerhals, M. Wellner, 2024). Στον Κανονισμό, όπως δημοσιεύθηκε, ενσωματώθηκαν τόσο η έννοια για το μοντέλο ΤΝ γενικού σκοπού, το οποίο ορίζεται ως «*μοντέλο ΤΝ, μεταξύ άλλων όταν ένα τέτοιο μοντέλο ΤΝ έχει εκπαιδευτεί με μεγάλο όγκο δεδομένων χρησιμοποιώντας αυτοεποπτεία σε κλίμακα, το οποίο παρουσιάζει σημαντική γενικότητα και είναι ικανό να εκτελεί αποτελεσματικά ευρύ φάσμα διακριτών καθηκόντων, ανεξάρτητα από τον τρόπο με τον οποίο το μοντέλο διατίθεται στην αγορά και μπορεί να ενσωματωθεί σε διάφορα κατάντη συστήματα ή εφαρμογές· αυτό δεν καλύπτει μοντέλα ΤΝ που χρησιμοποιούνται πριν από τη διάθεσή τους στην αγορά για δραστηριότητες έρευνας, ανάπτυξης και κατασκευής πρωτοτύπων*», όσο και η έννοια του συστήματος ΤΝ γενικού σκοπού «*σύστημα ΤΝ που βασίζεται σε μοντέλο ΤΝ γενικού σκοπού και το οποίο έχει την ικανότητα να εξυπηρετεί διάφορους σκοπούς, τόσο για άμεση χρήση όσο και για ενσωμάτωση σε άλλα συστήματα ΤΝ*»[23].

Ο Κανονισμός κατηγοριοποιεί πλέον τα μοντέλα γενικού σκοπού σε αυτά που δεν φέρουν συστημικό κίνδυνο και στα μοντέλα γενικού σκοπού συστημικού κινδύνου. πρώτα

[20] Οι υποχρεώσεις των παρόχων, των κατασκευαστών, των εισαγωγέων, των διανομέων και των χρηστών προβλέπονται στα άρθρα 16 έως και 29
[21] Άρθρο 71 Κανονισμού για την ΤΝ
[22] Αιτιολογική σκέψη 129 Κανονισμού για την ΤΝ
[23] Άρθρο 3 του Κανονισμού για την ΤΝ

υπόκεινται σε ελάχιστες απαιτήσεις τεκμηρίωσης, ενώ τα μοντέλα τεχνητής νοημοσύνης γενικού σκοπού με συστημικό κίνδυνο υπόκειται σε αυστηρότερη εποπτεία. Η διάκριση αυτή διασφαλίζει ότι τα μοντέλα τεχνητής νοημοσύνης γενικού σκοπού με συστημικό κίνδυνο, τα οποία έχουν καταστεί αναπόσπαστο μέρος διαφόρων εφαρμογών, εξακολουθούν να διέπονται από ένα πλαίσιο που ενθαρρύνει την καινοτομία, διασφαλίζοντας παράλληλα τη λογοδοσία και την ασφάλεια.

Το ChatGPT αντιμετωπίζεται από τον Κανονισμό ως μοντέλο τεχνητής νοημοσύνης γενικού σκοπού (N. Helberger, N. Diakopoulos, 2023) σύμφωνα με την υπ' αριθμ. 99 αιτιολογική σκέψη, δεδομένου ότι επιτρέπουν την ευέλικτη παραγωγή περιεχομένου, π.χ. με τη μορφή κειμένου, ήχου, εικόνων ή βίντεο, που μπορεί εύκολα να εξυπηρετήσει ευρύ φάσμα διακριτών εργασιών. Τα παραπάνω χαρακτηριστικά καθιστούν πιθανό να προκύψουν συστηματικοί κίνδυνοι λόγω των οποίων επιβάλλονται και αυστηρότερες απαιτήσεις. Τα γλωσσικά μοντέλα ως συστήματα γενικού σκοπού είναι υποχρεωμένα να προβαίνουν σε γνωστοποίηση προς τους χρήστες τους ότι το περιεχόμενο έχει δημιουργηθεί από σύστημα τεχνητής νοημοσύνης και προνοούν ώστε ο σχεδιασμός του μοντέλου να πραγματοποιείται με τρόπο που να αποτρέπει τη δημιουργία παράνομου περιεχομένου, καθώς και να δημοσιεύει περιλήψεις των προστατευόμενων με πνευματική ιδιοκτησία δεδομένων που χρησιμοποιήθηκαν για την εκπαίδευση. Το ίδιο το ChatGPT αναφέρει με μικρά γράμματα στο τέλος της σελίδας ότι *«Το ChatGPT μπορεί να κάνει λάθη. Να ελέγχεις τις σημαντικές πληροφορίες.»*.

Σε αντίθεση με τα όσα αναφέρθηκαν παραπάνω, για τα συστήματα τεχνητής νοημοσύνης ελαχίστου κινδύνου δεν επιβάλλονται απαιτήσεις, ενώ τα συστήματα τεχνητής νοημοσύνης περιορισμένου κινδύνου υπόκεινται πολύ ήπιες υποχρεώσεις διαφάνειας. Παραταύτα ο Κανονισμός παροτρύνει τους παρόχους αυτών των συστημάτων να υιοθετήσουν τις απαιτήσεις που προβλέπονται για συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου εθελοντικά μέσω κωδίκων δεοντολογίας καθώς και λοιπές εθελοντικές δεσμεύσεις που ενισχύουν την αξιοπιστία της τεχνητής νοημοσύνης.

Προκειμένου να καλυφθεί η μεταβατική περίοδος πριν από την πλήρη εφαρμογή του Κανονισμού, η Επιτροπή δρομολόγησε το Ευρωπαϊκό Σύμφωνο για την τεχνητή νοημοσύνη ,

μια πρωτοβουλία που στόχο έχει την εθελοντική συμμόρφωση με τις απαιτήσεις που θέτει ο Κανονισμός όσων ασχολούνται με την τεχνητή νοημοσύνη, πριν ακόμη αυτός τεθεί σε εφαρμογή (ΣΕΕ,2024).

Όσον αφορά την επιβολή του Κανονισμού και την εποπτεία περί συμμόρφωσης με αυτόν διακρίνονται δύο επίπεδα, το εθνικό και το ευρωπαϊκό. Συγκεκριμένα, τα κράτη μέλη θα πρέπει ορίσουν τις αρμόδιες εθνικές αρχές τους έως τις 2 Αυγούστου του 2025, οι οποίες θα είναι υπεύθυνες για την επιβολή και την εποπτεία συμμόρφωσης με τις διατάξεις για τα συστήματα τεχνητής νοημοσύνης. Από την άλλη, σε ευρωπαϊκό επίπεδο θεσπίζεται η Υπηρεσία τεχνητής νοημοσύνης ως εκτελεστικός φορέας της Επιτροπής για την εξασφάλιση εφαρμογής του Κανονισμού σε Ευρωπαϊκό επίπεδο, και την διαχείριση των μοντέλων τεχνητής νοημοσύνης γενικού σκοπού (Lawspot, 01.08.2024). Επιπλέον, θεσπίζεται το Ευρωπαϊκό Συμβούλιο Τεχνητής Νοημοσύνης, το οποίο θα αποτελείται από εκπροσώπους των κρατών μελών, εξειδικευμένους σε ζητήματα τεχνητής νοημοσύνης και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ως συμβουλευτικός παράγοντας σε θέματα που σχετίζονται με την τεχνητή νοημοσύνη. Σε εθνικό επίπεδο αναμένεται η επιλογή της αρμόδιας εποπτεύουσας αρχής με επικρατέστερη επιλογή αυτή της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα παρά τα προβλήματα που ενδέχεται να προκύψουν από την υπερφόρτωση αρμοδιοτήτων σε μια αρχή και την έλλειψη πόρων και ανθρωπίνου δυναμικού προς υποστήριξη της[24]. Μένει να δούμε εάν αυτή θα είναι η επιλογή που θα προκριθεί ή αν θα βρεθεί κάποια άλλη λύση όπως η ανάθεση σε άλλη ήδη υπάρχουσα ανεξάρτητη αρχή ή ενδεχομένως η δημιουργία μιας νέας ανεξάρτητης αρχής αποκλειστικά προς τον σκοπό αυτό.

Τέλος, ο Κανονισμός εκτός του περιορισμού της τεχνητής νοημοσύνης με σκοπό την διασφάλιση της αξιοπιστίας της και την προστασία των θεμελιωδών ανθρωπίνων

[24] Σύμφωνα με την ιταλική προστασίας δεδομένων Garante ο Κανονισμός για την τεχνητή νοημοσύνη βασίζεται στο άρθρο 16 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης, το οποίο αποτελεί τη νομική βάση και της νομοθεσίας για την προστασία των προσωπικών δεδομένων και ως εκ τούτου η ίδια είναι η καταλληλότερη αρχή για την εποπτεία και την εφαρμογή του κανονισμού (https://www.lawspot.gr/nomika-nea/stin-arhi-prostasias-dedomenon-prepei-na-anatethei-i-epopteia-toy-ai-act?lspt_destination=upgrade).

δικαιωμάτων επιδιώκει και την δημιουργία ενός περιβάλλοντος που ευνοεί την καινοτομία και τις επενδύσεις στον χώρο της τεχνητής νοημοσύνης. Προβλέπεται, λοιπόν, η δημιουργία δοκιμαστηρίων (regulatory sandboxes) στα οποία οι πάροχοι θα έχουν τη δυνατότητα να δοκιμάζουν νέες τεχνολογίες υπό αυστηρή εποπτεία προτού τεθούν σε λειτουργία ή διατεθούν στο κοινό. Με αυτόν τον τρόπο θα είναι δυνατό να εντοπιστούν πιθανά προβλήματα κατά την λειτουργία αυτών των τεχνολογιών και μέσω αλληλεπίδρασης παρόχων με τις αρμόδιες εποπτικές αρχές να επιτευχθεί ένα ικανό επίπεδο ασφαλούς και αξιόπιστης λειτουργίας.

Την 1η Αυγούστου του 2024 τέθηκε σε ισχύ ο Κανονισμός αλλά οι διατάξεις του θα τεθούν σε εφαρμογή σε δύο έτη από την έναρξη ισχύος, ήτοι στις 2 Αυγούστου του 2026. Εξαίρεση από την ως άνω ημερομηνία εφαρμογής του Κανονισμού αποτελούν οι απαγορεύσεις για τα συστήματα τεχνητής νοημοσύνης μη αποδεκτού κινδύνου που θα τεθούν σε εφαρμογή 6 μήνες μετά την έναρξη ισχύος, αλλά και τα μοντέλα τεχνητής νοημοσύνης γενικού σκοπού οι υποχρεώσεις των οποίων θα εφαρμοσθούν 12 μήνες μετά την έναρξη ισχύος.

3.4. Εθνικός νόμος 4961/2022

Παρότι στην παρούσα διπλωματική κύριο αντικείμενο αποτελεί η αλληλεπίδραση της τεχνητής νοημοσύνης, στην έννοια της οποίας συμπεριλαμβάνεται και η παραγωγική τεχνητή νοημοσύνη, αξίζει να μνημονευθεί η ριζοσπαστική προσπάθεια του εθνικού μας νομοθέτη για την ρύθμιση της τεχνητής νοημοσύνης τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα πριν ακόμη τη δημοσίευση του Κανονισμού για την τεχνητή νοημοσύνη με σκοπό την προώθηση της διαφάνειας στην λειτουργία της.

Φυσικά, σκοπός του Έλληνα νομοθέτη δεν είναι η παράκαμψη του Ευρωπαίου νομοθέτη αλλά η συμπλήρωση του και για τον λόγο αυτό δεν αλληλοκαλύπτει διατάξεις του Κανονισμού για την τεχνητή νοημοσύνη αλλά και του ΓΚΠΔ, στον οποίο μάλιστα παραπέμπει στο κείμενο του.

Στα πλαίσια του δημοσίου τομέα, ο νόμος προβλέπει ότι για να μπορέσει να χρησιμοποιηθεί ένα σύστημα τεχνητής νοημοσύνης θα πρέπει να προβλέπεται από ειδική νομοθετική διάταξη που θα εκδοθεί και θα προβλέπει και τις εγγυήσεις προστασίας των

θιγόμενων προσώπων αλλά και να συμπεριλαμβάνεται σε ένα μητρώο, όπου καταγράφονται όλα τα συστήματα τεχνητής νοημοσύνης που χρησιμοποιεί ο δημόσιος τομέας. Μια ρηξικέλευθη ρύθμιση του ν. 4961/2022 είναι η υποχρέωσης διενέργειας αλγοριθμικής εκτίμησης αντικτύπου, η οποία δεν προβλέπεται από το αντίστοιχο ενωσιακό νομοθετικό πλαίσιο αλλά αποτελεί αξιόλογος τρόπος μετριασμού των κινδύνων για τα ανθρώπινα δικαιώματα.

Στον ιδιωτικό τομέα, σε περίπτωση που οι επιχειρήσεις επιθυμούν να εντάξουν στην λειτουργία τους συστήματα τεχνητής νοημοσύνης, οφείλουν να τηρούν ορισμένες υποχρεώσεις διαφάνειας που επιβάλει η νομοθεσία. Συγκεκριμένα, είναι υποχρεωμένες να ενημερώνουν σχετικά τα υποκείμενα των οποίων τα δεδομένα τίθενται υπό επεξεργασία αλλά και να δημιουργήσει ένα μητρώο συστημάτων τεχνητής νοημοσύνης που χρησιμοποιεί (εξαιρούνται από το μητρώο οι μικρές επιχειρήσεις).

Στα πλαίσια εφαρμογής του ν. 4961/2022 ιδρύθηκε η συντονιστική επιτροπή για την τεχνητή νοημοσύνη αλλά και η επιτροπή για την εποπτεία στρατηγικής συντονισμού των αρμόδιων φορέων. Όπως προαναφέρθηκε, η υιοθέτηση του ως άνω εθνικού νόμου δεν επηρεάζει την ακώλυτη εφαρμογή του ενωσιακού νομοθετικού πλαισίου και δεν έρχεται σε σύγκρουση μαζί του, αντιθέτως επιχειρεί στην ενίσχυση της ρύθμισης της τεχνητής νοημοσύνης και της προστασίας των θεμελιωδών ανθρωπίνων δικαιωμάτων.

4. Συγκριτική επισκόπηση ΓΚΠΔ και Κανονισμού για την τεχνητή νοημοσύνη

Ο Κανονισμός της ΕΕ για την τεχνητή νοημοσύνη, συμπληρώνει τον ΓΚΠΔ, ρυθμίζοντας ειδικά τη χρήση και ανάπτυξη της τεχνητής νοημοσύνης. Ο Κανονισμός επιδιώκει να διασφαλίσει ότι οι τεχνολογίες τεχνητής νοημοσύνης αναπτύσσονται και χρησιμοποιούνται με τρόπο που να προστατεύει την ασφάλεια, την ιδιωτικότητα και τα θεμελιώδη δικαιώματα των πολιτών. Ενώ ο ΓΚΠΔ επικεντρώνεται γενικά στην προστασία των προσωπικών δεδομένων, ο Κανονισμός ρυθμίζει συγκεκριμένα τις εφαρμογές τεχνητής νοημοσύνης,

εισάγοντας πρόσθετες απαιτήσεις για την ασφάλεια και τη διαφάνεια στις διαδικασίες επεξεργασίας δεδομένων.

Η σχέση μεταξύ του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) και του νόμου για την Τεχνητή Νοημοσύνη (AI Act) αποτελεί ένα κρίσιμο ζήτημα για τη ρύθμιση της τεχνολογίας στην Ευρωπαϊκή Ένωση (ΕΕ). Και οι δύο κανονισμοί στοχεύουν στην προστασία των δικαιωμάτων των ατόμων, αλλά προσεγγίζουν αυτόν τον στόχο από διαφορετικές οπτικές γωνίες. Κοινό χαρακτηριστικό και των δύο κειμένων είναι η επιλογή του ευρωπαίου νομοθέτη για την υιοθέτηση των σχετικών διατάξεων υπό την μορφή του κανονισμού, καταδεικνύοντας της προσπάθεια της ένωσης για κοινή ενιαία ρύθμιση του ψηφιακού κόσμου σε όλα τα κράτη μέλη και όχι κατακερματισμό ρυθμίσεων βάσει διαφορετικών δικαιοδοσιών.

Ο ΓΚΠΔ εστιάζει στην προστασία των προσωπικών δεδομένων των υποκειμένων που βρίσκονται εντός της ΕΕ αλλά και στη διασφάλιση της ιδιωτικότητας και της ασφάλειας των δεδομένων σε έναν κόσμο όπου η ψηφιακή τεχνολογία και η τεχνητή νοημοσύνη κυριαρχούν. Από την άλλη ο Κανονισμός για την τεχνητή νοημοσύνη επικεντρώνεται στη ρύθμιση της χρήσης της τεχνητής νοημοσύνης με στόχο την προαγωγή της καινοτομίας, αλλά και την προστασία των θεμελιωδών δικαιωμάτων και της ασφάλειας των χρηστών, ενός αξιόπιστου περιβάλλοντος εξέλιξης της τεχνητής νοημοσύνης. Ο Κανονισμός για την τεχνητή νοημοσύνη δεν περιορίζεται μόνο στην προστασία δεδομένων αλλά σε όλο το φάσμα αλληλεπίδρασης της τεχνητής νοημοσύνης με την κοινωνία και την οικονομία με σκοπό την δημιουργία ενός ασφαλούς περιβάλλοντος ανάπτυξης του.

Ανωτέρω αναλύθηκαν οι βασικές αρχές του ΓΚΠΔ καθώς και τα δικαιώματα των υποκειμένων των δεδομένων που τίθενται σε επεξεργασία, με τα οποία οφείλουν να συμμορφώνονται και οι πάροχοι εφαρμογών τεχνητής νοημοσύνης. Αντίστοιχα, αναλύθηκαν περαιτέρω και οι αρχές που προβλέπει ο Κανονισμός για την τεχνητή νοημοσύνη αποβλέποντας μεν στην προστασία των θεμελιωδών δικαιωμάτων του ανθρώπου σε συνδυασμό, όμως, με τη δημιουργία ενός πλαισίου που θα επιτρέπει την ανάπτυξη και χρήση της τεχνητής νοημοσύνης με ασφάλεια και διαφάνεια.

Παρότι, λοιπόν, ο ΓΚΠΔ και ο Κανονισμός για την τεχνητή νοημοσύνη έχουν διαφορετική εστίαση, υπάρχουν αλληλοεπικαλύψεις στις υποχρεώσεις τους, ιδιαίτερα όταν η επεξεργασία δεδομένων αφορά προσωπικά δεδομένα μέσω συστημάτων τεχνητής νοημοσύνης. Και τα δύο νομοθετήματα προβλέπουν την αρχή της διαφάνειας, αλλά η έννοια της διαφάνειας διαφέρει μεταξύ των δύο κειμένων. Η διαφάνεια στον ΓΚΠΔ συνίσταται στην υποχρέωση των υπευθύνων επεξεργασίας να ενημερώνουν τα υποκείμενα σχετικά με την επεξεργασία των δεδομένων τους και με τις επιπτώσεις που μπορεί να έχουν. Αντιθέτως, η αρχή της διαφάνειας του Κανονισμού για την τεχνητή νοημοσύνη εστιάζει τις πληροφορίες που πρέπει να είναι σε θέση να δίνει ο πάροχος συστημάτων τεχνητής νοημοσύνης σχετικά με την ιχνηλασιμότητα και την επεξηγησιμότητα της λειτουργίας του (Ισπανική ΑΠΔΠΧ, 2023).

Επιπλέον, δεδομένου ότι οι αρμόδιοι εθνικοί εποπτικοί φορείς που είναι υπεύθυνοι για την επιβολή του ΓΚΠΔ ενδέχεται να έχουν κοινές αρμοδιότητες με αυτούς που θα αποφασιστεί εν τέλει να επιβλέπουν την εφαρμογή του Κανονισμού για την τεχνητή νοημοσύνη, ή ακόμη και ταυτίζονται. Εάν η ΑΠΔΠΧ δεν ορισθεί ως αρμόδια αρχή για την εποπτεία επιβολής του Κανονισμού για την τεχνητή νοημοσύνη, τότε σίγουρα θα υπάρχει αλληλοκάλυψη αρμοδιοτήτων σε περιπτώσεις επεξεργασίας προσωπικών δεδομένων με την χρήση, όμως, τεχνητής νοημοσύνης.

Η σύγκριση του GDPR με τον AI Act αναδεικνύει τις διαφορετικές προσεγγίσεις της ΕΕ στη ρύθμιση της ψηφιακής τεχνολογίας. Ενώ ο GDPR επικεντρώνεται στην προστασία των προσωπικών δεδομένων, ο AI Act στοχεύει στη συνολική ρύθμιση της τεχνητής νοημοσύνης. Οι αλληλοεπικαλύψεις τους δείχνουν την ανάγκη για συντονισμό και ολοκληρωμένη προσέγγιση, ιδιαίτερα καθώς η τεχνητή νοημοσύνη συνεχίζει να αναπτύσσεται και να ενσωματώνεται σε όλες τις πτυχές της ζωής.

Κατόπιν εξέτασης του ισχύοντος νομοθετικού πλαισίου υπάρχει σκέψη για το αν μπορεί να έχει ισχύ και να επαρκεί για κάθε νέα εφαρμογή τεχνητής νοημοσύνης που προκύπτει, όπως εν προκειμένω το ChatGPT και άλλα παρεμφερή γλωσσικά μοντέλα ή χρήζει επικαιροποίησης και θέσπισης εξειδικευμένων διατάξεων που αναφέρονται ρητά σε

συγκεκριμένες τεχνολογίες, όπως η παραγωγική τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα (Α.Βόρρας, Λ. Μήτρου, 2018).

5. Ζητήματα ηθικής γλωσσικών μοντέλων (ChatGPT κ.λπ.)

Εκτός των ζητημάτων μη συμμόρφωσης με το νομοθετικό πλαίσιο, το ChatGPT, ως παράδειγμα μεγάλου γλωσσικού μοντέλου τεχνητής νοημοσύνης (ΤΝ), έχει φέρει στο προσκήνιο μεταξύ άλλων και πολλά ηθικά ζητήματα που σχετίζονται με τη χρήση της τεχνολογίας στην επεξεργασία φυσικής γλώσσας από το ευρύ κοινό. Παρά την εντυπωσιακή ικανότητά του να κατανοεί και να δημιουργεί κείμενα, οι δυνατότητες του και η προσφορά του άνευ προϋποθέσεων στο ανθρώπινο σύνολο, έχει προκαλέσει ανησυχίες για τις επιπτώσεις που μπορεί να έχει σε μια «ηθική κοινωνία».

Ένα από τα κυριότερα ηθικά ζητήματα που προκύπτουν από τη χρήση του ChatGPT είναι η δυνατότητά του να παράγει είτε ακούσια είτε κατά ζήτηση και να διαδίδει ψευδείς πληροφορίες που οδηγούν σε παραπληροφόρηση και παραπλάνηση του κοινού (fake news). Το μοντέλο είναι σχεδιασμένο να δημιουργεί κείμενα σε φυσική γλώσσα που είναι πειστικά και ρεαλιστικά, αλλά δεν έχει τη δυνατότητα εξ ορισμού να διακρίνει μεταξύ αληθινών και ψευδών πληροφοριών με αποτέλεσμα να μπορεί να το εκμεταλλευτεί κάποιος κακόβουλα για τη δημιουργία ψεύτικων ειδήσεων, παραπλανητικών άρθρων, ή ακόμα και για τη διάδοση επικίνδυνων θεωριών συνωμοσίας. Υπεύθυνη για αυτόν τον κίνδυνο είναι η δυνατότητα των μεγάλων γλωσσικών μοντέλων να παράγουν σύνθετο περιεχόμενο χωρίς ευδιάκριτο διαχωρισμό του αληθινού από το ψευδές περιεχόμενο, ενώ ο τεράστιος όγκος δεδομένων που παράγεται καθιστά δυσχερή την χειροκίνητη ανθρώπινη εποπτεία (P. Hacker, A. Engel, M. Mauer, 2023).

Η δημιουργία ψευδών ειδήσεων από εφαρμογές τεχνητής νοημοσύνης έχει χρησιμοποιηθεί ευρέως στον χώρο της πολιτικής με στόχο να επηρεάσει τους εκλογείς. Τον Ιανουάριο του 2024 πολλοί πολίτες έλαβαν τηλεφώνημα από τον Τζο Μπαϊντεν, ο οποίος τους προέτρεπε να μην συμμετάσχουν στις προκριματικές εκλογές για τις προεδρικές εκλογές, ή τουλάχιστον έτσι νόμιζαν. Η κλήση του Προέδρου των ΗΠΑ δεν ήταν τίποτε άλλο

πέρα από ένα προϊόν τεχνητής νοημοσύνης που έγινε και θέμα σε όλα τα ειδησεογραφικά κανάλια μέχρι να αποδειχθεί πως δεν αληθεύει. Και ο αντίπαλος του, όμως, ο Ντόναλτ Τραμπ έχει πέσει θύμα δημιουργίας ψευδών ειδήσεων για το πρόσωπο του όταν είδαν το φως της δημοσιότητας φωτογραφίες που τον έδειχνα αγκαλιά με έφηβες κοπέλες στο αεροπλάνο γνωστού διακινητή (Ν. Παπάζογλου, 2024). Οι εν λόγω ψευδείς ειδήσεις που κυκλοφόρησαν και η ταχύτητα διάδοσης τους καταδεικνύουν από μόνες τους το μέγεθος του κινδύνου.

Τα ηθικά προβλήματα που προκύπτουν από τη χρήση του ChatGPT απαιτούν ιδιαίτερη προσοχή και ρύθμιση, ενώ η ανάπτυξη και η εφαρμογή των γλωσσικών μοντέλων πρέπει να γίνονται με σεβασμό στα ανθρώπινα δικαιώματα και την ιδιωτικότητα. Η υιοθέτηση κατάλληλων κανονιστικών πλαισίων και η συνεχής εποπτεία και επανεξέταση των χαρακτηριστικών τέτοιων τεχνολογιών είναι απαραίτητη για να διασφαλιστεί ότι τα οφέλη της τεχνητής νοημοσύνης θα μεγιστοποιηθούν, ενώ οι ηθικοί κίνδυνοι θα περιοριστούν.

Η χρήση του ChatGPT θέτει προβληματισμούς και ως προς επαγγελματικά, κοινωνικά και εκπαιδευτικά θέματα. Η χρήση του σε ορισμένους τομείς, όπως για παράδειγμα η εξυπηρέτηση πελατών, ενδέχεται να οδηγήσει ακόμη και σε απώλειες θέσεων εργασίας, ειδικά σε επαγγέλματα που βασίζονται στην παροχή υπηρεσιών και στην παραγωγή περιεχομένου βάσει των οδηγιών που παρέχονται. Επιπλέον, το ChatGPT και τα άλλα όμοια του θέτουν σε κίνδυνο την ποιότητα του εκπαιδευτικού συστήματος και την δημιουργία της κριτικής σκέψης των νέων. Οι μαθητές / φοιτητές κ.λπ. παρατηρείται ότι επαναπαύονται στις δυνατότητες της τεχνολογίας και ειδικότερα της τεχνητής νοημοσύνης για την πραγματοποίηση των υποχρεώσεων τους (π.χ. τις εργασίες τους) και δεν επιδιώκουν την μάθηση με ότι αυτό συνεπάγεται. Παραταύτα, γενικότερα παρατηρείται ότι η αυξανόμενη εξάρτηση από τα γλωσσικά μοντέλα για την παραγωγή κειμένων μπορεί να μειώσει την αξία της ανθρώπινης δημιουργικότητας και να αλλοιώσει την ποιότητα της ανθρώπινης επικοινωνίας. Συναφές είναι και το φαινόμενο της λογοκλοπής, δεδομένου ότι το ChatGPT για να παράγει το περιεχόμενο που του ζητείται αντλεί δεδομένα που πιθανώς προστατεύονται από τις διατάξεις της πνευματικής ιδιοκτησίας και αναπαράγει αυτούσια τμήματα αυτών χωρίς την άδεια των δημιουργών. Από την άλλη, η τεχνητή νοημοσύνη μπορεί να λειτουργήσει και ως βοηθός για τον εντοπισμό φαινομένων λογοκλοπής, συνεπώς

η ενσωμάτωση τέτοιων εργαλείων στο ChatGPT θα οδηγούσε στην απαλοιφή των φαινομένων λογοκλοπής.

Ένα άλλο κρίσιμο ηθικό ζήτημα αφορά την ενσωμάτωση της τεχνητής νοημοσύνης σε διαδικασίες αυτοματοποιημένης λήψης αποφάσεων κυρίως λόγω της έλλειψης διαφάνειας που διακρίνει τις αυτοματοποιημένες αποφάσεις. Αυτοματοποιημένη επεξεργασία και λήψη αποφάσεων έχουμε όταν αυτή πραγματοποιείται αποκλειστικά με τεχνικά μέσα χωρίς ανθρώπινη παρέμβαση (Ομάδα του Άρθρου 29, 2018). Το πρόβλημα εντοπίζεται στη διαδρομή που ακολουθούν τα δεδομένα από τη στιγμή που εισάγονται σε ένα σύστημα τεχνητής νοημοσύνης, εξ' ου και ο χαρακτηρισμός τους ως «μαύρα κουτιά» ("black boxes"). Όταν λαμβάνουμε μια απόφαση στην καθημερινότητα μας μπορούμε να την αιτιολογήσουμε αναφέροντας τι δεδομένα είχαμε, πως τα αξιολογήσαμε και πως καταλήξαμε στην απόφαση μας. Αντιθέτως, το σύστημα αυτοματοποιημένης λήψης απόφασης δεν μπορεί να παραπέμψει επ' ακριβώς στα δεδομένα που είχε στην διάθεση του και στα κριτήρια αξιολόγησης που επέλεξε. Εάν η τεχνητή νοημοσύνη χρησιμοποιείται για να λαμβάνει αποφάσεις ή να παρέχει συμβουλές σε κρίσιμες καταστάσεις (π.χ. στη δικαιοσύνη ή στην ιατρική), υπάρχουν ανησυχίες για το κατά πόσο αυτές οι αποφάσεις είναι δίκαιες και αξιόπιστες. Οι αλγοριθμικές αποφάσεις εξαρτώνται άμεσα από την ποιότητα των δεδομένων που έχουν εκπαιδευτεί. Εάν ο αλγόριθμος έχει εκπαιδευτεί με δεδομένα που εμπεριέχουν διακρίσεις, τότε και οι ληφθείσες αποφάσεις θα διαιωνίζουν τις εν λόγω διακρίσεις και θα δημιουργούν κοινωνικές ανισότητες. Το παραπάνω έρχεται σε αντίθεση με το άρθρο 22 του ΓΚΠΔ[25], σύμφωνα με το οποίο το υποκείμενο έχει το δικαίωμα να μην τίθεται σε μειονεκτική θέση από αμιγώς αυτοματοποιημένες αποφάσεις. Σε κάθε περίπτωση, βάσει και της αιτιολογικής σκέψης 71 του ΓΚΠΔ, η αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων θα πρέπει να συνοδεύεται από τις κατάλληλες εγγυήσεις ασφάλειας για να καθίσταται νόμιμη και επιτρεπτή. Συγκεκριμένα, απαιτείται αυστηρή διαφάνεια ώστε να μπορεί να αιτιολογηθεί επαρκώς η απόφαση, δυνατότητα του

[25] Αρ. 22 ΓΚΠΔ: «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»

υποκειμένου να εκφράσει την άποψη και την αμφισβήτηση του επί της απόφασης και να εξασφαλίζεται το δικαίωμα της ανθρώπινης παρέμβασης. Εάν όμως πρόκειται για επεξεργασία ειδικών κατηγοριών δεδομένων, όπως τα ευαίσθητα προσωπικά δεδομένα τότε θα πρέπει να τηρούνται συγκεκριμένες προϋποθέσεις που ορίζονται στο κείμενο του ΓΚΠΔ.

Επιπλέον, αμφιλεγόμενο είναι το ζήτημα της ευθύνης, καθώς είναι δύσκολο να αποδοθούν ευθύνες σε έναν αλγόριθμο για τυχόν λανθασμένες αποφάσεις ή αποτελέσματα (Floridi, 2018). Όταν μια απόφαση που λαμβάνεται από έναν αλγόριθμο αποδεικνύεται λανθασμένη ή άδικη, τίθεται το ζήτημα της ευθύνης. Ποιος είναι υπεύθυνος για τις συνέπειες μιας αυτοματοποιημένης απόφασης; Ο προγραμματιστής του αλγορίθμου, η εταιρεία που το χρησιμοποιεί, ή το ίδιο το σύστημα; Η ασαφής κατανομή της ευθύνης μπορεί να οδηγήσει σε περιπτώσεις όπου κανείς δεν λογοδοτεί για τις βλαπτικές συνέπειες των αποφάσεων, υπονομεύοντας την εμπιστοσύνη του κοινού στην τεχνολογία. Με την εξασφάλιση της ανθρώπινης παρέμβασης υποστηρίζεται η άποψη της μετάθεσης της ευθύνης και του βάρους απόδειξης στο άνθρωπο, ο οποίος θα πρέπει εκ των υστέρων να εκπληρώσει την αρχή της λογοδοσίας (Lazcoz & De Hert, 2022).

Τρόπος αυτοματοποιημένης επεξεργασίας αποτελεί και η κατάρτιση προφίλ, ήτοι η αυτοματοποιημένη αξιολόγηση συμπεριφορών και χαρακτηριστικών μιας προσωπικότητας. Για την κατάρτιση προφίλ ισχύουν οι ίδιοι κίνδυνοι που αναφέρθηκαν παραπάνω στα πλαίσια της αυτοματοποιημένης λήψης αποφάσεων και εφαρμόζονται οι ίδιες εγγυήσεις που προβλέπει ο ΓΚΠΔ για αυτή.

6. Νομολογία

Η παραγωγική τεχνητή νοημοσύνη και τα μεγάλα γλωσσικά μοντέλα είναι νέα ευρήματα της τεχνολογίας με αποτέλεσμα να μην έχουν προλάβει να απασχολήσουν ακόμη τα σε μεγάλο βαθμό τα ευρωπαϊκά σε κάποια υπόθεση ορόσημο που να δίνει κατευθυντήριες σε ουσιώδη προβλήματα που προκαλεί η χρήση τους σε σχέση με το νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων, παρά μόνο σε σχέση με τα πνευματικά δικαιώματα των δημιουργημάτων τους. Ωστόσο, το ChatGPT δεν παύει να αποτελεί προηγμένο είδος τεχνητής νοημοσύνης και ως εκ τούτου πρέπει να εξεταστεί βάσει ήδη υφιστάμενων αποφάσεων που αφορούν την χρήση τεχνητής νοημοσύνης και το δεσμεύουν.

i. C-634/21, SCHUFA Holding (Scoring), ΔΕΕ 957/07.12.2023

Η SCHUFA είναι ιδιωτική εταιρία γερμανικού δικαίου η οποία παρέχει στους αντισυμβαλλομένους της πληροφορίες σχετικά με τη φερεγγυότητα τρίτων, ιδίως καταναλωτών. Η εν λόγω αξιολόγηση από την γερμανική εταιρεία γίνεται στα πλαίσια μιας αδιαφανούς επεξεργασίας προσωπικών δεδομένων των καταναλωτών που αντλεί από διάφορες πηγές, ενώ αφορμή για την απόφαση του ΔΕΕ στάθηκε η επανειλημμένη άρνηση της Shufa να ανταποκριθεί σε αιτήματα άσκησης δικαιωμάτων των υποκειμένων, όπως το δικαίωμα πρόσβασης και διαγραφής δεδομένων επικαλούμενη το επιχειρηματικό της απόρρητο. Το ΔΕΕ χαρακτήρισε την εν λόγω πιστοληπτική αξιολόγηση ("scoring") ως αυτοματοποιημένη λήψη απόφασης υποκείμενη στα όσα ορίζει το άρθρο 22 ΓΚΠΔ και απεφάνθη ότι η Schufa όφειλε να ανταποκριθεί στο αίτημα του υποκειμένου για πρόσβαση στα δεδομένα της και διαγραφή ανακριβών δεδομένων.

Κατ' αντιστοιχία με την περίπτωση της αξιολόγησης από τη Schufa και οι περιπτώσεις εφαρμογών τεχνητής νοημοσύνης που χρησιμοποιούνται έστω και προπαρασκευαστικά για αξιολόγηση αιτήσεων κ.λπ. και επηρεάζουν την λήψη της τελικής απόφασης αλλά και το ίδιο το υποκείμενο, αποτελούν τρόπο αυτοματοποιημένης επεξεργασίας δεδομένων και κατάρτισης προφίλ και θα πρέπει να εξετάζονται υπό το πρίσμα των ειδικότερων διατάξεων του ΓΚΠΔ για την αυτοματοποιημένη επεξεργασίας προσωπικών δεδομένων (Lawspot, 12.12.2023). Τέτοια περίπτωση θα μπορούσε να είναι η χρήση του ChatGPT για προπαρασκευαστική αξιολόγηση βιογραφικών υποψήφιων εργαζομένων και η αντίστοιχη ταξινόμηση τους.

ii. Υπόθεση C-362/14 (Schrems I) & C-311/18 (Schrems II)

Με αφορμή τις υποθέσεις Schrems I και I θα εξετάσουμε το ζήτημα της εδαφικότητας του ΓΚΠΔ και της ασφαλούς διαβίβασης δεδομένων από την ΕΕ προς τρίτες χώρες. Σύμφωνα με το άρθρο 45 του ΓΚΠΔ η διαβίβαση προσωπικών δεδομένων σε τρίτες χώρες είναι εφικτή μόνο εφόσον η τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας των δεδομένων σύμφωνο με το επίπεδο προστασίας που παρέχει η ένωση. Στην περίπτωση του M. Schrems,

ο οποίος υπέβαλε καταγγελία στην ιρλανδική αρχή, ζητήθηκε να μην διαβιβάζονται τα δεδομένα του ως χρήστη του Facebook από την Facebook Ireland στους διακομιστές που έχει η εταιρεία στην Αμερική με την αιτιολογία ότι το επίπεδο προστασίας δεδομένων των ΗΠΑ δεν είναι επαρκές. Αποτέλεσμα των δύο ως άνω προσφυγών του M. Schrems ήταν η ακύρωση των αποφάσεων 2000/520 (απόφαση «ασφαλούς λιμένα») και 2016/1250 της Ευρωπαϊκής Επιτροπής που όριζαν εξ ορισμού τις ΗΠΑ ως «ασφαλή» τρίτη χώρα για την διαβίβαση προσωπικών δεδομένων από την ένωση με κύρια αιτιολογία την έλλειψη εκτελεστικών δικαιωμάτων που μπορούν να ασκήσουν τα υποκείμενα ενώπιον των αρμοδίων δικαστηρίων των ΗΠΑ. Οι ως άνω αποφάσεις άλλαξαν τα δεδομένα στον χώρο των διαβιβάσεων και θα πρέπει να ληφθούν υπόψη και για συστήματα τεχνητής νοημοσύνης και γλωσσικά μοντέλα (π.χ. το ChatGPT), των οποίων η εγκατάσταση βρίσκεται ως επί το πλείστον στις ΗΠΑ αλλά υφίσταται χρήση τους και συλλογή προσωπικών δεδομένων και εντός των ορίων της ΕΕ.

iii. Υπόθεση CNIL κατά Google LLC (2019)

Η CNIL, γαλλική Ανεξάρτητη Αρχή Προστασίας Δεδομένων έκρινε ότι η προβολή των στοχευμένων διαφημίσεων της Google, η λειτουργία των οποίων βασιζόταν σε λογισμικό τεχνητής νοημοσύνης μέσω της κατάρτισης προφίλ των χρηστών, παραβίαζε τον ΓΚΠΔ τόσο ως προς την υποχρέωση διαφάνειας και ενημέρωσης όσο και ως προς τη νόμιμη βάση επεξεργασίας. Οι ρυθμιστικές απαιτήσεις που προβλέπονται από την απόφαση CNIL σχετικά με τις αρχές του ΓΚΠΔ οφείλουν να λαμβάνονται υπόψη κατά τον σχεδιασμό και την ανάπτυξη των γλωσσικών μοντέλων, αναλογιζόμενοι και τον τεράστιο όγκο που επεξεργάζεται, ήτοι να ενημερώνεται το υποκείμενο, να γίνεται επεξεργασία με διαφανή τρόπο και πάντοτε υπό μια έγκυρη νόμιμη βάση.

Σκεπτόμενος κανείς την ευρεία χρήση του ChatGPT και των συγκρουσιακών σημείων που αυτό παρουσιάζει αναφορικά με τις διατάξεις του ΓΚΠΔ, είναι βέβαιο πως στο εγγύτερο μέλλον θα βρεθούμε αντιμέτωποι με ισχυρή νομολογία, που πιθανόν να ανατρέψει τα έως τώρα δεδομένα για το ChatGPT.

Συμπέρασμα

Η ολοένα αναπτυσσόμενη τεχνολογία και η απίστευτη ταχύτητα με την οποία εξαπλώνεται στην εποχή μας, μας κάνει να αναρωτιόμαστε αν το ισχύον νομοθετικό πλαίσιο που υπήρχε και πριν την εμφάνιση των νέων τεχνολογιών αρκεί ή εάν η νομοθεσία ακολουθεί την ανάπτυξη της τεχνολογίας και οφείλει να την ρυθμίζει σε μεταγενέστερο χρόνο από την αρχική εμφάνιση της. Η προσπάθεια για την ρύθμιση τεχνολογικών καινοτομιών έχει οδηγήσει στην πρωτόγνωρη παραγωγή νομοθετικών κειμένων σε ενωσιακό επίπεδο και στην δημιουργία ενός νέου κλάδου δικαίου, την «Τεχνολογία Δικαίου», ο οποίος εξελίσσεται ραγδαία όπως και το πεδίο που επιχειρεί να ρυθμίσει, η τεχνολογία (Ε. Μαργαρίτης, 2022).

Η παρούσα διπλωματική εργασία ανέλυσε την παραγωγική τεχνητή νοημοσύνη (AI), και συγκεκριμένα τα μεγάλα γλωσσικά μοντέλα, σε συνάρτηση με την προστασία των προσωπικών δεδομένων. Η μελέτη ανέδειξε την τεχνολογική επανάσταση που φέρνει η παραγωγική τεχνητή νοημοσύνη, όχι μόνο στον τομέα της επικοινωνίας και των επιχειρηματικών πρακτικών, αλλά και στην πρόκληση νέων νομικών και ηθικών προβλημάτων που απαιτούν άμεση αντιμετώπιση.

Η κύρια πρόκληση, ωστόσο, έγκειται στη συμμόρφωση αυτών των τεχνολογιών με το ισχύον νομοθετικό πλαίσιο προστασίας των προσωπικών δεδομένων, και συγκεκριμένα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Παρά το γεγονός ότι ο ΓΚΠΔ παρέχει ένα ισχυρό ουδέτερο πλαίσιο για την προστασία των δεδομένων στην ΕΕ, η φύση της παραγωγικής τεχνητής νοημοσύνης δημιουργεί νέες προκλήσεις που δεν είχαν προβλεφθεί κατά τη θέσπιση του κανονισμού.

Επιπλέον, η δημοσίευση του νέου Κανονισμού για την Τεχνητή Νοημοσύνη (AI Act) αποτελεί μια προσπάθεια της Ευρωπαϊκής Ένωσης να ρυθμίσει την ανάπτυξη και τη χρήση της τεχνητής νοημοσύνης. Παρά τις αλληλοεπικαλύψεις του με τον ΓΚΠΔ, ο νέος κανονισμός στοχεύει στη διασφάλιση της αξιοπιστίας και της ηθικής χρήσης της τεχνητής νοημοσύνης, κάτι που είναι κρίσιμο για την εμπιστοσύνη των πολιτών και των επιχειρήσεων.

Συνοψίζοντας, η παραγωγική τεχνητή νοημοσύνη έχει αναμφίβολα τεράστιο δυναμικό, αλλά η επιτυχία της και η αποδοχή της εξαρτώνται από τη διασφάλιση της προστασίας των προσωπικών δεδομένων και της συμμόρφωσης με τα ηθικά πρότυπα. Η ανάγκη για επικαιροποίηση των ρυθμίσεων και για συνεχή αξιολόγηση των κινδύνων που προκύπτουν από την λειτουργία των εφαρμογών τεχνητής νοημοσύνης κρίνεται απαραίτητη, προκειμένου να επιτευχθεί μια ισορροπία μεταξύ τεχνολογικής καινοτομίας και προστασίας των ατομικών δικαιωμάτων.

Η σταδιακή και συνεχής προσπάθεια της ΕΕ για ρύθμιση των νέων τεχνολογιών και δη της τεχνητής νοημοσύνης με προτεραιότητα την διασφάλιση της προστασίας των θεμελιωδών ανθρωπίνων δικαιωμάτων και των προσωπικών δεδομένων προκαλεί ανησυχία για το εάν θα υστερεί στον τομέα των σχετικών επενδύσεων σε αντίθεση με τρίτες χώρες που αποτελούν «παράδεισοι» για την ανάπτυξη της. Αρκεί μόνο να αναλογιστεί κανείς ότι, σύμφωνα με εκτιμήσεις, μεταξύ 2020 και 2028 η συνολική διαφορά μεταξύ ΗΠΑ και ΕΕ ως προς τις επενδύσεις για την τεχνητή νοημοσύνη υπερδιπλασιάστηκε με την ΕΕ να υστερεί κατά δέκα και πλέον δισεκατομμύρια ευρώ (Lawspot, 29.05.2024).

Βιβλιογραφία

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Ιγγλεζάκης Ιωάννης, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Κανονισμός 2016/679 και ο Εφαρμοστικός Νόμος (Ν.4624/2019), 3 η Έκδοση, 2020

Κανέλλος Λ., Εφαρμογές Τεχνητής Νοημοσύνης στο δίκαιο και στη δικαστική πρακτική, Νομική Βιβλιοθήκη, Αθήνα, 2021, σ. 26 επ.

Ιγγλεζάκης Ι., Το Δίκαιο της Ψηφιακής Οικονομίας, Εκδ. Σάκκουλα, Αθήνα- Θεσσαλονίκη, 2022, σ. 39-41 και 185 επ.

Λ. Μήτρου, Σ. Τάσσης, Η. Κωστή, Α. Βόρρας, Β. Καρκατζούνης, «Μπορεί ο Αλγόριθμος…», Πανεπιστημιακές Εκδόσεις Κρήτης, 2023, σ. 14 επ.

Α. Μικρουλέα, «Ανταγωνισμός και Ρύθμιση στην Ψηφιακή Οικονομία», Νομική Βιβλιοθήκη, 2023, σ. 297 επ.

Φ. Παναγοπούλου – Κουντατζή, «Τεχνητή Νοημοσύνη: Ο δρόμος προς ένα ψηφιακό συνταγματισμό, Μια ηθικοσυνταγματική θεώρηση», Εκδόσεις Παπαζήση, 2023, σελ. 140-143

ΕΛΛΗΝΙΚΗ ΑΡΘΟΓΡΑΦΙΑ

Σ. Τάσσης, «Η εποχή της Τεχνητής Νοημοσύνης», ΔιΜΕΕ, τ. 2/2018 – Έτος 15ο

Α. Βόρρας - Λ. Μήτρου, «Τεχνητή νοημοσύνη και προσωπικά δεδομένα Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679», ΔιΜΕΕ, τ. 2/2018 – Έτος 15ο

Μ. Δεληγιάννη, «Μια ανάλυση της πρότασης του Κανονισμού για την Τεχνητή Νοημοσύνη», ΣΥΝήΓΟΡΟΣ, τ. 146/2021, σελ. 28-32

«Νευρωνικά Δίκτυα (Neural Networks): Ορισμός & Εφαρμογές», Big Blue Data Academy, 2023, προσβάσιμο στο Νευρωνικά Δίκτυα (Neural Networks): Ορισμός & Εφαρμογές (bigblue.academy)

Ν. Θεογνώστου, «Αλγοριθμική Εκτίμηση Αντικτύπου σε σχέση με την Τεχνητή Νοημοσύνη - Η εφαρμογή του Νόμου 4961/2022», Επιθεώρηση Δικαίου Πληροφορικής, Τ.1 2023

«Η εξέλιξη της τεχνητής νοημοσύνης», prefer.gr, 20.08.2023, προσβάσιμο στο https://www.prefer.gr/technologia/i-exelixi-tis-technitis-noimosynis/4713/

Ο. Κοργιαλά, «Το ChatGPT υπό το φως του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων», Επιθεώρηση Δικαίου Πληροφορικής, Τ.2 2023

Η. Κωστή, «Τεχνητή νοημοσύνη και GDPR: Πόσο εφικτή είναι η συγκατάθεση;», rhetor.gr, 2023 προσβάσιμο στο https://www.rhetor.gr/techniti-noimosyni-kai-gdpr-poso-efikti-einai-i-sygkatathesi-482

Ε. Μαργαρίτης, «Δίκαιο της Τεχνολογίας ή Τεχνολογία του Δικαίου;», lawspot.gr, 2023 προσβάσιμο στο https://www.lawspot.gr/nomika-blogs/eyaggelos_margaritis/dikaio-tis-tehnologias-i-tehnologia-toy-dikaioy?lspt_destination=upgrade

Lawspot, "Τεχνητή Νοημοσύνη και προσωπικά δεδομένα: Οι επιπτώσεις των αποφάσεων Schufa του Δικαστηρίου της Ευρωπαϊκής Ένωσης", 12.12.2023 προσβάσιμο στο https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-kai-prosopika-dedomena-oi-epiptoseis-ton-apofaseon-schufa-toy?lspt_destination=upgrade

Γ. Θεοδωρίδου, «Η προστασία των προσωπικών δεδομένων στην εποχή της ανοιχτότητας», Επιθεώρηση Δικαίου Πληροφορικής, Τ. 1 2024 προσβάσιμο στο https://ejournals.lib.auth.gr/infolawj/article/viewFile/10158/9435

Ν. Παπάζογλου, «Fake news: Όταν η παραπληροφόρηση και η τεχνητή νοημοσύνη «ψηφίζουν»», 04.06.2024, προσβάσιμο στο https://www.insider.gr/business-stories/322883/fake-news-otan-i-parapliroforisi-kai-i-tehniti-noimosyni-psifizei

Lawspot, "AI Act: Σε ισχύ ο νέος ευρωπαϊκός Κανονισμός για την Τεχνητή Νοημοσύνη", 01.08.2024 προσβάσιμο στο https://www.lawspot.gr/nomika-nea/ai-act-se-ishy-o-neos-eyropaikos-kanonismos-gia-tin-tehniti-noimosyni?lspt_destination=upgrade

Lawspot, "Τεχνητή νοημοσύνη: Η Ευρωπαϊκή Ένωση πρέπει να ανοίξει το βήμα της", 29.05.2024 προσβάσιμο στο https://www.lawspot.gr/nomika-nea/tehniti-noimosyni-i-eyropaiki-enosi-prepei-na-anoixei-vima-tis?lspt_destination=upgrade

el.wikipedia.org, «Τεχνητή Νοημοσύνη» προσβάσιμο στο https://el.wikipedia.org/wiki/%CE%A4%CE%B5%CF%87%CE%BD%CE%B7%CF%84%CE%AE_%CE%BD%CE%BF%CE%B7%CE%BC%CE%BF%CF%83%CF%8D%CE%BD%CE%B7

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ – ΑΡΘΟΓΡΑΦΙΑ

Avron Barr & Edward Feigenbaum, The Handbook of Artificial Intelligence, 1981, σελ. 21 επ.

Stephen Hawking, "The best or worst thing to happen to humanity", University of Cambridge, 2016 προσβάσιμο στο https://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of

Conrad Sebastian, Künstliche Intelligenz – Die Risiken für den Datenschutz, Datenschutz und Datensicherheit 41 (12), 2017, σ. 740-744 προσβάσιμο στο https://www.researchgate.net/publication/321578188_Kunstliche_Intelligenz_-_Die_Risiken_fur_den_Datenschutz

Mantelero, A., 2018. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review, 34(4), προσβάσιμο στο https://doi.org/10.1016/j.clsr.2018.05.017

L. Mitrou, DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES - IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF?", 2018, προσβάσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914

Butterworth, M., 2018. The ICO and artificial intelligence: The role of fairness in the GDPR framework. Computer Law & Security Review (Volume 34, Issue 2), προσβάσιμο στο https://doi.org/10.1016/j.clsr.2018.01.004

Meg Leta Jones, Ellen Kaufman, and Elizabeth Edenberg, "AI and the Ethics of Automating Consent", IEEE Security & Privacy (Volume 16 , Issue: 3 , May/June 2018), pp. 64-72 προσβάσιμο στο https://www.researchgate.net/publication/325979872_AI_and_the_Ethics_of_Automating_Consent

Floridi, L. και συν., 2018. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds & Machines, 28(4), προσβάσιμο στο https://doi.org/10.1007/s11023-018-9482-5

Christopher Rigano, «A Brief History of Artificial Intelligence», Sidebar to the article Using Artificial Intelligence to Address Criminal Justice Needs, 30.09.2018, published in NIJ Journal issue no. 280, προσβάσιμο https://nij.ojp.gov/topics/articles/brief-history-artificial-intelligence#note3

Norwegian Data Protection Authority, "Artificial Intelligence and Privacy", Report, 2018, προσβάσιμο στο https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

Mazurek Grzegorz, Małagocka Karolina (2019), "Perception of privacy and data protection in the context of the development of artificial intelligence", Journal of Management Analytics, 6(4), σελ. 344–364

A. Bradfort, "The Brussels Effect: How the European Union Rules the World", 2019

C. Lexcellent, Artificial Intelligence versus Human Intelligence, Springler Briefs in Applied Sciences and Technology, 2019

M. Negnevitsky, Artificial Intelligence: A Guide to Intelligent Systems (3rd Edition), Adison Wesley, 2020

Burri Thomas, "The New Regulation of the European Union on Artificial Intelligence: Fuzzy Ethics Diffuse into Domestic Law and Sideline International Law", 2021, προσβάσιμο στο The New Regulation of the European Union on Artificial Intelligence: Fuzzy Ethics Diffuse into Domestic Law and Sideline International Law by Thomas Burri :: SSRN

The EAPIL blog, The EU's Upcoming Regulatory Framework on Artificial Intelligence and its Impact on PIL. 2021 προσβάσιμο στο https://eapil.org/2021/07/12/the-eus-upcoming-regulatory-framework-on-artificial-intelligence-and-its-impact-on-pil/

Lazcoz, G. & De Hert, P., 2022. Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities, προσβάσιμο στο SSRN: https://ssrn.com/abstract=4016502

P. Hacker, A. Engel, M. Mauer, "Regulating ChatGPT and other Large Generative AI Models", Fairness, Accountability, and Transparency (FAccT '23), June 12–15, 2023, Chicago, IL, USA. ACM, New York, NY, USA

A. Hughes "ChatGPT: Everything you need to know about OpenAI's GPT-4 tool", BBC Science Focus, 2023 προσβάσιμο στο https://www.sciencefocus.com/future-technology/gpt-3

Garante per la protezione dei dati personali (GPDP), "Artificial intelligence: stop to ChatGPT by the Italian SA
Personal data is collected unlawfully, no age verification system is in place for children", 2023 προσβάσιμο στο https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english

B. Tarnoff, "Weizenbaum's nightmares: how the inventor of the first chatbot turned against AI", The Guardian, 2023 προσβάσιμο στο https://www.theguardian.com/technology/2023/jul/25/joseph-weizenbaum-inventor-eliza-chatbot-turned-against-artificial-intelligence-ai

Ισπανική ΑΠΔΠΧ, "Artificial Intelligence: Transparency", 2023 προσβάσιμο στο https://www.aepd.es/en/prensa-y-comunicacion/blog/artificial-intelligence-transparency

Suarez, T. V. E., "ChatGPT: Risks and challenges from a Data Privacy perspective. Datenschutz Notizen | News-Blog Der DSN GROUP", 09.03.2023 προσβάσιμο στο https://www.datenschutz-notizen.de/chatgpt-risks-and-challenges-from-a-data-privacyperspective-0341134/

N. Helberger, N. Diakopoulos, "ChatGPT and the AI Act", Internet Policy Review, 2023 προσβάσιμο στο https://policyreview.info/pdf/policyreview-2023-1-1682.pdf

T. Kellerhals, M. Wellner, "Is AI regulation threatening innovation and ChatGPT?", kpmg.com, 2024 προσβάσιμο στο https://kpmg.com/ch/en/insights/technology/artificial-intelligence-eu-ai-act-challenge.html

C. Stryker - E. Kavlakoglu , "What is Artificial Intelligence (AI)?", 16.08.2024, προσβάσιμο στο https://www.ibm.com/topics/artificial-intelligence

Ahfaz Ahmed, "ChatGPT User Statistics (Aug 2024) — Growth Analysis", OPENAI JOURNEY, 2024 προσβάσιμο στο https://openaijourney.com/chatgpt-user-statistics/

C. Daffy, "Elon Musk's AI photo tool is generating realistic, fake images of Trump, Harris and Biden", CNN, 2024 προσβάσιμο στο https://edition.cnn.com/2024/08/15/tech/elon-musk-x-grok-ai-images/index.html

ΝΟΜΟΘΕΣΙΑ – ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ – ΟΔΗΓΙΕΣ – ΑΠΟΦΑΣΕΙΣ – ΕΚΘΕΣΕΙΣ - ΜΕΛΕΤΕΣ

Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΓΚΠΔ) προσβάσιμο στο https://eur-lex.europa.eu/EL/legal-content/summary/general-data-protection-regulation-gdpr.html

Χάρτης θεμελιωδών δικαιωμάτων της Ευρωπαϊκής Ένωσης, 2016 προσβάσιμο στο https://eur-lex.europa.eu/EL/legal-content/summary/charter-of-fundamental-rights-of-the-european-union.html

European Comission, Special Eurobarometer Report, "Attitudes towards the impact of digitisation and automation on daily life", 2017

Απόφαση 65/2018 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) προσβάσιμη στο https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf

Ομάδα του Άρθρου 29, 2018. Guidelines on transparency under Regulation 2016/679 (WP260rev01), προσβάσιμο στο https://ec.europa.eu/newsroom/article29/items/622227

European Data Protection Board, 2024. Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, προσβάσιμο στο https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en

European Data Protection Board, 2024. Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, προσβάσιμο στο https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

Ανεξάρτητη ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη συσταθείσα από την ευρωπαϊκή επιτροπή τον Ιούνιο του 2018 (AI HLEG), «Κατευθυντήριες Γραμμές Δεοντολογίας Για Αξιόπιστη Τεχνητή Νοημοσύνη», 2019 προσβάσιμο στο

https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf

Λευκή Βίβλος – Τεχνητή Νοημοσύνη, Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης COM (2020) 65 final, 2020, προσβάσιμο στο https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_el?filename=commission-white-paper-artificial-intelligence-feb2020_el.pdf

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4961 (ΦΕΚ Α 146/27.7.2022)

CEDPO (CONFETERATION OF EUROPEAN DATA PROTECTION ORGANISATIONS), "Generative AI: The Data Protection Implivations", 2023

CRS (Congressional Research Service), "Generative Artificial Intelligence and Data Privacy: A Primer", 2023 προσβάσιμο στο https://crsreports.congress.gov/product/pdf/R/R47569

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2024/1689 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 13ης Ιουνίου 2024 για τη θέσπιση εναρμονισμένων κανόνων σχετικά με την τεχνητή νοημοσύνη και την τροποποίηση των κανονισμών (ΕΚ) αριθ. 300/2008, (ΕΕ) αριθ. 167/2013, (ΕΕ) αριθ. 168/2013, (ΕΕ) 2018/858, (ΕΕ) 2018/1139 και (ΕΕ) 2019/2144 και των οδηγιών 2014/90/ΕΕ, (ΕΕ) 2016/797 και (ΕΕ) 2020/1828 (κανονισμός για την τεχνητή νοημοσύνη) προσβάσιμο στο https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=OJ:L_202401689
EDPB (European Data Protection Board), "Report of the work undertaken by the ChatGPT Taskforce", 2024 προσβάσιμο στο https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-chatgpt-taskforce_en

Δελτίου τύπου Συμβουλίου της Ευρωπαϊκής Ένωσης (ΣΕΕ), 2024 προσβάσιμο στο https://www.consilium.europa.eu/el/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

Information Comissioner's Office (ICO), "Big Data Artificial Intelligence Machine Learning and Data Protection", Version 2.2 προσβάσιμο στο https://ico.org.uk/media/for%20organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Ι. Πολυμένης, Διπλωματική Εργασία με θέμα «Τα δεδομένα μεγάλης κλίμακας: τεχνικές και εργαλεία ανάλυσης τους και η προσφορά τους ως υπηρεσία του υπολογιστικού νέφους», Πανεπιστήμιο Μακεδονίας, 2017 προσβάσιμο στο https://dspace.lib.uom.gr/handle/2159/20146

ΔΕΕ, 04.10.2024, C-621/22, Υπόθεση Koninklijke Nederlandse Lawn Tennisbon, προσβάσιμο στο https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0621

ΔΕΕ, 07.12.2023, C-634/21, SCHUFA Holding (Scoring), προσβάσιμο στο **https://curia.europa.eu/juris/document/document.jsf;jsessionid=9C4AF5671B9A390CEF93B4EDB0580167?text=&docid=280426&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=28405337**

ΔΕΕ, 24.09.2019, C-507/17, CNIL κατά Google LLC (2019), προσβάσιμο στο **https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:62017CJ0507**

ΔΕΕ, Υπόθεση C-362/14 (Schrems I) & C-311/18 (Schrems II), προσβάσιμο στο **https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362**