

ΠΑΝΤΕΙΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

PANTEION UNIVERSITY OF SOCIAL AND POLITICAL SCIENCES



ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΤΗΣ ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΗΣ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΤΜΗΜΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

«ΝΟΜΙΚΗ ΚΑΙ ΔΙΟΙΚΗΤΙΚΗ ΕΠΙΣΤΗΜΗ»

ΚΑΤΕΥΘΥΝΣΗ: ΕΘΝΙΚΗ ΚΑΙ ΕΝΩΣΙΑΚΗ ΔΙΟΙΚΗΣΗ

«ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΚΑΙ Ο ΚΑΝΟΝΙΣΜΟΣ 2016/679/ΕΕ ΣΤΗΝ
ΕΠΟΧΗ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ.

Ειδικότερα, τα βιομετρικά δεδομένα και η χρήση τεχνολογιών αναγνώρισης
προσώπου.»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μαρία Πετρούλα Καβαδάκη

A.M.: 7119M005

Αθήνα, 2021

Τριμελής Επιτροπή

Φερενίκη Παναγοπούλου-Κουτνατζή, Επίκουρη Καθηγήτρια Παντείου

Πανεπιστημίου (Επιβλέπουσα)

Ισμήνη Κριάρη, Καθηγήτρια Παντείου Πανεπιστημίου

Αντώνιος Χάνος, Αναπληρωτής Καθηγητής Παντείου Πανεπιστημίου



Copyright © Μαρία Πετρούλα Καβαδάκη, 2021

All rights reserved. Με επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας διπλωματικής εργασίας εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της διπλωματικής εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Η έγκριση της διπλωματικής εργασίας από το Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών δεν δηλώνει αποδοχή των γνώμων του συγγραφέα.

*Στους γονείς μου
και τα αδέρφια μου*

Συντομογραφίες

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

ΔΕΕ: Δικαστήριο Ευρωπαϊκής Ένωσης

ΔΕΚ: Δικαστήριο Ευρωπαϊκών Κοινοτήτων

ΕΔΔΑ: Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου

ΕΕ: Ευρωπαϊκή Ένωση

ΕΣΔΑ: Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου

ΕΣΠΔ: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η/Υ: ηλεκτρονικός υπολογιστής

ΗΠΑ: Ηνωμένες Πολιτείες της Αμερικής

κλπ.: και λοιπά

ν.: νόμος

παρ.: παράγραφος

π.χ.: παραδείγματος χάριν

ΣΔΕΕ: Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης

στοιχ.: στοιχείο

TN: Τεχνητή νοημοσύνη

ΧΘΔΕΕ: Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

AI: Artificial Intelligence

C: Case

EU: European Union

GDPR: General Data Protection Regulation

ICO: Information Commissioner's Office

PNR: Passenger Name Record

Ευχαριστίες

Θερμές ευχαριστίες οφείλονται στην οικογένειά μου και τους οικείους μου ανθρώπους για την συμπαράσταση και την ενθάρρυνση σε αυτό το όμορφο ταξίδι. Ιδιαίτερα θα ήθελα να ευχαριστήσω τη μητέρα μου και τον πατέρα μου, που με στηρίζουν από τα πρώτα μου βήματα, καθώς και τους αδερφούς μου, Γιάννη και Σωτήρη, οι οποίοι, παρά την απόσταση που μας χωρίζει, ήταν πάντα δίπλα μου από τα πιο μικρά στα πιο μεγάλα.

Ευχαριστίες επίσης οφείλονται στους καθηγητές του μεταπτυχιακού μου και ιδιαίτερα στην επιβλέπουσα Καθηγήτρια, κα Φερενίκη Παναγοπούλου-Κουτνατζή, για τη στήριξη και τη βοήθειά της κατά τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω τη φίλη και συμφοιτήτριά μου Αυγή Σαουλίδου, η οποία αποτέλεσε την ιδανική συνοδοιπόρο σε αυτό το μεταπτυχιακό.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Διαγράμματα.....	9
Περίληψη	10
Abstract	11
1. Εισαγωγή	12
Σκοπός-στόχοι.....	17
Διάρθρωση της μελέτης.....	17
Μεθοδολογία.....	18
2. Τεχνητή νοημοσύνη.....	18
2.1 Ορισμός.....	18
2.2 Διακρίσεις	19
2.2.1 Περιορισμένη τεχνητή νοημοσύνη	19
2.2.2 Γενική τεχνητή νοημοσύνη.....	20
2.3 Πεδία και εργαλεία εφαρμογών	21
2.3.1 Μηχανική μάθηση (Machine learning).....	21
2.3.2 Βαθιά Μάθηση (Deep learning)	22
2.3.3 Μεγάλα Δεδομένα (Big data)	22
2.3.4 Αλγόριθμοι.....	24
2.3.5 Αυτοματοποιημένη λήψη αποφάσεων	24
3. Η τεχνητή νοημοσύνη στο εννοιολογικό πλαίσιο του ΓΚΠΔ	25
3.1 Η έννοια των δεδομένων προσωπικού χαρακτήρα.....	25
3.1.1 Η συσχέτιση των δεδομένων	28
3.1.2 Η εξαγωγή περαιτέρω δεδομένων από ήδη διαθέσιμα προσωπικά δεδομένα (Re-identification).....	30
3.2 Η κατάρτιση προφίλ	31
3.2.1 Η κατάρτιση προφίλ με τεχνητή νοημοσύνη	32
3.2.2 Η υπόθεση της Cambridge Analytica	33
4. Οι βασικές αρχές προστασίας προσωπικών δεδομένων	35
4.1 Νομιμότητα, αντικειμενικότητα και διαφάνεια	35

4.2	Περιορισμός του σκοπού	37
4.3	Ελαχιστοποίηση των δεδομένων	41
4.4	Ακρίβεια.....	43
4.5	Λογοδοσία.....	45
5.	Νομιμότητα της επεξεργασίας των δεδομένων και τεχνητή νοημοσύνη	46
5.1	Η συγκατάθεση του υποκειμένου	47
5.1.1	Ειδική συγκατάθεση	49
5.1.2	Συγκεκριμένη συγκατάθεση	50
5.1.3	Ελεύθερη συγκατάθεση	51
5.1.4	Η συγκατάθεση σε περαιτέρω επεξεργασία δεδομένων.....	52
5.2	Το έννομο συμφέρον	56
6.	Ειδικές κατηγορίες προσωπικών δεδομένων	57
6.1	Τα βιομετρικά δεδομένα	58
6.2	Η απόφαση του ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012) και ο ρόλος της αρχής της αναλογικότητας	62
6.3	Οι εικόνες προσώπου ως βιομετρικά δεδομένα.....	66
6.4	Η τεχνολογία αναγνώρισης προσώπου (Facial recognition technology)	69
6.5	Η προστασία των ειδικών προσωπικών δεδομένων από τεχνολογίες αναγνώρισης προσώπου.....	73
7.	Η αρχή της διαφάνειας στην τεχνητή νοημοσύνη	76
7.1	Διαφάνεια των αλγορίθμων και αλγοριθμικός έλεγχος	77
7.2	Οπτικοποίηση και Διαδραστικότητα	77
7.3	Υποχρέωση ενημερώσεως του υποκειμένου	78
8.	Δικαιώματα των υποκειμένων	79
8.1	Το δικαίωμα πρόσβασης (άρθρο 15 ΓΚΠΔ).....	80
8.2	Το δικαίωμα διαγραφής (άρθρο 17 ΓΚΠΔ).....	81
8.3	Το δικαίωμα στη φορητότητα (άρθρο 20 ΓΚΠΔ)	82

8.4	Το δικαίωμα εναντίωσης (άρθρο 21§1 ΓΚΠΔ)	83
9.	Αυτοματοποιημένη λήψη αποφάσεων	84
9.1	Η απαγόρευση αυτοματοποιημένης λήψης αποφάσεων.....	84
9.2	Εξαιρέσεις από την απαγόρευση του άρθρου 22§1	86
9.3	Μέτρα προστασίας για τις περιπτώσεις α΄ και γ΄ του άρθρου 22§2.....	87
9.4	Αυτοματοποιημένη λήψη αποφάσεων και ευαίσθητα δεδομένα.....	88
10.	Εργαλεία συμμόρφωσης με τον ΓΚΠΔ	89
10.1	Προσέγγιση με βάση τον κίνδυνο.....	89
10.2	Ευθύνη του υπευθύνου επεξεργασίας.....	91
10.3	Προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού	92
10.4	Μελέτη εκτίμησης αντικτύπου στην προστασία δεδομένων	93
10.5	Υπεύθυνοι προστασίας δεδομένων (ΥΠΔ).....	94
10.6	Κώδικες δεοντολογίας και πιστοποίηση.....	94
10.7	Ο ρόλος των Αρχών προστασίας δεδομένων.....	95
11.	Επίλογος – Συμπεράσματα	97
	Βιβλιογραφία	104
	Νομοθετικά – Νομικά κείμενα	107
	Νομολογία.....	108
	Διπλωματικές – Πτυχιακές εργασίες	109
	Ηλεκτρονικές Πηγές	109

Διαγράμματα

Διάγραμμα 1. Η σχέση μεταξύ ταυτοποιήσιμου και μη ταυτοποιήσιμου συνόλου δεδομένων.....σελ. 24

Περίληψη

Η τεχνητή νοημοσύνη αποτελεί ένα από τα πιο σύγχρονα και πολλά υποσχόμενα τεχνολογικά επιτεύγματα, επηρεάζοντας ποικίλους τομείς της ζωής και της καθημερινότητάς μας. Από την Alexa και τη Siri, τα αυτοματοποιημένα αυτοκίνητα, έως αλγόριθμους και μηχανήματα που λαμβάνουν αποφάσεις για τον άνθρωπο (π.χ. πρόσληψη σε θέση εργασίας, αξιολόγηση πιστοληπτικής ικανότητας). Τα νομικά ερωτήματα που εγείρονται γύρω από το ζήτημα της τεχνητής νοημοσύνης είναι αρκετά. Η παρούσα εργασία πρόκειται να εξετάσει την τεχνητή νοημοσύνη υπό την προστασία των δεδομένων προσωπικού χαρακτήρα, όπως αυτή θεσμοθετείται και οριοθετείται από τον Κανονισμό 2016/679/ΕΕ.

Ειδικότερα, με μία πρώτη ανάγνωση φαίνεται ότι ο Γενικός Κανονισμός δε λαμβάνει υπόψη του τις νέες τεχνολογίες που προκύπτουν από τη χρήση της τεχνητής νοημοσύνης. Οι διατάξεις για την κατάρτιση προφίλ (άρθρο 4 ΓΚΠΔ) και για την αυτοματοποιημένη λήψη των αποφάσεων (άρθρο 22 ΓΚΠΔ) αποτελούν την εξαίρεση στον παραπάνω κανόνα, καθώς αναφέρονται συγκεκριμένα στις τεχνολογίες αυτές.

Παράλληλα, δεν είναι οι μόνες διατάξεις του Κανονισμού που μπορούν να τύχουν εφαρμογής σε περιπτώσεις χρήσης τεχνητής νοημοσύνης. Οι αρχές της προστασίας των προσωπικών δεδομένων καθορίζουν ένα θεμελιώδες επίπεδο προστασίας του υποκειμένου και από κοινού με την αρχή της διαφάνειας διαδραματίζουν ένα πολύ σημαντικό ρόλο στην προστασία των προσωπικών δεδομένων.

Επομένως, στην παρούσα εργασία πρόκειται να διερευνηθούν τα άρθρα του Κανονισμού, τα οποία εφαρμόζονται όταν λειτουργούν συστήματα τεχνητής νοημοσύνης, να αναδειχθούν οι προβληματικές γύρω από την εφαρμογή τους, καθώς και να προταθούν τρόποι επίλυσης αυτών.

Ειδική μνεία θα γίνει στα βιομετρικά δεδομένα ως μία από τις ειδικές κατηγορίες των προσωπικών δεδομένων, τα οποία αναλύονται υπό την οπτική της χρήσης τεχνολογιών αναγνώρισης προσώπου, που δύναται να θέσει σε κίνδυνο θεμελιώδη δικαιώματα του ανθρώπου, στα οποία περιλαμβάνονται και τα προσωπικά δεδομένα.

Λέξεις-κλειδιά: Τεχνητή νοημοσύνη, προσωπικά δεδομένα, Γενικός Κανονισμός 2016/679/ΕΕ, βιομετρικά δεδομένα, τεχνολογία αναγνώρισης προσώπου

Abstract

Artificial intelligence is one of the most promising technological accomplishments, already affecting various areas of our everyday lives. From Alexa and Siri, automated cars, to algorithms and machines that make human decisions (e.g., hiring or credit rating). The legal matters that arise concerning AI are many. This paper conducts research on AI and the protection of personal data, as enshrined by Regulation 2016/679/EU.

In particular, at first glance it seems that the General Regulation does not take into consideration the new technologies that arise from the use of AI. The provisions of profiling (article 4 GDPR) and automated decision-making (article 22 GDPR) are an exception to the aforementioned observation, since they are the only ones to refer explicitly to AI technologies.

At the same time, they are not the only provisions of the Regulation that can be applied in cases of use of artificial intelligence. The principles of personal data protection establish a fundamental safeguard of the subject, and together with the principle of transparency have a major role in personal data protection in the AI era.

Therefore, in the present paper we are going to investigate the articles of the Regulation, which are applied when operating artificial intelligence systems, to highlight the problems around their application, as well as to propose ways to solve them.

Special mention will be made of biometric data as one of the special categories of personal data, which are analyzed through facial recognition applications, that potentially violate fundamental human rights, including personal data. In particular, the ever-growing application of facial recognition technologies raise concerns regarding private data protection.

Key-words: Artificial intelligence, personal data, General Regulation 2016/679/EU, biometric data, facial recognition technology

1. Εισαγωγή

Σκεπτόμενοι την έννοια της τεχνητής νοημοσύνης και προσπαθώντας να αναζητήσουμε την ιστορική της πορεία στο πέρασμα του χρόνου, ως επί το πλείστον την ανάγουμε και τη συνδέουμε αυτομάτως με την εμφάνιση των ηλεκτρονικών υπολογιστών. Ωστόσο, οι απαρχές της απαντώνται σε διάστημα πολύ προγενέστερο της ύπαρξης του πρώτου υπολογιστή.

Περισσότερα από 2000 χρόνια πριν, φιλόσοφοι όπως ο Αριστοτέλης και ο Ηράκλειτος προσπάθησαν να περιγράψουν τους μηχανισμούς μάθησης, απομνημόνευσης, όρασης, αντίληψης και συλλογισμού. Απαρχές της τεχνητής νοημοσύνης συναντάμε στους συλλογισμούς του Αριστοτέλη (384-322 π.Χ.)¹, οι οποίοι παρείχαν πρότυπα εκφράσεων που εξήγαγαν σωστά συμπεράσματα από σωστές υποθέσεις βασισμένα στην αριστοτέλεια συλλογιστική. Συνεπώς, τα ερευνητικά πεδία που εξετάζει η ΤΝ βασίζονται ακριβώς σε αυτές τις δεξιότητες.

Αρκετά χρόνια αργότερα, τη δεκαετία του 1940, εμφανίστηκε η πρώτη μαθηματική περιγραφή τεχνητού νευρωνικού δικτύου², με πολύ περιορισμένες δυνατότητες επίλυσης αριθμητικών προβλημάτων. Το 1950, περίοδος κατά την οποία η συζήτηση για την πιθανότητα εμφάνισης μηχανών με νόηση ήταν στην ακμή της, ο μαθηματικός Alan Turing, πατέρας της πληροφορικής και προπάτορας της τεχνητής νοημοσύνης, εξέδωσε ένα άρθρο. Το άρθρο αυτό ξεκινάει με το κεφάλαιο «Το παιχνίδι της μίμησης», εισάγοντας τη δοκιμασία Turing, κατά την οποία θα μπορούσε να διαπιστωθεί και να εξακριβωθεί εάν μία μηχανή διαθέτει ευφυΐα.

¹ Ο Αριστοτέλης, στο έργο του *«Ηθικά Νικομάχεια»* επιχειρεί να προσεγγίσει την έννοια της ορθής σκέψης και του τρόπου κωδικοποίησής της, με την εφαρμογή κανόνων ανάλυσης της διαδικασίας της σκέψης, οι οποίοι αποτέλεσαν τη βάση για τη διαμόρφωση της λογικής. Οι αριστοτέλεια συλλογισμοί παρείχαν πρότυπα δομής επιχειρημάτων, που έδιναν πάντα σωστά συμπεράσματα, όταν ξεκινούσαν από σωστές υποθέσεις. Για παράδειγμα, «ο Σωκράτης είναι άνθρωπος», «όλοι οι άνθρωποι είναι θνητοί», άρα «ο Σωκράτης είναι θνητός». Θεωρήθηκε ότι αυτοί οι νόμοι της σκέψης κυβερνούν τη λειτουργία της νόησης. Διαθέσιμο στο <https://sites.google.com/site/artintelligen/home/aristoteles>. Ανάκτηση: Ιούνιος 2021.

² Το νευρωνικό δίκτυο είναι ένα δίκτυο από απλούς υπολογιστικούς κόμβους (νευρώνες, νευρώνια), διασυνδεδεμένους μεταξύ τους. Είναι εμπνευσμένο από το Κεντρικό Νευρικό Σύστημα (Κ.Ν.Σ.), το οποίο προσπαθεί να προσομοιώσει. Διαθέσιμο στο https://el.wikipedia.org/wiki/Νευρωνικό_δίκτυο. Ανάκτηση: Δεκέμβριος 2020.

Ειδικότερα, ο επιφανής μαθηματικός πρότεινε τη δοκιμασία Turing, κατά την οποία απαιτούνται τρία δωμάτια χωρίς άμεση επικοινωνία, δύο άνθρωποι (ο Α και ο Β) και ένας ηλεκτρονικός υπολογιστής³. Ο άνθρωπος Α βρίσκεται απομονωμένος στο πρώτο δωμάτιο και στέλνει ταυτόχρονα πληκτρολογημένες ερωτήσεις (ευφυΐας, υποκειμενικές, συναισθηματικές, κρίσεως, εγκυκλοπαιδικών γνώσεων) στον άνθρωπο Β και στον Η/Υ που βρίσκονται στα άλλα δύο δωμάτια. Τόσο ο άνθρωπος Β και όσο και ο Η/Υ απαντούν γραπτώς στις ερωτήσεις του Α, ο οποίος προσπαθεί μέσα από τις απαντήσεις να ανακαλύψει ποιος είναι ο Β και ποιος ο Η/Υ. Εάν ο Α δεν μπορεί να τις διαχωρίσει, τότε δύναται να θεωρηθεί ότι ο Η/Υ κατέχει ευφυΐα.

Ο όρος «τεχνητή νοημοσύνη» χρησιμοποιήθηκε για πρώτη φορά το 1956 από τον John McCarthy⁴ για την περιγραφή ενός θερινού εργαστηρίου με την ονομασία «The Dartmouth Summer Research Project on Artificial Intelligence», στο οποίο συζητήθηκε ως βασικό θέμα ότι «οι μηχανές σκέπτονται»⁵. Αυτό θεωρήθηκε ως το πρώτο συνέδριο της ΤΝ και υπήρξε καθοριστικό στη γέννηση, ανάπτυξη και υλοποίησή της. Δόθηκε δε η εγκυκλοπαιδική ερμηνεία αυτής ως η «ικανότητα της μηχανής να μπορεί να σκέπτεται και να μιμείται την ανθρώπινη συμπεριφορά και ευφυΐα, αλλά να μην την αντικαθιστά».

Κατά τη δεκαετία του 1990, με την αυξανόμενη πρόοδο του διαδικτύου (internet), ανάπτυξη γνώρισαν και οι ευφυείς πράκτορες⁶, οι οποίοι αποτελούν αυτόνομο λογισμικό ΤΝ τοποθετημένο σε κάποιο περιβάλλον με το οποίο αλληλοεπιδρά. Σήμερα, η ΤΝ έχει εξελιχθεί ώστε να καλύπτει όχι μόνο συστήματα που βασίζονται σε κανόνες και έμπειρα συστήματα, αλλά και συστήματα που βασίζονται

³ Russel, S., & Norvig, P. (2005). Τεχνητή Νοημοσύνη: μια σύγχρονη προσέγγιση. Γ. Ρεφανίδης, Φ. Σκουλαρίκης, & Τ. Άλβας, Μεταφρ.) Κλειδάριθμος. Βλ. περισσότερα στο <http://users.sch.gr/jenyk/index.php/artificialintelligence/ai-historicalreview/6-turingtest>. Ανάκτηση: Ιούνιος 2021.

⁴ Ο John McCarthy ήταν μαθηματικός και σημαντική φυσιογνωμία του πεδίου της θεωρητικής πληροφορικής, ο οποίος το 1971 έλαβε το Βραβείο Turing για τις σημαντικές του συνεισφορές στον τομέα της τεχνητής νοημοσύνης. Διαθέσιμο στο [https://en.wikipedia.org/wiki/John_McCarthy_\(computer_scientist\)](https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist)). Ανάκτηση: Δεκέμβριος 2020.

⁵ McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the Dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, 27(4), 12-12.

⁶ Οι πράκτορες στοχεύουν συνήθως στην παροχή βοήθειας στους χρήστες τους, στη συλλογή ή ανάλυση μεγάλων συνόλων δεδομένων ή στην αυτοματοποίηση επαναλαμβανόμενων εργασιών (π.χ. διαδικτυακό ρομπότ).

στην εξελικτική διαδικασία ή σε πράκτορες⁷. Περιοχές έρευνας περιλαμβάνουν την ανάπτυξη της γνώσης για συλλογιστικά μοντέλα, όπως οντολογίες και εφαρμογές εξόρυξης δεδομένων για την αυτόματη απόκτηση γνώσης.

Στη σύγχρονη εποχή, η αυξημένη χρήση των συστημάτων τεχνητής νοημοσύνης έχει βελτιώσει με ποικίλους τρόπους διάφορους τομείς της καθημερινότητας, επιτρέποντας στους χρήστες τους να πραγματοποιούν πλήθος εργασιών με ταχύτατους ρυθμούς. Τεχνολογίες τεχνητής νοημοσύνης συναντάμε πλέον σε μεγάλο βαθμό στην καθημερινότητά μας⁸. Αυτά τα προϊόντα υψηλής τεχνολογίας διατίθενται στο ευρύ κοινό σε εξαιρετικά χαμηλό κόστος, πράγμα που μεταβάλλει ριζικά τον τρόπο με τον οποίο οι άνθρωποι μοιράζονται πλέον τα προσωπικά τους δεδομένα.

Ειδικότερα, οι άνθρωποι, χρησιμοποιώντας συσκευές περιέχουσες συστήματα τεχνητής νοημοσύνης, εισάγουν σε αυτές το σύνολο σχεδόν των προσωπικών τους πληροφοριών, οι οποίες καθίστανται εν συνεχεία αντικείμενο επεξεργασίας από τους αλγόριθμους. Οι αλγόριθμοι με τη σειρά τους προσαρμόζουν τα αποτελέσματά τους με βάση τα ενδιαφέροντα του κάθε χρήστη. Όπως είναι όμως προφανές, μπορεί πλέον να γίνει λόγος για τη μεγαλύτερη σε όγκο συλλογή και περαιτέρω ανάλυση προσωπικών δεδομένων που έχει καταγραφεί στην ιστορία της ανθρωπότητας, η οποία γίνεται, τις περισσότερες φορές, με τη συγκατάθεση των ίδιων των φορέων τους⁹. Εξάλλου -όχι τυχαία- τα προσωπικά δεδομένα έχουν χαρακτηριστεί ως «το πετρέλαιο της νέας εποχής»¹⁰.

⁷ Βιαννιτάκη, Β. (2014). *Τεχνητή Νοημοσύνη, Ευφυείς Πράκτορες και Εφαρμογές στην Πληροφορική υγείας*, Πτυχιακή εργασία, ΤΕΙ Πελοποννήσου, σελ. 19-20. Διαθέσιμη στο <https://docplayer.gr/34426346-Ptyhiaki-ergasia-tehniti-noimosyni-eyfyeis-praktores-kai-efarmoges-stin-pliροφοriki-ygeias-viannitaki-vasiliki.html>. Ανάκτηση: Ιούνιος 2021.

⁸ Βλ. σχετικά Παναγιωτίδου, Μ. Ε. (2020). *Τεχνητή Νοημοσύνη και Δίκαιο: τεχνολογικά, νομικά και ηθικά ζητήματα*, Διπλωματική εργασία, Διδρυματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Πανεπιστήμιο Μακεδονίας και Δημοκρίτειο Πανεπιστήμιο Θράκης, σελ. 18-20. Διαθέσιμη στο <https://dspace.lib.uom.gr/handle/2159/23990>. Ανάκτηση: Ιούνιος 2021.

⁹ Hildebrandt, M. (2016). Law as Information in the Era of Data-driven Agency. *The Modern Law Review*, 79(1), 1-30. Διαθέσιμο στο <https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2230.12165>. Ανάκτηση: Ιούνιος 2021.

¹⁰ Bhatt, B. (2018). *Data is the new oil*, Medium. Διαθέσιμο στο <https://medium.com/@BhaskarBhatt/data-is-the-new-oil-dcad95dd25e6>. Ανάκτηση: Μάρτιος 2021.

Για το λόγο αυτό, εγείρονται πλέον σοβαρά ερωτήματα ηθικής και νομικής φύσης, αναφορικά με την εν γένει νομιμότητα της διαδικασίας αυτής, διότι γίνεται αντιληπτό ότι η προστασία της ιδιωτικότητας και η διασφάλιση των προσωπικών δεδομένων των χρηστών είναι εξαιρετικά δύσκολα επιτεύξιμοι στόχοι στη σύγχρονη εποχή. Στη βάση αυτής της εγγενούς ανησυχίας, τα τελευταία χρόνια, νομοθετικές πρωτοβουλίες επιχειρούν να οριοθετήσουν τον αντίκτυπο της τεχνητής νοημοσύνης τόσο στο νόμο όσο και στην κοινωνία.

Ειδικότερα, αναφορικά με το ζήτημα της συλλογής προσωπικών δεδομένων, τα συστήματα τεχνητής νοημοσύνης βελτιώνουν την ποιότητα και τις αποδόσεις τους μέσω αυτής. Συγκεκριμένα, τα συστήματα τεχνητής νοημοσύνης, συγκεντρώνουν και αναλύουν όσο το δυνατόν περισσότερα προσωπικά δεδομένα του χρήστη τους με σκοπό να τον κατηγοριοποιήσουν και να ανταποκριθούν στη συνέχεια με μεγαλύτερη ακρίβεια στα ενδιαφέροντά του¹¹. Κατ' αυτόν τον τρόπο, προσωποποιούνται για παράδειγμα οι διαφημίσεις που λαμβάνει ο χρήστης, οι οποίες επιλέγονται ως συμβατές με τις προτιμήσεις του, στη βάση προηγούμενης συλλογής δεδομένων που υποδείκνυε η δραστηριότητά του. Καθώς τα συστήματα αυτά εξαρτώνται απόλυτα από τα δεδομένα που θα συλλέξουν, έχουν διαμορφωθεί με τρόπο ώστε να συγκεντρώνουν το σύνολο των δεδομένων που παρέχονται σε αυτά, τα οποία εν συνεχεία μπορούν να κατηγοριοποιηθούν, ανάλογα με τον επιδιωκόμενο κάθε φορά σκοπό¹². Συνεπώς, είναι φανερό η στενή σχέση εξάρτησης που δημιουργείται ανάμεσα στα συστήματα της τεχνητής νοημοσύνης και τα προσωπικά δεδομένα, καθώς για την αποτελεσματικότερη λειτουργία των πρώτων χρειάζεται η συλλογή και επεξεργασία των δεύτερων. Το ανησυχητικό φαινόμενο βέβαια είναι ότι σε πολλές περιπτώσεις, η συλλογή και ανάλυση των συλλεγμένων δεδομένων γίνεται αυτόματα χωρίς να διασφαλίζεται η απαραίτητη γνώση του χρήστη¹³.

Τα συστήματα τεχνητής νοημοσύνης επηρεάζουν καταλυτικά την πληροφοριακή ιδιωτικότητα των χρηστών τους, φθάνοντας στο σημείο να προκαλούν

¹¹ Βλ. Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review*, 34(2), σελ. 257-268.

¹² Conti, M., Passarella, A., & Das, S. K. (2017). The Internet of People (IoP): A new wave in pervasive mobile computing. *Pervasive and Mobile Computing*, 41, 1-27.

¹³ Βλ. Information Commissioner Office – ICO (2017). Big data, artificial intelligence, machine learning and data protection. Διαθέσιμο στο <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Ανάκτηση: Μάρτιος 2021.

σε ορισμένες περιπτώσεις εύλογες ανησυχίες για την ίδια την αυτονομία των επιμέρους χρηστών. Ειδικότερα, η πληροφοριακή ιδιωτικότητα συνίσταται στο δικαίωμα καθενός να διαχειρίζεται αυτοτελώς τις πληροφορίες που τον αφορούν σε σχέση με τις προτιμήσεις του, τις πεποιθήσεις και τις αξίες του, καθώς και πληθώρα άλλων ευαίσθητων πληροφοριών που θα μπορούσαν να διαμορφώσουν την ταυτότητά του. Πρόκειται δηλαδή για το σημείο τομής του δικαιώματος στην ιδιωτική σφαίρα και της πληροφοριακής αυτοδιάθεσης¹⁴. Τα δεδομένα αυτά δε θα πρέπει να γίνονται αντικείμενο δημοσίου ελέγχου, καθώς θα μπορούσαν να οδηγήσουν στην ενίσχυση των διακρίσεων κάθε είδους. Η πληροφοριακή ιδιωτικότητα αντανακλά στην πραγματικότητα θεμελιώδη δημοκρατικά αξιώματα, όπως αυτά της ελευθερίας και της αξιοπρέπειας. Η μαζική συλλογή και περαιτέρω επεξεργασία των πληροφοριών αυτών, ενδεχομένως να θέσει σημαντικά εμπόδια στο προσωπικό δικαίωμα αυτοκαθορισμού του κάθε προσώπου, οι ευαίσθητες πληροφορίες του οποίου βρίσκονται πλέον σε μεγάλο βαθμό συγκεντρωμένες σε βάσεις δεδομένων¹⁵.

Σε επίπεδο ενωσιακού δικαίου, η νομοθεσία για την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων επιχειρεί να παρακολουθήσει, ήδη από τη δεκαετία του 1990 τις τεχνολογικές εξελίξεις στον τομέα αυτό¹⁶. Ο πρόσφατος Κανονισμός για τα προσωπικά δεδομένα, ο οποίος δεν αναφέρεται βέβαια ευθέως παρά μόνο σε ορισμένα σημεία στη χρήση συστημάτων τεχνητής νοημοσύνης επιχειρεί ωστόσο να συμπλεύσει με τις ραγδαίες τεχνολογικές εξελίξεις στον τομέα αυτό, επιδιώκοντας ταυτόχρονα τη διασφάλιση των θεμελιωδών δικαιωμάτων και ελευθεριών των επιμέρους προσώπων-χρηστών των συστημάτων τεχνητής νοημοσύνης¹⁷. Σκοπίμως βέβαια, στον Κανονισμό δεν γίνεται χρήση εξειδικευμένης τεχνολογικής ορολογίας, προκειμένου να διασφαλίζεται η ευρεία υπαγωγή στους

¹⁴ Παπαδόπουλος, Γ. Κ. (2006). *Πληροφοριακή Ιδιωτικότητα και ΜΜΕ*, Διπλωματική εργασία, Νομική Σχολή ΕΚΠΑ, σελ. 28. Διαθέσιμη στο <https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1323447/theFile>. Ανάκτηση: Ιούνιος 2021.

¹⁵ Βλ. Glancy, D. J. (2012). Privacy in autonomous vehicles. *Santa Clara L. Rev.*, 52, 1171.

¹⁶ Βλ. *Butterworth*, 2018.

¹⁷ Mitrou, L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? *Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'*, σελ. 24-26. Διαθέσιμο στο https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914. Ανάκτηση: Ιούνιος 2021.

τιθέμενους κανόνες τεχνολογικών εξελίξεων οι οποίες δεν ήταν τότε γνωστές στον ενωσιακό νομοθέτη. Σε κάθε πάντως περίπτωση, ο Κανονισμός οφείλει να εφαρμόζεται σε περιπτώσεις χρήσης συστημάτων τεχνητής νοημοσύνης, τόσο κατά το στάδιο της συλλογής, όσο και κατά το στάδιο της επεξεργασίας δεδομένων από τους αλγορίθμους¹⁸.

Σκοπός-στόχοι

Σκοπός του παρόντος πονήματος είναι η κατά το δυνατόν εξοικείωση του αναγνώστη με ένα σύγχρονο ζήτημα, που εγείρει πλέον οικουμενικό ενδιαφέρον. Ειδικότερα, η μελέτη επιδιώκει να διευκρινίσει ζητήματα αναφορικά με την έννοια της τεχνητής νοημοσύνης και τη χρήση αυτής και των εφαρμογών της, σε συνδυασμό και με γνώμονα την προστασία των προσωπικών δεδομένων, όπως αυτή παρέχεται από τον Κανονισμό 2016/679/ΕΕ. Βασική επιδίωξη της παρούσας εργασίας αποτελεί η διερεύνηση της συμβατότητας ή μη της χρήσης συστημάτων τεχνητή νοημοσύνης και της προστασίας των δεδομένων προσωπικού χαρακτήρα.

Διάρθρωση της μελέτης

Στο εν λόγω πόνημα, επιχειρείται η εξέταση γενικών ζητημάτων σχετιζόμενων με τις εφαρμογές τεχνητής νοημοσύνης υπό το πρίσμα των διατάξεων του Κανονισμού 2016/679/ΕΕ. Στο πρώτο κεφάλαιο, η εργασία επιδιώκει την εξοικείωση του αναγνώστη με τον ορισμό της έννοιας της τεχνητής νοημοσύνης και τους τρόπους με τους οποίους αυτή εφαρμόζεται. Στο επόμενο κεφάλαιο, αναπτύσσονται συνοπτικά τα άρθρα του Κανονισμού που αφορούν ζητήματα σχετιζόμενα με την έννοια της τεχνητής νοημοσύνης, τις βασικές αρχές της προστασίας και τη νομιμότητα της επεξεργασίας των δεδομένων. Εν συνεχεία, η εργασία επικεντρώνεται στις ειδικές κατηγορίες προσωπικών δεδομένων και καταπιάνεται συγκεκριμένα από τα βιομετρικά δεδομένα, ενώ επιχειρεί να οριοθετήσει την επιτρεπόμενη χρήση τους στο πεδίο της τεχνολογίας αναγνώρισης προσώπου. Το έβδομο κεφάλαιο αναλύει την έννοια της διαφάνειας, η οποία παίζει σημαντικό ρόλο κατά την εφαρμογή τεχνολογιών τεχνητής νοημοσύνης, ενώ αμέσως παρακάτω γίνεται μνεία στα δικαιώματα των υποκειμένων και στα εργαλεία συμμόρφωσης με τον ΓΚΠΔ. Αξιοσημείωτη είναι τέλος η αναφορά που κάνει ο ίδιος ο Κανονισμός στην αυτοματοποιημένη λήψη αποφάσεων και γι' αυτό το λόγο προτιμήθηκε η ανάλυση του ζητήματος εξολοκλήρου στο κεφάλαιο 9.

¹⁸ Mitrou, L. (2018), σελ. 26-27.

Καταληκτικά, αποτυπώνονται τα συμπεράσματα, που προκύπτουν από τη μελέτη ως προς τη συμβατότητα της τεχνητής νοημοσύνης και της προστασίας προσωπικών δεδομένων, ενώ παράλληλα γίνονται προτάσεις, που κινούνται προς αυτή την κατεύθυνση.

Μεθοδολογία

Για τη σύνταξη της παρούσας ακολουθήθηκε η εξής μέθοδος: αρχικά επιχειρήθηκε η αναλυτική μελέτη ελληνικών και ξενόγλωσσων συγγραμμάτων, άρθρων, μελετών και ερευνών σε σχέση με το υπό συζήτηση πρόβλημα. Εν συνεχεία επισκοπήθηκε ο υπάρχων Γενικός Κανονισμός με τα ζητήματα που αναφέρονται από τη χρησιμοποίηση τεχνητής νοημοσύνης στη σύγχρονη πραγματικότητα. Έπειτα, από το συνδυασμό των ανωτέρω, επιχειρήθηκε η ανεύρεση των νομικών προβλημάτων που μπορούν να προκύψουν από τα κανονιστικά ελλείμματα σε σχέση με τη χρήση μοντέλων τεχνητής νοημοσύνης. Τέλος, μέσω της συνδυαστικής αξιοποίησης των ανωτέρω στοιχείων, υποβλήθηκε το προτεινόμενο μοντέλο επίλυσης του υπό κρίση προβλήματος.

2. Τεχνητή νοημοσύνη

2.1 Ορισμός

Ως «νοημοσύνη» ορίζεται το σύνολο των πνευματικών λειτουργιών που χρησιμοποιούμε για να αντιμετωπίσουμε νέες καταστάσεις και να λύσουμε προβλήματα, αξιοποιώντας προηγούμενες εμπειρίες. Σχετικά με την ΤΝ έχουν διατυπωθεί ποικίλοι ορισμοί ανά τους καιρούς, οι οποίοι ταξινομούνται σε τέσσερις διαφορετικές κατηγορίες, ανάλογα με την προσέγγισή τους ως προς τον στόχο αυτής. Άλλοι προσεγγίζουν την ΤΝ ως ένα σύστημα που σκέπτεται σαν τον άνθρωπο ή σκέπτεται ορθολογικά, ενώ άλλοι την προσεγγίζουν ως ένα σύστημα που ενεργεί σαν τον άνθρωπο ή ενεργεί ορθολογικά. Συνδέοντας τις διαφορετικές προσεγγίσεις, προκύπτει ένας γενικότερος ορισμός για την ΤΝ, σύμφωνα με τον οποίο: «Τεχνητή νοημοσύνη είναι ο τομέας της επιστήμης των υπολογιστών, ο οποίος ασχολείται με τη σχεδίαση και υλοποίηση προγραμμάτων που μπορούν να μιμηθούν τις ανθρώπινες γνωστικές ικανότητες, εμφανίζοντας έτσι χαρακτηριστικά, που συνήθως αποδίδουμε

σε ανθρώπινη συμπεριφορά, όπως η μάθηση, η επίλυση προβλημάτων, η κατανόηση της φυσικής γλώσσας, η επίλυση προβλημάτων, κλπ.»¹⁹.

Με άλλα λόγια, η ΤΝ προσδιορίζεται ως η ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες του ανθρώπου, όπως η μάθηση, ο σχεδιασμός και η δημιουργικότητα²⁰. Ως εκ τούτου, καθιστά τις μηχανές ικανές να «κατανοούν» το περιβάλλον τους, να επιλύουν προβλήματα και να δρουν προς την επίτευξη ενός συγκεκριμένου στόχου. Ο υπολογιστής λαμβάνει δεδομένα (ήδη έτοιμα ή συλλεγμένα μέσω αισθητήρων, π.χ. μέσω κάμερας), τα επεξεργάζεται και ανταποκρίνεται βάσει αυτών. Τα συστήματα ΤΝ είναι ικανά να προσαρμόζουν τη συμπεριφορά τους, σε ένα ορισμένο βαθμό, αναλύοντας τις συνέπειες προηγούμενων δράσεων και επιλύοντας προβλήματα με αυτονομία.

2.2 Διακρίσεις

Η τεχνητή νοημοσύνη χωρίζεται σε δύο μεγάλες γενικές κατηγορίες²¹, που αναφέρονται κυρίως στην εξάρτηση της εφαρμογής από τη συμμετοχή του ανθρώπινου παράγοντα: την περιορισμένη ή αδύναμη και τη γενική ή ισχυρή τεχνητή νοημοσύνη.

2.2.1 Περιορισμένη τεχνητή νοημοσύνη

Στην περίπτωση αυτή, τα συστήματα δύνανται να εκτελούν μία ή συγκεκριμένες μόνο εργασίες, για τις οποίες έχουν ειδικά σχεδιαστεί²². Τα συστήματα αυτής της κατηγορίας μπορεί να είναι εξαιρετικά αξιόπιστα και αποτελεσματικά στην εργασία που έχουν προγραμματιστεί να επιτελούν, ωστόσο δε διαθέτουν καμία ικανότητα γενίκευσης ούτε μπορούν να «σκεφτούν» από μόνα τους²³. Ουσιαστικά

¹⁹ Γεωργούλη, Α. (2015). *Τεχνητή νοημοσύνη*, σελ. 13. Διαθέσιμο στο <https://repository.kallipos.gr/pdfviewer/web/viewer.html?file=/bitstream/11419/3381/1/Τεχνητή%20Νοημοσύνη.pdf>. Ανάκτηση: Ιούνιος 2021.

²⁰ Ευρωπαϊκό Κοινοβούλιο. (2020). *Τί είναι η Τεχνητή Νοημοσύνη και πώς χρησιμοποιείται;*. Διαθέσιμο στο <https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoeitai>. Ανάκτηση: Ιανουάριος 2021.

²¹ Τάσσης, Σπ. (2019). *Το Δίκαιο στην Εποχή της Τεχνητής Νοημοσύνης*, Lawspot, Διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis. Ανάκτηση: Μάρτιος 2021.

²² Κουσούνη-Πανταζοπούλου, Α. (2019). *Νομικές διαστάσεις της τεχνητής νοημοσύνης (παρόν και μέλλον)*, ΕλλΔνη 1/2019, Sakkoulas Online. Διαθέσιμο στο <https://www.sakkoulas-online.gr/reader/492bbd0fc687934eccbd/>. Ανάκτηση: Μάρτιος 2021.

²³ Βλ. σχετικά και UK-RAS NETWORK – Robotics & Autonomous Systems. (2017). *Artificial Intelligence and Robotics*, UK-RAS White papers, σελ. 29. Διαθέσιμο στο <https://www.ukras.org/wp->

βοηθούν τον άνθρωπο στην επίτευξη των σκοπών του, πρόκειται δηλαδή για μια ευφυή διάδραση και συνεργασία του ανθρώπου με τη μηχανή. Τα τελευταία χρόνια, η αύξηση της υπολογιστικής ισχύος των ηλεκτρονικών υπολογιστών, καθώς και η διάθεση μεγάλου όγκου δεδομένων έχουν συμβάλει αποφασιστικά στη σημείωση αξιοσημείωτης προόδου στον τομέα της περιορισμένης τεχνητής νοημοσύνης. Χαρακτηριστικά αναφέρονται οι περιπτώσεις των «chatbots»²⁴, τα οποία παρέχουν βοήθεια απαντώντας σε συγκεκριμένες ερωτήσεις, ο «deep blue»²⁵, ένας υπολογιστής σκακιού που αναπτύχθηκε από την εταιρεία IBM και κατάφερε να κερδίσει τον παγκόσμιο πρωταθλητή σκακιού Gary Kasparov, και το σύστημα ηλεκτρονικών υπολογιστών²⁶, το οποίο νίκησε τον πρωταθλητή του κινέζικου επιτραπέζιου παιχνιδιού «Go».

2.2.2 Γενική τεχνητή νοημοσύνη

Η γενική τεχνητή νοημοσύνη²⁷ έχει ως σκοπό την πραγμάτωση δραστηριοτήτων κατά τρόπο που να προσομοιάζει στον ανθρώπινο. Πρόκειται για την υπερνοημοσύνη που θα μπορεί να λειτουργεί σε νοητικό επίπεδο, όπως ο άνθρωπος. Σε αυτή την περίπτωση, το σύστημα δεν αφομοιώνει απλώς πληροφορίες, όπως κάνει ένα σύστημα περιορισμένης νοημοσύνης, που αναπτύχθηκε παραπάνω, αλλά είναι σε

content/uploads/2021/01/UKRASWP_ArtificialIntelligence2017_online.pdf. Ανάκτηση: Μάρτιος 2021.

²⁴ Το chatbot είναι μια εφαρμογή λογισμικού που χρησιμοποιείται για τη διεξαγωγή μιας συνομιλίας στο διαδίκτυο μέσω κειμένου ή κειμένου σε ομιλία, αντί της παροχής άμεσης επαφής με έναν ζωντανό ανθρώπινο πράκτορα. Διαθέσιμο στο <https://en.wikipedia.org/wiki/Chatbot>. Ανάκτηση: Δεκέμβριος 2020.

²⁵ Ο «deep blue» ήταν ένας υπολογιστής ο οποίος μπορούσε να παίζει σκάκι και κατασκευάστηκε από την IBM. Στις 11 Μαΐου 1997 νίκησε τον παγκόσμιο πρωταθλητή στο σκάκι Γκάρι Κασπάροφ στον εικοστό έκτο αγώνα, με δύο νίκες και τρεις ισοπαλίες. Διαθέσιμο στο https://el.wikipedia.org/wiki/Deep_blue. Ανάκτηση: Δεκέμβριος 2020.

²⁶ Ο AlphaGo χρησιμοποιεί ένα αλγόριθμο MCTS (Monte Carlo Tree Search) με συνδυασμό τεχνικών μηχανικής μάθησης με διακλαδώσεις, και ειδικότερα με εντατική εξάσκηση με παιχνίδια με ανθρώπους και με παιχνίδια με τον υπολογιστή. Διαθέσιμο στο <https://el.wikipedia.org/wiki/AlphaGo>. Ανάκτηση: Δεκέμβριος 2020.

²⁷ Στις αρχές, η γενική τεχνητή νοημοσύνη αναφερόταν ως «δυνατή». Βλ. και High Level Expert Group on Artificial Intelligence. (2018). *A definition of AI: Main capabilities and scientific disciplines*, σελ. 6. Διαθέσιμο στο <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Ανάκτηση: Απρίλιος: 2021.

θέση να τροποποιεί την ίδια του τη λειτουργία και να επαναπρογραμματίζεται αυτόνομα, προκειμένου να επιτελέσει γενικές εργασίες²⁸. Με βάση τα σημερινά επιστημονικά δεδομένα, έχουμε ακόμη αρκετό δρόμο έως τη γενική ΤΝ, καθώς είναι πολλές οι προκλήσεις σχετικά με την ανάπτυξη των ικανοτήτων των συστημάτων που απαιτούνται για την ένταξη στην κατηγορία αυτή, όπως για παράδειγμα η δυνατότητα των μηχανών να αυτοκαθορίζουν τον σκοπό τους, η επίτευξη κοινής λογικής κλπ²⁹. Θεωρείται ότι η ανάπτυξη της γενικής τεχνητής νοημοσύνης θα μπορούσε να οδηγήσει σε μία περίοδο τεχνολογικής εξέλιξης, η οποία θα άλλαζε βαθιά τον ανθρώπινο πολιτισμό.

2.3 Πεδία και εργαλεία εφαρμογών

2.3.1 Μηχανική μάθηση (Machine learning)

Η μάθηση αποτελεί μία από τις πιο θεμελιώδεις ιδιότητες του νοήμονος ανθρώπου και ορίζεται ως το φαινόμενο κατά το οποίο ένα σύστημα βελτιώνει την απόδοσή του κατά την εκτέλεση μιας συγκεκριμένης εργασίας, χωρίς να υπάρχει ανάγκη να προγραμματιστεί εκ νέου³⁰. Όσον αφορά τη μηχανική μάθηση, πρόκειται για μία δημοφιλή τεχνική του τομέα της τεχνητής νοημοσύνης, η οποία χρησιμοποιεί αλγόριθμους εκπαιδευμένους, οι οποίοι περιλαμβάνουν τεράστιες ποσότητες δεδομένων, με σκοπό τη βελτίωση της απόδοσης ενός συστήματος επί της εκτέλεσης συγκεκριμένης εργασίας, με την πάροδο του χρόνου. Οι εν λόγω εργασίες τείνουν να περιλαμβάνουν τη λήψη αποφάσεων ή την αναγνώριση μοτίβων, με πολυάριθμα πιθανά αποτελέσματα σε μία σειρά τομέων κι εφαρμογών.

Πιο συγκεκριμένα, μηχανική μάθηση ονομάζουμε τη δημιουργία μοντέλων ή προτύπων από ένα σύνολο δεδομένων που προέρχονται από ένα υπολογιστικό σύστημα. Ανάλογα με το είδος του προβλήματος έχουν αναπτυχθεί διάφορες τεχνικές μηχανικής μάθησης, δύο από αυτές είναι: η μάθηση με επίβλεψη, όπου το σύστημα

²⁸ Ένα τέτοιο σύστημα μπορεί π.χ. να είναι σε θέση να υποστηρίξει τον άνθρωπο στη βιομηχανική παραγωγή, να συζητά φιλοσοφικά ζητήματα και παράλληλα να παίζει δημιουργικά με παιδιά. Βλ. UK-RAS NETWORK – Robotics & Autonomous Systems, 2017.

²⁹ Βλ. και Consultive Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. (2019). *Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, σελ. 5. Διαθέσιμο στο <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>. Ανάκτηση: Ιανουάριος 2021.

³⁰ Γεωργούλη, Α. (2015), σελ. 127.

καλείται να μάθει από ένα σύνολο δεδομένων και η μάθηση χωρίς επίβλεψη, όπου το σύστημα πρέπει να μάθει από τη δημιουργία προτύπων³¹.

2.3.2 Βαθιά Μάθηση (Deep learning)

Η «βαθιά μάθηση» είναι ένα υποσύνολο της μηχανικής μάθησης, δηλαδή πρόκειται για ένα πεδίο που εξετάζει τους αλγορίθμους υπολογιστών που μαθαίνουν και βελτιώνονται μόνοι τους³². Με άλλα λόγια αποτελεί έναν άλλο τρόπο, για να περιγράψουμε τα μεγάλα νευρωνικά δίκτυα, μια τεχνολογία που συναντάμε κάθε μέρα όταν κάνουμε περιήγηση στο διαδίκτυο ή όταν χρησιμοποιούμε το κινητό μας τηλέφωνο. Η κατάρτιση ενός μοντέλου βαθιάς μάθησης απαιτεί πολλά δεδομένα. Μάλιστα, όσο περισσότερα είναι τα δεδομένα με τα οποία τροφοδοτείται, τόσο πιο ακριβές θα είναι και το μοντέλο deep learning. Οι επιστήμονες έχουν καταφέρει να προσεγγίσουν όλο και περισσότερο την κατασκευή μοντέλων βαθιάς μάθησης που έχουν μεγαλύτερη ακρίβεια και που μπορούν να μάθουν χωρίς επίβλεψη. Έτσι, η βαθιά μάθηση πρόκειται να γίνει ταχύτερη και να απαιτεί λιγότερη δουλειά³³.

2.3.3 Μεγάλα Δεδομένα (Big data)

Τα μεγάλα δεδομένα συνιστούν έναν ευρύτερο όρο για οποιαδήποτε συλλογή συνόλων δεδομένων τόσο μεγάλων και σύνθετων, που είναι δύσκολο να γίνει επεξεργασία με τη χρήση χειροκίνητων εργαλείων ή παραδοσιακών εφαρμογών επεξεργασίας δεδομένων³⁴. Η ανάπτυξη ενός συγκεκριμένου ορισμού, βάσει του οποίου οποιαδήποτε μορφή επεξεργασίας δεδομένων θα χαρακτηρίζεται αποκλειστικά ως μεγάλα δεδομένα ή όχι είναι δύσκολη. Τα μεγάλα δεδομένα έχουν περιγραφεί περισσότερο ως ένα φαινόμενο παρά ως μία τεχνολογία, διάκριση, η οποία έχει

³¹ Βλαχάβας, Ι., Κεφαλάς, Π., Βασιλειάδης, Ν., Κόκκορας, Φ., & Σακελλαρίου, Η. (2006). Τεχνητή νοημοσύνη. Γ' Έκδοση, Β. Γκιούρδας Εκδοτική.

³² Oppermann, A. (2019). *What is Deep Learning and How does it work?*, Towards Data Science. Διαθέσιμο στο <https://towardsdatascience.com/what-is-deep-learning-and-how-does-it-work-2ce44bb692ac>. Ανάκτηση: Απρίλιος 2021.

³³ Swanson, B.-M. (2017). *What is Deep Learning?*, Oracle AI and Data Science Blog. Διαθέσιμο στο <https://blogs.oracle.com/datascience/what-is-deep-learning>. Ανάκτηση: Μάρτιος 2021.

³⁴ Διαθέσιμο στο https://en.wikipedia.org/wiki/Big_data. Ανάκτηση: Ιανουάριος 2021.

αποδειχθεί ιδιαίτερα χρήσιμη³⁵. Σύμφωνα με το λεξικό Gartner IT³⁶, τα μεγάλα δεδομένα ορίζονται ως «πληροφοριακά στοιχεία, υψηλού όγκου, υψηλής ταχύτητας και μεγάλης ποικιλίας, τα οποία απαιτούν καινοτόμες και αποδοτικές, ως προς το κόστος, μορφές επεξεργασίας πληροφοριών, με σκοπό τη βελτίωση της λήψης αποφάσεων».

Όσον αφορά τον όγκο (volume), τα μεγάλα δεδομένα χρησιμοποιούν μαζικά σύνολα δεδομένων, συμπεριλαμβανομένων, για παράδειγμα, μεταδεδομένων από αναζήτηση στο διαδίκτυο, συναλλαγές με χρεωστικές και πιστωτικές κάρτες, αναρτήσεις σε μέσα κοινωνικής δικτύωσης, δεδομένα τοποθεσίας κινητού τηλεφώνου ή δεδομένα από αισθητήρες αυτοκινήτων και άλλων συσκευών. Ο όγκος των δεδομένων που υφίστανται επεξεργασία σε παγκόσμιο επίπεδο εξακολουθεί να αυξάνεται με γοργούς ρυθμούς. Παράλληλα, η διατήρηση πολύ μεγάλων όγκων δεδομένων καθίσταται δυνατή, χάρη στο συνεχώς μειούμενο κόστος αποθήκευσης και στη διαθεσιμότητα των υπηρεσιών που στηρίζονται στη τεχνολογία νέφους (cloud technology).

Σε επίπεδο ποικιλομορφίας (variety), τα μεγάλα δεδομένα περιλαμβάνουν, συχνά, τη σύνδεση δεδομένων που προέρχονται από διαφορετικές πηγές. Προς το παρόν, προκύπτει ότι οι αναλύσεις μεγάλων δεδομένων χρησιμοποιούν κυρίως δομημένα δεδομένα, όπως για παράδειγμα δεδομένα σε πίνακες με προκαθορισμένα πεδία, ενώ μπορεί να περιλαμβάνουν και μη δομημένα δεδομένα. Για παράδειγμα, είναι πιθανόν να προκύψει μία ροή από το σύνολο των δεδομένων που προέρχονται από συγκεκριμένη πηγή μέσω κοινωνικής δικτύωσης, όπως το Twitter. Σε τέτοιες περιπτώσεις, επιδιώκεται, συνήθως, η ανάλυση συναισθημάτων, δηλαδή η ανάλυση της άποψης των υποκειμένων για προϊόντα ή οργανισμούς. Ένας έμπορος λιανικής πώλησης μπορεί να συνδυάσει τα δεδομένα αυτά με δεδομένα που έχει συλλέξει ο ίδιος από σημεία πώλησης ή κάρτες πιστότητας, ώστε να παράξει λεπτομερή πληροφόρηση για σκοπούς μάρκετινγκ³⁷.

³⁵ Information Commissioner Office – ICO (2014). *Big data and data protection*. Διαθέσιμο στο <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220>.

Ανάκτηση: Ιανουάριος 2021.

³⁶ Βλ. Information Technology Gartner Glossary. Διαθέσιμο στο <https://www.gartner.com/en/information-technology/glossary/big-data>. Ανάκτηση: Ιανουάριος 2021.

³⁷ *Information Commissioner Office – ICO*. (2014), σελ. 8-9.

Τέλος, σε επίπεδο ταχύτητας (velocity), η ανάλυση των δεδομένων πραγματοποιείται όσο το δυνατόν πιο γρήγορα, ακόμη και σε πραγματικό χρόνο, προκειμένου να μπορεί να χρησιμοποιηθεί για την ανάλυση δεδομένων «σε κίνηση», ενόσω αυτά παράγονται ή καταγράφονται, καθώς και για την ανάλυση δεδομένων που βρίσκονται αποθηκευμένα. Μία πιθανή εφαρμογή ανάλυσης «σε κίνηση» αποτελούν οι πληρωμές με πιστωτικές κάρτες. Για παράδειγμα, η εταιρία VISA αναζητά, μέσω της ανάλυσης μεγάλων δεδομένων, την ανάπτυξη νέων τρόπων εξουσιοδότησης των πληρωμών με πιστωτική κάρτα³⁸.

2.3.4 Αλγόριθμοι

Ως αλγόριθμος ορίζεται μια πεπερασμένη σειρά ενεργειών, αυστηρά καθορισμένων και εκτελέσιμων σε πεπερασμένο χρόνο, που στοχεύουν στην επίλυση ενός προβλήματος³⁹. Πιο απλά, αλγόριθμο ονομάζουμε μία σειρά από εντολές που έχουν αρχή και τέλος, είναι σαφείς και έχουν ως σκοπό την επίλυση κάποιου προβλήματος. Για παράδειγμα, τα βήματα που ακολουθεί ένα παιδί για να πάει στο σχολείο θα μπορούσαν να είναι τα εξής: «Σήκω από το κρεβάτι», «Βγάλε τις πιτζάμες σου», «Βάλε τα ρούχα σου για το σχολείο», «Επισκέψου το μπάνιο», «Πάρε κλειδιά», «Βγες από το σπίτι», «Κλείδωσε», «Ακολούθησε τον δρόμο για το σχολείο»⁴⁰.

Οι αλγόριθμοι αναφέρονται σε οποιαδήποτε εντολή, όπως κώδικα ηλεκτρονικού υπολογιστή, η οποία εκτελεί ένα σύνολο άλλων εντολών. Πρόκειται για μία ενέργεια η οποία είναι απαραίτητη κατά την επεξεργασία δεδομένων από ηλεκτρονικό υπολογιστή.

2.3.5 Αυτοματοποιημένη λήψη αποφάσεων

Η διαδικασία αυτή περιλαμβάνει γενικά τη συλλογή δεδομένων μεγάλης κλίμακας από διάφορους αισθητήρες, την επεξεργασία των δεδομένων από αλγορίθμους και την αυτοματοποιημένη απόδοση αυτών. Πρόκειται για ένα αποτελεσματικό μέσο διαχείρισης, οργάνωσης και ανάλυσης μεγάλων όγκων δεδομένων και διαμόρφωσης της διαδικασίας λήψης αποφάσεων. Η αυτοματοποιημένη

³⁸ Όπως παραπάνω.

³⁹ Διαθέσιμο στο <https://el.wikipedia.org/wiki/Αλγόριθμος>. Ανάκτηση: Δεκέμβριος 2020.

⁴⁰ Προφανώς, για την επίτευξη του ίδιου σκοπού μπορούν να ακολουθηθούν διαφορετικά βήματα. Επίσης, η σειρά των βημάτων θα μπορούσε να είναι διαφορετική. Για παράδειγμα, κάποιο παιδί ενδέχεται να επισκεφθεί πρώτα το μπάνιο και έπειτα να βγάλει τα ρούχα του. Διαθέσιμο στο <https://contia.gr/αλγόριθμος/>. Ανάκτηση: Δεκέμβριος 2020.

λήψη αποφάσεων μπορεί να στηρίζεται ή να μη στηρίζεται στην τεχνητή νοημοσύνη, με το βαθμό της ανθρώπινης παρέμβασης να ποικίλλει. Περαιτέρω, μπορεί να λαμβάνει αποφάσεις και να δημιουργεί γνώση ή πληροφορία, επιδρώντας σε σημαντικό βαθμό στα ανθρώπινα δικαιώματα και ειδικά στα προσωπικά δεδομένα, όπως θα αναλυθεί παρακάτω.

Οι αποφάσεις αυτές μπορεί να βασίζονται σε οποιοδήποτε είδος δεδομένων, όπως δεδομένα παρεχόμενα απευθείας από τα φυσικά πρόσωπα (π.χ. απαντήσεις σε ερωτηματολόγιο), δεδομένα που αποτελούν προϊόντα παρατήρησης (π.χ. δεδομένα τοποθεσίας που συλλέγονται μέσω μιας εφαρμογής) ή εξαγόμενα δεδομένα, όπως η δημιουργία προφίλ ενός φυσικού προσώπου (π.χ. βαθμολόγηση πιστοληπτικής ικανότητας)⁴¹.

3. Η τεχνητή νοημοσύνη στο εννοιολογικό πλαίσιο του ΓΚΠΔ

Σε αντίθεση με την Οδηγία 95/46/EK⁴², ο Κανονισμός 2016/679 για την προστασία δεδομένων προσωπικού χαρακτήρα στο σύνολό του κάνει αναφορές σε όρους σχετικούς με το διαδίκτυο, όπως είναι τα μέσα κοινωνικής δικτύωσης, οι ιστότοποι και τα επιγραμμικά δεδομένα. Ωστόσο, δεν υπάρχει ρητή αναφορά στον όρο «τεχνητή νοημοσύνη» ούτε σε όρους που εκφράζουν σχετικές έννοιες, όπως ευφυή συστήματα, μηχανική μάθηση ή μεγάλα δεδομένα. Αυτό αντικατοπτρίζει το γεγονός ότι ο ΓΚΠΔ επικεντρώνεται στις προκλήσεις, που αναδύονται από το διαδίκτυο -οι οποίες δεν ελήφθησαν υπόψη στην Οδηγία για την προστασία των δεδομένων του 1995- παρά σε νέα θέματα που αφορούν την ΤΝ, η οποία άρχισε να αναδεικνύεται, κυρίως με κοινωνική σημασία, τα τελευταία χρόνια. Ωστόσο, όπως θα αναλύσουμε παρακάτω, πολλές διατάξεις του ΓΚΠΔ είναι σχετικές με την τεχνητή νοημοσύνη.

3.1 Η έννοια των δεδομένων προσωπικού χαρακτήρα

Θεμελιώδης για το ουσιαστικό πεδίο εφαρμογής του Κανονισμού είναι η έννοια των «δεδομένων προσωπικού χαρακτήρα», όπως αυτή ορίζεται στο άρθρο 4 παρ. 1. Η διάταξη του ΓΚΠΔ αφορά μόνο τα προσωπικά δεδομένα, αποκλείοντας πληροφορίες

⁴¹ Ομάδα εργασίας του άρθρου 29. (2018) Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού 2016/679. Διαθέσιμο στο https://www.dpa.gr/sites/default/files/2020-05/wp251rev01_el.pdf. Ανάκτηση: Ιούνιος 2021.

⁴² Οδηγία 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

που δεν αφορούν τον άνθρωπο (π.χ. δεδομένα για φυσικά φαινόμενα), καθώς και πληροφορίες που, αν και αφορούν τον άνθρωπο, δεν αναφέρονται σε συγκεκριμένα άτομα (π.χ. γενικές ιατρικές πληροφορίες για την ανθρώπινη φυσιολογία ή τις παθολογίες) ή έχουν ανωνυμοποιηθεί, ώστε να έχουν χάσει τη σύνδεσή τους με συγκεκριμένα άτομα. Πιο συγκεκριμένα, τα δεδομένα προσωπικού χαρακτήρα ορίζονται ως «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»⁴³. Η συνεισφορά του εν λόγω ορισμού, σε σχέση με τον προηγούμενο της Οδηγίας 95/46/EK, είναι ότι χαρακτηρίζει ρητά ως προσωπικά δεδομένα τα δεδομένα θέσεως και τα επιγραμμικά δεδομένα (δεδομένα σε απευθείας σύνδεση-online)⁴⁴.

Μέσω της ψευδωνυμοποίησης, τα στοιχεία δεδομένων που προσδιορίζουν ένα άτομο (π.χ. το όνομα) αντικαθίστανται με ένα ψευδώνυμο, ενώ ο σύνδεσμος μεταξύ του ψευδώνυμου και των στοιχείων αναγνώρισης δεδομένων μπορεί να ανιχνευθεί χρησιμοποιώντας ξεχωριστές πληροφορίες (π.χ. μέσω ενός πίνακα που συνδέει ψευδώνυμα και πραγματικά ονόματα). Στην αιτιολογική σκέψη 26 ορίζεται ότι «τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο και άρα προσωπικά δεδομένα»⁴⁵.

⁴³ Βλ. άρθρο 4 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

⁴⁴ Βλ. αναλυτικότερα Παναγοπούλου-Κουτνατζή, Φ. (2017). Ο Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων 679/2016/ΕΕ. Εκδόσεις Σακκουλάς.

⁴⁵ Βλ. αιτιολογική σκέψη 26 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Οι αρχές της προστασίας δεδομένων θα πρέπει να εφαρμόζονται σε κάθε πληροφορία η οποία αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, η οποία θα μπορούσε να αποδοθεί σε φυσικό πρόσωπο με τη χρήση συμπληρωματικών πληροφοριών, θα πρέπει να θεωρούνται πληροφορίες σχετικά με ταυτοποιήσιμο φυσικό πρόσωπο. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν, όπως για παράδειγμα ο διαχωρισμός του, είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου. Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα

Όσον αφορά τα ανωνυμοποιημένα δεδομένα, στην αιτιολογική σκέψη 9 του Κανονισμού 2018/1807⁴⁶ ορίζεται ότι εάν οι τεχνολογικές εξελίξεις καταστήσουν δυνατή τη μετατροπή ανωνυμοποιημένων δεδομένων σε δεδομένα προσωπικού χαρακτήρα, τότε αυτά τα δεδομένα θα αντιμετωπίζονται ως προσωπικά δεδομένα και κατ' επέκταση θα εφαρμόζεται ο ΓΚΠΔ.

Η έννοια των μη προσωπικών δεδομένων δεν ορίζεται θετικά στη νομοθεσία της ΕΕ, οπότε θα μπορούσαμε να πούμε ότι περιλαμβάνει όσα δεδομένα δεν αποτελούν προσωπικά δεδομένα, όπως αυτά ορίζονται στον ΓΚΠΔ. Ο Κανονισμός 2018/1807 παρέχει τα ακόλουθα παραδείγματα μη προσωπικών δεδομένων:

- συγκεντρωτικά και ανωνυμοποιημένα σύνολα δεδομένων που χρησιμοποιούνται για την ανάλυση μαζικών δεδομένων,
- δεδομένα για τη γεωργία ακριβείας που μπορούν να συμβάλουν στην παρακολούθηση και τη βελτιστοποίηση της χρήσης φυτοφαρμάκων και νερού, ή
- δεδομένα σχετικά με τις ανάγκες συντήρησης για βιομηχανικά μηχανήματα⁴⁷.

χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας. Οι αρχές της προστασίας δεδομένων δεν θα πρέπει συνεπώς να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή πληροφορίες που δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί ή να μην μπορεί πλέον να εξακριβωθεί. Ο παρών κανονισμός δεν αφορά συνεπώς την επεξεργασία τέτοιων ανώνυμων πληροφοριών, ούτε μεταξύ άλλων για στατιστικούς ή ερευνητικούς σκοπούς.».

⁴⁶ Κανονισμός (ΕΕ) 2018/1807 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14^{ης} Νοεμβρίου 2018 σχετικά με ένα πλαίσιο για την ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση.

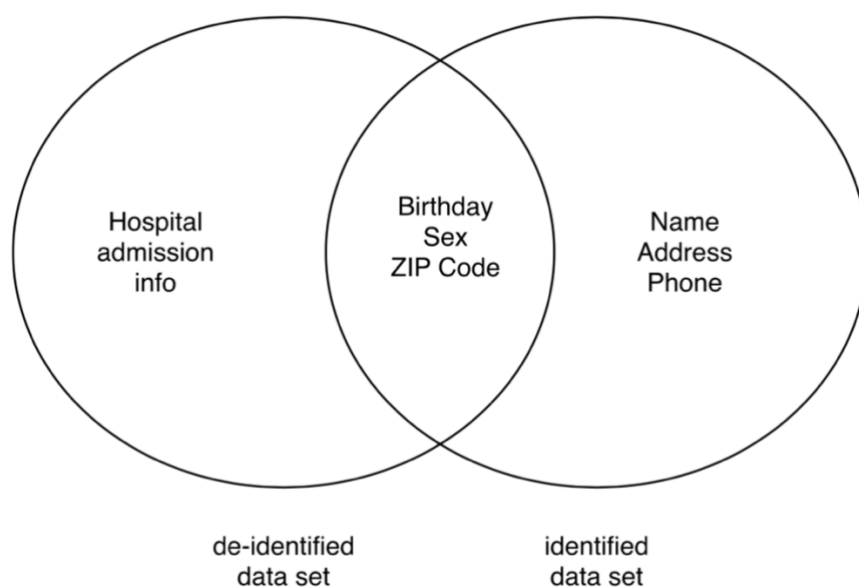
⁴⁷ Βλ. αιτιολογική σκέψη 9 του Κανονισμού 2018/1807/ΕΕ: «Μεγάλες πηγές δεδομένων μη προσωπικού χαρακτήρα είναι το επεκτεινόμενο διαδίκτυο των πραγμάτων, η τεχνητή νοημοσύνη και η εκμάθηση μηχανής, για παράδειγμα ως αποτέλεσμα της χρήσης τους σε αυτοματοποιημένες διαδικασίες βιομηχανικής παραγωγής. Συγκεκριμένα παραδείγματα δεδομένων μη προσωπικού χαρακτήρα είναι τα συγκεντρωτικά και ανωνυμοποιημένα σύνολα δεδομένων που χρησιμοποιούνται για την ανάλυση μαζικών δεδομένων, τα δεδομένα για τη γεωργία ακριβείας που μπορούν να συμβάλουν στην παρακολούθηση και τη βελτιστοποίηση της χρήσης φυτοφαρμάκων και νερού ή τα δεδομένα σχετικά με τις ανάγκες συντήρησης για βιομηχανικά μηχανήματα. Εάν οι τεχνολογικές εξελίξεις καταστήσουν δυνατή τη μετατροπή ανωνυμοποιημένων δεδομένων σε δεδομένα προσωπικού χαρακτήρα, τότε αυτά τα δεδομένα θα

Όπως ορίζονται εννοιολογικά τα δεδομένα προσωπικού χαρακτήρα στον ΓΚΠΔ, εγείρονται δύο καίρια ζητήματα όσον αφορά την τεχνητή νοημοσύνη. Αρχικά, το ζήτημα της συσχέτισης των ανωνυμοποιημένων δεδομένων με προσωπικά δεδομένα του υποκειμένου και κατά δεύτερον της εξαγωγής περαιτέρω προσωπικών πληροφοριών από προσωπικά δεδομένα που είναι ήδη διαθέσιμα, τα οποία αναλύονται αμέσως κατωτέρω.

3.1.1 Η συσχέτιση των δεδομένων

Η τεχνητή νοημοσύνη, η μηχανική μάθηση και γενικότερα οι σύγχρονες τεχνολογίες αυξάνουν την δυνατότητα ταυτοποίησης των φαινομενικά ανώνυμων δεδομένων, καθώς επιτρέπουν τη σύνδεση μη ταυτοποιήσιμων δεδομένων (συμπεριλαμβανομένων των δεδομένων που έχουν ανωνυμοποιηθεί ή ψευδωνυμοποιηθεί) με άλλα δεδομένα προσωπικού χαρακτήρα των υποκειμένων.

Η εκ νέου ταυτοποίηση των υποκειμένων των δεδομένων βασίζεται συνήθως σε στατιστικούς συσχετισμούς μεταξύ μη ταυτοποιήσιμων και ταυτοποιήσιμων δεδομένων που αφορούν τα ίδια υποκείμενα.



Διάγραμμα 1. Η σχέση μεταξύ ταυτοποιήσιμου και μη ταυτοποιήσιμου συνόλου δεδομένων⁴⁸.

αντιμετωπίζονται ως δεδομένα προσωπικού χαρακτήρα και θα εφαρμόζεται αναλόγως ο Κανονισμός (ΕΕ) 2016/679.».

⁴⁸ European Parliament - EPRS. (2020) *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, Scientific Foresight Unit. Διαθέσιμο στο

Το Διάγραμμα 1 απεικονίζει τη σύνδεση μεταξύ ενός ταυτοποιήσιμου και ενός μη ταυτοποιήσιμου συνόλου δεδομένων, που επέτρεψε την εκ νέου ταυτοποίηση του αρχείου υγείας του κυβερνήτη της Μασαχουσέτης. Πιο συγκεκριμένα, γίνεται αντιπαραβολή μίας λίστας ψηφοφόρων με μία ανωνυμοποιημένη λίστα νοσηλευόμενων ενός δημοσίου νοσοκομείου. Αυτό το αποτέλεσμα αποκτήθηκε αναζητώντας μη ταυτοποιήσιμα δεδομένα, που ταίριαζαν με την ημερομηνία γέννησης του κυβερνήτη, τον ταχυδρομικό κώδικα και το φύλο του⁴⁹. Σύμφωνα με αυτή την έρευνα, το 87% του πληθυσμού των ΗΠΑ μπορεί να ταυτοποιηθεί από την τριπλέτα «ταχυδρομικός κώδικας, ημερομηνία γεννήσεως και φύλο».

Αντίστοιχο παράδειγμα αποτελεί η περίπτωση της βάσης δεδομένων του Netflix, στην οποία οι ανώνυμες αξιολογήσεις ταινιών θα μπορούσαν να ταυτοποιηθούν εκ νέου, συνδέοντάς τις με τις μη ανωνυμοποιημένες αξιολογήσεις στο IMDb (βάση δεδομένων ταινιών διαδικτύου). Στην πραγματικότητα, γνωρίζοντας μόνο δύο μη ανωνυμοποιημένες κριτικές από έναν χρήστη του IMDb, δύναται να προσδιοριστούν οι κριτικές από τον ίδιο χρήστη στην ανώνυμη βάση δεδομένων. Ομοίως, έχει αποδειχθεί ότι ένας ανώνυμος χρήστης μιας διαδικτυακής υπηρεσίας μπορεί να ταυτοποιηθεί από μία υπηρεσία, εάν αυτή γνωρίζει ότι ο χρήστης έχει εγκαταστήσει συγκεκριμένο αριθμό εφαρμογών στη συσκευή του και ότι η υπηρεσία έχει πρόσβαση σε ολόκληρη τη λίστα των εφαρμογών που εγκαθίστανται από κάθε χρήστη⁵⁰.

Χάρη στην τεχνητή νοημοσύνη και τα μεγάλα δεδομένα, η ταυτοποίηση των υποκειμένων των δεδομένων έχει διευκολυνθεί και αυξηθεί ραγδαία. Ο προσωπικός χαρακτήρας ενός αναγνωριστικού δεδομένων δεν θεωρείται πλέον χαρακτηριστικό αυτού του στοιχείου ξεχωριστά. Έχει μάλλον γίνει χαρακτηριστικό με βάση τα συμφραζόμενα. Όπως φαίνεται και παραπάνω, ένα φαινομενικά ανωνυμοποιημένο στοιχείο δεδομένων αποκτά προσωπικό χαρακτήρα στο πλαίσιο περαιτέρω προσωπικών δεδομένων που επιτρέπουν την εκ νέου ταυτοποίηση. Για παράδειγμα, η αναγνωρισιμότητα των κριτικών ταινιών Netflix ενισχύεται από τη διαθεσιμότητα των

[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf). Ανάκτηση: Απρίλιος 2021.

⁴⁹ Sweeney, L. (2000). Simple demographics often identify people uniquely. *Health (San Francisco)*, 671(2000), 1-34.

⁵⁰ Achara, J. P., Acs, G., & Castelluccia, C. (2015). On the unicity of smartphone applications. Σε *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, σελ. 27-36.

ονομαστικών κριτικών τους στο IMDb. Όπως υποστηρίχθηκε, σε οποιοδήποτε εύλογο περιβάλλον υπάρχει μια πληροφορία που από μόνη της είναι «αθώα», αλλά σε συνδυασμό με ακόμη και μια τροποποιημένη έκδοση των δεδομένων προκαλεί παραβίαση απορρήτου⁵¹.

3.1.2 Η εξαγωγή περαιτέρω δεδομένων από ήδη διαθέσιμα προσωπικά δεδομένα (Re-identification)

Όπως σημειώθηκε παραπάνω, τα συστήματα TN μπορούν να εξάγουν νέες πληροφορίες σχετικά με τα προσωπικά δεδομένα, εφαρμόζοντας αλγοριθμικά μοντέλα σε αυτά. Το βασικό ζήτημα, υπό το πρίσμα της προστασίας των δεδομένων προσωπικού χαρακτήρα, είναι εάν οι νέες πληροφορίες πρέπει να αντιμετωπίζονται ως νέα προσωπικά δεδομένα, διαφορετικά από τα δεδομένα από τα οποία συνήχθη το συμπέρασμα. Ας υποθέσουμε, για παράδειγμα, ότι ο σεξουαλικός προσανατολισμός ενός ατόμου συνάγεται από τα χαρακτηριστικά του προσώπου του ή ότι ο τύπος της προσωπικότητας ενός ατόμου συνάγεται από τη διαδικτυακή του δραστηριότητα. Ως εκ τούτου, ο σεξουαλικός προσανατολισμός ή η προσωπικότητα αποτελούν νέο κομμάτι προσωπικών δεδομένων; Εάν ναι, τότε αυτό ισχύει ακόμη και στην περίπτωση που το συμπέρασμα που εξήχθη δεν είναι βέβαιο και αποτελεί μία πιθανότητα; Εάν θεωρηθεί ότι τα συμπεράσματα, που εξάγονται, υπολογίζονται ως νέα προσωπικά δεδομένα, τότε η αυτοματοποιημένη εξαγωγή συμπερασμάτων θα μπορούσε να προκαλέσει όλες τις συνέπειες της επεξεργασίας των προσωπικών δεδομένων σύμφωνα με τον ΓΚΠΔ (π.χ. ανάγκη μιας νομικής βάσης για την επεξεργασία, όροι για την επεξεργασία ευαίσθητων δεδομένων, δικαιώματα του υποκειμένου των δεδομένων).

Προκειμένου να ορισθεί ένα νομικό καθεστώς σχετικά με τις πληροφορίες που συνάγονται αυτόματα, δηλαδή με αυτοματοποιημένες διαδικασίες, χρήσιμο είναι να ληφθεί υπόψη η αντιμετώπιση του ζητήματος όσον αφορά τις μη αυτοματοποιημένες διαδικασίες. Είναι γεγονός πως υπάρχει αβεβαιότητα σχετικά με το εάν τα συμπεράσματα, που εξάγονται από μη αυτοματοποιημένες διαδικασίες μπορούν να θεωρηθούν ως προσωπικά δεδομένα. Το ζήτημα αυτό εξετάστηκε από το ΔΕΚ στις συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, όπου αρνήθηκε ότι η νομική ανάλυση από τον αρμόδιο αξιωματικό σχετικά με αίτηση για άδεια παραμονής θα

⁵¹ Dwork, C., Naor, M., Pitassi, T., & Rothblum, G. N. (2010). Differential privacy under continual observation. Σε *Proceedings of the forty-second ACM symposium on Theory of computing*, σελ. 715-724.

μπορούσε να υπαχθεί στα προσωπικά δεδομένα⁵². Σύμφωνα με το ΔΕΚ και τον γενικό Εισαγγελέα, μόνο τα δεδομένα στα οποία βασίστηκε η ανάλυση (δηλαδή τα δεδομένα εισαγωγής για τον αιτούντα), καθώς και το τελικό συμπέρασμα της ανάλυσης (η διαπίστωση ότι η αίτηση απορρίφθηκε) έπρεπε να θεωρηθούν προσωπικά δεδομένα. Δεν μπορούσε όμως να ισχύσει το ίδιο και για τα ενδιάμεσα στάδια.

Στην επακόλουθη απόφαση για την υπόθεση C-434/16⁵³, σχετικά με το αίτημα ενός υποψηφίου να ασκήσει τα δικαιώματά του για την προστασία δεδομένων προσωπικού χαρακτήρα σχετικά με τις εξετάσεις και τα σχόλια των εξεταστών, το ΔΕΚ ξέφυγε από το σκεπτικό που ανέπτυξε στις υποθέσεις C-141/12 και C-372/12, υποστηρίζοντας ότι και τα σχόλια του εξεταστή αποτελούν προσωπικά δεδομένα. Ωστόσο, το Δικαστήριο όρισε ότι τα δικαιώματα προστασίας δεδομένων, και ιδίως το δικαίωμα της διόρθωσης, θα πρέπει να κατανοούνται σε σχέση με τον σκοπό των επίμαχων δεδομένων. Επομένως, σύμφωνα με το Δικαστήριο, το δικαίωμα διόρθωσης δεν περιλαμβάνει δικαίωμα διόρθωσης των απαντήσεων ενός υποψηφίου ή των σχολίων του εξεταστή (εκτός εάν καταγράφηκαν εσφαλμένα). Στην πραγματικότητα, σύμφωνα με το ΔΕΚ, ο νόμος περί προστασίας δεδομένων δεν αποσκοπεί στη διασφάλιση της ακρίβειας των διαδικασιών λήψης αποφάσεων ή ορθών διοικητικών πρακτικών. Έτσι, ένας εξεταστής έχει το δικαίωμα να έχει πρόσβαση τόσο στα δεδομένα των εξετάσεων (στις απαντήσεις των εξετάσεων) όσο και στη συλλογιστική που βασίζεται σε τέτοια δεδομένα (τα σχόλια), αλλά αυτός ή αυτή δεν έχει δικαίωμα να διορθώσει τα συμπεράσματα των εξεταστών (το σκεπτικό) ή το τελικό αποτέλεσμα.

3.2 Η κατάρτιση προφίλ

Προκειμένου να επιτευχθεί η κατάρτιση προφίλ απαιτείται επεξεργασία δεδομένων, η οποία στηρίζεται εμφανώς σε τεχνολογίες τεχνητής νοημοσύνης. Αυτή η επεξεργασία συνίσταται στη χρήση των δεδομένων που αφορούν το άτομο για την εξαγωγή πληροφοριών σχετικά με περαιτέρω πτυχές του ίδιου ατόμου. Στο άρθρο 4

⁵² Συνεκδικασθείσες υποθέσεις ΔΕΚ C-141/12 και C-372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel. (2014). Διαθέσιμες στο <http://curia.europa.eu/juris/document/document.jsf?jsessionid=321F7A8E18D8C2D9E1A03C78EA34596D?text=&docid=155114&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1014939>. Ανάκτηση: Φεβρουάριος 2021.

⁵³ Υπόθεση C-434/16, Peter Nowak v. Data Protection Commissioner. (2017). Διαθέσιμη στο <https://curia.europa.eu/juris/document/document.jsf?text=&docid=198059&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=5643272>. Ανάκτηση: Φεβρουάριος 2021.

του Κανονισμού η κατάρτιση προφίλ ορίζεται ως «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα, που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου»⁵⁴.

Σύμφωνα με την Ομάδα εργασίας του άρθρου 29, η κατάρτιση προφίλ στοχεύει στην ταξινόμηση των ατόμων σε κατηγορίες ομάδων που μοιράζονται τα χαρακτηριστικά που συνάγονται⁵⁵. Σε γενικές γραμμές, η δημιουργία προφίλ σημαίνει συλλογή πληροφοριών για ένα άτομο (ή ομάδα ατόμων) και αξιολόγηση των χαρακτηριστικών ή των προτύπων συμπεριφοράς τους, με αποτέλεσμα αυτά να τοποθετούνται σε μια συγκεκριμένη κατηγορία ή ομάδα, με κύριο στόχο την ανάλυση και/ή την πραγματοποίηση προβλέψεων.

3.2.1 Η κατάρτιση προφίλ με τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη και τα μεγάλα δεδομένα, σε συνδυασμό με τη διαθεσιμότητα εκτεταμένων υπολογιστικών πόρων, έχουν αυξήσει σημαντικά τις ευκαιρίες και έχουν διευκολύνει τη διαδικασία κατάρτισης προφίλ. Πράγματι, οι προσεγγίσεις που βασίζονται στη μηχανική μάθηση, όπως περιγράφεται στις προηγούμενες ενότητες, συχνά προορίζονται να παρέχουν συμπεράσματα -όπως ταξινομήσεις, προβλέψεις ή αποφάσεις- όταν εφαρμόζονται σε δεδομένα που αφορούν πρόσωπα.

Ένας ταξινομητής, για παράδειγμα, έχει εκπαιδευτεί σε ένα τεράστιο σύνολο προηγούμενων παραδειγμάτων, τα οποία συνδέουν ορισμένα χαρακτηριστικά των ατόμων (προβλέψεις), με ένα άλλο χαρακτηριστικό των ίδιων ατόμων (στόχος). Μέσω της εκπαίδευσης, το σύστημα έχει μάθει ότι ένα αλγοριθμικό μοντέλο μπορεί να εφαρμοστεί σε νέες περιπτώσεις: εάν το μοντέλο έχει προγνωστικές τιμές για ένα νέο άτομο, προσδίδει μια αντίστοιχη τιμή-στόχο για αυτό το άτομο, δηλαδή ένα νέο στοιχείο δεδομένων που το αφορά⁵⁶.

⁵⁴ Βλ. άρθρο 4 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

⁵⁵ Ομάδα εργασίας του άρθρου 29. (2018), σελ. 7.

⁵⁶ European Parliament – EPRS. (2020), σελ. 39.

Για παράδειγμα, η πιθανότητα εμφάνισης καρδιακής νόσου των αιτούντων ασφάλιση μπορεί να προβλεφθεί με βάση τα αρχεία της υγείας τους, αλλά και βάσει καθημερινών συνηθειών (όπως η διατροφή, η σωματική άσκηση). Αντίστοιχα, η πιστοληπτική ικανότητα των αιτούντων δάνειο μπορεί να προβλεφθεί βάσει του οικονομικού ιστορικού τους, αλλά και βάσει της διαδικτυακής δραστηριότητας και της κοινωνικής τους κατάστασης. Αυτές οι προβλέψεις μπορεί να προκαλέσουν αυτοματοποιημένους προσδιορισμούς που αφορούν, αντίστοιχα, την τιμή της ασφάλισης υγείας ή τη χορήγηση ενός δανείου.

Μια συνηθισμένη εκπαίδευση που λαμβάνουν τα συστήματα μπορεί επίσης να αφορά την τάση ενός ατόμου να ανταποκρίνεται με ορισμένους τρόπους σε ορισμένα ερεθίσματα. Αυτό θα επέτρεπε τη μετάβαση από την πρόβλεψη σε ενδεχόμενη τροποποίηση συμπεριφοράς (τόσο νόμιμη επιρροή όσο και παράνομη ή ανήθικη χειραγώγηση). Ας υποθέσουμε, για παράδειγμα, ότι ένα σύστημα «μαθαίνει» μια συσχέτιση μεταξύ ορισμένων χαρακτηριστικών και δραστηριοτήτων (αγορές, προτιμήσεις κ.λπ.) ενός ατόμου και του προφίλ του ως συγκεκριμένου τύπου καταναλωτή και ότι το σύστημα έχει επίσης μάθει (ή έχει ενημερωθεί) ότι αυτό το είδος καταναλωτή ενδιαφέρεται για ορισμένα προϊόντα και είναι πιθανό να ανταποκριθεί σε συγκεκριμένα είδη διαφημίσεων⁵⁷. Κατά συνέπεια, μπορεί να στείλει σε ένα άτομο, που έχει αυτές τις δυνατότητες και έχει εμπλακεί σε τέτοιες δραστηριότητες, τα μηνύματα που είναι πιθανότερο να προκαλέσουν την επιθυμητή αγοραστική συμπεριφορά. Το ίδιο μοντέλο μπορεί να επεκταθεί και στην πολιτική, όσον αφορά τα μηνύματα που μπορεί να προκαλέσουν την επιθυμητή συμπεριφορά ψηφοφορίας, όπως συνέβη στην κάτωθι περίπτωση.

3.2.2 Η υπόθεση της Cambridge Analytica

Οι κίνδυνοι που ελλοχεύουν από την κατάρτιση προφίλ παρουσιάστηκαν ενδελεχώς στην υπόθεση της Cambridge Analytica. Η συγκεκριμένη υπόθεση σχετίζεται με απόπειρες επηρεασμού της συμπεριφοράς των ψήφων των πολιτών -στις εκλογές των Ηνωμένων Πολιτειών της Αμερικής του 2016 και πιθανώς και στο δημοψήφισμα του Brexit- με βάση τη μαζική επεξεργασία προσωπικών δεδομένων.

Αρχικά, τα άτομα που είχαν εγγραφεί ως ψηφοφόροι στις ΗΠΑ κλήθηκαν να λάβουν μέρος σε ένα λεπτομερές τεστ προσωπικότητας με πολιτικό χαρακτήρα διαθέσιμο στο διαδίκτυο (που περιλάμβανε περίπου 120 ερωτήσεις). Τα άτομα που θα

⁵⁷ Όπως παραπάνω.

λάμβαναν το τεστ, επρόκειτο να ανταμειφθούν με ένα μικρό χρηματικό ποσό (από δύο έως πέντε δολάρια), με την προϋπόθεση ότι τα δεδομένα που θα συλλέγονταν, θα χρησιμοποιούνταν για σκοπούς ακαδημαϊκής έρευνας.

Αυτό είχε ως αποτέλεσμα περίπου 320.000 ψηφοφόροι να συμμετάσχουν στη διαδικτυακή έρευνα. Κάθε άτομο, προκειμένου να λάβει τη συμφωνηθείσα αμοιβή, έπρεπε να παρέχει πρόσβαση στην προσωπική του σελίδα στο Facebook. Αυτό επέτρεψε στο σύστημα να συνδέσει τις απαντήσεις κάθε ατόμου με τις πληροφορίες που περιλαμβάνονται στη σελίδα του στο Facebook. Κατά την πρόσβαση στη σελίδα ενός δοκιμαστή, η Cambridge Analytica συγκέντρωσε όχι μόνο δεδομένα από τη σελίδα Facebook των δοκιμαστών, αλλά και από τις σελίδες Facebook των φίλων τους, δηλαδή συνολικά μεταξύ 30 και 50 εκατομμυρίων ατόμων. Μετά από αυτήν τη φάση συλλογής δεδομένων, η Cambridge Analytica διέθεσε δύο σύνολα προσωπικών δεδομένων προς επεξεργασία: τα δεδομένα σχετικά με τους δοκιμαστές, που συνίστανται στις πληροφορίες από τις σελίδες τους στο Facebook σε συνδυασμό με τις απαντήσεις τους στο ερωτηματολόγιο, και τα δεδομένα σχετικά με τους φίλους τους, που αποτελούνται μόνο από τις πληροφορίες της σελίδας τους στο Facebook.

Η Cambridge Analytica χρησιμοποίησε τα δεδομένα σχετικά με τους συμμετέχοντες στις δοκιμές ως εκπαιδευτικό σύνολο για τη δημιουργία ενός μοντέλου για την προβολή των φίλων τους και άλλων ατόμων. Πιο συγκεκριμένα, τα δεδομένα σχετικά με τους συμμετέχοντες στις δοκιμές αποτελούσαν ένα τεράστιο σετ εκπαίδευσης, όπου οι πληροφορίες από τις σελίδες Facebook ενός ατόμου (όπως «Like», δημοσιεύσεις, σύνδεσμοι κ.λπ.) παρείχαν τιμές για προβλέψεις (χαρακτηριστικά), ενώ οι απαντήσεις στο ερωτηματολόγιο (και ψυχολογικές και πολιτικές στάσεις που εκφράστηκαν με τέτοιες απαντήσεις) παρείχαν τις τιμές στους στόχους.

Χάρη στους αλγόριθμους, η Cambridge Analytica μπορούσε να χρησιμοποιήσει αυτά τα δεδομένα για να δημιουργήσει ένα μοντέλο που συσχετίζει τις πληροφορίες στις σελίδες του Facebook με τις προβλέψεις σχετικά με την ψυχολογία του ατόμου και τις πολιτικές του προτιμήσεις. Σε αυτό το σημείο η Cambridge Analytica ασχολήθηκε με μαζική κατάρτιση προφίλ, δηλαδή, με την επέκταση των διαθέσιμων δεδομένων για τα άτομα που δεν έλαβαν τη δοκιμή (τα δεδομένα τους στο Facebook και τυχόν περαιτέρω δεδομένα που ήταν διαθέσιμα σε αυτά), με τις προβλέψεις που παρέχονται από το μοντέλο. Για παράδειγμα, εάν οι δοκιμαστές που έχουν ένα συγκεκριμένο μοτίβο επισημάνσεων «Like» και οι αναρτήσεις στο Facebook

ταξινομήθηκαν ως νευρωτικές προσωπικότητες, η ίδια αξιολόγηση θα μπορούσε να επεκταθεί και σε μη δοκιμαστές που έχουν παρόμοια μοτίβα στα δεδομένα τους στο Facebook.

Τελικά, όπως επιβεβαιώνεται από την ίδια την Επιτροπή εστάλησαν στην Cambridge Analytica τα προσωπικά δεδομένα έως και 2,7 εκ. Ευρωπαίων ή προσώπων που διαμένουν στην ΕΕ, ενδεχομένως με ανάρμοστο τρόπο. Αξίζει μάλιστα να σημειωθεί ότι η υπόθεση Facebook αποτελεί χαρακτηριστικό παράδειγμα παραβίασης προσωπικών δεδομένων από την ίδια την επιχείρηση (δηλαδή από τον υπεύθυνο της επεξεργασίας). Για τη χρήση των δεδομένων από την Cambridge Analytica δεν χρειάστηκε καμία εξωτερική παραβίαση συστημάτων ή κακόβουλη επίθεση από hackers. Δυστυχώς, το ίδιο το σύστημα είχε σχεδιαστεί με τέτοιο τρόπο ώστε να είναι δυνατή η χρήση των δεδομένων του χωρίς ιδιαίτερη δυσκολία⁵⁸.

4. Οι βασικές αρχές προστασίας προσωπικών δεδομένων

Ο Κανονισμός κατοχυρώνει στο άρθρο 5 τις γενικές αρχές που διέπουν την επεξεργασία των προσωπικών δεδομένων. Οι αρχές αυτές, που πρέπει να συντρέχουν σωρευτικά, συμπυκνώνουν την ουσία των ρυθμίσεων της προστασίας δεδομένων και αποδίδουν τη γενική φιλοσοφία των ειδικότερων διατάξεων του Κανονισμού.

Έχει παρατηρηθεί ότι η τεχνητή νοημοσύνη και τα μεγάλα δεδομένα δύνανται να θέσουν υπό αμφισβήτηση και κίνδυνο βασικές αρχές προστασίας δεδομένων⁵⁹. Σε αυτήν την ενότητα, θα εξετάσουμε κάθε αρχή ξεχωριστά, ώστε να προσδιορίσουμε το βαθμό στον οποίο αυτή μπορεί να κινδυνεύει από τις τεχνολογίες της τεχνητής νοημοσύνης.

4.1 Νομιμότητα, αντικειμενικότητα και διαφάνεια

Η αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας, η οποία είναι η βασική αρχή που διέπει την επεξεργασία προσωπικών δεδομένων, ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων⁶⁰.

⁵⁸ Βλ. Ομάδα Εργασίας του ΣΕΒ για τα Προσωπικά Δεδομένα. (2018) *Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)*, σελ. 76-80. Διαθέσιμο στο https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf. Ανάκτηση: Ιανουάριος 2021.

⁵⁹ *European Parliament – EPRS*. (2020), σελ. 44.

⁶⁰ Βλ. άρθρο 5 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

Η έννοια της διαφάνειας καθορίζεται στην αιτιολογική σκέψη 58, η οποία εστιάζει στη συνοπτικότητα, την προσβασιμότητα, την εύκολη κατανόηση και τη σαφήνεια. Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και κατανοητή, και να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, όπου απαιτείται, απεικόνιση⁶¹.

Οι αρχές της νόμιμης και διαφανούς επεξεργασίας προϋποθέτουν την ενημέρωση του υποκειμένου των δεδομένων σχετικά με την ύπαρξη της επεξεργασίας και τους σκοπούς της⁶². Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων κάθε περαιτέρω πληροφορία που είναι απαραίτητη για να διασφαλίσει τη δίκαιη και διαφανή επεξεργασία, λαμβάνοντας υπόψη τις ειδικές συνθήκες και το πλαίσιο εντός του οποίου υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα. Επιπλέον, ορίζεται ρητά ότι το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για ενδεχόμενη κατάρτιση του προφίλ του, καθώς και για τις συνέπειες που μπορεί να αποφέρει αυτή στα προσωπικά του δεδομένα.

Η αρχή της διαφάνειας συνδέεται επίσης με τη λογοδοσία, δεδομένου ότι προϋποθέτει οι παρεχόμενες πληροφορίες να καθιστούν δυνατό τον έλεγχο συμμόρφωσης. Η διαφάνεια θέτει συγκεκριμένα ζητήματα σε σχέση με την τεχνητή νοημοσύνη και τα μεγάλα δεδομένα, λόγω της πολυπλοκότητας της επεξεργασίας που εμπλέκεται σε εφαρμογές ΤΝ, της αβεβαιότητας του αποτελέσματός της και του πολλαπλού σκοπού της. Η νέα διάσταση της αρχής σχετίζεται με τη λήψη αυτοματοποιημένων αποφάσεων, όπως αυτή ρυθμίζεται ρητά στον Κανονισμό.

⁶¹ Αιτιολογική σκέψη 58 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, κατά περίπτωση, απεικόνιση. Οι πληροφορίες αυτές θα μπορούσαν να παρέχονται σε ηλεκτρονική μορφή, για παράδειγμα, όταν απευθύνονται στο κοινό, μέσω ιστοσελίδας. Αυτό έχει ιδιαίτερη σημασία σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν, όπως στην περίπτωση επιγραμμικής διαφήμισης. Δεδομένου ότι τα παιδιά χρήζουν ειδικής προστασίας, κάθε ενημέρωση και ανακοίνωση, εάν η επεξεργασία απευθύνεται σε παιδιά, θα πρέπει να διατυπώνεται σε σαφή και απλή γλώσσα την οποία το παιδί να μπορεί να κατανοεί εύκολα.».

⁶² Βλ. αιτιολογική σκέψη 60 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

Αναμφισβήτητα, η ιδέα της διαφάνειας μπορεί να επεκταθεί σε αυτοματοποιημένα συμπεράσματα, ακόμα και όταν δεν έχει ακόμη εκδοθεί συγκεκριμένη απόφαση.

Μια συγκεκριμένη πτυχή της διαφάνειας στο πλαίσιο της μηχανικής μάθησης αφορά την πρόσβαση σε δεδομένα, ιδίως στο εκπαιδευτικό σύνολο ενός συστήματος. Ενδέχεται να χρειαστεί πρόσβαση σε δεδομένα για τον εντοπισμό πιθανών αιτιών «αδικίας» που προκύπτουν από ανεπαρκή ή μεροληπτικά δεδομένα ή από αλγόριθμο εκπαίδευσης. Αυτό είναι ιδιαίτερα σημαντικό όταν το αλγοριθμικό μοντέλο, που εκπαιδεύεται, είναι αδιαφανές, έτσι ώστε να μην μπορούν να εντοπιστούν πιθανά ελαττώματα κατά την επιθεώρησή του.

Επιπροσθέτως, η αιτιολογική σκέψη 71 επισημαίνει μια διαφορετική διάσταση της νομιμότητας, δηλαδή αυτό που θα μπορούσαμε να ονομάσουμε ως ουσιαστική νομιμότητα, η οποία αφορά το περιεχόμενο μιας αυτοματοποιημένης συμπερίληψης ή απόφασης, βάσει ενός συνδυασμού κριτηρίων, τα οποία μπορούν να συνοψιστούν με αναφορά στα προαναφερθέντα πρότυπα αποδοχής, συνάφειας και αξιοπιστίας⁶³.

Προκειμένου να διασφαλιστεί νόμιμη και διαφανής επεξεργασία όσον αφορά το υποκείμενο των δεδομένων, λαμβάνοντας υπόψη τις ειδικές συνθήκες και το πλαίσιο εντός του οποίου υποβάλλονται σε επεξεργασία τα προσωπικά δεδομένα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση προφίλ, να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες στα προσωπικά δεδομένα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα προσωπικά δεδομένα με τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, διακρίσεις εις βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος.

4.2 Περιορισμός του σκοπού

Ακολουθώντας, σύμφωνα με την αρχή του περιορισμού του σκοπού, τα προσωπικά δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς

⁶³ Βλ. αιτιολογική σκέψη 71 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

αυτούς⁶⁴. Η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1. Η αρχή αυτή έχει θεμελιώδη σημασία για το δίκαιο της προστασίας προσωπικών δεδομένων, διότι η νομιμότητα της επεξεργασίας κρίνεται με βάση τον σκοπό της επεξεργασίας και είναι σημαντικό αυτός να είναι καθορισμένος και σαφής. Επιπλέον, δε, ο σκοπός της επεξεργασίας αποτελεί βασική προϋπόθεση και για άλλες διατάξεις του Κανονισμού.

Η έννοια του σκοπού αναφέρεται επίσης στο άρθρο 6 του Κανονισμού⁶⁵, το οποίο ορίζει ότι για τη σύννομη επεξεργασία των δεδομένων απαιτείται αυτή να γίνεται για έναν ή περισσότερους συγκεκριμένους σκοπούς, για τους οποίους συναινεί το υποκείμενο. Αντίστοιχα, στο εδάφιο στ' ορίζεται ότι η επεξεργασία είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος. Ωστόσο, η έννοια του σκοπού περιλαμβάνεται έμμεσα και στις υπόλοιπες διατάξεις που ορίζουν τις βάσεις για τη νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως για την εκτέλεση σύμβασης, για συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας, για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή άλλου φυσικού προσώπου. Τέλος, η έννοια του σκοπού περιλαμβάνεται στο άρθρο 13 παράγραφος 1 στοιχείο γ'⁶⁶ και στο άρθρο 14 παράγραφος 1 στοιχείο γ'⁶⁷, που απαιτούν από τους υπευθύνους επεξεργασίας να παρέχουν πληροφορίες σχετικά με «τους σκοπούς της επεξεργασίας για τους οποίους

⁶⁴ Βλ. άρθρο 5 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

⁶⁵ Βλ. άρθρο 6 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

⁶⁶ Άρθρο 13 παρ. 1 στοιχ. γ' του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Όταν δεδομένα προσωπικού χαρακτήρα που αφορούν υποκείμενο των δεδομένων συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων όλες τις ακόλουθες πληροφορίες: ... γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία...».

⁶⁷ Άρθρο 14 παρ. 1 στοιχ. γ' του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων τις ακόλουθες πληροφορίες: ... γ) τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα, καθώς και τη νομική βάση για την επεξεργασία...».

προορίζονται τα προσωπικά δεδομένα καθώς και τη νομική βάση για την επεξεργασία».

Επικρατεί μια σύγχυση μεταξύ της χρήσης της τεχνολογίας ΤΝ και των μεγάλων δεδομένων και της αρχής του περιορισμού του σκοπού, καθώς αυτές οι τεχνολογίες επιτρέπουν την επαναχρησιμοποίηση προσωπικών δεδομένων για νέους σκοπούς διαφορετικούς από εκείνους για τους οποίους συλλέχθηκαν αρχικά τα δεδομένα. Για παράδειγμα, δεδομένα που συλλέγονται κατά τη σύναψη μίας σύμβασης στο διαδίκτυο (π.χ. αγορά ενδυμάτων από εμπορικό κατάστημα) με σκοπό τη διαχείριση αυτής, μπορούν να υποβληθούν σε επεξεργασία προκειμένου να γίνουν γνωστές οι προτιμήσεις των καταναλωτών και να σταλούν στοχευμένες διαφημίσεις σε αυτούς. Αντίστοιχα, τα «Like» που προορίζονται να εκφράσουν και να γνωστοποιήσουν τη γνώμη κάποιου σχετικά με μία δημοσίευση στο κοινωνικό δίκτυο Facebook, δύνανται να χρησιμοποιηθούν για τον εντοπισμό καταναλωτικών ή ακόμη και πολιτικών προτιμήσεων.

Ο σκοπός της επεξεργασίας πρέπει να καθοριστεί και να επισημανθεί κατά το στάδιο της συλλογής, έτσι ώστε τα υποκείμενα των δεδομένων να είναι σε θέση να ασκούν έλεγχο στα δεδομένα τους. Η σαφής οριοθέτηση του σκοπού είναι σημαντική όχι μόνο για να επιτρέψει στα υποκείμενα των δεδομένων να ασκήσουν αποτελεσματικά τα δικαιώματά τους, αλλά και να καθορίσουν τη συνολική συμμόρφωση με το νόμο και την αξιολόγησή του. Για παράδειγμα, η συμμόρφωση με την αρχή του περιορισμού του σκοπού απαγορεύει τη χρήση ηχογραφημένων φωνών από τη Siri ή την Alexa για την ανάλυση αυτών των φωνών και την εξαγωγή βιομετρικών ευρημάτων⁶⁸. Υπό αυτό το πρίσμα, θα μπορούσαμε να πούμε πως η αρχή του περιορισμού του σκοπού συνδέεται άρρηκτα με τη διαφάνεια και τη νομιμότητα⁶⁹.

Η αρχή του περιορισμού του σκοπού φαίνεται να έρχεται σε αντίθεση με τις δυνατότητες επεξεργασίας που προσφέρει η ΤΝ, καθώς η χρήση αλγορίθμων και μηχανικής μάθησης βασίζεται και τροφοδοτείται από την τάση συλλογής όσο το δυνατόν περισσότερων δεδομένων και τη δημιουργία νέων δεδομένων και νέων τύπων δεδομένων. Ειδικότερα, η αρχή του περιορισμού του σκοπού αποτρέπει την αυθαίρετη επαναχρησιμοποίηση των δεδομένων και θέτει υπό το πρίσμα και της αρχής της

⁶⁸ Conrad, C. S. (2017). Künstliche Intelligenz—Die Risiken für den Datenschutz. *Datenschutz und Datensicherheit-DuD*, 41(12), σελ. 740-744.

⁶⁹ Mitrou, L. (2018), σελ. 47.

λογοδοσίας ως βασικό παράγοντα τη συμβατότητα μεταξύ των σκοπών. Σύμφωνα με την αιτιολογική σκέψη 50 του Κανονισμού, οι ακόλουθοι παράγοντες πρέπει να λαμβάνονται υπόψη κατά την εξακρίβωση συμβατότητας της περαιτέρω επεξεργασίας:

- οποιαδήποτε σύνδεση μεταξύ του αρχικού σκοπού και των σκοπών της περαιτέρω επιδιωκόμενης επεξεργασίας,
- το πλαίσιο στο οποίο συλλέχθηκαν τα δεδομένα,
- η σχέση του υποκειμένου των δεδομένων με τον υπεύθυνο επεξεργασίας και πώς αυτό μπορεί να επηρεάσει τις εύλογες προσδοκίες του υποκειμένου σε σχέση με περαιτέρω επεξεργασία,
- η φύση των προσωπικών δεδομένων,
- οι συνέπειες της περαιτέρω επεξεργασίας για το υποκείμενο των δεδομένων.

Εάν η περαιτέρω επεξεργασία δεν θεωρείται συμβατή με την αρχική, πρέπει να αναζητηθεί ένας νέος νομικός λόγος, όπως μια νεότερη συγκατάθεση.

Αντιθέτως, η αρχή του περιορισμού του σκοπού δεν εμποδίζει την περαιτέρω χρήση προσωπικών δεδομένων για επιστημονικούς ή/και στατιστικούς σκοπούς⁷⁰. Η επιστημονική έρευνα πρέπει να ερμηνευτεί ευρέως ώστε να περιλαμβάνει την τεχνολογική ανάπτυξη, τη βασική έρευνα, καθώς και την εφαρμοσμένη και ιδιωτικά χρηματοδοτούμενη έρευνα⁷¹. Η χρήση δεδομένων προσωπικού χαρακτήρα για

⁷⁰ Kindt, E. J. (2016). Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. Σε *Computer Law & Security Review*, 32(5), σελ. 729-748.

⁷¹ Βλ. αιτιολογική σκέψη 159 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για σκοπούς επιστημονικής έρευνας, ο παρών κανονισμός θα πρέπει να ισχύει και για την επεξεργασία αυτή. Για τους σκοπούς του παρόντος κανονισμού, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας θα πρέπει να ερμηνεύεται διασταλτικά, δηλαδή να περιλαμβάνει παραδείγματος χάριν τεχνολογική ανάπτυξη και επίδειξη, βασική έρευνα, εφαρμοσμένη έρευνα και ιδιωτικά χρηματοδοτούμενη έρευνα. Επιπλέον, θα πρέπει να λαμβάνει υπόψη τον στόχο της Ένωσης δυνάμει του άρθρου 179 παράγραφος 1 ΣΛΕΕ για την επίτευξη ενός ευρωπαϊκού χώρου έρευνας. Στους σκοπούς επιστημονικής έρευνας θα πρέπει να περιλαμβάνονται και μελέτες που πραγματοποιούνται για το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας. Για να ληφθούν υπόψη οι ιδιαιτερότητες της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας, θα πρέπει να ισχύουν ειδικοί όροι ιδίως όσον αφορά τη δημοσίευση ή με άλλο τρόπο δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σκοπών επιστημονικής έρευνας. Εάν το αποτέλεσμα της επιστημονικής έρευνας ειδικότερα στον τομέα της υγείας αιτιολογεί τη λήψη περαιτέρω μέτρων προς το συμφέρον του υποκειμένου των δεδομένων, ισχύουν οι γενικοί κανόνες του παρόντος κανονισμού όσον αφορά τα μέτρα αυτά.».

επιστημονική έρευνα υπόκειται στις ειδικές διατάξεις του άρθρου 89 του Κανονισμού και στις κατάλληλες διασφαλίσεις που παρέχονται, συμπεριλαμβανομένης της διασφάλισης των δικαιωμάτων του υποκειμένου των δεδομένων και της λήψης τεχνικών και οργανωτικών μέτρων ασφαλείας. Όσον αφορά την επιστημονική έρευνα σε σχέση με την τεχνητή νοημοσύνη, πρέπει να σημειωθεί ότι είναι δύσκολο να γίνει διάκριση μεταξύ επιστημονικής ανάπτυξης και εφαρμογής της ΤΝ. Η Νορβηγική Αρχή προστασίας δεδομένων θεωρεί ότι είναι δύσκολο να γίνει μια τέτοια διαφοροποίηση, καθώς τα μοντέλα ΤΝ αναπτύσσονται και βελτιώνονται συνεχώς, καθώς τροφοδοτούνται με περισσότερα δεδομένα και ως εκ τούτου να διακρίνουν «πού αρχίζει η έρευνα και τελειώνει η χρήση»⁷².

4.3 Ελαχιστοποίηση των δεδομένων

Το άρθρο 5 παράγραφος 1 στοιχείο γ' ορίζει την αρχή της ελαχιστοποίησης των δεδομένων, σύμφωνα με την οποία τα προσωπικά δεδομένα πρέπει να είναι «κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία»⁷³. Σχετικά με την τεχνητή νοημοσύνη, επικρατεί μία σύγκρουση μεταξύ της αρχής της ελαχιστοποίησης και της ίδιας της ιδέας των μεγάλων δεδομένων και της ανάλυσης δεδομένων, η οποία περιλαμβάνει τη χρήση ΤΝ και στατιστικών μεθόδων για την ανακάλυψη νέων συσχετίσεων σε τεράστια σύνολα δεδομένων.

Για την επίλυση της σύγκρουσης αυτής, έχει υποστηριχθεί ότι η αρχή της ελαχιστοποίησης πρέπει να συνδέεται με την αρχή της αναλογικότητας. Από αυτήν την άποψη, η επεξεργασία πρέπει να περιορίζεται σε αυτό που είναι απαραίτητο για την εκπλήρωση ενός νόμιμου σκοπού. Επιπλέον, η επεξεργασία δεδομένων ενδέχεται να μην επηρεάζει δυσανάλογα τα συμφέροντα, τα δικαιώματα και τις ελευθερίες που διακυβεύονται. Οι κατηγορίες και ο όγκος των δεδομένων που επιλέγονται για επεξεργασία πρέπει να είναι τα απαραίτητα προκειμένου να επιτευχθεί ο δηλωμένος γενικός στόχος των εργασιών επεξεργασίας. Πρέπει να υπάρχει δίκαιη ισορροπία μεταξύ όλων των ενδιαφερόμενων συμφερόντων σε όλα τα στάδια της επεξεργασίας.

Η συγκεκριμένη αρχή φαίνεται να έρχεται σε αντίθεση με τις ανάγκες της μηχανικής μάθησης. Η αρχή της ελαχιστοποίησης δεδομένων -σχεδόν εξ ορισμού- κινείται αντίστροφα με τα μεγάλα δεδομένα και τα συστήματα μηχανικής μάθησης, τα

⁷² Datatilsynet. (2018). *Artificial Intelligence and Privacy*. Διαθέσιμο στο <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>. Ανάκτηση: Απρίλιος 2021.

⁷³ Βλ. άρθρο 5 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

οποία βασίζονται και ορισμένες φορές εξαρτώνται από μια «υπερβολική» συλλογή δεδομένων, καθώς και τη δυνατότητα να συνδυάσουν αυτά και να τα επαναχρησιμοποιήσουν. Η ελαχιστοποίηση των δεδομένων δεν έχει να κάνει μόνο με την ποσότητα των δεδομένων που χρησιμοποιούνται, αλλά και με το εάν αυτά είναι απαραίτητα για τους σκοπούς της επεξεργασίας ή τον υπερβαίνουν. Εάν η επεξεργασία ικανοποιεί την αρχή του περιορισμού του σκοπού, τότε θα ικανοποιεί επίσης την αρχή ελαχιστοποίησης των δεδομένων⁷⁴. Αυτό δεν είναι υποθετικό πρόβλημα: σε μια μελέτη επιχειρήσεων στο Ηνωμένο Βασίλειο, τη Γαλλία και τη Γερμανία, το 72% δήλωσε ότι είχε συγκεντρώσει δεδομένα που δεν χρησιμοποίησαν στη συνέχεια⁷⁵.

Η πρόκληση για τους υπευθύνους επεξεργασίας δεδομένων είναι να καθορίσουν εξαρχής: α) τους σκοπούς της επεξεργασίας, μια πρόκληση που δεν είναι καθόλου εύκολη, καθώς δεν είναι συνήθως δυνατό να προβλεφθεί τί θα μάθει ο αλγόριθμος και β) τα δεδομένα που θα είναι σχετικά, περιορίζοντας έτσι την ποσότητα των δεδομένων που περιλαμβάνονται στην εκπαίδευση ή στη χρήση ενός μοντέλου. Υπό αυτό το πρίσμα, η αρχή ελαχιστοποίησης των δεδομένων σχετίζεται τόσο με τον όγκο των δεδομένων όσο και με τη δραστηριότητα επεξεργασίας. Η συμμόρφωση με την αρχή μπορεί να περιορίσει την έκταση της παρέμβασης στην ιδιωτική ζωή ενός ατόμου ή ακόμη και να οδηγήσει σε αποχή από τη χρήση μοντέλων/μεθόδων ΤΝ, εάν ο στόχος της επεξεργασίας μπορεί να επιτευχθεί με λιγότερο επεμβατικό για την ιδιωτική ζωή τρόπο.

Η ελαχιστοποίηση δεν αποκλείει τη συμπερίληψη πρόσθετων προσωπικών δεδομένων σε μια επεξεργασία, εφόσον η προσθήκη τέτοιων δεδομένων παρέχει ένα όφελος, σε σχέση με τους σκοπούς της επεξεργασίας που υπερτερούν των πρόσθετων κινδύνων για τα υποκείμενα των δεδομένων. Ακόμη και η χρησιμότητα της μελλοντικής επεξεργασίας μπορεί να δικαιολογήσει τη διατήρηση των δεδομένων, αρκεί να υπάρχουν κατάλληλα μέτρα ασφαλείας. Ειδικότερα, η ψευδωνυμοποίηση, σε συνδυασμό με άλλα μέτρα ασφαλείας, μπορεί να συμβάλει στον περιορισμό των κινδύνων και συνεπώς να αυξήσει τη συμβατότητα της διατήρησης με την ελαχιστοποίηση.

⁷⁴ Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. Σε *Computer Law & Security Review*, 34(2), σελ. 257-268.

⁷⁵ *Information Commissioner Office – ICO*. (2017), σελ. 40.

Επιπροσθέτως, η επεξεργασία προσωπικών δεδομένων για απλούς στατιστικούς σκοπούς μπορεί να υπόκειται σε πιο ήπιες απαιτήσεις ελαχιστοποίησης. Σε μια τέτοια περίπτωση, οι πληροφορίες των υποκειμένων των δεδομένων θεωρούνται μόνο ως είσοδος σε ένα εκπαιδευτικό σύνολο (ή μια στατιστική βάση δεδομένων) και δεν χρησιμοποιούνται για προβλέψεις ή αποφάσεις που αφορούν άτομα. Αυτό αναφέρεται στην αιτιολογική σκέψη 162⁷⁶, που συνδέει την επεξεργασία δεδομένων με στατιστικούς σκοπούς. Δεδομένου ότι το υποκείμενο των δεδομένων δεν επηρεάζεται ατομικά από τη στατιστική επεξεργασία, η αρχή της αναλογικότητας, όσον αφορά την προστασία των δεδομένων, αφορά τη σύγκριση μεταξύ του έννομου συμφέροντος για τη λήψη των στατιστικών αποτελεσμάτων και των κινδύνων κατάχρησης των δεδομένων για μη στατιστικούς σκοπούς.

4.4 Ακρίβεια

Σύμφωνα με την αρχή της ακρίβειας, η οποία κατοχυρώνεται στο άρθρο 5 παράγραφος 1 στοιχ. δ' του Κανονισμού⁷⁷, τα προσωπικά δεδομένα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται, ενώ πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα, τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Η ποιότητα των δεδομένων είναι ιδιαίτερα σημαντική στην εποχή των μεγάλων δεδομένων, καθώς τα δεδομένα συλλέγονται και δημιουργούνται συχνά χωρίς κανένα

⁷⁶ Αιτιολογική σκέψη 162 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Όταν δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία για στατιστικούς σκοπούς, ο παρών κανονισμός θα πρέπει να ισχύει και για την επεξεργασία αυτή. Το ενωσιακό δίκαιο ή το δίκαιο των κρατών μελών θα πρέπει, εντός των ορίων του παρόντος κανονισμού, να καθορίζει το στατιστικό περιεχόμενο, τον έλεγχο της πρόσβασης, τις προδιαγραφές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για στατιστικούς σκοπούς και κατάλληλα μέτρα που διασφαλίζουν τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων και που αποσκοπούν στην εξασφάλιση του στατιστικού απορρήτου. Ο όρος «στατιστικοί σκοποί» σημαίνει κάθε πράξη συλλογής και την επεξεργασία δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία για την πραγματοποίηση στατιστικών ερευνών ή για την παραγωγή στατιστικών αποτελεσμάτων. Τα εν λόγω στατιστικά αποτελέσματα μπορούν να χρησιμοποιηθούν περαιτέρω για διάφορους σκοπούς, μεταξύ άλλων και για σκοπούς επιστημονικής έρευνας. Ο στατιστικός σκοπός συνεπάγεται ότι το αποτέλεσμα της επεξεργασίας για στατιστικούς σκοπούς δεν είναι δεδομένα προσωπικού χαρακτήρα αλλά συγκεντρωτικά δεδομένα και ότι το αποτέλεσμα αυτό ή τα δεδομένα προσωπικού χαρακτήρα δεν χρησιμοποιούνται προς υποστήριξη μέτρων ή αποφάσεων που αφορούν συγκεκριμένο φυσικό πρόσωπο.».

⁷⁷ Βλ. άρθρο 5 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

ποιοτικό έλεγχο⁷⁸. Αυτή η αρχή ισχύει και για τα προσωπικά δεδομένα που χρησιμοποιούνται ως είσοδος για το σύστημα TN, ειδικά όταν τα προσωπικά δεδομένα χρησιμοποιούνται για την εξαγωγή συμπερασμάτων ή τη λήψη αποφάσεων σχετικά με τα υποκείμενα των δεδομένων. Τα ανακριβή δεδομένα μπορεί να εκθέσουν τα υποκείμενα των δεδομένων σε βλάβη, όποτε αντιμετωπίζονται με τρόπους που δεν ταιριάζουν στην ταυτότητά τους.

Όσον αφορά τα συστήματα μηχανικής μάθησης, πρέπει να γίνει διάκριση εάν τα προσωπικά δεδομένα χρησιμοποιούνται σε ένα εκπαιδευτικό σύνολο, για γενικές στατιστικές συσχετίσεις ή ως εισαγωγή σε έναν αλγόριθμο για την κατάρτιση προφίλ. Προφανώς, όταν τα δεδομένα είναι διαθέσιμα για το εκπαιδευτικό σύνολο, είναι αυξημένος ο κίνδυνος για την εξαγωγή συμπερασμάτων που αφορούν τα άτομα. Η ανωνυμοποίηση ή ψευδωνυμοποίηση, με ισχυρά μέτρα ασφαλείας μπορεί να συμβάλει στη μείωση αυτού του κινδύνου.

Ζητήματα ακρίβειας μπορεί να προκύψουν λόγω της εσφαλμένης ερμηνείας της έννοιας και των επιπτώσεων των αποτελεσμάτων TN⁷⁹. Οι ανακριβείς προβλέψεις μπορεί να είναι το αποτέλεσμα της σύγχυσης και της αιτιώδους συνάφειας. Οι συσχετίσεις που προσδιορίστηκαν από τους αλγόριθμους δείχνουν κάποιο είδος σχέσης μεταξύ διαφορετικών δεδομένων, αλλά χωρίς απαραίτητα να εξηγήσουν ποια είναι αυτή η σχέση, ούτε εάν υπάρχει αιτιώδης σύνδεσμος μεταξύ των δεδομένων⁸⁰. Η ανακρίβεια μπορεί να προκύψει επίσης λόγω ενός συγκεκριμένου τύπου προκατάληψης, η άνιση βασική αλήθεια, η οποία συμβαίνει εάν οι ικανότητες ή οι

⁷⁸ Βλ. European Union Agency for Fundamental Rights. (2018). *#BigData: Discrimination in data-supported decision making*, σελ. 5. Διαθέσιμο στο <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making>. Ανάκτηση: Ιανουάριος 2021.

⁷⁹ Για παράδειγμα, εάν η τράπεζα επεκτείνει πίστωση κάθε φορά σε άτομα με το 70% «κίνδυνο αθέτησης», το 70% αυτών των ατόμων, στην πραγματικότητα, θα αθετήσει. Ένα τέτοιο σύστημα μπορεί να είναι άδικο στην εφαρμογή, ωστόσο, εάν οι υπάλληλοι δανείων ερμηνεύουν λανθασμένα τον «κίνδυνο 70% της αθέτησης» ως απλά «κακό πιστωτικό κίνδυνο» και αρνούνται να επεκτείνουν την πίστωση σε όλους με αυτό το σκορ -παρόλο που σχεδόν το ένα τρίτο αυτών οι αιτούντες προβλέπεται να είναι ένας καλός πιστωτικός κίνδυνος. Βλ. Microsoft, *The Future Computed*, σελ. 59. Διαθέσιμο στο <https://news.microsoft.com/uploads/2018/01/The-Future-Computed.pdf>. Ανάκτηση: Μάρτιος 2021.

⁸⁰ Hildebrandt, M. (2008). Defining profiling: a new type of knowledge?. Σε *Profiling the European citizen*, σελ. 17-45. Springer, Dordrecht.

κίνδυνοι κατανέμονται άνισα μεταξύ προστατευόμενων ομάδων, με αποτέλεσμα τη λεγόμενη «στατιστική διάκριση»⁸¹.

Η αρχή της ακρίβειας απαιτεί ότι οι υπεύθυνοι επεξεργασίας δεδομένων που εκτελούν διαδικασίες μηχανικής εκμάθησης πρέπει να διασφαλίζουν ότι τα δεδομένα εκπαίδευσης είναι αντιπροσωπευτικά του περιβάλλοντος στο οποίο θα αναπτυχθεί ο εκπαιδευμένος αλγόριθμος και ότι δεν ενσωματώνει την υπάρχουσα πραγματική μεροληψία⁸². Είναι ενδιαφέρον να σημειωθεί ότι τα δεδομένα εκπαίδευσης μπορούν να αξιολογηθούν για μεροληψία, ελλιπή ή λαμβάνοντας υπόψη άσχετους παράγοντες, αλλά δεν μπορεί να εκτιμηθεί για την ακρίβεια σε σχέση με το υποκείμενο των δεδομένων, διότι το γεγονός που προβλέπει δεν σχετίζεται ακόμη με συγκεκριμένα δεδομένα θέμα⁸³.

4.5 Λογοδοσία

Το άρθρο 5 παράγραφος 2 του ΓΚΠΔ ορίζει ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 («λογοδοσία»). Σε γενικές γραμμές, η αρχή της λογοδοσίας θα επιβάρυνε τους υπεύθυνους επεξεργασίας δεδομένων με το βάρος της εφαρμογής συγκεκριμένων μέτρων εντός των οργανισμών τους προκειμένου να διασφαλιστεί ότι πληρούνται οι απαιτήσεις προστασίας δεδομένων. Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν την εφαρμογή εκτιμήσεων αντικτύπου για την προστασία δεδομένων ή τη χρήση ενός συστήματος προστασίας προσωπικών δεδομένων. Η λογοδοσία τονίζεται περαιτέρω από διάφορες διατάξεις σε όλο το Γενικό Κανονισμό Προστασίας Δεδομένων. Για παράδειγμα, το άρθρο 24 του ΓΚΠΔ ορίζει ότι: «ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό». Οι επεξεργαστές δεδομένων δεσμεύονται επίσης από την αρχή της λογοδοσίας.

Η απόδειξη της συμμόρφωσης σημαίνει, μεταξύ άλλων, ότι ο υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να εξηγήσει τον τρόπο με τον οποίο εφαρμόστηκε η επεξεργασία δεδομένων προσωπικού χαρακτήρα και τον τρόπο με τον

⁸¹ Hacker, P. (2018). Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, 55(4).

⁸² *Information Commissioner Office – ICO*. (2017), σελ. 45.

⁸³ Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review*, 34(2), σελ. 257-268.

οποίο ελήφθη μια συγκεκριμένη απόφαση⁸⁴. Στο περιβάλλον τεχνητής νοημοσύνης, η ανταπόκριση στις απαιτήσεις λογοδοσίας δεν φαίνεται να είναι εύκολη υπόθεση, δεδομένης της αδιαφάνειας της επεξεργασίας και της χρήσης αλγορίθμων, οι οποίοι οδηγούνται στη λήψη αποφάσεων βασιζόμενοι στην ανάλυση μεγάλων ποσοτήτων δεδομένων για τη δημιουργία συσχετίσεων. Τα συστήματα τεχνητής νοημοσύνης των οποίων οι αποφάσεις δεν μπορούν να εξηγηθούν εγείρουν θεμελιώδη ζητήματα λογοδοσίας.

5. Νομιμότητα της επεξεργασίας των δεδομένων και τεχνητή νοημοσύνη

Σύμφωνα με το άρθρο 6 του Κανονισμού, ορίζεται ότι για την επεξεργασία δεδομένων προσωπικού χαρακτήρα απαιτείται νομική βάση. Η ιδέα αυτή εισήχθη για πρώτη φορά στην Οδηγία για την προστασία των δεδομένων του 1995⁸⁵ και στη συνέχεια θεμελιώθηκε στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων⁸⁶, σύμφωνα με το οποίο τα προσωπικά δεδομένα πρέπει να υποβληθούν σε επεξεργασία για καθορισμένους σκοπούς και βάσει της συγκατάθεσης του ενδιαφερομένου ή για άλλους θεμιτούς λόγους, που προβλέπονται στο νόμο.

Η επεξεργασία προσωπικών δεδομένων στο πλαίσιο της εφαρμογής τεχνητής νοημοσύνης εγείρει ορισμένα ζητήματα σχετικά με την ύπαρξη έγκυρης νομικής βάσης επεξεργασίας. Προκειμένου να προσδιοριστεί πότε μια νομική βάση μπορεί να επιτρέπει την επεξεργασία με βάση την τεχνητή νοημοσύνη, πρέπει να εξετάσουμε ξεχωριστά τις νομικές βάσεις που ορίζονται στο άρθρο 6 του Κανονισμού, το οποίο ορίζει ότι η επεξεργασία προσωπικών δεδομένων είναι νόμιμη μόνο υπό τις ακόλουθες προϋποθέσεις: α) συγκατάθεση του υποκειμένου των δεδομένων, β) για την εκτέλεση σύμβασης, γ) για συμμόρφωση με έννομη υποχρέωση, δ) για τη διαφύλαξη ζωτικού συμφέροντος ε) για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο

⁸⁴ Χριστάκου, Α. (2020). *Οι νομικές επιπτώσεις των αλγορίθμων στον εργασιακό χώρο*. Διπλωματική εργασία, σελ. 42, Νομική Σχολή ΕΚΠΑ. Διαθέσιμη στο <https://pergamos.lib.uoa.gr/uoa/dl/object/2934613>. Ανάκτηση: Ιούνιος 2021.

⁸⁵ Βλ. Οδηγία 95/46/ΕΚ.

⁸⁶ Άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ: «1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν, 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγμένα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους, 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.».

συμφέρον ή κατά την άσκηση δημόσιας εξουσίας , ή στ) για σκοπούς εννόμων συμφερόντων.

5.1 Η συγκατάθεση του υποκειμένου

Η συγκατάθεση, σύμφωνα με το άρθρο 4§11 του Κανονισμού, ορίζεται ως κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Αυτός ο ορισμός συμπληρώνεται από την αιτιολογική σκέψη 32 που ορίζει ότι η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς⁸⁷.

Η συγκατάθεση διαδραματίζει βασικό ρόλο στην κατανόηση της προστασίας των δεδομένων, που βασίζεται πράγματι στο μοντέλο «ειδοποίησης και συγκατάθεσης», σύμφωνα με το οποίο η προστασία των δεδομένων στοχεύει στην προστασία ενός δικαιώματος «ενημερωτικής αυτοδιάθεσης». Αυτό το δικαίωμα ασκείται πράγματι με τη συγκατάθεση ή την άρνηση ικανοποίησης της επεξεργασίας των δεδομένων κάποιου, αφού του δοθεί επαρκής ενημέρωση. Υπό αυτό το πρίσμα έχουν υποστηριχθεί δύο κριτικές⁸⁸.

⁸⁷ Βλ. αιτιολογική σκέψη 32 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς. Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό και να μην διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται.».

⁸⁸ Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century. Διαθέσιμο στο

Σύμφωνα με την πρώτη κριτική, η συγκατάθεση συχνά υπάρχει δίχως λόγο, καθώς δε βασίζεται σε πραγματική γνώση της διακυβευόμενης επεξεργασίας, ούτε σε μια πραγματική ευκαιρία επιλογής. Από τη μία πλευρά, η σημερινή επεξεργασία προσωπικών δεδομένων είναι τόσο περίπλοκη που τα περισσότερα υποκείμενα των δεδομένων δεν έχουν τις δεξιότητες να τα κατανοήσουν και να προβλέψουν τους σχετικούς κινδύνους. Επιπλέον, ακόμη και αν τα υποκείμενα των δεδομένων διέθεταν τέτοιες δεξιότητες, δεν θα είχαν το χρόνο και την ενέργεια να εξετάσουν τις λεπτομέρειες κάθε πολιτικής απορρήτου. Από την άλλη πλευρά, η άρνηση συγκατάθεσης μπορεί να συνεπάγεται την αδυναμία χρήσης (ή περιορισμού στη χρήση) υπηρεσιών που είναι σημαντικές ή ακόμη και απαραίτητες για τα υποκείμενα των δεδομένων.

Η δεύτερη κριτική συνίσταται στο ότι η συγκατάθεση, όταν στοχεύει σε συγκεκριμένους σκοπούς, δεν περιλαμβάνει (και επομένως αποκλείει, όταν θεωρείται απαραίτητη βάση της επεξεργασίας) μελλοντικές, συχνά άγνωστες, χρήσεις των δεδομένων, ακόμη και όταν τέτοιες χρήσεις είναι κοινωνικά ωφέλιμες, όπως εξέταση αρχείων υγείας και εργαστηριακών αποτελεσμάτων για ιατρική έρευνα ή ανάλυση πολλών αρχείων αναζήτησης στο Διαδίκτυο για την χαρτογράφηση εστιών γρίπης και εντοπισμός επικίνδυνων αλληλεπιδράσεων με τα φάρμακα.

Αυτές οι κριτικές σχετικά με τη συγκατάθεση έχουν αντιμετωπιστεί με την παρατήρηση ότι είναι δυνατή η εφαρμογή των αρχών της συγκατάθεσης και του περιορισμού του σκοπού με τρόπους, που έχουν σημασία τόσο για το υποκείμενο των δεδομένων όσο και για τη μελλοντική ωφέλιμη χρήση των δεδομένων⁸⁹.

Πρώτον, υποστηρίχθηκε ότι οι ειδοποιήσεις συγκατάθεσης πρέπει να επικεντρώνονται στο πιο σημαντικό ζήτημα και ότι πρέπει να είναι άμεσες και φιλικές προς τον χρήστη. Συγκεκριμένα, πρέπει να δίνονται απλές και σαφείς πληροφορίες σχετικά με τον τρόπο συγκατάθεσης σε σχέση με την υπό κρίση επεξεργασία, όπως αυτές που αφορούν την παρακολούθηση των χρηστών ή τη διαβίβαση δεδομένων σε τρίτους. Περαιτέρω, κουμπιά opt-out ή opt-in θα μπορούσαν να παρουσιαστούν σε

https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf. Ανάκτηση: Ιούνιος 2021.

⁸⁹ Calo, R. (2011). Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev.*, 87, 1027. Διαθέσιμο στο <https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1020&context=ndlr>. Ανάκτηση: Ιούνιος 2021.

όλους τους χρήστες, για να παρέχουν τρόπους για να εκφράσουν τις προτιμήσεις τους σχετικά με την παρακολούθηση ή την κατάρτιση προφίλ. Δεύτερον, ο ΓΚΠΔ επιτρέπει την περαιτέρω επεξεργασία των δεδομένων που συλλέχθηκαν για ορισμένους σκοπούς, εφόσον οι περαιτέρω σκοποί είναι συμβατοί με τους αρχικούς.

Συμπερασματικά, φαίνεται ότι οι έννοιες της συγκατάθεσης και του περιορισμού του σκοπού μπορούν να ερμηνευθούν με τρόπους που συνάδουν τόσο με την προστασία του υποκειμένου των δεδομένων όσο και με την ανάγκη αξιοποίησης των ευεργετικών χρήσεων της τεχνητής νοημοσύνης. Ωστόσο, η ΤΝ και τα μεγάλα δεδομένα εγείρουν ζητήματα σχετικά με 3 χαρακτηριστικά της συγκατάθεσης, όπως αυτά ορίζονται στο άρθρο 8 παρ. 1 του Κανονισμού και θα αναλυθούν αμέσως.

5.1.1 Ειδική συγκατάθεση

Το πρώτο ζήτημα αφορά την εξειδίκευση της συγκατάθεσης. Ειδικότερα, τίθεται το ερώτημα εάν η συγκατάθεση για επεξεργασία για συγκεκριμένο σκοπό καλύπτει και την περαιτέρω επεξεργασία με βάση την τεχνητή νοημοσύνη, συνήθως για ανάλυση δεδομένων και κατάρτιση προφίλ. Για παράδειγμα, τα δεδομένα που συλλέγονται από τις πωλήσεις μπορούν να χρησιμοποιηθούν για την ανάλυση των προτιμήσεων των καταναλωτών και την αποστολή στοχευμένων διαφημίσεων; Αυτό φαίνεται να αποκλείεται, δεδομένου ότι η συγκατάθεση πρέπει να είναι ειδική, έτσι ώστε να μην μπορεί να επεκταθεί πέρα από αυτό που αναφέρεται ρητά. Ωστόσο, το γεγονός ότι το υποκείμενο των δεδομένων έχει συναινέσει μόνο στην επεξεργασία για έναν συγκεκριμένο σκοπό δεν αποκλείει απαραίτητα ότι τα δεδομένα μπορούν να υποβληθούν σε επεξεργασία για έναν περαιτέρω νόμιμο σκοπό. Άρα η επεξεργασία επιτρέπεται, όταν καλύπτεται από νομική βάση και είναι συμβατή με τον σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα.

Η απαίτηση ειδικότητας μετριάζεται για την επιστημονική έρευνα όπως αναφέρεται στην αιτιολογική σκέψη 33, η οποία επιτρέπει τη συγκατάθεση όχι μόνο για συγκεκριμένα ερευνητικά έργα, αλλά και για τομείς επιστημονικής έρευνας⁹⁰.

⁹⁰ Βλ. αιτιολογική σκέψη 33 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Συχνά, δεν είναι δυνατόν να προσδιορίζεται πλήρως ο σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας κατά τον χρόνο συλλογής των δεδομένων. Ως εκ τούτου, τα υποκείμενα των δεδομένων θα πρέπει να μπορούν να δώσουν τη συγκατάθεσή τους για ορισμένους τομείς της επιστημονικής έρευνας, όταν ακολουθούνται τα αναγνωρισμένα πρότυπα δεοντολογίας για την επιστημονική έρευνα. Τα υποκείμενα των δεδομένων θα πρέπει να έχουν τη

Συχνά δεν είναι δυνατόν να προσδιοριστεί πλήρως ο σκοπός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας κατά τη στιγμή της συλλογής δεδομένων. Επομένως, τα υποκείμενα των δεδομένων πρέπει να έχουν τη δυνατότητα να δώσουν τη συγκατάθεσή τους σε ορισμένους τομείς της έρευνας, όταν τηρούν τα αναγνωρισμένα ηθικά πρότυπα για την επιστημονική έρευνα. Τα υποκείμενα των δεδομένων πρέπει να έχουν την ευκαιρία να δώσουν τη συγκατάθεσή τους μόνο σε ορισμένους τομείς έρευνας ή σε τμήματα ερευνητικών έργων στο βαθμό που επιτρέπεται από τον επιδιωκόμενο σκοπό.

5.1.2 Συγκεκριμένη συγκατάθεση

Ένα άλλο χαρακτηριστικό που πρέπει να έχει η συγκατάθεση είναι η λεπτομέρεια και η ακρίβεια, δηλαδή για παράδειγμα δεν αρκεί μια γενική συναίνεση για οποιοδήποτε είδος ανάλυσης δεδομένων και κατάρτισης προφίλ ώστε να επιτρέπεται η αποστολή στοχευμένης εμπορικής ή πολιτικής διαφήμισης με βάση την τεχνητή νοημοσύνη. Η αιτιολογική σκέψη 43 πραγματεύεται το συγκεκριμένο χαρακτηριστικό ως εξής: Η συγκατάθεση θεωρείται ότι δεν παρέχεται ελεύθερα, εάν δεν επιτρέπει χωριστή συγκατάθεση σε διαφορετικές διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα, παρά το γεγονός ότι είναι κατάλληλη σε κάθε περίπτωση.

Αυτό έχει δύο επιπτώσεις στην εφαρμογή ΤΝ. Πρώτον, φαίνεται ότι το υποκείμενο των δεδομένων δεν πρέπει να συναινεί από κοινού σε ουσιαστικά διαφορετικά είδη επεξεργασίας που βασίζονται σε ΤΝ (π.χ. σε οικονομικές και πολιτικές διαφημίσεις). Δεύτερον, η χρήση μιας υπηρεσίας δεν πρέπει κατ' αρχήν να εξαρτάται από μια συμφωνία που υπόκειται σε πρακτικές κατάρτισης προφίλ. Η συγκατάθεση στο προφίλ πρέπει να είναι ξεχωριστή και να μην αποτελεί προϋπόθεση για την πρόσβαση στην υπηρεσία⁹¹.

δυνατότητα να παρέχουν τη συναίνεσή τους μόνο σε ορισμένους τομείς της έρευνας ή μόνο σε μέρη προγραμμάτων έρευνας, στον βαθμό που επιτρέπεται από τον επιδιωκόμενο σκοπό.».

⁹¹ Ομάδα εργασίας του άρθρου 29. (2020). Κατευθυντήριες γραμμές για την συγκατάθεση υπό το πρίσμα του Κανονισμού 2016/679. Διαθέσιμο στο https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_el.pdf. Ανάκτηση: Φεβρουάριος 2021.

5.1.3 Ελεύθερη συγκατάθεση

Το τρίτο ζήτημα αφορά το κατά πόσο μπορεί να δοθεί ελεύθερα η συγκατάθεση, ειδικά σε μια διαδικασία κατάρτισης προφίλ. Αυτό το ζήτημα αντιμετωπίζεται στην αιτιολογική σκέψη 42, η οποία αποκλείει την ελευθερία συναίνεσης, όταν «το υποκείμενο των δεδομένων δεν έχει γνήσια ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να ανακαλέσει τη συγκατάθεση χωρίς ζημία». Ακόμη, σύμφωνα με την αιτιολογική σκέψη 43, η συγκατάθεση δεν είναι ελεύθερη σε περιπτώσεις «σαφούς ανισορροπίας».

Προκειμένου να διασφαλιστεί ότι η συγκατάθεση παρέχεται ελεύθερα, αυτή δεν πρέπει να παρέχει έγκυρη νομική βάση για την επεξεργασία προσωπικών δεδομένων σε μια συγκεκριμένη περίπτωση όπου υπάρχει σαφής ανισορροπία μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας.

Οι καταστάσεις ανισορροπίας είναι διαδεδομένες στα τυπικά περιβάλλοντα, στα οποία εφαρμόζεται η ανάλυση δεδομένων μέσω της τεχνητής νοημοσύνης σε προσωπικά δεδομένα. Τέτοιες καταστάσεις υπάρχουν στον ιδιωτικό τομέα, ειδικά όταν ένα μέρος έχει κυριαρχία στην αγορά (όπως στην περίπτωση του Facebook ή του Twitter), ή μια θέση εξουσίας (όπως στην περίπτωση των εργοδοτών σε σχέση με τους υπαλλήλους τους). Υπάρχουν επίσης μεταξύ δημόσιων αρχών και ατόμων που υπόκεινται στις εξουσίες αυτών των αρχών. Σε όλες αυτές τις περιπτώσεις, η συγκατάθεση δεν μπορεί να παράσχει επαρκή νομική βάση, εκτός εάν μπορεί να αποδειχθεί ότι δεν υπάρχουν κίνδυνοι «εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικής αρνητικής συνέπειας εάν [το υποκείμενο των δεδομένων] δεν συναινέσει»⁹².

Τέλος, η συγκατάθεση θα πρέπει να θεωρείται άκυρη, όταν η άρνηση ή η ανάκληση συγκατάθεσης συνδέεται με ζημία που δεν σχετίζεται με τη διαθεσιμότητα των προσωπικών δεδομένων για τα οποία απορρίφθηκε η συγκατάθεση (π.χ. οι ασθενείς ενημερώνονται ότι για να λάβουν ιατρική θεραπεία πρέπει να συναινέσουν ότι τα ιατρικά τους δεδομένα χρησιμοποιούνται για σκοπούς που δεν χρειάζονται για τη θεραπεία αυτή). Αυτό ισχύει επίσης για περιπτώσεις στις οποίες απαιτείται η συγκατάθεση από τον πάροχο μιας υπηρεσίας, παρόλο που η επεξεργασία δεν είναι απαραίτητη για την εκτέλεση της υπηρεσίας.

⁹² Ομάδα εργασίας του άρθρου 29. (2020), σελ. 9.

5.1.4 Η συγκατάθεση σε περαιτέρω επεξεργασία δεδομένων

Ένα βασικό ζήτημα σχετικά με τις εφαρμογές τεχνητής νοημοσύνης αφορά τον συσχετισμό και επαναπροσδιορισμό των προσωπικών δεδομένων. Αυτό είναι ένα ζήτημα για το οποίο η διάταξη του Κανονισμού είναι ασαφής. Η γενική ιδέα αναφέρεται στο άρθρο 5 παράγραφος 1 στοιχείο β' ως άρθρωση της αρχής του περιορισμού του σκοπού, ο οποίος αναφέρεται αμέσως παραπάνω. Τα προσωπικά δεδομένα δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο που δεν είναι συμβατός με τους αρχικούς σκοπούς. Η απαγόρευση επαναπροσδιορισμού επιβεβαιώνεται επίσης στην Αιτιολογική Σκέψη 50, σύμφωνα με την οποία η περαιτέρω επεξεργασία προσωπικών δεδομένων για νέους σκοπούς επιτρέπεται μόνο όταν είναι συμβατή με τους αρχικούς σκοπούς. Η επεξεργασία προσωπικών δεδομένων για σκοπούς άλλους από εκείνους για τους οποίους συλλέχθηκαν αρχικά τα προσωπικά δεδομένα πρέπει να επιτρέπεται μόνο όταν η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους συλλέχθηκαν αρχικά τα προσωπικά δεδομένα⁹³.

⁹³ Αιτιολογική σκέψη 50 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους από εκείνους για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά θα πρέπει να επιτρέπεται μόνο εφόσον η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά. Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα. Εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, το δίκαιο της Ένωσης ή κράτους μέλους μπορεί να καθορίζει και να προσδιορίζει τα καθήκοντα και τους σκοπούς για τους οποίους πρέπει να θεωρείται συμβατή και σύννομη η περαιτέρω επεξεργασία. Η περαιτέρω επεξεργασία για λόγους αρχειοθέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς θα πρέπει να θεωρείται συμβατή σύννομη πράξη επεξεργασίας. Η νομική βάση που προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μπορεί επίσης να συνιστά τη νομική βάση για την περαιτέρω επεξεργασία. Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας· το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους· τη φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων· και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και

Ωστόσο, η συμβατότητα τεκμαίρεται, σύμφωνα με το άρθρο 5, όταν η περαιτέρω επεξεργασία προορίζεται να εξυπηρετήσει σκοπούς που σχετίζονται με αρχειοθέτηση, επιστημονική ή ιστορική έρευνα ή στατιστικά στοιχεία: η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης για λόγους δημοσίου συμφέροντος, για επιστημονικούς ή ιστορικούς ερευνητικούς σκοπούς ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1, δεν θεωρείται ασυμβίβαστη με τους αρχικούς σκοπούς

Η συμβατότητα τεκμαίρεται επίσης όταν η νέα επεξεργασία βασίζεται σε νόμο, για λόγους δημοσίου συμφέροντος. Εάν η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας αποστολής που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση επίσημης εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, η νομοθεσία της Ένωσης ή των κρατών μελών μπορεί να καθορίσει και να προσδιορίσει τα καθήκοντα και τους σκοπούς για τους οποίους πρέπει να ληφθεί υπόψη η περαιτέρω επεξεργασία ως συμβατό και νόμιμο.

Το άρθρο 6 παράγραφος 4 του Κανονισμού ορίζει ότι ο νόμος που επιτρέπει τον επαναπροσδιορισμό των δεδομένων «συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία» και περιγράφει πιθανούς παράγοντες που πρέπει να ληφθούν υπόψη για τον προσδιορισμό της συμβατότητας. Ειδικότερα, ορίζει ότι όταν η επεξεργασία για σκοπούς διαφορετικούς από εκείνους για τους οποίους έχουν

τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας. Όταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασίας να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η εφαρμογή των αρχών που καθορίζονται στον παρόντα κανονισμό και, ιδίως, η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τους άλλους αυτούς σκοπούς και σχετικά με τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος προβολής αντιρρήσεων. Η επισήμανση πιθανών εγκληματικών πράξεων ή απειλών κατά της δημόσιας ασφάλειας από τον υπεύθυνο επεξεργασίας και η διαβίβαση των σχετικών δεδομένων προσωπικού χαρακτήρα σε αρμόδια αρχή σε μία μεμονωμένη υπόθεση ή σε περισσότερες από μία υποθέσεις που αφορούν την ίδια αξιόποινη πράξη ή τις ίδιες απειλές για τη δημόσια ασφάλεια θα πρέπει να θεωρείται ως εμπίπτουσα στο πλαίσιο του θεμιτού συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας. Ωστόσο, η διαβίβαση αυτή στο πλαίσιο του θεμιτού συμφέροντος του υπευθύνου επεξεργασίας ή η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να απαγορεύεται, εάν η επεξεργασία δεν είναι συμβατή με νομική, επαγγελματική ή άλλη δεσμευτική υποχρέωση τήρησης απορρήτου.».

συλλεχθεί τα προσωπικά δεδομένα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή σε μια νομοθεσία της Ένωσης ή των κρατών μελών που αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για την προστασία των στόχων που αναφέρεται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβώσει εάν η επεξεργασία για άλλο σκοπό είναι συμβατή με το σκοπό για τον οποίο αρχικά συλλέχθηκαν τα προσωπικά δεδομένα, λαμβάνει υπόψη, μεταξύ άλλων:

- τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα προσωπικά δεδομένα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,
- το πλαίσιο εντός του οποίου συλλέχθηκαν τα προσωπικά δεδομένα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,
- τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,
- τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,
- την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

Το ζήτημα του παραδεκτού της επεξεργασίας προσωπικών δεδομένων για νέους και διαφορετικούς σκοπούς είναι κρίσιμο στην εποχή της τεχνητής νοημοσύνης και των μεγάλων δεδομένων, όταν διατίθενται τεράστιες και ποικίλες μάζες δεδομένων και στη συνέχεια αναπτύσσονται μέθοδοι για τη συσχέτιση και τον εντοπισμό πιθανών αιτιώδων συνδέσμων. Όπως προαναφέρθηκε, αυτό μπορεί να οδηγήσει στην ανακάλυψη απροσδόκητων συνδέσεων που βασίζονται στο συνδυασμό διαφορετικών συνόλων δεδομένων (π.χ., συνδέσεις μεταξύ προτιμήσεων τρόπου ζωής στα κοινωνικά δίκτυα και των συνθηκών υγείας, μεταξύ συμπεριφοράς καταναλωτή και τάσεων της αγοράς, μεταξύ ερωτημάτων Διαδικτύου και εξάπλωσης ασθενειών, μεταξύ προτιμήσεων στο Διαδίκτυο και πολιτικών προτιμήσεων κ.λπ.). Τα αποτελέσματα αυτών των αναλύσεων (π.χ., συσχετίσεις που ανακαλύφθηκαν μεταξύ των δεδομένων

των καταναλωτών και των προτιμήσεών τους, των δυνατοτήτων δαπανών και των προμηθειών αγοράς κ.λπ.) μπορούν στη συνέχεια να χρησιμοποιηθούν για την αξιολόγηση ή την επιρροή της ατομικής συμπεριφοράς (π.χ., στέλνοντας στοχευμένες διαφημίσεις).

Ο επαναπροσδιορισμός είναι το κλειδί στον τομέα των μεγάλων δεδομένων και της τεχνητής νοημοσύνης, καθώς η κατασκευή μεγάλων συνόλων δεδομένων συχνά περιλαμβάνει τη συγχώνευση δεδομένων που είχαν συλλεχθεί ξεχωριστά για διαφορετικούς σκοπούς και την επεξεργασία τέτοιων δεδομένων για την αντιμετώπιση ζητημάτων που δεν εξετάστηκαν κατά τη στιγμή της συλλογής. Ένα βασικό ζήτημα για το μέλλον του ΓΚΠΔ αφορά το βαθμό στον οποίο ο έλεγχος συμβατότητας θα μας επιτρέψει να κάνουμε μια λογική διάκριση μεταξύ αποδεκτών και απαράδεκτων επαναχρησιμοποιήσεων των δεδομένων για τους σκοπούς της ανάλυσης.

Η Αιτιολογική Σκέψη 50 δεν βοηθά ιδιαίτερα στην αντιμετώπιση αυτού του ζητήματος, καθώς φαίνεται ότι υποδεικνύει ότι δεν απαιτείται νομική βάση για συμβατό επαναπροσδιορισμό. Ειδικότερα, ορίζει ότι «όταν η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα προσωπικά δεδομένα συλλέχθηκαν αρχικά [...] δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των προσωπικών δεδομένων». Επιπλέον, η Αιτιολογική Σκέψη 50 φαίνεται να προϋποθέτει ότι είναι αποδεκτή η επεξεργασία για στατιστικούς σκοπούς, επιβεβαιώνοντας ότι «η περαιτέρω επεξεργασία για [...] στατιστικούς σκοπούς πρέπει να θεωρηθεί ως συμβατή νόμιμη πράξη επεξεργασίας». Αυτό το τεκμήριο περιορίστηκε από την Ομάδα εργασίας του άρθρου 29, η οποία υποστήριξε ότι η συμβατότητα πρέπει να ελεγχθεί και σε αυτή την περίπτωση, δηλαδή της στατιστικής επεξεργασίας.

Φαίνεται λοιπόν ότι χρειάζονται δύο απαιτήσεις για να επιτραπεί ο επαναπροσδιορισμός: α) η νέα επεξεργασία πρέπει να είναι συμβατή με τον σκοπό για τον οποίο συλλέχθηκαν τα δεδομένα και β) η νέα επεξεργασία πρέπει να έχει νομική βάση (που μπορεί να είναι, αλλά δεν είναι απαραίτητα, το ίδιο με την αρχική επεξεργασία). Σύμφωνα με την αιτιολογική σκέψη 50, φαίνεται ότι η στατιστική επεξεργασία θα πρέπει να θεωρείται ότι είναι συμβατή, εκτός εάν φαίνεται ότι υπάρχουν λόγοι ασυμβατότητας.

Εφαρμόζοντας αυτά τα κριτήρια στην επαναχρησιμοποίηση δεδομένων που βασίζονται στην τεχνητή νοημοσύνη, πρέπει να διακρίνουμε εάν τα δεδομένα επαναχρησιμοποιούνται για στατιστικούς σκοπούς ή μάλλον για δημιουργία προφίλ. Η

επαναχρησιμοποίηση για έναν απλώς στατιστικό σκοπό θα πρέπει γενικά να είναι αποδεκτή, δεδομένου ότι επηρεάζει μεμονωμένα το υποκείμενο των δεδομένων, και επομένως θα πρέπει να είναι συμβατή με την αρχική επεξεργασία. Εάν η στατιστική επεξεργασία κατευθύνεται προς έναν επιτρεπόμενο στόχο, όπως η ασφάλεια ή η έρευνα αγοράς, μπορεί επίσης να βασιστεί στη νομική βάση του άρθρου 6 παράγραφος 1 στοιχείο στ', δηλαδή στην αναγκαιότητα επίτευξης σκοπών που σχετίζονται με νόμιμα συμφέροντα.

5.2 Το έννομο συμφέρον

Το άρθρο 6 παράγραφος 1 στοιχείο στ' παρέχει μια γενική νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλαδή την αναγκαιότητα της επεξεργασίας για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν τα συμφέροντα αυτά παρακάμπτονται από τα συμφέροντα ή τα θεμελιώδη δικαιώματα και ελευθερίες του υποκειμένου των δεδομένων που απαιτούν προστασία των προσωπικών δεδομένων⁹⁴.

Ζήτημα γεννάται ως προς το σε ποιο βαθμό μπορεί να ισχύει το άρθρο 6 παράγραφος 1 στοιχείο στ' για την επεξεργασία προσωπικών δεδομένων με συστήματα τεχνητής νοημοσύνης⁹⁵. Πρέπει να διακρίνουμε τη χρήση προσωπικών δεδομένων σε ένα εκπαιδευτικό σύνολο για τη δημιουργία ή την εκμάθηση ενός αλγοριθμικού μοντέλου και τη χρήση τους ως είσοδο σε ένα αλγοριθμικό μοντέλο δεδομένων. Στην πρώτη περίπτωση, αρκεί να ληφθούν ισχυρά μέτρα ασφαλείας, τα οποία συνήθως θα πρέπει να περιλαμβάνουν ψευδωνυμοποίηση των δεδομένων και ανωνυμοποίησή τους μόλις ολοκληρωθεί το μοντέλο, καθώς φαίνεται ότι τα δικαιώματα του υποκειμένου των δεδομένων δεν επηρεάζονται σοβαρά. Επομένως, εάν ο υπεύθυνος επεξεργασίας έχει έννομο συμφέρον (συμπεριλαμβανομένων και των οικονομικών συμφερόντων), φαίνεται ότι θα μπορούσε να τηρηθεί το πρότυπο που ορίζεται στο άρθρο 6 παράγραφος 1 στοιχείο στ'.

Η κατάσταση είναι διαφορετική όταν τα δεδομένα των υποκειμένων χρησιμοποιούνται σε αλγοριθμικό μοντέλο, προκειμένου να εξαχθούν συμπεράσματα σχετικά με το υποκείμενο αυτό. Σε μια τέτοια περίπτωση, πρέπει να δοθεί

⁹⁴ Άρθρο 6 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

⁹⁵ Kamara, I., & De Hert, P. (2018). Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach. *Brussels Privacy Hub*, 4(12), σελ. 10-14. Διαθέσιμο στο <https://brusselsprivacyhub.eu/publications/wp412.html>. Ανάκτηση: Ιούνιος 2021.

προτεραιότητα στο συμφέρον του υποκειμένου των δεδομένων, σύμφωνα με την εκτίμησή του. Επομένως, το υποκείμενο των δεδομένων θα πρέπει να δώσει τη συγκατάθεσή του για επεξεργασία και να του δοθεί η δυνατότητα να εξαιρεθεί (opt-out).

Ο έλεγχος του εννόμου συμφέροντος είναι αρκετά σημαντικός για την αντιμετώπιση του παραδεκτού αυτών των εφαρμογών που μπορεί να επηρεάσουν σοβαρά τα άτομα και την κοινωνία, ακόμη και όταν αυτές είναι τεχνολογικά ορθές και εκπαιδευμένες δίχως διακρίσεις. Όταν μια εφαρμογή παρέχει οφέλη που αντισταθμίζονται από τα μειονεκτήματα που επιβάλλονται στα υποκείμενα των δεδομένων, θα πρέπει να συμπεράνουμε ότι η εφαρμογή δεν έχει βάση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ'. Αυτό μπορεί να συμβαίνει, όπως σημειώνεται παραπάνω, για συστήματα που προορίζονται να ανιχνεύουν τη στάση των ατόμων από τα πρόσωπα, ή επίσης να εκτιμούν την απόδοση των εργαζομένων με βάση τη συστηματική παρακολούθηση ή να εντοπίζουν και να επηρεάζουν τις πολιτικές απόψεις. Σε όλες αυτές τις περιπτώσεις, δεδομένου ότι η διαφορά στη γνώση και την εξουσία και την έλλειψη επαρκών πληροφοριών, η συγκατάθεση από το υποκείμενο των δεδομένων δεν θα πληροί την απαίτηση ελευθερίας και πληροφόρησης στον ΓΚΠΔ, και επομένως δεν θα μπορούσε να παράσχει μια εναλλακτική νομική βάση. Επομένως, η επεξεργασία πρέπει να θεωρηθεί παράνομη.

Ο περιορισμός του πεδίου εφαρμογής του άρθρου 6 παράγραφος 1 στοιχείο στ' μπορεί να συνίσταται στο γεγονός ότι φαίνεται να υιοθετεί ατομικιστική προοπτική, καθώς απαιτεί μόνο μια ισορροπία μεταξύ των συμφερόντων των υπεύθυνων επεξεργασίας και του υποκειμένου των δεδομένων, χωρίς να λαμβάνονται υπόψη ευρύτερα συμφέροντα, που αφορούν ομάδες ή ακόμη και για την κοινωνία στο σύνολό της. Ωστόσο, αυτός ο περιορισμός του πεδίου εφαρμογής του ελέγχου εξισορρόπησης σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ' μπορεί να έχει λόγο, δεδομένου ότι η εκτίμηση της κοινωνικής αξίας μιας διαδικασίας επεξεργασίας και η απόφαση να απαγορευτεί βάσει αυτής της αξιολόγησης, πρέπει να εγκριθούν βάσει μιας ευρείας συζήτησης και σύμφωνα με την αποφασιστικότητα ή τουλάχιστον προς τις κατευθύνσεις των πολιτικά υπεύθυνων οργάνων.

6. Ειδικές κατηγορίες προσωπικών δεδομένων

Το άρθρο 9 του Κανονισμού εξετάζει τα λεγόμενα ευαίσθητα δεδομένα (ή αλλιώς, ειδικές κατηγορίες δεδομένων), δηλαδή τα προσωπικά δεδομένα των οποίων

η επεξεργασία ενδέχεται να επηρεάσει σε μεγαλύτερο βαθμό τα υποκείμενα εκθέτοντάς τα σε σοβαρούς κινδύνους. Στις ειδικές κατηγορίες δεδομένων συγκαταλέγονται, μεταξύ άλλων, τα δεδομένα που αφορούν την υγεία, τα γενετικά δεδομένα και τα βιομετρικά δεδομένα, με σκοπό την ταυτοποίηση του προσώπου (άρθρο 9 παρ. 1 του Κανονισμού). Συγκεκριμένα, ο κανόνας στο άρθρο 9§1 ορίζει ότι απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν πληροφορίες που εντάσσονται στις ειδικές αυτές κατηγορίες⁹⁶. Από την άποψη αυτή, η ΤΝ παρουσιάζει ορισμένες προκλήσεις.

Σχετικά με την τεχνητή νοημοσύνη και τα βιομετρικά δεδομένα, θα μπορούσαμε να πούμε ότι εγείρονται ορισμένα ζητήματα. Χάρη στην τεχνητή νοημοσύνη, μη ταυτοποιήσιμα προσωπικά δεδομένα, όσα δηλαδή δεν μπορούν να συνδεθούν με ένα συγκεκριμένο άτομο, δύνανται να επαναπροσδιοριστούν και να επανασυνδεθούν με τα συγκεκριμένα άτομα. Η εκ νέου αναγνώριση ευαίσθητων δεδομένων μπορεί να έχει σοβαρές συνέπειες για το υποκείμενο των δεδομένων, όπως για παράδειγμα στην περίπτωση κατά την οποία τα μη ταυτοποιήσιμα ιατρικά αρχεία που έχουν καταστεί προσιτά στο κοινό επαναπροσδιορίζονται σε μεταγενέστερο στάδιο, έτσι ώστε το κοινό να γνωρίζει τις ιατρικές καταστάσεις των ενδιαφερομένων.

Η δεύτερη πρόκληση συνδέεται με την εξαγωγή περαιτέρω δεδομένων από ήδη διαθέσιμα προσωπικά δεδομένα. Χάρη στην τεχνητή νοημοσύνη και τα μεγάλα δεδομένα, μπορεί να είναι δυνατή η σύνδεση παρατηρήσιμης συμπεριφοράς και γνωστών χαρακτηριστικών των ατόμων -όπως διαδικτυακή δραστηριότητα, αγορές, επισημάνσεις «Like», κινήσεις- με μη παρατηρήσιμα ευαίσθητα δεδομένα, όπως η ψυχολογική τους κατάσταση, η κατάσταση της υγείας τους ο σεξουαλικός προσανατολισμός, ή οι πολιτικές τους προτιμήσεις. Η εξαγωγή περαιτέρω δεδομένων οδηγεί σε συμπεράσματα που μπορεί να εκθέσουν τα ενδιαφερόμενα άτομα σε διακρίσεις ή χειραγώγηση.

6.1 Τα βιομετρικά δεδομένα

Στην «εποχή της ασφάλειας» οι νέες τεχνολογίες καλούνται να διαδραματίσουν έναν ολοένα αυξανόμενο ρόλο. Μεταξύ αυτών τη μερίδα του λέοντος κατέχει η λεγόμενη επιστήμη της βιομετρίας. Η χρήση τεχνολογιών που παρέχουν τη δυνατότητα

⁹⁶ Βλ. άρθρο 9 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

ηλεκτρονικής αναγνώσεως και επεξεργασίας βιομετρικών δεδομένων εξαπλώνεται με αλματώδη ταχύτητα τόσο στο δημόσιο όσο και τον ιδιωτικό τομέα⁹⁷.

Τι είναι όμως τα βιομετρικά δεδομένα; Τα βιομετρικά χαρακτηριστικά συνιστούν βιολογικές ιδιότητες, πτυχές συμπεριφοράς, φυσιολογικά χαρακτηριστικά, προσωπικά γνωρίσματα ή επαναλαμβανόμενες κινήσεις⁹⁸. Τυπικά παραδείγματα τέτοιων βιομετρικών δεδομένων είναι τα σωματικά χαρακτηριστικά (π.χ. τα δακτυλικά αποτυπώματα, η ίρις του ματιού, η δομή του προσώπου, η φωνή, αλλά και η γεωμετρία των χεριών, η μορφή των φλεβών) και τα χαρακτηριστικά συμπεριφοράς, όπως η ιδιόχειρη υπογραφή, ο ιδιαίτερος τρόπος βαδίσματος, ομιλίας ή πληκτρολόγησης κ.λπ.. Σύμφωνα με τον ορισμό του Κανονισμού (άρθρο 4 στοιχ. 14), ως βιομετρικά δεδομένα νοούνται «τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα». Πρόκειται, δηλαδή, για γνωρίσματα τα οποία, λόγω του αποκλειστικού τους δεσμού με ένα συγκεκριμένο άτομο, μπορούν να χρησιμοποιηθούν για την αναγνώριση ή την επαλήθευση της ταυτότητάς του. Προκύπτει, λοιπόν, ότι τα βιομετρικά δεδομένα, ως άμεσα συνδεδεμένα με το ανθρώπινο σώμα, θα πρέπει να κριθούν από τη φύση τους ως ευαίσθητα προσωπικά δεδομένα⁹⁹. Ο νέος Κανονισμός αναγνωρίζει αυτήν την ιδιαιτερότητα των βιομετρικών, αλλά και των γενετικών δεδομένων, κατατάσσοντάς τα στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (άρθρο 9 παρ. 1)¹⁰⁰.

Στο πλαίσιο των βιομετρικών συστημάτων, ένα βιομετρικό δείγμα συγκρίνεται με ένα βιομετρικό «πρότυπο», το οποίο είναι αποθηκευμένο σε μια βάση δεδομένων

⁹⁷ Υποστηρίζεται για παράδειγμα ότι η βιομετρία ως μέθοδος διακρίβωσης της ταυτότητας και πιστοποίησης της αυθεντικότητας μπορεί να αντικαταστήσει τον κωδικό πρόσβασης, το λεγόμενο password, για την πρόσβαση στα συστήματα Η/Υ ή τις τραπεζικές κάρτες ανάληψης χρημάτων σε συνδυασμό με την χρήση ενός προσωπικού κωδικού (PIN), ενώ ήδη χρησιμοποιούνται μηχανές αναγνώρισης δακτυλικών αποτυπωμάτων για τον έλεγχο κατά την είσοδο σε κτίρια ή σε χώρους με υψηλές προδιαγραφές ασφαλείας.

⁹⁸ Βλ. Ομάδα εργασίας του άρθρου 29. Γνώμη 4/2007, σελ. 9.

⁹⁹ Ιγγλεζάκης, Ι. (2003). *Ευαίσθητα προσωπικά δεδομένα*, Σάκκουλας, Αθήνα.

¹⁰⁰ Jasserand, C. (2016). Legal nature of biometric data: From generic personal data to sensitive data. *Eur. Data Prot. L. Rev.*, 2, σελ. 297.

και χρησιμοποιείται ως μέτρο σύγκρισης. Τα γνωρίσματα και οι κινήσεις είναι μοναδικά για το άτομο και μετρήσιμα, ακόμη κι αν τα πρότυπα που χρησιμοποιούνται στην πράξη για την τεχνική μέτρησή τους εμπεριέχουν έναν ορισμένο βαθμό πιθανολογήσεως¹⁰¹.

Στο σύγχρονο κόσμο της «κοινωνίας της πληροφορίας» η μέθοδος της βιομετρίας χρησιμοποιείται κατά κύριο λόγο σε εφαρμογές που έχουν ως πρωταρχικό σκοπό τη διακρίβωση της ταυτότητας ενός ατόμου και την πιστοποίηση της αυθεντικότητας της δηλούμενης ταυτότητας μέσω της χρήσης εξατομικευμένων σωματικών χαρακτηριστικών. Για παράδειγμα, οι κάμερες υψηλής ανάλυσης επιτρέπουν με μια μόνο λήψη τη βιομετρική ανάλυση του προσώπου καθενός από τους χιλιάδες θεατές που ακολουθούν μια διαδήλωση ή βρίσκονται σε ένα στάδιο¹⁰². Ως εκ τούτου είναι φανερή η προτίμηση των υπηρεσιών ασφαλείας στις βιομετρικές τεχνολογίες, με τη βοήθεια των οποίων η συλλογή, αποθήκευση και επεξεργασία βιομετρικών δεδομένων αποδεικνύεται ιδιαίτερα χρήσιμη για την επίλυση υποθέσεων που σχετίζονται με φόνους, βιασμούς, ληστείες, τρομοκρατικές επιθέσεις και άλλες εγκληματικές ενέργειες.

Ιστορικά, οι παραπάνω τεχνικές δεν αναπτύχθηκαν στους κόλπους της ΕΕ, αλλά ξεκίνησαν με πρωτοβουλία των ΗΠΑ. Μετά την επίθεση στους δίδυμους πύργους, η σύνδεση των τρομοκρατικών χτυπημάτων με τα αεροπορικά μέσα έστρεψε τα βλέμματα στην ανάγκη ελέγχου και αξιοποίησης δεδομένων επιβατών πτήσεων. Συγκεκριμένα, το Γραφείο Προστασίας Τελωνείων και Συνόρων του Υπουργείου Εσωτερικής Ασφάλειας των ΗΠΑ άρχισε να απαιτεί από τις αεροπορικές εταιρίες που δρομολογούν πτήσεις προς τις ΗΠΑ ή διέρχονται από αυτές να του επιτρέπουν πρόσβαση στα «Μανιφέστα Επιβατών (Passenger Manifests)», γνωστά και ως «PNR (Passenger Name Record)», που τηρεί κάθε αεροπορική εταιρία, πριν από την άφιξη κάθε πτήσης στα αεροδρόμια των ΗΠΑ, προκειμένου να διευκολύνεται ο

¹⁰¹ Ο βαθμός πιθανολογήσεως μπορεί να οφείλεται είτε σε εξωγενείς παράγοντες (π.χ. διαφορά θερμοκρασίας, υγρασία, σκόνη) είτε σε ενδογενείς παράγοντες, οι οποίοι σχετίζονται με την ψυχολογική κατάσταση του ενδιαφερομένου (άγχος, ιδρώτας). Ειδικά για την εξέταση των δακτυλικών αποτυπωμάτων λέγεται ότι η πιθανότητα λάθους είναι 1 προς 1.000.000. Βλ. *Ομάδα Εργασίας του άρθρου 29*. Γνώμη 4/2007, σελ. 10.

¹⁰² Παναγοπούλου-Κουντατζή, Φ. (2013). *Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012)*, ΔίΜΕΕ, σελ. 482-492

προγενέστερος έλεγχος των επιβατών με σκοπό την ασφάλεια των πτήσεων και την πρόληψη και αντιμετώπιση τυχόν τρομοκρατικών ενεργειών μέσα από τον εντοπισμό υπόπτων υψηλού κινδύνου.

Η εμφάνιση παρόμοιων περιστατικών τρομοκρατίας στον ευρωπαϊκό χώρο ανάγκασαν την ΕΕ να υιοθετήσει αντίστοιχα συστήματα, όπως τη Συνθήκη του Schengen, της Europol και της Eurojust. Στη συνέχεια, προέβη σε Συμφωνίες PNR με τις ΗΠΑ, αλλά και με άλλες χώρες (όπως ο Καναδάς ή η Αυστραλία). Εν τω μεταξύ, η Οδηγία 95/46/EK όριζε ότι προκειμένου να είναι επιτρεπτή η διαβίβαση προσωπικών δεδομένων σε τρίτη χώρα, πρέπει σε αυτήν να διασφαλίζεται ικανοποιητικό επίπεδο προστασίας των εν λόγω δεδομένων¹⁰³. Οι ΗΠΑ, όμως, δεν αποτελούσαν «ασφαλή τρίτη χώρα» κατά την έννοια της Οδηγίας. Η λύση δόθηκε με την υιοθέτηση από τις αμερικανικές αρχές του συστήματος «Ασφαλούς Λιμένος (Safe Harbour)», που κρίθηκε αρχικά από την Επιτροπή ως επαρκές στοιχείο ούτως ώστε οι ΗΠΑ να θεωρηθούν ασφαλής τρίτη χώρα και η μεταφορά προσωπικών δεδομένων από χώρες της ΕΕ να είναι νομικά δυνατή.

Με τη θέση σε ισχύ της Οδηγίας 2016/681 «σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων», η χρήση των δεδομένων PNR ως αποφασιστικό όπλο στον αγώνα κατά της τρομοκρατίας αποκτά πλέον ένα ολοκληρωμένο νομικό πλαίσιο. Είναι χαρακτηριστικό ότι ο κοινοτικός νομοθέτης εντοπίζει τον κίνδυνο από την άλογη αξιοποίηση τέτοιων δεδομένων και ορίζει ότι προκειμένου η επεξεργασία δεδομένων PNR να είναι περιορισμένη, τα δεδομένα PNR που συλλέγονται βάσει της παρούσας οδηγίας πρέπει να υφίστανται επεξεργασία μόνο για τον σκοπό της πρόληψης, ανίχνευσης, διερεύνησης και δίωξης τρομοκρατικών και σοβαρών εγκλημάτων¹⁰⁴. Τα δεδομένα που συλλέγονται απαριθμούνται στην Οδηγία¹⁰⁵ και αποτελούν κατά κύριο

¹⁰³ Βλ. άρθρο 25 παρ. 1 της Οδηγίας 95/46/EK. Η ίδια αρχή με κάποιες παραλλαγές επαναλαμβάνεται και στο άρθρο 45 παρ. 1 του Κανονισμού 2016/679/ΕΕ: «Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί εφόσον η Επιτροπή έχει αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό. Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια».

¹⁰⁴ Βλ. άρθρο 1 παρ. 2 της Οδηγίας 2016/681/ΕΕ.

¹⁰⁵ Βλ. Παράρτημα Ι της Οδηγίας 2016/681/ΕΕ.

λόγο πληροφορίες που «μαρτυρούν» τη διαδρομή που ακολουθούν οι επιβάτες κατά την είσοδο, έξοδο και γενικά τη μετακίνησή τους εντός ΕΕ, παράλληλα με την ταυτοποίηση των προσώπων. Με μια πρώτη ανάγνωση, οι πληροφορίες αυτές φαίνονται πράγματι στοχευμένες και σε γενικές γραμμές δεν επεμβαίνουν στην στενή σφαίρα της ιδιωτικότητας των ατόμων και, συνεπώς, η επεξεργασία τους κρίνεται δικαιολογημένη εφόσον επιβάλλεται να αντιμετωπιστούν ζητήματα εθνικής ασφάλειας.

6.2 Η απόφαση του ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012) και ο ρόλος της αρχής της αναλογικότητας

Όπως προκύπτει από την ανωτέρω ανάλυση, η ευρεία χρήση των βιομετρικών εφαρμογών εγκυμονεί πολλούς κινδύνους για τα ανθρώπινα δικαιώματα και κυρίως για το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Γι' αυτό, ακόμα κι αν δεχθούμε μια κάποιου είδους επέμβαση στο ατομικό δικαίωμα του πληροφοριακού αυτοκαθορισμού (στο βαθμό που δεν προσβάλλεται ο πυρήνας της ανθρώπινης προσωπικότητας), η επέμβαση αυτή θα πρέπει να υπακούει στη συνταγματική αρχή της αναλογικότητας¹⁰⁶. Θα πρέπει να εκτιμάται η εύλογη σχέση μεταξύ του βιομετρικού συστήματος και του επιδιωκόμενου σκοπού της δημόσιας ασφάλειας, να εκτιμάται, δηλαδή, αν η αναμενόμενη ωφέλεια από την χρήση του βιομετρικού συστήματος βρίσκεται σε ορθολογική αντιστοιχία με τον περιορισμό του δικαιώματος στην προστασία προσωπικών δεδομένων. Για παράδειγμα, υπάρχουν περιπτώσεις όπου η χρήση βιομετρικών συστημάτων καίτοι ενέχει σημαντικούς κινδύνους από πλευράς προστασίας προσωπικών δεδομένων, εντούτοις γίνεται δεκτή με βάση την αρχή της αναλογικότητας διότι ικανοποιεί υψηλές απαιτήσεις ασφάλειας στον έλεγχο προσβάσεως (ταυτοποίησεως και αυθεντικοποίησεως) σε συγκεκριμένους φυσικούς χώρους (π.χ. κρίσιμες εγκαταστάσεις) ή υπολογιστικά συστήματα (π.χ. κρίσιμες εφαρμογές στρατού, τραπεζών κ.λπ.)¹⁰⁷.

¹⁰⁶ Βλ. αιτιολογική σκέψη 22 της Οδηγίας 2016/681/ΕΕ: «...η εφαρμογή της παρούσας Οδηγίας θα πρέπει να διασφαλίζει πλήρως την τήρηση των θεμελιωδών δικαιωμάτων και το δικαίωμα στην ιδιωτική ζωή καθώς και την αρχή της αναλογικότητας. Θα πρέπει επίσης να διασφαλίζει ουσιαστικά τις αρχές της αναγκαιότητας και της αναλογικότητας στην προσπάθεια επίτευξης των στόχων γενικού συμφέροντος που αναγνωρίζει η Ένωση και υπεράσπισης των δικαιωμάτων και των ελευθεριών των άλλων στο πλαίσιο της καταπολέμησης της τρομοκρατίας και των σοβαρών εγκλημάτων...».

¹⁰⁷ Βλ. ενδεικτικά τις Αποφάσεις 52/2008, 39/2004, 52/2003, 9/2003 της ΑΠΔΠΧ, διαθέσιμες στο <https://www.dpa.gr>.

Στην υπόθεση Michael Schwarz κατά κρατιδίου Bochum ενώπιον του ΔΕΕ, ο Michael Schwarz αιτήθηκε από το κρατίδιο Bochum της Γερμανίας τη χορήγηση διαβατηρίου, αρνούμενος όμως να υποστεί την υποχρεωτική λήψη των ψηφιακών δακτυλικών του αποτυπωμάτων. Κατόπιν της απορρίψεως του αιτήματός του από το κρατίδιο του Bochum, ο Schwarz προσέφυγε ενώπιον του διοικητικού δικαστηρίου ζητώντας του να διατάξει το εν λόγω κρατίδιο να του χορηγήσει διαβατήριο χωρίς λήψη των ψηφιακών δακτυλικών του αποτυπωμάτων, ισχυριζόμενος μεταξύ άλλων ότι ο Κανονισμός προσβάλλει το δικαίωμα προστασίας των προσωπικών δεδομένων. Το διοικητικό δικαστήριο με τη σειρά του υπέβαλε προδικαστικό ερώτημα στο ΔΕΕ, το οποίο κλήθηκε να εξετάσει το κύρος του επίμαχου άρθρου του εν λόγω Κανονισμού.

Το ΔΕΕ κατά την εξέταση ενδεχόμενης προσβολής των θεμελιωδών δικαιωμάτων του σεβασμού της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων εστίασε την ανάλυσή του στον έλεγχο τήρησης της αρχής της αναλογικότητας. Ειδικότερα, το ΔΕΕ, αφού αποδέχθηκε καταρχήν ότι η προβλεπόμενη από τον Κανονισμό επεξεργασία βιομετρικών στοιχείων αποτελεί περιορισμό του δικαιώματος προστασίας των προσωπικών δεδομένων, προέβη σε ενδελεχή έλεγχο και των τριών πτυχών της αρχής της αναλογικότητας προκειμένου να διαπιστώσει αν τα υιοθετούμενα μέτρα ασφαλείας για την εξακρίβωση της γνησιότητας του διαβατηρίου και της ταυτότητας του κατόχου του είναι κατάλληλα, πρόσφορα και αναλογικά προς τον επιδιωκόμενο σκοπό γενικού συμφέροντος αναγνωριζόμενο από την Ένωση και συγκεκριμένα αυτόν της αποτροπής τη παράνομης εισόδου προσώπων στο έδαφός της. Ο σκοπός αυτός ικανοποιείται μέσω της πρόληψης της πλαστογραφήσεως των διαβατηρίων και της καταπολέμησης της δόλιας χρήσεώς τους, ήτοι της χρήσεως από άλλα πρόσωπα πλην του νόμιμου κατόχου τους¹⁰⁸.

¹⁰⁸ Βλ. Ομάδα Εργασίας του άρθρου 29. Γνώμη 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες: «Κατά την ανάλυση της αναλογικότητας ενός προτεινόμενου βιομετρικού συστήματος, μία πρώτη μέριμνα είναι να διερευνηθεί αν το σύστημα είναι αναγκαίο για την κάλυψη της προσδιορισθείσας ανάγκης, ήτοι αν είναι ουσιώδους σημασίας για την ικανοποίηση της εν λόγω ανάγκης ή είναι απλώς πιο εύχρηστο ή αποδοτικό ως προς το κόστος. Ένας δεύτερος παράγοντας που πρέπει να λαμβάνεται υπόψη είναι αν το σύστημα είναι πιθανό να είναι αποτελεσματικό όσον αφορά την κάλυψη της εν λόγω ανάγκης με βάση τα συγκεκριμένα χαρακτηριστικά της βιομετρικής τεχνολογίας που προβλέπεται να χρησιμοποιηθεί. Μια τρίτη πτυχή που πρέπει να αξιολογείται είναι αν η προκύπτουσα συρρίκνωση της ιδιωτικότητας είναι αναλογική με οποιοδήποτε αναμενόμενο όφελος. Εάν το όφελος είναι σχετικά μικρό, όπως η ενίσχυση της ευχρηστίας ή μια μικρή εξοικονόμηση κόστους, τότε η συρρίκνωση της ιδιωτικής

Έτσι, κατά την εξέταση του σταδίου της προσφορότητας, το Δικαστήριο έκρινε ότι η χρήση των δακτυλικών αποτυπωμάτων είναι ικανή να μειώσει τον κίνδυνο της πλαστογραφήσεως, διευκολύνοντας τον έλεγχο γνησιότητας από τις αρμόδιες αρχές. Αναφορικά με την καταπολέμηση της δόλιας χρήσεως, το Δικαστήριο έκρινε ότι αν και η μέθοδος αυτή παρουσιάζει ποσοστό σφάλματος, εντούτοις περιορίζει δραστικά τον κίνδυνο εσφαλμένων εγκρίσεων εισόδου στο έδαφος της Ενώσεως, ο οποίος θα υφίστατο σε περίπτωση μη εφαρμογής της. Άλλωστε, όπως σημειώνει, η έλλειψη αντιστοιχίας (μεταξύ διαβατηρίου και κατόχου) δε συνεπάγεται αυτόματο αποκλεισμό της εισόδου του ενδιαφερομένου στο έδαφος της Ενώσεως, αλλά έχει ως μοναδική συνέπεια την κινητοποίηση των αρμόδιων αρχών και τη διενέργεια περαιτέρω ελέγχων προς οριστική εξακρίβωση της ταυτότητάς του.

Κατά την εξέταση της αναγκαιότητας της επεξεργασίας βιομετρικών δεδομένων, το Δικαστήριο έκρινε ότι τόσο η διαδικασία λήψης των αποτυπωμάτων όσο και η διαδικασία λήψεως εικόνας προσώπου δεν είναι ιδιαίτερα «δυσάρεστες» σωματικά ή ψυχολογικά. Αυτό που δεν έλαβε επαρκώς υπόψη του το Δικαστήριο είναι το γεγονός ότι η ενσωμάτωση στο διαβατήριο περισσότερων του ενός βιομετρικών στοιχείων συνιστά έντονη παρέμβαση στο δικαίωμα ιδιωτικότητας, αφενός διότι μπορεί να λάβει χώρα και εν αγνοία του ατόμου και αφετέρου διότι επιτρέπει το συνδυασμό των στοιχείων αυτών για το ίδιο πρόσωπο και, κατ' επέκταση, την εξαγωγή περαιτέρω συμπερασμάτων που το αφορούν. Εξάλλου, η μοναδική πραγματική εναλλακτική της λήψεως ψηφιακών δακτυλικών αποτυπωμάτων λύση που προτάθηκε κατά την ενώπιον του Δικαστηρίου διαδικασία ήταν η λήψη εικόνας της ίριδας του ματιού. Και δεν προκύπτει από κανένα σημείο, σύμφωνα με το Δικαστήριο, ότι η διαδικασία αυτή θίγει τα κρίσιμα δικαιώματα λιγότερο από τη λήψη ψηφιακών δακτυλικών αποτυπωμάτων. Ως εκ τούτου, το Δικαστήριο δεν προέβη σε ενδελεχή εξέταση άλλων ηπιότερων αλλά εξίσου αποτελεσματικών βιομετρικών συστημάτων, που σχετίζονται με βιομετρικά χαρακτηριστικά που δεν αφήνουν ίχνη εν αγνοία του προσώπου. Αξιολόγησε μόνο το υψηλότερο κόστος της σαρώσεως της ίριδας του ματιού, χωρίς να παραδεχθεί ότι το μέσο αυτό είναι φιλικότερο στην ιδιωτικότητα του

ζωής δεν είναι σκόπιμη. Η τέταρτη πτυχή της αξιολόγησης της επάρκειας ενός βιομετρικού συστήματος είναι να εξεταστεί αν ένα μέσο με λιγότερες επιπτώσεις σε βάρος της ιδιωτικότητας θα μπορούσε να επιτύχει τον επιδιωκόμενο σκοπό.». Διαθέσιμο στο <https://www.pdpjournals.com/docs/87998.pdf>. Ανάκτηση: Μάρτιος 2021.

ατόμου¹⁰⁹. Βέβαια, δεν πρέπει να παραγνωρίζεται το γεγονός ότι εάν το Δικαστήριο προέβαινε σε ενδελεχή έλεγχο της αρχής της αναγκαιότητας αναζητώντας άλλα, κατά την κρίση του, λιγότερο επαχθή μέσα θα υπέπιπτε στον κίνδυνο του δικαστικού ακτιβισμού, υποκαθιστώντας τη βούληση του νομοθέτη¹¹⁰.

Τέλος, κατά την εξέταση της αρχής της αναλογικότητας *stricto sensu*, το Δικαστήριο αναγνώρισε τον κίνδυνο χρησιμοποίησης των ψηφιακών δακτυλικών αποτυπωμάτων για άλλους σκοπούς πέραν των προβλεπόμενων και έμμεσου ελέγχου των κατόχων τους, διευκρίνισε όμως ότι ο οικείος Κανονισμός απαιτεί την αποθήκευση των ψηφιακών δακτυλικών αποτυπωμάτων μόνο εντός του ίδιου του διαβατηρίου και μόνο για τον σκοπό αποτροπής της παράνομης εισόδου στο έδαφος της Ένωσης, χωρίς να προβλέπει την κεντρική αποθήκευση των βιομετρικών δεδομένων σε βάσεις δεδομένων. Αυτό, βέβαια, δε σημαίνει ότι ο Κανονισμός αποκλείει αυτό το ενδεχόμενο. Διότι, ακόμα κι αν διακρίναμε με αυστηρότητα τα βιομετρικά δεδομένα τα οποία συλλέγονται και αποθηκεύονται για δημόσιους σκοπούς από συγκεκριμένες υπηρεσίες (π.χ. έλεγχος συνόρων), από αυτά που συγκεντρώνονται από ιδιώτες στη βάση συμβατικών υποχρεώσεων με τη συγκατάθεση του ενδιαφερομένου¹¹¹, θα ήταν δύσκολο να διασφαλιστεί ότι τα δεύτερα δε θα διασυνδέονταν με τα πρώτα. Συνεπώς, δεν αποκλείεται το ενδεχόμενο της εντάξεως όλων των πολιτών που διαθέτουν διαβατήρια στην κατηγορία των υπόπτων για διάπραξη εγκλημάτων¹¹².

¹⁰⁹ Η βιομετρία που βασίζεται στη λήψη εικόνας της ίριδας του ματιού θεωρείται λιγότερο επεμβατική των δακτυλικών αποτυπωμάτων, ενώ ως περισσότερο φιλική προς την ιδιωτικότητα και από τις δύο προηγούμενες μεθόδους θεωρείται η βιομετρία βάσει της γεωμετρίας της παλάμης, η οποία όμως δεν εξετάστηκε ως δυνατή εναλλακτική λύση για το Δικαστήριο. Βλ. σχετικά Φάκου, Γ. (2016). *Συστήματα αναγνώρισης βιομετρικών χαρακτηριστικών*, Πτυχιακή εργασία, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας. Διαθέσιμη στο <http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/5896/ΣΥΣΤΗΜΑΤΑ%20ΑΝΑΓ%20ΝΩΡΙΣΗΣ%20ΒΙΟΜΕΤΡΙΚΩΝ%20ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ..pdf?sequence=1&isAllowed=y>.

Ανάκτηση: Μάρτιος 2021.

¹¹⁰ Παναγοπούλου-Κουτνατζή, Φ. (2013), σελ. 482-492.

¹¹¹ Βλ. Ομάδα εργασίας του άρθρου 29. (2003). *Εγγραφο εργασίας σχετικά με τα στοιχεία βιομετρίας*. Διαθέσιμο στο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf. Ανάκτηση: Απρίλιος 2021.

¹¹² Μαντζούφας, Π. (2010). *Βιοπολιτική και βιομετρία*, Όμιλος "Αριστόβουλος Μάνεσης". Διαθέσιμο στο <https://www.constitutionalism.gr/1828-biopolitiki-kai-biometria/>. Ανάκτηση: Μάρτιος 2021.

Ο έλεγχος των τριών σταδίων της αρχής της αναλογικότητας από το Δικαστήριο οδήγησε στο αποτέλεσμα ότι το μέτρο λήψεως των βιομετρικών δεδομένων συνιστά θεμιτό περιορισμό της ιδιωτικότητας και του δικαιώματος προστασίας προσωπικών δεδομένων, που πραγματοποιείται για το γενικότερο συμφέρον της δημόσιας ασφάλειας. Παρά τις αμφιβολίες που διατυπώθηκαν για το εάν ο έλεγχος αυτός ήταν πλήρης, ιδιαίτερα ως προς τον μη ενδελεχή έλεγχο κατά το στάδιο εξέτασης της αναγκαιότητας, η παράλειψη αυτή του Δικαστηρίου ίσως υποδηλώνει τις δυσκολίες της αρχής της αναλογικότητας κατά την εξέταση συγκρουόμενων αγαθών, όπως αυτών της δημόσιας ασφάλειας και της προστασίας των προσωπικών δεδομένων¹¹³. Σε κάθε περίπτωση, ακόμα κι αν δεχτούμε ότι πρόκειται για δικαιολογημένη υποχώρηση του δικαιώματος της προστασίας προσωπικών δεδομένων προς χάριν της δημόσιας ασφάλειας, τότε σαφώς αυτή χρήζει αυστηρής νομοθετικής αντιμετώπισης. Διότι οι κίνδυνοι από την επεξεργασία βιομετρικών δεδομένων είναι πολλοί. Περισσότεροι όμως είναι οι κίνδυνοι από τη μη ρύθμιση των αναφύομενων προβλημάτων και από την εν κρυπτώ διαδικασία συλλογής βιομετρικών δεδομένων για μη προβλεπόμενους ή αλλιώς αδιαφανείς σκοπούς¹¹⁴.

6.3 Οι εικόνες προσώπου ως βιομετρικά δεδομένα

Οι εικόνες του προσώπου αποτελούν βιομετρικά δεδομένα, τα οποία ορίζονται ως τα δεδομένα προσωπικού χαρακτήρα που προκύπτουν από ειδική τεχνική επεξεργασία συνδεδεμένη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου¹¹⁵. Οι εικόνες προσώπου, σε σχέση με άλλα βιομετρικά αναγνωριστικά, όπως δακτυλικά αποτυπώματα ή DNA, είναι πιο εύκολο να καταγραφούν, διότι ένα άτομο συνήθως δεν μπορεί να αποφύγει τη λήψη και την παρακολούθηση της εικόνας του προσώπου του στο δημόσιο χώρο.

Η νομοθεσία της ΕΕ ρυθμίζει την επεξεργασία εικόνων προσώπου βάσει του κοινοτικού κεκτημένου για την προστασία δεδομένων. Στον τομέα της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις, η Οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου (Οδηγία 2016/680/ΕΕ) αποτελεί το νομοθετικό κείμενο που θεσπίζει ένα ολοκληρωμένο σύστημα προστασίας

¹¹³ Παναγοπούλου-Κουντατζή, Φ. (2013), σελ. 482-492.

¹¹⁴ Όπως παραπάνω.

¹¹⁵ Άρθρο 4 παρ. 14 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

προσωπικών δεδομένων στο πλαίσιο της επιβολής του νόμου¹¹⁶ και εφαρμόζεται σε αυτές τις περιπτώσεις. Η Οδηγία αναφέρεται συγκεκριμένα στις εικόνες προσώπου ως «βιομετρικά δεδομένα» όταν χρησιμοποιούνται για βιομετρική αντιστοίχιση για τους σκοπούς της μοναδικής ταυτοποίησης ή ελέγχου ταυτότητας ενός φυσικού προσώπου¹¹⁷.

Ειδικότερα, διακρίνονται δύο κατηγορίες πληροφοριών που θεωρούνται βιομετρικά δεδομένα: 1) τα φυσικά χαρακτηριστικά, τα οποία αφορούν σωματικά χαρακτηριστικά όπως χαρακτηριστικά προσώπου, δακτυλικά αποτυπώματα, αμφιβληστροειδή και ίριδα και 2) τα συμπεριφορικά χαρακτηριστικά, όπως βαθιά ριζωμένες συνήθειες, ενέργειες, χαρακτηριστικά προσωπικότητας, εθισμοί¹¹⁸. Αυτό περιλαμβάνει χαρακτηριστικά συμπεριφοράς που θα μπορούσαν να επιτρέψουν τη μοναδική ταυτοποίηση ενός ατόμου, όπως μια χειρόγραφη υπογραφή ή ένας συγκεκριμένος τρόπος περπατήματος ή κίνησης. Οι ψηφιακές εικόνες προσώπου ανήκουν στην πρώτη κατηγορία.

Η αιτιολογική σκέψη 51 του ΓΚΠΔ κάνει διάκριση μεταξύ της νομικής φύσης των απλών «φωτογραφιών» και των βιομετρικών «εικόνων προσώπου». Ο ορισμός των βιομετρικών δεδομένων ισχύει για φωτογραφίες μόνο όταν αυτές υποβάλλονται σε επεξεργασία με συγκεκριμένα τεχνικά μέσα που επιτρέπουν τη μοναδική ταυτοποίηση ή πιστοποίηση φυσικού προσώπου¹¹⁹.

Σύμφωνα, λοιπόν, με την εν λόγω κατάταξη των βιομετρικών δεδομένων στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, και τη διάταξη του άρθρου 9 παρ. 1 του ΓΚΠΔ, απαγορεύεται κατ' αρχήν η επεξεργασία τους. Στην παράγραφο 2 του ίδιου άρθρου ο νομοθέτης εισήγαγε με περιοριστική απαρίθμηση τις περιπτώσεις στις οποίες δεν εφαρμόζεται η παράγραφος 1 και αίρεται η σχετική απαγόρευση. Ειδικότερα, επιτρέπεται η επεξεργασία αυτής της κατηγορίας προσωπικών δεδομένων, όταν:

- το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα,

¹¹⁶ Βλ. FRA, Council of Europe and EDPS. (2018). *Handbook on European data protection law*. Publications Office, σελ. 31-33. Διαθέσιμο σε https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Ανάκτηση: Μάρτιος 2021

¹¹⁷ Άρθρο 3 της Οδηγίας 2016/680/ΕΕ.

¹¹⁸ *Ομάδας εργασίας άρθρου 29*, Γνώμη 3/2012, σελ. 20 επ.

¹¹⁹ Βλ. αιτιολογική σκέψη 51 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

- η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας,
- η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,
- η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο,
- η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,
- η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,
- η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,
- η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,
- η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, ή
- η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.

6.4 Η τεχνολογία αναγνώρισης προσώπου (Facial recognition technology)

Οι τεχνολογίες αναγνώρισης προσώπου αποτελούν βιομετρικά συστήματα που επιτρέπουν την αυτόματη αναγνώριση και αντιστοίχιση του προσώπου ενός ατόμου. Η τεχνολογία εξάγει και επεξεργάζεται περαιτέρω βιομετρικά δεδομένα δημιουργώντας ένα «βιομετρικό πρότυπο»¹²⁰. Όσον αφορά τις εικόνες προσώπου, ένα βιομετρικό πρότυπο μπορεί να ανιχνεύει και να μετρά διάφορα χαρακτηριστικά του προσώπου. Η «τεχνολογία αναγνώρισης προσώπου (FRT)» επιτρέπει την αυτόματη ταυτοποίηση ενός ατόμου με αντιστοίχιση δύο ή περισσότερων προσώπων από ψηφιακές εικόνες, ανιχνεύοντας και μετρώντας διάφορα χαρακτηριστικά του προσώπου, εξάγοντάς τα από την εικόνα και, σε ένα δεύτερο βήμα, συγκρίνοντάς τα με χαρακτηριστικά που λαμβάνονται από άλλα πρόσωπα.

Στον ιδιωτικό τομέα, η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται ευρέως για διαφήμιση, μάρκετινγκ και άλλους σκοπούς, με κατάρτιση προφίλ και ταυτοποίηση μεμονωμένων πελατών προκειμένου να προβλέψουν τις προτιμήσεις τους σχετικά με τα προϊόντα βάσει των εκφράσεων του προσώπου τους. Επίσης, χρησιμοποιείται τεχνολογία αναγνώρισης προσώπου για να αναλύσει τις εκφράσεις του προσώπου των υποψηφίων για εργασία σε συνεντεύξεις¹²¹, καθώς και μεγάλα διαδικτυακά και κοινωνικά μέσα, όπως το Facebook, αναπτύσσουν τεχνολογίες αναγνώρισης προσώπου για τη βελτίωση των συστημάτων τους, π.χ. ως προς τις ετικέτες προσώπων¹²².

Η πρόσφατη εξέλιξη της τεχνητής νοημοσύνης που ενδυνάμωσε την τεχνολογία αναγνώρισης προσώπου δεν είναι «ελκυστική» μόνο στον ιδιωτικό τομέα. Ανοίγει επίσης νέες δυνατότητες στον τομέα της δημόσιας διοίκησης, συμπεριλαμβανομένου της επιβολής του νόμου και της διαχείρισης των συνόρων. Μια σημαντική αύξηση της ακρίβειας που επιτεύχθηκε τα τελευταία χρόνια ώθησε πολλές δημόσιες αρχές και

¹²⁰ Ομάδα εργασίας άρθρου 29. Γνώμη 3/2012, σελ. 20 επ.

¹²¹ Hymas, Ch. (2019). *AI used for first time in job interviews in UK to find best applicants*, The Telegraph. Διαθέσιμο στο <https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/?fbclid=IwAR2YAjJpQqpSIIdhNyZebyxrSvAxxg-8SlSqEGbNK12kJoag5I1OoewPUQ3Bk>. Ανάκτηση: Μάρτιος 2021.

¹²² Simonite, T. (2017). *Facebook Can Now Find Your Face, Even When It's Not Tagged*, Wired. Διαθέσιμο στο <https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/>. Ανάκτηση: Απρίλιος 2021.

ιδιωτικές επιχειρήσεις να αρχίσουν να χρησιμοποιούν, να δοκιμάζουν ή να σχεδιάζουν τη χρήση τεχνολογιών αναγνώρισης προσώπου σε όλο τον κόσμο.

Αυτό, με τη σειρά του, πυροδότησε μια έντονη συζήτηση σχετικά με τον πιθανό αντίκτυπο στα θεμελιώδη δικαιώματα. Για παράδειγμα, η σε μεγάλη κλίμακα χρήση της τεχνολογίας αναγνώρισης προσώπου σε συνδυασμό με κάμερες παρακολούθησης στη Λαϊκή Δημοκρατία της Κίνας έχει οδηγήσει σε πολλές συζητήσεις και ανησυχίες σχετικά με πιθανές παραβιάσεις ανθρωπίνων δικαιωμάτων, ιδίως όσον αφορά τον εντοπισμό μελών ορισμένων εθνοτικών μειονοτήτων¹²³. Μετά από αυξημένη χρήση της αναγνώρισης προσώπου στις ΗΠΑ, μια εθνική έρευνα που δημοσιεύθηκε τον Σεπτέμβριο του 2019 από το Pew Research Center διαπιστώνει ότι, ενώ ένας στους δύο Αμερικανούς πολίτες (56%) εμπιστεύεται τις υπηρεσίες επιβολής του νόμου να χρησιμοποιούν αυτές τις τεχνολογίες με υπευθυνότητα, μικρότερο ποσοστό πολιτών λένε ότι έχουν τέτοια εμπιστοσύνη σε εταιρείες τεχνολογίας (36%) ή διαφημιστές (18%)¹²⁴.

Μέχρι σήμερα, υπάρχουν λίγα παραδείγματα της εθνικής νομοθεσίας κρατών, που χρησιμοποιούν οι αρχές επιβολής τεχνολογίες ζωντανής αναγνώρισης προσώπου στην Ευρώπη. Στο Ηνωμένο Βασίλειο, η αστυνομική βάση δεδομένων περιλαμβάνει περί τα 23 εκατομμύρια πρόσωπα και οι αστυνομικές δυνάμεις κάνουν εκτεταμένη χρήση τεχνολογιών αναγνώρισης προσώπου, καθώς και δοκιμές με βιντεοεπιτήρηση δημόσιων χώρων, χωρίς να υπάρχει προηγούμενη επιστημονική έρευνα αξιοπιστίας των συστημάτων και κατάλληλο νομοθετικό πλαίσιο εγγυήσεων. Σοβαροί προβληματισμοί έχουν εκδηλωθεί, από τον Βρετανό Επίτροπο Βιομετρικών, που στην ετήσια έκθεσή του¹²⁵ επισημαίνει τον κίνδυνο ότι χωρίς νομικό πλαίσιο η στάθμιση

¹²³ Mozur, P. (2019). *How China Is Using A.I. to Profile a Minority*, The New York Times. Διαθέσιμο στο <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>. Ανάκτηση: Απρίλιος 2021.

¹²⁴ Smith, A. (2019). *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, Pew Research Center. Διάθεσιμο στο <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/>. Ανάκτηση: Μάρτιος 2021.

¹²⁵ Βλ. Wiles, P. (2019). *Commissioner for the retention and use of biometric material*, Annual Report 2018. Διαθέσιμο στο https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf.

Ανάκτηση: Μάρτιος 2021.

μεταξύ προστασίας δεδομένων και δημόσιου συμφέροντος αφέθηκε στην αστυνομία, ενώ παράλληλα η τεχνολογία αυτή λειτουργεί με διακρίσεις¹²⁶, αναγνωρίζοντας εσφαλμένα περισσότερο γυναίκες και έγχρωμα άτομα.

Άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν εμπλακεί σε δοκιμές και έχουν κάνει σχέδια για χρήση τεχνολογίας αναγνώρισης προσώπου. Για παράδειγμα, στην Ουγγαρία, ένα έργο που ονομάζεται «Szitakötő» (dragonfly) σχεδιάζει να αναπτύξει 35.000 κάμερες με δυνατότητα αναγνώρισης προσώπου στη Βουδαπέστη και σε ολόκληρη τη χώρα. Οι κάμερες πρόκειται να τραβήξουν εικόνες από πινακίδες οδήγησης και εικόνες προσώπου για τη διατήρηση της δημόσιας τάξης, συμπεριλαμβανομένης και της οδικής ασφάλειας¹²⁷. Η τσεχική κυβέρνηση ενέκρινε ένα σχέδιο για την επέκταση της χρήσης κάμερας αναγνώρισης προσώπου -από 100 έως 145- στο Διεθνές Αεροδρόμιο της Πράγας¹²⁸. Η σουηδική αρχή προστασίας δεδομένων ενέκρινε πρόσφατα τη χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία για βοήθεια εντοπισμού υπόπτων εγκληματιών, κάτι που επιτρέπει στην αστυνομία να συγκρίνει τις εικόνες προσώπου από πλάνια CCTV σε μία λίστα παρακολούθησης που περιέχει πάνω από 40.000 εικόνες¹²⁹. Η Ελλάδα από πλευράς της αποφάσισε και ενέκρινε την προμήθεια τεχνολογίας αναγνώρισης προσώπου για την Ελληνική Αστυνομία¹³⁰.

Η επεξεργασία εικόνων προσώπου αναμένεται να εισαχθεί συστηματικότερα σε συστήματα πληροφορικής μεγάλης κλίμακας της ΕΕ, που χρησιμοποιούνται για

¹²⁶ Sample, I. (2019). *Watchdog criticises 'chaotic' police use of facial recognition*, The Guardian. Διαθέσιμο στο <https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition>. Ανάκτηση: Φεβρουάριος 2021.

¹²⁷ Vass, Á. (2019). *CCTV: Is It Big Brother or the Eye of Providence?*, HUNGARY today. Διαθέσιμο στο <https://hungarytoday.hu/cctv-is-it-big-brother-or-the-eye-of-providence/>. Ανάκτηση: Απρίλιος 2021.

¹²⁸ Mayhew, S. (2019). *Expanded use of facial recognition at Prague international airport approved*, BIMOETRIC UPDATE.COM. Διαθέσιμο στο <https://www.biometricupdate.com/201903/expanded-use-of-facial-recognition-at-prague-international-airport-approved>. Ανάκτηση: Απρίλιος 2021.

¹²⁹ Homy, M. (2019). *Police Use of Facial Recognition Tech Approved in Sweden*, Bloomberg Law. Διαθέσιμο στο <https://news.bloomberglaw.com/tech-and-telecom-law/police-use-of-facial-recognition-tech-approved-in-sweden>. Ανάκτηση: Απρίλιος 2021.

¹³⁰ Βλ. Homo Digitalis. (2019). *Προ των πυλών η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία στην Ελλάδα*. Διαθέσιμο στο <https://www.homodigitalis.gr/posts/4662>. Ανάκτηση: Μάρτιος 2021.

σκοπούς ασύλου, μετανάστευσης και ασφάλειας. Αυτές οι εικόνες θα λαμβάνονται σε ελεγχόμενα περιβάλλοντα -για παράδειγμα, σε αστυνομικά τμήματα ή σημεία διέλευσης συνόρων-, όπου η ανάλυση των εικόνων είναι υψηλότερη σε σύγκριση με αυτό των καμερών CCTV. Παρά την έντονη ώθηση από την ιδιωτική βιομηχανία και άλλους ενδιαφερόμενους να χρησιμοποιήσουν την τεχνολογία αναγνώρισης προσώπου, έχει προκύψει ισχυρός αντίλογος αναφέροντας μειονεκτήματα. Αυτό οδήγησε, για παράδειγμα, τον μεγαλύτερο εταιρικό προμηθευτή φωτογραφικών μηχανών σώματος στον κόσμο (Αχον) να ανακοινώσει ότι δεν θα χρησιμοποιήσει τεχνολογία αναγνώρισης προσώπου σε κανένα από τα προϊόντα του, επειδή ήταν πολύ αναξιόπιστη για τα όργανα επιβολής του νόμου και «θα μπορούσε να επιδεινώσει τις υπάρχουσες ανισότητες στην αστυνόμευση, για παράδειγμα με την επιβολή κυρώσεων σε μειονότητες»¹³¹. Αντίστοιχα, η πόλη του Σαν Φρανσίσκο στις Ηνωμένες Πολιτείες, μεταξύ άλλων πόλεων, έχει απαγορεύσει τη χρήση της τεχνολογίας λόγω της υπερβολικά παρεμβατικής φύσης στην ιδιωτική ζωή των ανθρώπων και για την αποφυγή πιθανής κατάχρησης από τις υπηρεσίες επιβολής του νόμου¹³².

Ο κίνδυνος σφαλμάτων στην αντιστοίχιση προσώπων είναι η πιο συχνή ανησυχία σχετικά με τα θεμελιώδη δικαιώματα. Τα θεμελιώδη δικαιώματα που επηρεάζονται περιλαμβάνουν, μεταξύ άλλων, την ανθρώπινη αξιοπρέπεια, το δικαίωμα σεβασμού της ιδιωτικής ζωής, την προστασία των προσωπικών δεδομένων, τη μη διάκριση, τα δικαιώματα του παιδιού και των ηλικιωμένων, τα δικαιώματα των ατόμων με αναπηρίες, την ελευθερία του συνέρχεσθαι και ένωση, η ελευθερία της έκφρασης, το δικαίωμα χρηστής διοίκησης και το δικαίωμα αποτελεσματικής προσφυγής και δίκαιης δίκης. Για παράδειγμα, η τεχνολογία αναγνώρισης προσώπου έχει υψηλότερα ποσοστά σφάλματος όταν χρησιμοποιείται σε γυναίκες και άτομα χρώματος, παράγοντας προκατειλημμένα αποτελέσματα, τα οποία μπορούν τελικά να οδηγήσουν σε διακρίσεις. Η χρήση της τεχνολογίας αναγνώρισης προσώπου μπορεί επίσης να έχει αρνητικό αντίκτυπο στην ελευθερία του συνέρχεσθαι, εάν οι άνθρωποι φοβούνται ότι

¹³¹ Crawford, K. (2019). Halt the use of facial-recognition technology until it is regulated. *Nature*, 572(7771), σελ. 565-566.

¹³² Conger, K., Fausset, R., & Kovalesski, S. F. (2019). *San Francisco bans facial recognition technology*, The New York Times. Διάθεσιμο στο <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>. Ανάκτηση: Απρίλιος 2021.

η τεχνολογία αναγνώρισης προσώπου χρησιμοποιείται για την ταυτοποίησή τους («chilling effect»).

6.5 Η προστασία των ειδικών προσωπικών δεδομένων από τεχνολογίες αναγνώρισης προσώπου

Τα δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων έχουν κεντρική σημασία για την ανάπτυξη της τεχνολογίας αναγνώρισης προσώπου σε δημόσιους χώρους. Αν και τα δύο είναι στενά συνδεδεμένα, πρόκειται για δυο ξεχωριστά, αυτοτελή δικαιώματα. Έχουν επίσης περιγραφεί ως το «κλασικό» δικαίωμα στην προστασία της ιδιωτικής ζωής και ένα πιο «σύγχρονο» δικαίωμα, το δικαίωμα στην προστασία των δεδομένων¹³³. Και τα δύο προσπαθούν να προστατεύσουν παρόμοιες αξίες, δηλαδή την αυτονομία και την ανθρώπινη αξιοπρέπεια των ατόμων, παρέχοντάς τους μια προσωπική ιδιωτική σφαίρα στην οποία μπορούν ελεύθερα να αναπτύξουν τις προσωπικότητές τους, να σκεφτούν και να διαμορφώσουν τις απόψεις τους. Αποτελούν λοιπόν βασική προϋπόθεση για την άσκηση άλλων θεμελιωδών δικαιωμάτων, όπως η ελευθερία σκέψης, συνείδησης και θρησκείας (άρθρο 10 του Χάρτη), η ελευθερία έκφρασης και πληροφόρησης (άρθρο 11 του Χάρτη), και η ελευθερία του συνέρχεσθαι και συνεταιρίζεσθαι (Άρθρο 12 του Χάρτη)¹³⁴.

Η χρήση ζωντανών τεχνολογιών αναγνώρισης προσώπου συνεπάγεται τη συλλογή, σύγκριση ή/και αποθήκευση εικόνων προσώπου σε ένα σύστημα πληροφορικής για σκοπούς αναγνώρισης. Συνεπώς, συνιστά παρέμβαση στο δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που ορίζεται στο άρθρο 8 του Χάρτη και το δικαίωμα στην ιδιωτική ζωή σύμφωνα με το άρθρο 7 του Χάρτη. Οι εικόνες προσώπου αποτελούν προσωπικά δεδομένα, όπως επιβεβαιώνεται επίσης από το ΔΕΕ¹³⁵ και το ΕΔΑΔ¹³⁶ και αναλύσαμε και παραπάνω. Το ΕΔΑΔ διαπίστωσε επίσης

¹³³ Βλ. συνεκδικασθείσες υποθέσεις ΔΕΕ C-92/09 και C-93/09, Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen, παρ. 71. Διαθέσιμες στο <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62009CJ0092>. Ανάκτηση: Ιούνιος 2021.

¹³⁴ FRA, 2018.

¹³⁵ Υπόθεση ΔΕΕ C-291/2012 Michael Schwarz κατά κρατιδίου Bochum. Διαθέσιμη στο <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0291&qid=1624360124936>.

Ανάκτηση: Ιούνιος 2021.

¹³⁶ Υπόθεση ΕΔΑΔ 37138/14 Szabó and Vissy κατά Ουγγαρίας. Διαθέσιμη στο <https://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22szabo%20vissy%22%5D,%22document>

ότι η εικόνα του προσώπου ενός ατόμου αποτελεί ένα από τα βασικά χαρακτηριστικά της προσωπικότητάς του, καθώς αποκαλύπτει τα μοναδικά χαρακτηριστικά του ατόμου και διακρίνει το άτομο από τους συνομηλίκους του. Το δικαίωμα στην προστασία της εικόνας του προσώπου είναι επομένως ένα από τα βασικά στοιχεία της προσωπικής ανάπτυξης.

Η έννοια της «ιδιωτικής ζωής» είναι ένας ευρύτερος όρος που δεν υπόκειται στον εξαντλητικό ορισμό. Καλύπτει τη σωματική και ψυχολογική ακεραιότητα ενός ατόμου και μπορεί, ως εκ τούτου, να αγκαλιάσει πολλές πτυχές της φυσικής και κοινωνικής ταυτότητας του ατόμου¹³⁷. Υπάρχει επίσης μια ζώνη αλληλεπίδρασης ενός ατόμου με άλλους, ακόμη και σε δημόσιο πλαίσιο, η οποία μπορεί να πέσει εντός του πεδίου της «ιδιωτικής ζωής». Σε άλλο πλαίσιο, το ΕΔΔΑ έχει χρησιμοποιήσει την έννοια της «λογικής προσδοκίας της ιδιωτικής ζωής», η οποία αναφέρεται στο βαθμό στον οποίο οι άνθρωποι μπορούν να περιμένουν την ιδιωτικότητα σε δημόσιους χώρους χωρίς να υπόκεινται σε επιτήρηση, ως έναν από τα τους παράγοντες, αν και όχι απαραίτητα καθοριστικούς, να αποφασίσουν για παραβίαση του δικαιώματος σεβασμού της ιδιωτικής ζωής. Ωστόσο, η συνάφεια και το πεδίο εφαρμογής της φαίνεται να είναι περιορισμένη. Η επεξεργασία εικόνων προσώπου σε βάσεις δεδομένων μεγάλης κλίμακας ενδέχεται, καθώς εξελίσσεται η τεχνολογία αναγνώρισης προσώπου, να εγείρει ζητήματα χωρίς προβλήματα σχετικά με τα δικαιώματα προστασίας της ιδιωτικής ζωής, καθώς και των προσωπικών δεδομένων. Δεδομένου ότι αυτά τα δύο δικαιώματα δεν είναι απόλυτα δικαιώματα, μπορεί να υπόκεινται σε περιορισμούς, αλλά οποιαδήποτε παρέμβαση πρέπει να αιτιολογείται επαρκώς και δεν μπορεί σε καμία περίπτωση να θέσει σε κίνδυνο τον ουσιαστικό, αναφαίρετο πυρήνα αυτού του δικαιώματος¹³⁸.

Η ζωντανή τεχνολογία αναγνώρισης προσώπου περιλαμβάνει τη βιομετρική επεξεργασία εικόνων προσώπου που έχουν ληφθεί σε δημόσιο χώρο, με σκοπό τον

[collectionid2%22:%5B%22GRANDCHAMBER%22,%22CHAMBER%22%5D,%22itemid%22:%5B%22001-160020%22%5D%7D](#). Ανάκτηση: Ιούνιος 2021.

¹³⁷ Βλ. συνεκδικασθείσες υποθέσεις ΕΔΔΑ 1874/13 και 8567/13, López Ribalda και λοιποί κατά Ισπανίας, παρ. 87. Διαθέσιμες στο <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22002-12630%22%5D%7D>. Ανάκτηση: Ιούνιος 2021.

¹³⁸ Βλ. European Court of Human Rights. (2020). *Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence*. Διαθέσιμο στο https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Ανάκτηση: Απρίλιος 2021.

προσδιορισμό της ταυτότητας ενός ατόμου και την πιθανή διατήρηση αυτών των εικόνων. Κατά συνέπεια, τόσο η αρχική βιομετρική επεξεργασία των εικόνων του προσώπου όσο και η σύγκριση των δεδομένων με μια «λίστα παρακολούθησης» - παράλληλα με τη συμπλήρωση της λίστας παρακολούθησης με εικόνες προσώπου- αποτελούν παρεμβολές με το δικαίωμα σεβασμού της ιδιωτικής ζωής και την προστασία προσωπικών δεδομένων¹³⁹. Δεδομένου ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί περιορισμό αυτών των δικαιωμάτων, πρέπει να υποβληθεί σε αυστηρή δοκιμή αναγκαιότητας και αναλογικότητας, συμπεριλαμβανομένης μιας σαφούς νομικής βάσης για να το πράξει και ενός θεμιτού σκοπού που επιδιώκεται. Μια τέτοια δοκιμή πρέπει να λαμβάνει υπόψη το πλαίσιο και όλες τις σχετικές περιστάσεις.

Δίπλα στις θεμελιώδεις διασφαλίσεις δικαιωμάτων και τις βασικές αρχές προστασίας δεδομένων που απορρέουν από το άρθρο 8 του Χάρτη, όπως ερμηνεύεται από το ΔΕΕ, οι ειδικές εγγυήσεις βάσει του κεκτημένου της ΕΕ για την προστασία των δεδομένων επιβεβαιώνουν περαιτέρω τον έλεγχο αναγκαιότητας και αναλογικότητας. Σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχείο ζ' του Κανονισμού, η επεξεργασία βιομετρικών δεδομένων επιτρέπεται μόνο όταν η επεξεργασία είναι «απαραίτητη για λόγους ουσιαστικού δημοσίου συμφέροντος, βάσει της νομοθεσίας της Ένωσης ή των κρατών μελών που είναι ανάλογες προς τον στόχο που επιδιώκεται, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και ειδικά μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων». Το άρθρο 10 της Οδηγίας 680/2016/ΕΕ ορίζει παρόμοιες, αν και λίγο πιο ανεκτές συνθήκες¹⁴⁰.

¹³⁹ Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. Διαθέσιμο στο <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>. Ανάκτηση: Ιούνιος 2021.

¹⁴⁰ Βλ. άρθρο 10 της Οδηγίας 680/2016/ΕΕ: «Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων για την αποκλειστική ταυτοποίηση ενός φυσικού προσώπου ή δεδομένων που αφορούν στην υγεία ή τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό επιτρέπονται μόνο όταν είναι απολύτως αναγκαίες, με την επιφύλαξη των κατάλληλων διασφαλίσεων για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων και εφόσον: α) επιτρέπονται από το δίκαιο της Ένωσης ή των κρατών μελών· β) επιβάλλονται για την προστασία των ζωτικών συμφερόντων του υποκειμένου των

Η συλλογή και επεξεργασία εικόνων προσώπου με τεχνολογίες αναγνώρισης προσώπου πρέπει να είναι αυστηρά σύμφωνη με τον ευρωπαϊκό νόμο περί προστασίας δεδομένων. Ακολουθώντας τις κύριες νομικές βάσεις της προστασίας δεδομένων, πρέπει να γίνεται επεξεργασία εικόνων προσώπου:

- με νόμιμο, αντικειμενικό και διαφανή τρόπο,
- για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς, και
- τηρώντας τις αρχές επεξεργασία δεδομένων, όπως της ελαχιστοποίησης δεδομένων, της ακρίβειας δεδομένων, του περιορισμού αποθήκευσης, της ακεραιότητας, της εμπιστευτικότητας και της λογοδοσίας¹⁴¹.

7. Η αρχή της διαφάνειας στην τεχνητή νοημοσύνη

Όπως αναφέραμε και παραπάνω, οι περισσότεροι άνθρωποι συχνά τείνουν να αγνοούν το γεγονός της επεξεργασίας των προσωπικών τους δεδομένων. Χαρακτηριστική περίπτωση αποτελεί η καταγραφή της τοποθεσίας του κινητού τηλεφώνου και η επεξεργασία των δεδομένων, που απορρέουν από το φιλτράρισμα των αποτελεσμάτων αναζήτησης στο διαδίκτυο, ενώ πρόκειται για ενέργειες που πλέον θα μπορούσαν να χαρακτηριστούν καθημερινές, ενδέχεται να μην είναι εμφανείς στο μέσο χρήστη.

Οι εφαρμογές της τεχνητής νοημοσύνης και της μηχανικής μάθησης, για τις οποίες υπάρχει κίνδυνος να μεροληπτούν κατά τη διαδικασία λήψης αποφάσεων, όχι μόνο περιορίζουν τα θεμελιώδη δικαιώματα των ατόμων, αλλά μπορούν επίσης να υπονομεύσουν την εμπιστοσύνη στη δικαιοσύνη και τη νομιμότητα των αποφάσεων αυτών. Η εμπιστοσύνη βασίζεται στη διαφάνεια και την προσβασιμότητα στη λήψη αποφάσεων, ενώ παράλληλα συμβάλλει στη διασφάλιση και την επίδειξη σεβασμού στα προσωπικά δεδομένα και τα δικαιώματα των ατόμων. Εν αντιθέσει, η έλλειψη αυτής επηρεάζει τις αντιλήψεις των ανθρώπων και καθίσταται εμπόδιο στην ανταλλαγή δεδομένων, με αποτέλεσμα να επηρεάζονται κοινωνικά και οικονομικά συμφέροντα.

Σε μια ευρύτερη προοπτική, η διαφάνεια εκφράζεται ως ανάγκη να αντιμετωπιστεί η «αδιαφάνεια του αλγορίθμου». Η σοβαρότητα του προβλήματος

δεδομένων ή άλλου φυσικού προσώπου· ή γ) η επεξεργασία αυτή αφορά σε δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων.».

¹⁴¹ Βλ. άρθρο 5 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

καθίσταται ιδιαίτερα εμφανής, αν αναλογιστεί κανείς ότι οι αλγόριθμοι δεν είναι αδιαφανείς μόνο για τους τελικούς χρήστες τους, αλλά και για τους ίδιους τους σχεδιαστές τους, οι οποίοι χάνουν την ικανότητα να κατανοήσουν τη λογική πίσω από τα αποτελέσματα που εξάγονται. Πάνω απ' όλα, η διαφάνεια αποτελεί ουσιαστική θεμελιώδη αρχή της προστασίας δεδομένων, που συνδέεται αυστηρά με τη δικαιοσύνη. Εάν δεν παρέχονται στα άτομα κατάλληλες πληροφορίες και έλεγχος (π.χ. σχετικά με την κατάρτιση ενός προφίλ), τότε θα υπόκεινται σε αποφάσεις που δεν κατανοούν και δεν έχουν κανέναν έλεγχο σε αυτές.

7.1 Διαφάνεια των αλγορίθμων και αλγοριθμικός έλεγχος

Προκειμένου να διασφαλιστεί ότι τεχνικές τεχνητής νοημοσύνης, όπως είναι η μηχανική μάθηση, συμμορφώνονται με τις αρχές προστασίας δεδομένων, είναι απαραίτητη η διαφάνεια των αλγορίθμων που χρησιμοποιούνται σε αυτές τις περιπτώσεις. Μία δημοφιλής προσέγγιση επίτευξης της διαφάνειας αλγορίθμων είναι ο αλγοριθμικός έλεγχος. Η ιδέα αυτή ορίζει ότι η δυνατότητα ελέγχου των αλγορίθμων θα πρέπει να εντοπίζεται κατά τη φάση ανάπτυξης ώστε να επιτρέπεται σε τρίτα μέρη να ελέγχουν, να παρακολουθούν και να αξιολογούν τη συμπεριφορά του αλγορίθμου. Για επιχειρήσεις που δραστηριοποιούνται στον ιδιωτικό τομέα, η έννοια ενός αλγοριθμικού ελέγχου συνδέεται με έναν έλεγχο ευθύνης, ο οποίος, αν και πραγματοποιείται εσωτερικά του οργανισμού για την προστασία των πληροφοριών που κατέχει ο ίδιος, μπορεί να παρέχει διασφάλιση στο κοινό.

Η έλλειψη τεχνικής ικανότητας και υπολογιστικών πόρων θεωρείται ένα πιθανό εμπόδιο στον έλεγχο των αλγορίθμων, όμως αποτελεί και απόδειξη της θετικής εξέλιξης κατά την εφαρμογή του ελέγχου.

7.2 Οπτικοποίηση και Διαδραστικότητα

Μία διαφορετική προσέγγιση στη διαφάνεια των αλγορίθμων είναι ο συνδυασμός της οπτικοποίησης και της διαδραστικότητας. Πολλές έρευνες έχουν διεξαχθεί επί του συγκεκριμένου ζητήματος, ιδιαίτερα όσον αφορά στη χρήση αναλύσεων μεγάλων δεδομένων για συστήματα προτάσεων. Έρευνες δείχνουν ότι εργαλεία οπτικοποίησης, όπως τα TalkExplorer και SetFusion, επιτρέπουν στα φυσικά πρόσωπα να κατανοήσουν καλύτερα τους λόγους για τους οποίους διατυπώθηκαν οι συγκεκριμένες προτάσεις για αυτούς, ενώ παράλληλα τους επιτρέπουν να αναπτύσσουν περισσότερο ακριβείς προτάσεις για τους ίδιους¹⁴². Οι οπτικές

¹⁴² Information Commissioner Office – ICO. (2017), σελ. 88.

επεξηγήσεις και η διαδραστικότητα σε αυτά τα συστήματα διευκολύνονται μέσω διαφόρων χαρακτηριστικών, όπως τα διαγράμματα Venn.

Όταν η εφαρμογή των συστημάτων διαδραστικής οπτικοποίησης είναι δύσκολη για συγκεκριμένους τύπους ανάλυσης μεγάλων δεδομένων, μία παρόμοια αλλά περισσότερο απλή προσέγγιση μπορεί να υιοθετηθεί, κατά την οποία τα φυσικά πρόσωπα έχουν τη δυνατότητα να ελέγξουν και να διορθώσουν τις εκροές του αλγορίθμου μηχανικής εκμάθησης. Για παράδειγμα, εάν ένας οργανισμός πραγματοποιεί αυτόματη κατάρτιση προφίλ για τους πελάτες του, ώστε να καθορίσει το ύψος των ασφαλιστρών, μπορεί να επιτρέψει στους πελάτες να ελέγξουν τα προφίλ και να διορθώσουν μη έγκυρες ταμπέλες που πιθανώς τους έχουν αποδοθεί. Πέραν της απόδειξης συμμόρφωσης με την αρχή της ακρίβειας της προστασίας δεδομένων, οι ενέργειες αυτές μπορούν να οδηγήσουν σε συνολική βελτίωση της ακρίβειας της εφαρμογής μηχανικής εκμάθησης¹⁴³.

7.3 Υποχρέωση ενημερώσεως του υποκειμένου

Η διαφάνεια στο στάδιο, κατά το οποίο τα δεδομένα προσωπικού χαρακτήρα συλλέγονται ή επεξεργάζονται για περαιτέρω σκοπούς, εξετάζεται στα άρθρα 13 και 14 του Κανονισμού, τα οποία απαιτούν να ενημερώνεται το υποκείμενο των δεδομένων σχετικά με τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα προσωπικά δεδομένα, καθώς και τη νομική βάση για την επεξεργασία.

Πρέπει επίσης να παρέχονται πληροφορίες σχετικά με τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτο μέρος, όταν η επεξεργασία βασίζεται σε έννομο συμφέρον¹⁴⁴. Όταν τα δεδομένα υποβάλλονται σε επεξεργασία για σκοπούς που δεν μπορούσαν να προβλεφθούν κατά τη στιγμή της συλλογής των δεδομένων - όπως συμβαίνει συχνά με τις εφαρμογές μηχανικής μάθησης- οι πληροφορίες πρέπει να παρέχονται πριν από τη νέα επεξεργασία, όπως ορίζεται στο άρθρο 13 παράγραφος 3 και 14 παράγραφος 4. Δηλαδή, όταν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί περαιτέρω τα προσωπικά δεδομένα για σκοπούς διαφορετικούς από εκείνους για τους οποίους συλλέχθηκαν τα δεδομένα, ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων, πριν από την περαιτέρω επεξεργασία, πληροφορίες σχετικά με τον άλλο σκοπό.

¹⁴³ Όπως παραπάνω.

¹⁴⁴ Άρθρο 6 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

Η υποχρέωση παροχής πληροφοριών στο υποκείμενο των δεδομένων δεν ισχύει όταν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή συνεπάγεται δυσανάλογη προσπάθεια, ιδίως όταν μιλάμε για επεξεργασία για σκοπούς αρχειοθέτησης για δημόσιο συμφέρον, επιστημονικούς ή ιστορικούς ερευνητικούς σκοπούς ή στατιστικούς σκοπούς, υπό την επιφύλαξη των όρων και των εγγυήσεων που αναφέρονται στο άρθρο 89 παράγραφος 1 ή στο βαθμό που η υποχρέωση, που αναφέρεται στην παράγραφο 1 του άρθρου 14, ενδέχεται να καταστήσει αδύνατη ή να βλάψει σοβαρά την επίτευξη των στόχων της εν λόγω επεξεργασίας¹⁴⁵. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών, καθώς και των εννόμων συμφερόντων του υποκειμένου των δεδομένων, συμπεριλαμβανομένης της δημοσιοποίησης των πληροφοριών.

Οι πληροφορίες πρέπει να είναι εύκολα διαθέσιμες και να διατυπώνονται σε σαφή και κατανοητή γλώσσα (άρθρο 12 ΓΚΠΔ), επιτρέποντας έτσι στα άτομα να ασκήσουν τα δικαιώματα που τους παρέχει ο Κανονισμός. Από την πλευρά του υποκειμένου των δεδομένων, κάθε ουσιαστική πληροφορία, σχετικά με τη λογική που εμπλέκεται στην αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και των προβλεπόμενων συνεπειών της εν λόγω επεξεργασίας, μπορεί να εξαρτάται από το δικαίωμα πρόσβασης σε σχετικά δεδομένα προσωπικού χαρακτήρα.

Μια εγγενής δυσκολία στην παροχή πληροφοριών για έναν αλγόριθμο τεχνητής νοημοσύνης και των χρήσεων του έγκειται στο ότι η μηχανή δε δύναται να εκφραστεί με ανθρώπινους όρους. Ένας άλλος τεχνικός περιορισμός, που προκύπτει από τις διαδικασίες σχεδιασμού, αφορά στην μεταγενέστερη παραγωγή απροβλέπτων αποτελεσμάτων, τα οποία δεν είναι δυνατόν να προβλεφθούν κατά τη διαδικασία του σχεδιασμού. Επιπλέον, πρέπει να ληφθεί υπόψη η δυναμική φύση των αλγορίθμων, η οποία συνεχώς ενημερώνεται και αλλάζει.

8. Δικαιώματα των υποκειμένων

Το συνταγματικό δικαίωμα στην προστασία δεδομένων, το οποίο κατοχυρώνεται στο άρθρο 9Α Συντάγματος, δεν είναι απλώς ένα αμυντικό ατομικό δικαίωμα, αλλά εξοπλίζεται με υποκειμενικά δικαιώματα έναντι του υπεύθυνου

¹⁴⁵ Άρθρο 14 παρ. 5 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

επεξεργασίας, τα οποία κατοχυρώνονται στο τρίτο κεφάλαιο (άρθρα 12-23) του Κανονισμού. Η τεχνητή νοημοσύνη σχετίζεται με ορισμένα δικαιώματα προστασίας δεδομένων. Ο ΓΚΠΔ αναφέρεται ρητά στην κατάρτιση προφίλ και στην αυτοματοποιημένη λήψη αποφάσεων ως προς το δικαίωμα πρόσβασης και το δικαίωμα ένστασης, αλλά η τεχνητή νοημοσύνη εγείρει επίσης ζητήματα αναφορικά με άλλα δικαιώματα, όπως τα δικαιώματα διαγραφής και φορητότητας.

8.1 Το δικαίωμα πρόσβασης (άρθρο 15 ΓΚΠΔ)

Μια βασική πτυχή της διαφάνειας (και κατά συνέπεια της λογοδοσίας) συνίσταται στα δικαιώματα των υποκειμένων των δεδομένων να έχουν πρόσβαση σε πληροφορίες σχετικά με την επεξεργασία των δεδομένων τους. Τα υποκείμενα των δεδομένων, σύμφωνα με το άρθρο 15 του Κανονισμού, έχουν το δικαίωμα λήψης επιβεβαίωσης από τον υπεύθυνο επεξεργασίας σχετικά με το κατά πόσον υφίσταται επεξεργασία προσωπικών δεδομένων, που το αφορούν ή όχι, και, όπου συμβαίνει αυτό, έχουν δικαίωμα πρόσβασης στα προσωπικά δεδομένα και τις πληροφορίες σχετικά με την επεξεργασία τους.

Ειδικότερα, οι πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων είναι οι εξής: α) οι σκοποί της επεξεργασίας, β) οι σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, γ) οι αποδέκτες ή οι κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς, δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα, ε) η ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία, στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή.

Παρακάτω, το άρθρο 15 παράγραφος 1 στοιχείο η' αφορά ειδικά την αυτοματοποιημένη λήψη αποφάσεων, απαιτώντας από τον υπεύθυνο επεξεργασίας να παρέχει, όταν του ζητείται από το υποκείμενο των δεδομένων, τις ίδιες πληροφορίες που θα έπρεπε να είχαν παρασχεθεί πριν από την έναρξη της επεξεργασίας σύμφωνα με το άρθρο 13 παράγραφος 2 στοιχείο στ' και 14 παράγραφος 2 ζ'. Οι υποχρεωτικές πληροφορίες αφορούν την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων και σημαντικών πληροφοριών σχετικά με τη λογική, καθώς και τη σημασία και τις

προβλεπόμενες συνέπειες μιας τέτοιας επεξεργασίας για το υποκείμενο των δεδομένων.

Το δικαίωμα πρόσβασης σε πληροφορίες αναφέρεται επίσης στην αιτιολογική σκέψη 63, όπου ορίζεται ότι το δικαίωμα πρόσβασης περιλαμβάνει το δικαίωμα γνώσης του υποκειμένου των δεδομένων, όπου είναι δυνατόν, σχετικά με τη λογική που ακολουθείται σε οποιαδήποτε αυτόματη επεξεργασία προσωπικών δεδομένων και, τουλάχιστον όταν έχει ως αποτέλεσμα την κατάρτιση προφίλ, τις συνέπειες αυτής της επεξεργασίας.

Υπήρξε ευρεία συζήτηση σχετικά με το κατά πόσον το άρθρο 15 πρέπει να θεωρηθεί ότι παρέχει στα υποκείμενα των δεδομένων το δικαίωμα να λαμβάνουν εξατομικευμένη εξήγηση αυτοματοποιημένων αξιολογήσεων και αποφάσεων¹⁴⁶. Δυστυχώς, η διατύπωση του άρθρου 15 είναι πολύ ασαφής και αυτή η ασάφεια αντικατοπτρίζεται και στην αιτιολογική σκέψη 63. Ειδικότερα, δε διευκρινίζεται εάν η υποχρέωση παροχής πληροφοριών σχετικά με την «λογική»¹⁴⁷, που ακολουθείται σε αυτοματοποιημένες διαδικασίες, αφορά μόνο την παροχή γενικών πληροφοριών σχετικά με τις μεθόδους που υιοθετούνται στο σύστημα, ή και συγκεκριμένες πληροφορίες σχετικά με τον τρόπο με τον οποίο αυτές οι μέθοδοι εφαρμόστηκαν στο υποκείμενο των δεδομένων (δηλ. ατομική εξήγηση).

8.2 Το δικαίωμα διαγραφής (άρθρο 17 ΓΚΠΔ)

Το δικαίωμα διαγραφής ή λήθης του άρθρου 17 ΓΚΠΔ παρέχει τη δυνατότητα στα φυσικά πρόσωπα των οποίων τα προσωπικά δεδομένα τυγχάνουν επεξεργασίας να ζητούν τη διαγραφή τους, όταν δεν υπάρχει έγκυρη νομική βάση για την επεξεργασία, αλλά και να λαμβάνει τα κατάλληλα μέτρα, ώστε να ενημερώνει άλλους υπεύθυνους

¹⁴⁶ Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2). Διαθέσιμο στο https://www.researchgate.net/publication/309322060_The_Ethics_of_Algorithms_Mapping_the_Debate. Ανάκτηση: Ιούνιος 2021.

¹⁴⁷ Βλ. αιτιολογική σκέψη 63 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ: «...Επομένως, κάθε υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να γνωρίζει και να του ανακοινώνεται ιδίως για ποιους σκοπούς γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, εφόσον είναι δυνατόν για πόσο διάστημα γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ποιοι αποδέκτες λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα, ποια λογική ακολουθείται στην τυχόν αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα και ποιες θα μπορούσαν να είναι οι συνέπειες της εν λόγω επεξεργασίας, τουλάχιστον όταν αυτή βασίζεται σε κατάρτιση προφίλ...».

επεξεργασίας, όταν τα προσωπικά δεδομένα έχουν δημοσιοποιηθεί. Ωστόσο, το δικαίωμα αυτό δεν είναι απόλυτο, αλλά υπόκειται σε μια σειρά από εξαιρέσεις, όπως είναι λ.χ. η περίπτωση όπου η επεξεργασία των δεδομένων είναι απαραίτητη για την άσκηση του δικαιώματος στην ελευθερία της έκφρασης και του δικαιώματος στην ενημέρωση.

Το δικαίωμα περιορίζεται για ορισμένους νόμιμους λόγους και συγκεκριμένα, όταν η επεξεργασία είναι απαραίτητη: α) για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση, β) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κρατών μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας, γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παρ. 2 στοιχεία η' και θ', καθώς και το άρθρο 9 παράγραφος 3, δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παρ. 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταντήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη των σκοπών της εν λόγω επεξεργασίας, ή ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Ένα ζήτημα που προκύπτει από την εφαρμογή τεχνολογιών τεχνητής νοημοσύνης μπορεί να αφορά εάν ακόμη και τα συμπεράσματα που εξάγονται από προσωπικά δεδομένα ή επίσης τα συμπεράσματα δεδομένων ομάδας (όπως ένα εκπαιδευμένο αλγόριθμο μοντέλο) θα πρέπει να διαγραφούν ως συνέπεια της υποχρέωσης διαγραφής των συλλεγόμενων προσωπικών δεδομένων που επέτρεψαν την εξαγωγή τέτοιων συμπερασμάτων. Η απάντηση φαίνεται θετική στην πρώτη περίπτωση και αρνητική στη δεύτερη, καθώς τα δεδομένα που είναι ενσωματωμένα σε αλγοριθμικό μοντέλο δεν είναι πλέον προσωπικά. Ωστόσο, η διαγραφή των δεδομένων που χρησιμοποιούνται για την κατασκευή ενός αλγοριθμικού μοντέλου, μπορεί να καταστήσει δύσκολη ή αδύνατη την απόδειξη της ορθότητας αυτού του μοντέλου.

8.3 Το δικαίωμα στη φορητότητα (άρθρο 20 ΓΚΠΔ)

Το άρθρο 20 ΓΚΠΔ προβλέπει ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς

χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλο υπεύθυνο επεξεργασίας, χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας, στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα, υπό ορισμένες προϋποθέσεις.

Το πεδίο εφαρμογής της διάταξης είναι περιορισμένο, καθώς ισχύει μόνο: α) όταν η επεξεργασία βασίζεται σε συγκατάθεση (άρθρο 6 παρ. 1, άρθρο 9 παρ. 2 στοιχ. α' ΓΚΠΔ) ή σε σύμβαση (άρθρο 6 παρ. 1 στοιχ. β' ΓΚΠΔ), β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα και γ) εφόσον τα προσωπικά δεδομένα αφορούν το υποκείμενο των δεδομένων και έχουν χορηγηθεί από αυτό¹⁴⁸.

Αυτή η διάταξη αφορά κυρίως τους παρόχους υπηρεσιών κοινωνικής δικτύωσης (social networking sites) και υπηρεσιών νεφούπολογιστικής (cloud computing) που θα πρέπει να καθιστούν δυνατή την εξαγωγή των δεδομένων χρηστών τους, ώστε να λάβει χώρα η μεταφορά τους σε άλλο πάροχο υπηρεσιών¹⁴⁹. Επιπλέον, καταλαμβάνει και ποικίλες διαδικτυακές εφαρμογές, εφαρμογές ευφών συσκευών και άλλες αυτοματοποιημένες εφαρμογές¹⁵⁰.

Δεν είναι εύκολο να προσδιοριστεί το εύρος αυτού του δικαιώματος όσον αφορά την επεξεργασία που βασίζεται σε τεχνητή νοημοσύνη. Πρώτον, πρέπει να προσδιοριστεί εάν τα δεδομένα που «παρέχονται» από το υποκείμενο των δεδομένων αφορούν μόνο τα δεδομένα που εισάγονται από το υποκείμενο των δεδομένων (π.χ. τα στοιχεία του) ή και τα δεδομένα που συλλέγονται από το σύστημα κατά την παρακολούθηση της δραστηριότητας του υποκειμένου των δεδομένων. Δεύτερον, πρέπει να καθοριστεί εάν το δικαίωμα αφορά επίσης τα δεδομένα που συνάγονται από τα δεδομένα που συλλέχθηκαν σχετικά με το υποκείμενο των δεδομένων.

8.4 Το δικαίωμα εναντίωσης (άρθρο 21§1 ΓΚΠΔ)

Το δικαίωμα εναντίωσης προβλέπει ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιτάσσεται, οποτεδήποτε, για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων που το αφορούν, όταν η νόμιμη βάση της επεξεργασίας είναι η εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, όπως και όταν η επεξεργασία είναι

¹⁴⁸ Παναγοπούλου-Κουτνατζή, Φ. (2017). *Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2019/ΕΕ*, Σάκκουλας Αθήνα-Θεσσαλονίκη.

¹⁴⁹ Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, 2, σελ. 287.

¹⁵⁰ Παναγοπούλου-Κουτνατζή, Φ. (2017).

απαραίτητη για την ικανοποίηση των εννόμων συμφερόντων του υπεύθυνου επεξεργασίας (άρθρο 6 παρ. 1 στοιχ. ε' και στ' ΓΚΠΔ). Το δικαίωμα αυτό ισχύει και όταν η επεξεργασία προσωπικών δεδομένων είναι νόμιμη, δεν αποτελεί δηλ. προϋπόθεση να είναι παράνομη η επεξεργασία, προκειμένου να ασκηθεί το εν λόγω δικαίωμα. Εάν πληρούνται όλες αυτές οι προϋποθέσεις, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να τερματίσει την επεξεργασία.

Το δικαίωμα εναντίωσης είναι ιδιαίτερα σημαντικό όσον αφορά την κατάρτιση προφίλ, καθώς φαίνεται ότι μόνο σε πολύ ειδικές περιπτώσεις ο υπεύθυνος επεξεργασίας μπορεί να έχει επιτακτικούς νόμιμους λόγους για να συνεχίσει να σχεδιάζει ένα υποκείμενο δεδομένων, που αντιτίθεται στην κατάρτιση προφίλ για προσωπικούς λόγους.

Το δικαίωμα δεν ισχύει για την επεξεργασία που βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, καθώς σε αυτήν την περίπτωση το υποκείμενο των δεδομένων μπορεί να εμποδίσει τη συνέχιση της επεξεργασίας μόνο με την ανάκληση της συγκατάθεσης (σύμφωνα με το άρθρο 7 παράγραφος 3 του ΓΚΠΔ).

Ο Κανονισμός, κατά τη ρύθμιση του δικαιώματος εναντίωσης, αναφέρεται ρητά στην κατάρτιση προφίλ και εισάγει ειδικούς κανόνες σχετικά με το άμεσο μάρκετινγκ και τις στατιστικές επεξεργασίες. Τέτοιες διατάξεις σχετίζονται με την τεχνητή νοημοσύνη, δεδομένου ότι η δημιουργία προφίλ και τα στατιστικά στοιχεία είναι πράγματι βασικές εφαρμογές της ΤΝ στα προσωπικά δεδομένα.

9. Αυτοματοποιημένη λήψη αποφάσεων

Στο άρθρο 22 του ΓΚΠΔ εισάγεται η έννοια της αυτοματοποιημένης λήψης αποφάσεων. Η διάταξη αυτή θα μπορούσε να χαρακτηριστεί ως η πιο σχετική του Κανονισμού με την τεχνητή νοημοσύνη και τη μηχανική μάθηση.

9.1 Η απαγόρευση αυτοματοποιημένης λήψης αποφάσεων

Το πρώτο εδάφιο του άρθρου 22 προβλέπει ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο¹⁵¹.

¹⁵¹ Άρθρο 22 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

Παρόλο που αυτή η διάταξη αναφέρεται σε δικαίωμα, δεν προβλέπει δικαίωμα εναντίωσης του υποκειμένου σε αυτοματοποιημένη λήψη αποφάσεων, δηλαδή, δεν υποθέτει ότι η αυτοματοποιημένη λήψη αποφάσεων είναι γενικά επιτρεπτή εφόσον το υποκείμενο των δεδομένων δεν αντιτίθεται σε αυτό. Αντ' αυτού, ουσιαστικά ορίζει ότι απαγορεύονται οι αυτοματοποιημένες αποφάσεις που επηρεάζουν τα υποκείμενα των δεδομένων, εκτός εάν αυτές εντάσσονται σε μία από τις εξαιρέσεις που προβλέπονται στην παράγραφο 2¹⁵².

Αντικείμενο της ρύθμισης του άρθρου 22 ΓΚΠΔ είναι κάθε απόφαση που μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, λαμβανόμενη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο, όπως η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση¹⁵³.

Όπως επισημαίνει η Ομάδα εργασίας του άρθρου 29, η αυτοματοποιημένη λήψη αποφάσεων αφορά τη λήψη αποφάσεων με τεχνολογικά μέσα και χωρίς τη συμμετοχή του ανθρώπου. Αυτό πραγματοποιείται με τη συλλογή δεδομένων απευθείας από φυσικά πρόσωπα, π.χ. μέσω ερωτηματολογίου, ή με τη συλλογή δεδομένων από μια εφαρμογή (π.χ. δεδομένων τοποθεσίας) ή με την εξαγωγή δεδομένων από ένα προφίλ που έχει δημιουργηθεί, όπως συμβαίνει στην αξιολόγηση της πιστοληπτικής ικανότητας¹⁵⁴. Η επεξεργασία, στη συνέχεια, η οποία βασίζεται σε αυτά τα δεδομένα, γίνεται αυτοματοποιημένα και λαμβάνεται μια απόφαση που παράγει έννομες συνέπειες για ένα φυσικό πρόσωπο, π.χ. έγκριση ή απόρριψη δανείου, ακύρωση σύμβασης, απόκτηση δικαιώματος ή αποκλεισμός από συγκεκριμένη κοινωνική παροχή, άρνηση παροχής ιθαγένειας¹⁵⁵.

Η αιτιολογική σκέψη 71 αναφέρει ορισμένα παραδείγματα αποφάσεων που έχουν σημαντικά αποτελέσματα για το υποκείμενο, όπως η αυτόματη απόρριψη μιας διαδικτυακής πιστωτικής αίτησης ή πρακτικές ηλεκτρονικής πρόσληψης. Υποστηρίχθηκε ότι τέτοια αποτελέσματα δεν μπορούν να είναι απλώς συναισθηματικά

¹⁵² Mendoza, I., & Bygrave, L. A. (2017). The right not to be subject to automated decisions based on profiling. In *EU Internet Law*, σελ. 77-98. Springer, Cham. Διαθέσιμο στο <https://www.duo.uio.no/bitstream/handle/10852/52308/225.pdf?sequence=1>. Ανάκτηση: Ιούνιος 2021.

¹⁵³ Βλ. αιτιολογική σκέψη 71 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

¹⁵⁴ Ομάδα εργασίας του άρθρου 29. (2018), σελ. 9 επ.

¹⁵⁵ Ομάδα εργασίας του άρθρου 29. (2018), σελ. 25.

και ότι συνήθως δεν προκαλούνται μέσω στοχευμένης διαφήμισης, εκτός εάν «η διαφήμιση συνεπάγεται κατάφωρα αθέμιτη διάκριση με τη μορφή διαδικτυακής επένδυσης και η διάκριση έχει ασήμαντες οικονομικές συνέπειες (π.χ. το υποκείμενο των δεδομένων πρέπει να πληρώσει μια πολύ υψηλότερη τιμή για αγαθά ή υπηρεσίες από άλλα άτομα)»¹⁵⁶.

Πολλές αποφάσεις που λαμβάνονται σήμερα από συστήματα τεχνητής νοημοσύνης εμπίπτουν στο πεδίο εφαρμογής του άρθρου 22, καθώς οι αλγόριθμοι τεχνητής νοημοσύνης αναπτύσσονται όλο και περισσότερο στις προσλήψεις εργαζομένων, στη χορήγηση δανείων από πιστωτικά ιδρύματα, στις υπηρεσίες υγείας και κοινωνικής ασφάλισης και την εκπαίδευση. Με τη χρήση ΤΝ καθίσταται σχεδόν δεδομένο ότι μια απόφαση θα βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία. Αυτό οφείλεται στο γεγονός ότι οι άνθρωποι μπορεί να μην έχουν πρόσβαση σε όλες τις πληροφορίες που χρησιμοποιούνται από συστήματα ΤΝ και ενδέχεται να μην έχουν τη δυνατότητα να αναλύουν και να αναθεωρούν τον τρόπο με τον οποίο χρησιμοποιούνται αυτές οι πληροφορίες. Μπορεί να είναι αδύνατο, ή μπορεί να χρειαστεί υπερβολική προσπάθεια για την πραγματοποίηση μιας αποτελεσματικής επανεξέτασης -εκτός εάν το σύστημα έχει σχεδιαστεί αποτελεσματικά με διαφάνεια. Έτσι, ειδικά όταν αναπτύσσεται ένα αδιαφανές σύστημα μεγάλης κλίμακας, οι άνθρωποι είναι πιθανό να εκτελούν απλώς τις αυτοματοποιημένες προτάσεις της τεχνητής νοημοσύνης.

9.2 Εξαιρέσεις από την απαγόρευση του άρθρου 22§1

Εξαίρεση από την απαγόρευση αυτοματοποιημένης λήψης αποφάσεων προβλέπεται, σύμφωνα με την παρ. 2 του ίδιου άρθρου, όταν η σχετική απόφαση:

- είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων,
- επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους-μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας και το οποίο προβλέπει επίσης κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων ή

¹⁵⁶ Mendoza, I., & Bygrave, L. A. (2017), όπως παραπάνω.

- βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων¹⁵⁷.

Με βάση την ευρεία εξαίρεση του στοιχείου α', η αυτοματοποιημένη λήψη αποφάσεων επιτρέπεται σε βασικούς τομείς όπως η πρόσληψη εργαζομένων και η χορήγηση δανείων. Ωστόσο, για να ισχύει η εξαίρεση, οι αποφάσεις που βασίζονται αποκλειστικά στην αυτοματοποιημένη επεξεργασία πρέπει να είναι «αναγκαίες». Αυτή η αναγκαιότητα μπορεί να εξαρτάται από τον υψηλό αριθμό περιπτώσεων που πρέπει να εξεταστούν (π.χ. πολύ υψηλός αριθμός αιτήσεων για εργασία). Η αναγκαιότητα της χρήσης ΤΝ στην λήψη αποφάσεων μπορεί επίσης να συνδέεται με τις ικανότητες της τεχνητής νοημοσύνης να ξεπεράσει την ανθρώπινη κρίση.

Σε αυτό το πλαίσιο, αξίζει να αναρωτηθούμε εάν η ανθρώπινη συμμετοχή θα εξακολουθήσει να συμβάλλει στην ισχυρότερη προστασία των υποκειμένων των δεδομένων ή εάν η καλύτερη απόδοση των μηχανών -ακόμη και σε σχέση με τις πολιτικές και νομικές αξίες που διακυβεύονται, π.χ. εξασφάλιση «ισότητας ευκαιριών» για όλους τους αιτούντες μια θέση -θα καταστήσουν την ανθρώπινη παρέμβαση περιττή ή δυσλειτουργική. Εκτός του πεδίου της σύμβασης και της νομικής εξουσιοδότησης, η συγκατάθεση μπορεί να παρέχει τη βάση για αυτοματοποιημένη λήψη αποφάσεων σύμφωνα με το άρθρο 22 παράγραφος 2 στοιχείο γ'. Ωστόσο, δεν πληρούνται πάντα οι προϋποθέσεις για έγκυρη συγκατάθεση, ακόμη και σε περιπτώσεις κατά τις οποίες η αυτοματοποιημένη λήψη αποφάσεων φαίνεται κατάλληλη. Για παράδειγμα, στην περίπτωση που μια ΜΚΟ χρησιμοποιεί μια αυτοματοποιημένη μέθοδο για την κατάρτιση προφίλ και την ταξινόμηση των αιτούντων άσυλο σε ένα κράτος, προκειμένου να προσδιορίσει την ανάγκη τους και, κατά συνέπεια, να καταλείψει ορισμένα οφέλη σε αυτούς, είναι πολύ αμφίβολο ότι η συγκατάθεση του αιτούντος μπορεί να θεωρηθεί ελεύθερη, καθώς η μη συγκατάθεσή του θα συνεπαγόταν τον αποκλεισμό από τη διαδικασία χορήγησης ασύλου.

9.3 Μέτρα προστασίας για τις περιπτώσεις α' και γ' του άρθρου 22§2

Στις περιπτώσεις του άρθρου 22 παράγραφος 2 στοιχεία α' και γ' -δηλαδή όταν η αυτοματοποιημένη λήψη απόφασης είναι απαραίτητη για σύναψη σύμβασης ή υπάρχει ρητή συγκατάθεση- το άρθρο 22 παράγραφος 3 απαιτεί να ληφθούν ορισμένα κατάλληλα μέτρα προστασίας. Πιο συγκεκριμένα, ο υπεύθυνος επεξεργασίας δεδομένων εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων,

¹⁵⁷ Βλ. άρθρο 22 παρ. 2 του Γενικού Κανονισμού για την Προστασία των Δεδομένων 2016/679/ΕΕ.

τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης εκ μέρους του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης¹⁵⁸.

Σύμφωνα με την Ομάδα εργασίας του άρθρου 29, ορισμένα από αυτά τα μέτρα αφορούν τη μείωση του κινδύνου, όπως για παράδειγμα έλεγχοι διασφάλισης ποιότητας, αλγοριθμικός έλεγχος, ελαχιστοποίηση δεδομένων, ανωνυμοποίηση ή ψευδωνυμοποίηση, καθώς και μηχανισμοί πιστοποίησης¹⁵⁹. Ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα κατάλληλα για να διασφαλίσει, συγκεκριμένα, ότι οι παράγοντες που οδηγούν σε ανακρίβειες στα προσωπικά δεδομένα διορθώνονται και ο κίνδυνος σφαλμάτων ελαχιστοποιείται, να διασφαλίζει τα προσωπικά δεδομένα με τρόπο που λαμβάνει υπόψη τους πιθανούς κινδύνους που ενέχονται για τα δικαιώματα του υποκειμένου των δεδομένων και να αποτρέπει, μεταξύ άλλων, τις διακρίσεις στα φυσικά πρόσωπα με βάση τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, τη σεξουαλική ζωή ή το γενετήσιο προσανατολισμό.

Ως εκ τούτου, τα δεδομένα εισαγωγής πρέπει να αποδεικνύεται ότι δεν είναι ανακριβή ή άσχετα και ότι δεν παραβιάζουν τις εύλογες προσδοκίες των υποκειμένων των δεδομένων σε σχέση με τον σκοπό για τον οποίο τα δεδομένα συλλέχθηκαν¹⁶⁰. Όσον αφορά τη μηχανική μάθηση, αυτό θα πρέπει να ισχύει όχι μόνο για τα δεδομένα που αφορούν το άτομο που εμπλέκεται σε μια συγκεκριμένη απόφαση, αλλά και για τα δεδομένα σε ένα εκπαιδευτικό σύνολο, όπου οι προκαταλήψεις που ενσωματώνονται στο εκπαιδευτικό σύνολο μπορεί να επηρεάσουν το αλγοριθμικό μοντέλο που έχει μάθει, και ως εκ τούτου την ακρίβεια των συμπερασμάτων του συστήματος.

9.4 Αυτοματοποιημένη λήψη αποφάσεων και ευαίσθητα δεδομένα

Το άρθρο 22 παράγραφος 4 εισάγει απαγόρευση, που περιορίζεται κατ' εξαίρεση, στην αυτοματοποιημένη λήψη αποφάσεων για ευαίσθητα δεδομένα, δηλαδή τις ειδικές κατηγορίες που ορίζονται στο άρθρο 9 παράγραφος 1. Ειδικότερα, οι αποφάσεις που αναφέρονται στην παράγραφο 2 του άρθρου 22 ΓΚΠΔ δε βασίζονται σε ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο

¹⁵⁸ Βλ. άρθρο 22 παρ. 3 του Γενικού Κανονισμού για την Προστασία των Δεδομένων 2016/679/ΕΕ.

¹⁵⁹ Ομάδα εργασίας του άρθρου 29. (2018), σελ. 40.

¹⁶⁰ Ομάδα εργασίας του άρθρου 29. (2018), σελ. 21 επ.

9 παράγραφος 1, εκτός εάν εφαρμόζεται το άρθρο 9 παράγραφος 2 στοιχείο α' ή ζ' και αν υφίστανται κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων.

Η εξαίρεση αφορά τις περιπτώσεις στις οποίες το υποκείμενο των δεδομένων έχει δώσει ρητή συγκατάθεση (άρθρο 9 παράγραφος 2 στοιχείο α') ή η επεξεργασία είναι απαραίτητη για λόγους δημοσίου συμφέροντος (άρθρο 9 παράγραφος 2 στοιχείο ζ'). Ο ρόλος της συγκατάθεσης του υποκειμένου των δεδομένων πρέπει να αποσαφηνιστεί δεδομένου ότι η συγκατάθεση δεν αποκλείει ότι η μέθοδος που χρησιμοποιείται για την απόφαση είναι απαράδεκτη (όπως όταν είναι διακριτική).

Όπως σημειώνεται παραπάνω, η απαγόρευση επεξεργασίας ευαίσθητων δεδομένων μπορεί να καταστεί αμφίβολη στην περίπτωση της ΤΝ. Πρώτα απ' όλα, τα ευαίσθητα δεδομένα μπορούν να συναχθούν και από μη ευαίσθητα δεδομένα. Για παράδειγμα, ο σεξουαλικός προσανατολισμός μπορεί να συναχθεί από τη δραστηριότητα στο διαδίκτυο ενός υποκειμένου δεδομένων, τις προτιμήσεις ή ακόμη και τα χαρακτηριστικά του προσώπου. Σε αυτήν την περίπτωση, η συναγωγή ευαίσθητων δεδομένων θα πρέπει να υπολογίζεται ως επεξεργασία ευαίσθητων δεδομένων και, ως εκ τούτου, θα πρέπει να θεωρηθεί παράνομη, εκτός εάν πληρούνται οι προϋποθέσεις του άρθρου 9.

Δεύτερον, όπως αναλύθηκε και παραπάνω, τα μη ευαίσθητα δεδομένα μπορούν να λειτουργήσουν ως διακομιστές μεσολάβησης για ευαίσθητα δεδομένα που σχετίζονται με αυτά, παρόλο που τα τελευταία δεν συνάγονται από το σύστημα. Για παράδειγμα, ο τόπος κατοικίας μπορεί να αποτελέσει αντικείμενο συσχέτισης με την εθνικότητα του υποκειμένου. Σε αυτήν την περίπτωση, μπορεί να λάβει χώρα παράνομη διάκριση.

10. Εργαλεία συμμόρφωσης με τον ΓΚΠΔ

Σε αυτή την ενότητα πρόκειται να αναλύσουμε τα εργαλεία συμμόρφωσης που προσφέρει ο ΓΚΠΔ, καθώς και να εξετάσουμε το ενδεχόμενο αξιοποίησης του καθενός, όταν γίνεται χρήση των τεχνολογιών της τεχνητής νοημοσύνης.

10.1 Προσέγγιση με βάση τον κίνδυνο

Η υιοθέτηση της προσέγγισης με βάση τον κίνδυνο ή αλλιώς κινδυνοκεντρική προσέγγιση (risk based approach) συνίσταται στην οριοθέτηση των περιπτώσεων ανάλογα με το βαθμό διακινδύνευσης των δικαιωμάτων του υποκειμένου των

δεδομένων και η αντίστοιχη διαβαθμισμένη επιβολή υποχρεώσεων¹⁶¹ και αποτελεί άλλον ένα νεωτερισμό του Κανονισμού 2016/679.

Σύμφωνα με την αιτιολογική σκέψη 75 του Κανονισμού, κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων μπορεί να προκύψουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με διαφορετικό βαθμό πιθανότητας και σοβαρότητας και μπορούν να οδηγήσουν σε σωματική, υλική ή μη υλική βλάβη. Οι κίνδυνοι που μπορεί να προκύψουν είναι διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδωνυμοποίησης, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα¹⁶².

Ακολουθώς, απαιτείται να γίνουν οι εξής ενέργειες: α) εντοπισμός του κινδύνου, β) αξιολόγηση της πιθανότητας εμφάνισης του κινδύνου και της βαρύτητας των ζημιών και γ) κατηγοριοποίηση του κινδύνου¹⁶³. Σύμφωνα με την αιτιολογική σκέψη 76, η πιθανότητα και η σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων θα πρέπει να καθορίζονται σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

Όσον αφορά την τεχνητή νοημοσύνη, έχει ιδιαίτερο νόημα και βαρύτητα η προσέγγιση με βάση τον κίνδυνο, όπως αυτή αναπτύχθηκε αμέσως παραπάνω. Ήδη στις ΗΠΑ σημειώνονται προσπάθειες για προσέγγιση βασισμένη στον κίνδυνο για την προστασία δεδομένων στο δημόσιο τομέα¹⁶⁴. Έχει σημειωθεί μεγάλη πρόοδος σχετικά με τα δεδομένα, η οποία απαιτεί από τους οργανισμούς να εκπαιδεύουν τους υπαλλήλους σχετικά με προκαταλήψεις και παραπλανητικά στοιχεία του αυτοματισμού και να διορίζουν υπαλλήλους που να είναι επιφορτισμένοι με την αναθεώρηση αυτοματοποιημένων αποφάσεων, να ελέγχουν τακτικά συστήματα υπολογιστών.

¹⁶¹ Μήτρου, Λ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (νέο δίκαιο-νέες υποχρεώσεις-νέα δικαιώματα). *Νέο Δίκαιο-Νέες Υποχρεώσεις-Νέα Δικαιώματα*, 1η έκδοση, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη, σελ. 95 επ.

¹⁶² Βλ. αιτιολογική σκέψη 75 του Γενικού Κανονισμού για την Προστασία των Δεδομένων 2016/679/ΕΕ.

¹⁶³ Ιγγλεζάκης, Ι. (2020). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019)* (No. IKEEBOOK-2020-731). Interactive Books, σελ. 194 επ.

¹⁶⁴ *European Parliament – EPRS*. (2020), σελ. 66 επ.

Για παράδειγμα, υποστηρίχθηκε ότι η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ πρέπει να διαδραματίσει βασικό ρόλο στη διασφάλιση της νομιμότητας και της ακρίβειας των συστημάτων αξιολόγησης πιστοληπτικής ικανότητας, δεδομένου του τεράστιου αντίκτυπου που μπορεί να έχει ένα αρνητικό πιστωτικό αποτέλεσμα στη ζωή των ανθρώπων. Άλλες προτεινόμενες λύσεις περιλαμβάνουν τον έλεγχο, τον εντοπισμό των καταναλωτών και τη δυνατότητα στους καταναλωτές όχι μόνο να έχουν πρόσβαση στα δεδομένα τους, αλλά και να ελέγχουν το σύστημα¹⁶⁵.

Ένα σοβαρό ζήτημα σχετικά με τα μέτρα πρόληψης και μετριασμού των κινδύνων αφορά το κατά πόσον τα ίδια μέτρα πρέπει να απαιτούνται από όλους τους υπεύθυνους επεξεργασίας που συμμετέχουν σε παρόμοιες διεργασίες ή εάν απαιτείται διαφοροποιημένη προσέγγιση, που λαμβάνει υπόψη το μέγεθος των υπεύθυνων επεξεργασίας και την οικονομική και τεχνική τους ικανότητα να υιοθετούν τις πιο αποτελεσματικές προφυλάξεις. Πιο συγκεκριμένα, θα πρέπει να εφαρμόζονται τα ίδια πρότυπα τόσο στις μεγάλες-πολυεθνικές εταιρίες του Διαδικτύου, που διαθέτουν τεράστια περιουσιακά στοιχεία και ισχυρές τεχνολογίες και κέρδος μονοπωλιακών ενοικίων, όσο και σε μικρές νεοσύστατες επιχειρήσεις, οι οποίες προσπαθούν να αναπτύξουν καινοτόμες λύσεις με ελάχιστους πόρους. Ενδεχομένως να βρεθεί λύση σε αυτό το ζήτημα λαμβάνοντας υπόψη ότι τα μέτρα πρόληψης και μετριασμού των κινδύνων είναι το αντικείμενο των υποχρεώσεων βέλτιστης προσπάθειας, με αυστηρότητα που μπορεί να επεκταθεί ανάλογα. Επομένως, ενδέχεται να απαιτηθούν αυστηρότερα μέτρα πρόληψης κινδύνου στο βαθμό που ο υπεύθυνος επεξεργασίας προκαλεί αμφοτέρους έναν σοβαρότερο κοινωνικό κίνδυνο, με την επεξεργασία μεγαλύτερης ποσότητας προσωπικών δεδομένων σε μεγαλύτερο σύνολο ατόμων και έχει την ικανότητα να ανταποκρίνεται στον κίνδυνο με αποτελεσματικό και οικονομικά βιώσιμο τρόπο.

10.2 Ευθύνη του υπευθύνου επεξεργασίας

Το άρθρο 24 ΓΚΠΔ προβλέπει την υποχρέωση του υπευθύνου επεξεργασίας, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, να

¹⁶⁵ Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Wash. L. Rev.*, 89, 1. Διαθέσιμο στο https://digitalcommons.law.umaryland.edu/fac_pubs/1431/. Ανάκτηση: Ιούνιος 2021.

εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον κανονισμό.

Ενδεικτικά, αναφέρονται ορισμένα μέτρα (τεχνικά και οργανωτικά), τα οποία οφείλει να λάβει ο υπεύθυνος επεξεργασίας¹⁶⁶:

- Χαρτογράφηση δεδομένων (data mapping)
- Ταξινόμηση των προσωπικών δεδομένων σε κατηγορίες
- Εργαλεία που βοηθούν στην άρση ελαττωμάτων που έχουν διαπιστωθεί
- Μέτρα για τη διασφάλιση της διαφάνειας της επεξεργασίας έναντι των υποκειμένων των δεδομένων
- Ορισμός υπεύθυνου για την εφαρμογή του Κανονισμού ή ομάδας συμμόρφωσης
- Θέσπιση εσωτερικών πολιτικών για εξουσιοδοτημένη πρόσβαση σε δεδομένα

Τέτοια μέτρα πρέπει να επανεξετάζονται και να επικαιροποιούνται, όταν κάτι τέτοιο κρίνεται απαραίτητο. Όσον αφορά τις εφαρμογές τεχνητής νοημοσύνης, τα μέτρα περιλαμβάνουν ελέγχους για την επάρκεια και την πληρότητα των εκπαιδευτικών συνόλων, για το εύλογο των συμπερασμάτων, καθώς και για την ύπαρξη αιτιών προκατάληψης και αδικίας¹⁶⁷.

10.3 Προστασία δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει εγκαίρως μέτρα για την αποτροπή παραβίασης της προστασίας δεδομένων, ρυθμίζοντας κατάλληλα τις τεχνολογικές εφαρμογές που αναπτύσσει και/ή χρησιμοποιεί¹⁶⁸. Το άρθρο 25 παράγραφος 1 ορίζει ότι τόσο κατά τη στιγμή του καθορισμού των μέσω επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά τα κατάλληλα τεχνικά και οργανωτικά μέτρα που έχουν σχεδιαστεί για την αποτελεσματική εφαρμογή των αρχών προστασίας δεδομένων, όπως η ψευδωνυμοποίηση ή η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων κατά την επεξεργασία.

Το άρθρο 25 παράγραφος 2 αφορά την ελαχιστοποίηση δεδομένων και είναι σχετικό με τεχνολογίες τεχνητής νοημοσύνης και μεγάλων δεδομένων, καθώς απαιτεί

¹⁶⁶ Ιγγλεζάκης, Ι. (2020), σελ. 199-200.

¹⁶⁷ *European Parliament – EPRS*. (2020), σελ. 67.

¹⁶⁸ Ιγγλεζάκης, Ι. (2020), σελ. 201 επ.

την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για να διασφαλιστεί ότι, από το σχεδιασμό, υφίσταται επεξεργασία μόνο των προσωπικών δεδομένων που είναι απαραίτητα για το συγκεκριμένο σκοπό της επεξεργασίας. Τα μέτρα αυτά πρέπει να αφορούν το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, το βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Τέλος, αμφισβητείται η δυνατότητα διατήρησης των δεδομένων λαμβάνοντας υπόψη τους μελλοντικούς ακόμη μη καθορισμένους σκοπούς, εκτός εάν ορίζεται το πεδίο εφαρμογής των μελλοντικών χρήσεων (π.χ. επιστημονική έρευνα).

10.4 Μελέτη εκτίμησης αντικτύπου στην προστασία δεδομένων

Η ανάλυση μεγάλων δεδομένων μπορεί να περιλαμβάνει καινοτόμες, περίπλοκες και μερικές φορές μη αναμενόμενες χρήσεις προσωπικών δεδομένων. Ο ΓΚΠΔ ορίζει ότι η εκπόνηση μελέτης εκτίμησης του αντικτύπου του κινδύνου θα πρέπει να λαμβάνει χώρα σε συγκεκριμένες περιπτώσεις, κατά τις οποίες είναι πιθανό να προκύψει υψηλός κίνδυνος για τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων, ιδιαίτερα σε περιπτώσεις κατά τις οποίες η επεξεργασία περιλαμβάνει νέες τεχνολογίες. Είναι πολύ πιθανό, η πλειοψηφία των εφαρμογών μεγάλων δεδομένων που περιλαμβάνουν την επεξεργασία προσωπικών δεδομένων να εμπίπτει στη συγκεκριμένη κατηγορία. Ο ΓΚΠΔ αναφέρεται σε συστηματική κι εκτεταμένη αξιολόγηση των υποκειμένων, βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, όπου οι αποφάσεις που λαμβάνονται βάσει αυτής της επεξεργασίας επηρεάζουν σημαντικά τα υποκείμενα των δεδομένων.

Όταν η αξιολόγηση καθορίζει ότι η επεξεργασία συνεπάγεται «υψηλό κίνδυνο», σύμφωνα με το άρθρο 36 παράγραφος 1, ο υπεύθυνος επεξεργασίας θα πρέπει προληπτικά να ζητήσει τη συμβουλή της εποπτικής αρχής (της εθνικής Αρχής προστασίας δεδομένων)¹⁶⁹. Ο υπεύθυνος επεξεργασίας συμβουλευέται την εποπτική αρχή πριν από την επεξεργασία, όταν μια εκτίμηση αντικτύπου στην προστασία δεδομένων υποδεικνύει ότι η επεξεργασία θα οδηγούσε σε υψηλό κίνδυνο, εάν δεν ληφθούν μέτρα από τον υπεύθυνο επεξεργασίας για τον μετριασμό του κινδύνου.

Η εκτίμηση αντικτύπου πρέπει να κοινοποιείται στην εποπτική αρχή. Η αρχή πρέπει να παρέχει γραπτές συμβουλές στον υπεύθυνο επεξεργασίας όπου η εποπτική αρχή είναι της γνώμης ότι η προβλεπόμενη επεξεργασία που αναφέρεται στην

¹⁶⁹ Διαθέσιμη στο <https://www.dpa.gr>. Ανάκτηση: Απρίλιος 2021.

παράγραφο 1 θα παραβίαζε τον παρόντα κανονισμό, ιδίως όταν ο υπεύθυνος επεξεργασίας έχει εντοπίσει ή μετριάσει ανεπαρκώς τον κίνδυνο.

10.5 Υπεύθυνοι προστασίας δεδομένων (ΥΠΔ)

Μία από τις σημαντικές καινοτομίες του Κανονισμού είναι και η εισαγωγή του θεσμού του υπεύθυνου προστασίας δεδομένων (ΥΠΔ), καθώς υποχρεώνει τους υπεύθυνους επεξεργασίας και τους εκτελούντες επεξεργασία να οργανώνουν ένα εσωτερικό σύστημα ελέγχου και συμμόρφωσης με τις διατάξεις. Κατ' αυτόν τον τρόπο έχουν δημιουργηθεί οι προϋποθέσεις για την εφαρμογή στην πράξη της αρχής της λογοδοσίας, αφού ο ΥΠΔ είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ.

Ειδικότερα, το άρθρο 37 ΓΚΠΔ υποχρεώνει τον υπεύθυνο και τον εκτελούντα την επεξεργασία να ορίσουν ΥΠΔ στις εξής περιπτώσεις:

- Όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα,
- Όταν οι βασικές δραστηριότητες συνιστούν πράξεις επεξεργασίας, οι οποίες λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή
- Όταν οι βασικές δραστηριότητες συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10¹⁷⁰.

Αυτή η διάταξη σχετίζεται με την τεχνητή νοημοσύνη, καθώς διάφορες εφαρμογές βασίζονται σε σύνολα δεδομένων που συλλέγονται από την παρακολούθηση της συμπεριφοράς του υποκειμένου των δεδομένων (π.χ. τη διαδικτυακή συμπεριφορά τους ή την οδηγική συμπεριφορά τους). Μια εξειδικευμένη και αμερόληπτη εσωτερική αναθεώρηση θα μπορούσε αναμφισβήτητα να είναι χρήσιμη σε τέτοιες περιπτώσεις¹⁷¹.

10.6 Κώδικες δεοντολογίας και πιστοποίηση

Τα άρθρα 40-43 του Κανονισμού ρυθμίζουν τους κώδικες δεοντολογίας και την πιστοποίηση. Παρόλο που αυτές οι διατάξεις δεν κάνουν ρητή αναφορά στην τεχνητή νοημοσύνη, οι κώδικες δεοντολογίας και η χορήγηση πιστοποίησης ενδέχεται να είναι

¹⁷⁰ Βλ. άρθρο 37 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

¹⁷¹ *European Parliament – EPRS*. (2020), σελ. 68.

ιδιαίτερα συναφείς με την τεχνητή νοημοσύνη, λαμβανομένων υπόψη των κινδύνων που ενέχει η εφαρμογή τεχνητής νοημοσύνης, όπως αυτοί αναπτύχθηκαν λεπτομερώς, και της περιορισμένης καθοδήγησης που παρέχουν οι νομικές διατάξεις.

Η τήρηση των κωδίκων δεοντολογίας και των μηχανισμών πιστοποίησης, σύμφωνα με τα άρθρα 24 και 25 μπορεί να συμβάλει στην απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας και με τις απαιτήσεις της ιδιωτικότητας ήδη από το σχεδιασμό. Η ιδέα της πιστοποίησης για εφαρμογές τεχνητής νοημοσύνης έχει υποστηριχθεί από την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή (ΕΟΚΕ)¹⁷², η οποία ζητά την ανάπτυξη ενός ισχυρού συστήματος πιστοποίησης βάσει διαδικασιών, που θα επιτρέπουν στις εταιρείες να δηλώνουν ότι τα συστήματα ΤΝ που χρησιμοποιούν είναι αξιόπιστα και ασφαλή. Έτσι, προτείνει την ανάπτυξη ενός ευρωπαϊκού αξιόπιστου πιστοποιητικού επιχειρηματικής τεχνητής νοημοσύνης, που βασίζεται εν μέρει στον κατάλογο αξιολόγησης που προτάθηκε από την ομάδα εμπειρογνομόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη. Από την άλλη πλευρά, δημιουργούνται ορισμένες δυσχέρειες σε ένα γενικό πλαίσιο πιστοποίησης, με βάση την πολυπλοκότητα των τεχνολογιών ΤΝ, την ποικιλομορφία τους, καθώς και την ταχεία εξέλιξή τους¹⁷³.

10.7 Ο ρόλος των Αρχών προστασίας δεδομένων

Όπως φαίνεται στις προηγούμενες ενότητες, υπάρχουν διάφορες αναφορές στον Κανονισμό που υποστηρίζουν μια προληπτική προσέγγιση βάσει του κινδύνου για την τεχνητή νοημοσύνη και τα μεγάλα δεδομένα. Θα εξαρτηθεί από τη δημιουργικότητα των τεχνολογικών και νομικών εμπειρογνομόνων, ιδίως εκείνων που έχουν το ρόλο των υπευθύνων προστασίας δεδομένων, να παρέχουν επαρκείς λύσεις. Σημαντικό ρόλο μπορούν επίσης να διαδραματίσουν οι αρχές προστασίας δεδομένων, κατά την επιβολή του νόμου περί προστασίας δεδομένων, αλλά και κατά την προώθηση κατάλληλων προτύπων. Ο Κανονισμός κάνει ρητή αναφορά τόσο στις εθνικές αρχές

¹⁷² Βλ. σχετικά Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή. (2019). *Η ΕΟΚΕ προτείνει τη θέσπιση ενωσιακού συστήματος πιστοποίησης για αξιόπιστα προϊόντα τεχνητής νοημοσύνης*. <https://www.eesc.europa.eu/el/news-media/eesc-info/112019/articles/74868>. Ανάκτηση: Απρίλιος 2021.

¹⁷³ Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., ... & Schwartz, O. (2018). *AI now report 2018* (σελ. 1-62). New York: AI Now Institute at New York University. Διαθέσιμο στο https://ainowinstitute.org/AI_Now_2018_Report.pdf. Ανάκτηση: Ιούνιος 2021.

προστασίας δεδομένων όσο και στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, στο οποίο αποδίδει σημαντικό ρόλο.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων είναι η συνέχεια της ομάδας εργασίας του άρθρου 29, που ιδρύθηκε με την Οδηγία για την προστασία δεδομένων του 1995¹⁷⁴. Περιλαμβάνει εκπροσώπους των αρχών προστασίας δεδομένων των κρατών μελών και των ευρωπαϊκών εποπτικών αρχών προστασίας δεδομένων, προκειμένου να διασφαλιστεί η συνεπής εφαρμογή του Κανονισμού. Σύμφωνα με την αιτιολογική σκέψη 77, καθοδήγηση για την εφαρμογή των κατάλληλων μέτρων και για την απόδειξη της συμμόρφωσης από τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, ιδίως όσον αφορά τον προσδιορισμό των κινδύνων που συνδέονται με την επεξεργασία, την εκτίμησή τους από άποψη προέλευσης, φύσης, πιθανότητας και σοβαρότητας και τον εντοπισμό των βέλτιστων πρακτικών για τον περιορισμό των κινδύνων, θα μπορούσε να παρέχεται ιδίως με εγκεκριμένους κώδικες συμπεριφοράς, εγκεκριμένες πιστοποιήσεις, κατευθυντήριες γραμμές που παρέχονται από το Συμβούλιο Προστασίας Δεδομένων ή με τις υποδείξεις που παρέχει ο υπεύθυνος προστασίας δεδομένων. Το Συμβούλιο Προστασίας Δεδομένων μπορεί επίσης να εκδίδει κατευθυντήριες γραμμές σχετικά με τις πράξεις επεξεργασίας που θεωρείται ότι είναι απίθανο να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, στις οποίες θα αναφέρεται ποια μέτρα μπορεί να αρκούν στην περίπτωση αυτή για την αντιμετώπιση του σχετικού κινδύνου.

Μια ρητή αναφορά στην αυτοματοποιημένη λήψη αποφάσεων περιλαμβάνεται στο άρθρο 70 παράγραφος 1 του Κανονισμού, το οποίο απαριθμεί τα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας των Δεδομένων. Όσον αφορά την αυτοματοποιημένη λήψη αποφάσεων, το Συμβούλιο θα πρέπει με δική του πρωτοβουλία ή, κατά περίπτωση, κατόπιν αιτήματος της Επιτροπής, να εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για τον περαιτέρω προσδιορισμό των κριτηρίων και των προϋποθέσεων για τη λήψη αποφάσεων που βασίζονται σε κατάρτιση προφίλ δυνάμει του άρθρου 22 παράγραφος 2¹⁷⁵.

¹⁷⁴ Οδηγία 95/46/EK.

¹⁷⁵ Βλ. άρθρο 70 παρ. 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων 2016/679/ΕΕ.

11. Επίλογος – Συμπεράσματα

Είναι απολύτως λογικό να αμφισβητείται η συμβατότητα του ΓΚΠΔ με την τεχνητή νοημοσύνη και τα μεγάλα δεδομένα, καθώς αυτός βασίζεται σε αρχές, όπως ο περιορισμός του σκοπού, η ελαχιστοποίηση των δεδομένων, η ειδική μεταχείριση των ευαίσθητων δεδομένων ή ο περιορισμός αυτοματοποιημένων αποφάσεων, που, με μία πρώτη ματιά, δε συμβαδίζουν με την εκτεταμένη χρήση της τεχνητής νοημοσύνης. Είναι αλήθεια ότι η πλήρης ανάπτυξη της ισχύος της τεχνητής νοημοσύνης και των μεγάλων δεδομένων απαιτεί τη συλλογή τεράστιων ποσοτήτων δεδομένων, σχετικά με τα υποκείμενα και τις κοινωνικές τους σχέσεις, και την επεξεργασία δεδομένων για σκοπούς, που δεν είχαν καθοριστεί πλήρως τη στιγμή συλλογής τους. Ωστόσο, υπάρχουν τρόποι εφαρμογής των αρχών προστασίας δεδομένων, ώστε να είναι συνεπείς με τις ωφέλιμες χρήσεις της τεχνητής νοημοσύνης και των μεγάλων δεδομένων.

Ο Κανονισμός επιτρέπει την εξαγωγή συμπερασμάτων, που βασίζονται σε προσωπικά δεδομένα, συμπεριλαμβανομένης και της κατάρτισης προφίλ, αλλά μόνο υπό ορισμένες προϋποθέσεις και εφόσον θεσπιστούν οι κατάλληλες διασφαλίσεις. Σύμφωνα με το άρθρο 22 του ΓΚΠΔ, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να μην υπόκεινται σε απόφαση, η οποία βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένου και του προφίλ, όταν αυτή παράγει έννομα αποτελέσματα που τα αφορούν ή τα επηρεάζει σημαντικά. Όταν οι υπεύθυνοι επεξεργασίας δεδομένων χρησιμοποιούν μηχανική εκμάθηση για να πραγματοποιούν αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ των υποκειμένων των δεδομένων, πρέπει, μεταξύ άλλων, να συμμορφώνονται με την αρχή προστασίας δεδομένων της νόμιμης, δίκαιης και διαφανούς επεξεργασίας. Αυτό μπορεί να είναι δύσκολο να επιτευχθεί λόγω του τρόπου με τον οποίο λειτουργεί η μηχανική εκμάθηση ή/και του τρόπου με τον οποίο η μηχανική μάθηση ενσωματώνεται σε μια ευρύτερη ροή εργασίας που μπορεί να περιλαμβάνει τη χρήση δεδομένων διαφορετικής προέλευσης και αξιοπιστίας, συγκεκριμένων παρεμβάσεων από ανθρώπινους χειριστές και της ανάπτυξης προϊόντων και υπηρεσιών ΤΝ.

Για τη συμμόρφωσή τους, οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να εκτιμήσουν πώς η χρήση της τεχνολογίας για την αυτοματοποιημένη επεξεργασία επηρεάζει τα διάφορα στάδια του προφίλ και το επίπεδο κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Σε ορισμένες περιπτώσεις όπου η αυτοματοποιημένη επεξεργασία ή η κατάρτιση προφίλ επιτρέπεται από το νόμο, οι

υπεύθυνοι επεξεργασίας δεδομένων πρέπει να εφαρμόσουν επιπλέον κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των νόμιμων συμφερόντων των υποκειμένων των δεδομένων. Τέτοια μέτρα θα περιλαμβάνουν την αποτροπή λήψης αποφάσεων από τις μηχανές προτού τα υποκείμενα των δεδομένων μπορούν να εκφράσουν την άποψή τους, επιτρέποντας ουσιαστική ανθρώπινη αναθεώρηση όταν λαμβάνεται μια απόφαση από μια μηχανή και διασφάλιση ότι τα υποκείμενα των δεδομένων μπορούν να αμφισβητήσουν την απόφαση. Οι διατάξεις του ΓΚΠΔ κυρίως στοχεύουν στο ότι μια απόφαση που επηρεάζει σημαντικά ένα άτομο δεν μπορεί απλώς να βασίζεται σε μια πλήρως αυτοματοποιημένη αξιολόγηση των προσωπικών του χαρακτηριστικών. Ωστόσο, στο πλαίσιο της τεχνητής νοημοσύνης, υποστηρίζεται ότι, σε ορισμένες περιπτώσεις, μπορεί να είναι πιο επωφελές για τα υποκείμενα των δεδομένων εάν η τελική απόφαση βασίζεται, πράγματι, σε μια αυτοματοποιημένη αξιολόγηση¹⁷⁶.

Ο Κανονισμός παρέχει γενικά σημαντικές ενδείξεις για την προστασία δεδομένων σε σχέση με εφαρμογές της τεχνητής νοημοσύνης. Επιπλέον, μπορεί να ερμηνευθεί και να εφαρμοστεί με τέτοιο τρόπο ώστε να μην παρεμποδίζει την ευεργετική εφαρμογή της ΤΝ στα προσωπικά δεδομένα και ότι δε θέτει τις εταιρείες της ΕΕ σε μειονεκτική θέση σε σύγκριση με τους μη ευρωπαίους ανταγωνιστές. Έτσι, ο ΓΚΠΔ δεν φαίνεται να απαιτεί καμία σημαντική αλλαγή για την αντιμετώπιση της ΤΝ.

Τούτου λεχθέντος, ορισμένα ζητήματα προστασίας δεδομένων που σχετίζονται με την τεχνητή νοημοσύνη δεν απαντώνται ρητά στον Κανονισμό, το οποίο μπορεί να οδηγήσει σε αβεβαιότητες και κόστος και μπορεί να εμποδίσει περαιτέρω την ανάπτυξη εφαρμογών ΤΝ.

¹⁷⁶ Εάν μια απόφαση για εμάς λαμβάνεται από έναν άνθρωπο ή από μια μηχανή, προς το παρόν το καλύτερο που μπορούμε να ελπίζουμε είναι ότι μια απόφαση που παράγει νομικά αποτελέσματα ή μας επηρεάζει σημαντικά θα είναι τόσο δίκαιη όσο μπορεί να είναι ο άνθρωπος. Μια ενδιαφέρουσα πιθανότητα, ωστόσο, είναι ότι οι μηχανές ενδέχεται σύντομα να είναι σε θέση να ξεπεράσουν ορισμένους βασικούς περιορισμούς των ανθρώπινων υπευθύνων λήψης αποφάσεων και να μας παρέχουν αποφάσεις που είναι αποδεδειγμένα δίκαιες. Πράγματι, μπορεί ήδη σε ορισμένα πλαίσια να έχει νόημα να αντικατασταθεί το τρέχον μοντέλο, σύμφωνα με το οποίο τα άτομα μπορούν να προσφύγουν σε έναν άνθρωπο κατά μιας απόφασης μηχανής, με το αντίστροφο μοντέλο σύμφωνα με το οποίο τα άτομα θα έχουν το δικαίωμα να προσφύγουν σε μια μηχανή κατά μιας απόφασης που λαμβάνεται από έναν άνθρωπο.

- Οι υπεύθυνοι επεξεργασίας και τα υποκείμενα των δεδομένων θα πρέπει να έχουν την κατάλληλη καθοδήγηση σχετικά με τον τρόπο με τον οποίο η ΤΝ μπορεί να εφαρμοστεί σε προσωπικά δεδομένα. Αυτό μπορεί να αποτρέψει το κόστος που συνδέεται με τη νομική αβεβαιότητα, ενισχύοντας παράλληλα τη συμμόρφωση.
- Η παροχή επαρκούς καθοδήγησης απαιτεί μια πολυεπίπεδη προσέγγιση, η οποία περιλαμβάνει την κοινωνία των πολιτών, τους αντιπροσωπευτικούς φορείς, τις εξειδικευμένες υπηρεσίες και όλα τα ενδιαφερόμενα μέρη. Απαιτείται μια ευρεία συζήτηση, με συμμετοχή όχι μόνο των πολιτικών και διοικητικών αρχών, αλλά και της κοινωνίας των πολιτών και των ακαδημαϊκών. Αυτή η συζήτηση πρέπει να αντιμετωπίσει τα ζητήματα του καθορισμού των προτύπων που πρέπει να εφαρμόζονται στην επεξεργασία προσωπικών δεδομένων με τεχνολογίες ΤΝ, ιδίως για να διασφαλιστεί η μη παραβίαση των δικαιωμάτων των ατόμων.
- Οι θεμελιώδεις αρχές προστασίας δεδομένων -ειδικά ο περιορισμός και η ελαχιστοποίηση του σκοπού- πρέπει να ερμηνεύονται με τέτοιο τρόπο ώστε να μην αποκλείουν τη χρήση προσωπικών δεδομένων για σκοπούς μηχανικής μάθησης. Δεν πρέπει να αποκλείουν τη δημιουργία σετ εκπαίδευσης και τη δημιουργία αλγοριθμικών μοντέλων, όπου τα προκύπτοντα συστήματα ΤΝ είναι κοινωνικά ωφέλιμα και συμμορφώνονται με τα δικαιώματα προστασίας δεδομένων.
- Η χρήση προσωπικών δεδομένων σε ένα εκπαιδευτικό σύνολο, με σκοπό την εκμάθηση γενικών συσχετισμών και σύνδεσης, θα πρέπει να διακρίνεται από τη χρήση τους για ατομικό προφίλ, δηλαδή για τη διενέργεια αξιολογήσεων των ατόμων.
- Η εξαγωγή νέων προσωπικών δεδομένων, όπως γίνεται στην κατάρτιση προφίλ, θα πρέπει να θεωρείται ως δημιουργία νέων προσωπικών δεδομένων, όταν παρέχονται στοιχεία για τη λήψη αξιολογήσεων και αποφάσεων. Το ίδιο θα πρέπει να ισχύει και για τον επαναπροσδιορισμό ανώνυμων ή ψευδώνυμων δεδομένων. Και οι δύο θα πρέπει να υπόκεινται στους περιορισμούς του Κανονισμού στη συλλογή νέων δεδομένων.
- Μπορεί να καταστεί χρήσιμο να θεσπιστούν υποχρεώσεις για την κοινοποίηση στις αρχές προστασίας δεδομένων για εφαρμογές που

περιλαμβάνουν εξατομικευμένο προφίλ και λήψη αποφάσεων, συνοδευόμενες ενδεχομένως από τη δυνατότητα υποβολής ενδείξεων σχετικά με τη συμμόρφωση με την προστασία δεδομένων.

- Το περιεχόμενο της υποχρέωσης των υπεύθυνων επεξεργασίας να παρέχουν πληροφορίες (και τα αντίστοιχα δικαιώματα των υποκειμένων των δεδομένων) σχετικά με τη «λογική» ενός συστήματος ΤΝ πρέπει να προσδιοριστεί, με κατάλληλα παραδείγματα, σε σχέση με διαφορετικές τεχνολογίες.
- Εξίσου σημαντικό είναι να διασφαλιστεί ότι το δικαίωμα εξαίρεσης από την κατάρτιση προφίλ και τη μεταφορά δεδομένων μπορεί εύκολα να ασκηθεί μέσω κατάλληλων διεπαφών του χρήστη, πιθανώς σε τυποποιημένες μορφές. Για αυτό το λόγο πρέπει να προσδιοριστούν οι κανονιστικές και τεχνολογικές απαιτήσεις σχετικά με την τεχνητή νοημοσύνη και από προεπιλογή.
- Η δυνατότητα επαναπροσδιορισμού δεδομένων για εφαρμογές ΤΝ που δεν περιλαμβάνουν προφίλ -επιστημονικές και στατιστικές έρευνες- μπορεί να είναι ευρεία, αρκεί να υπάρχουν κατάλληλες προφυλάξεις αποτρέποντας τις καταχρηστικές χρήσεις προσωπικών δεδομένων.
- Πρέπει να ληφθούν ισχυρά μέτρα εναντίον εταιρειών και δημόσιων αρχών που σκόπιμα κάνουν κατάχρηση της εμπιστοσύνης των υποκειμένων των δεδομένων με κατάχρηση των προσωπικών τους δεδομένων, για συμμετοχή σε εφαρμογές που χειρίζονται υποκείμενα δεδομένων κατά των συμφερόντων τους. Η συλλογική επιβολή στον τομέα προστασίας δεδομένων πρέπει να ενεργοποιηθεί και να διευκολυνθεί.

Τέλος, πολύ σημαντική είναι η πρωτοβουλία της Ευρωπαϊκής Επιτροπής για ένα σχέδιο Κανονισμού της τεχνητής νοημοσύνης, που έχει ως στόχο την εγγύηση των θεμελιωδών δικαιωμάτων των πολιτών και των επιχειρήσεων της ΕΕ, ενισχύοντας παράλληλα την αποδοχή της ΤΝ, τις επενδύσεις και την καινοτομία¹⁷⁷.

Όσον αφορά τη χρήση τεχνολογιών αναγνώρισης προσώπου, δεδομένης της καινοτομίας της τεχνολογίας καθώς και της έλλειψης εμπειρίας και λεπτομερών

¹⁷⁷ Βλ. περισσότερα <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.
Ανάκτηση: Ιούνιος 2021.

μελετών σχετικά με τον αντίκτυπο αυτών, πολλές πτυχές πρέπει να ληφθούν υπόψη πριν από την ανάπτυξη ενός τέτοιου συστήματος σε εφαρμογές πραγματικής ζωής.

Ακολουθώντας το παράδειγμα των ευρείας κλίμακας συστημάτων πληροφορικής της ΕΕ, ένα σαφές και επαρκώς λεπτομερές νομικό πλαίσιο πρέπει να ρυθμίζει την ανάπτυξη και τη χρήση τεχνολογιών αναγνώρισης προσώπου. Ο καθορισμός του πότε είναι απαραίτητη και αναλογική η επεξεργασία των εικόνων του προσώπου θα εξαρτηθεί από τον σκοπό για τον οποίο χρησιμοποιείται η τεχνολογία και από τις διασφαλίσεις που ισχύουν για την προστασία ατόμων των οποίων οι εικόνες του προσώπου υπόκεινται σε αυτοματοποιημένη επεξεργασία από πιθανές αρνητικές συνέπειες. Οι μορφές αναγνώρισης προσώπου που συνεπάγονται πολύ υψηλό βαθμό εισβολής στα θεμελιώδη δικαιώματα, που διακυβεύουν τον απαραβίαστο βασικό πυρήνα ενός ή περισσότερων θεμελιωδών δικαιωμάτων, είναι παράνομες.

Όταν οι εικόνες προσώπου εξάγονται από βιντεοκάμερες που αναπτύσσονται σε δημόσιους χώρους, η εκτίμηση της αναγκαιότητας και της αναλογικότητας της αναγνώρισης προσώπου πρέπει επίσης να εξετάσει πού βρίσκονται οι κάμερες. Υπάρχει μια διαφορά μεταξύ ενός αθλητικού ή πολιτιστικού γεγονότος και εκδηλώσεων όπου οι άνθρωποι ασκούν ένα από τα θεμελιώδη δικαιώματά τους. Η ανάπτυξη τεχνολογιών αναγνώρισης προσώπου κατά τη διάρκεια των διαδηλώσεων μπορεί να προκαλέσει ένα ψυχρό αποτέλεσμα, με το οποίο τα άτομα αποφεύγουν να ασκήσουν νόμιμα την ελευθερία του συνέρχεσθαι και του συνεταιρίζεσθαι λόγω του φόβου για τις αρνητικές συνέπειες που μπορεί να ακολουθήσουν. Είναι δύσκολο να φανταστεί κανείς καταστάσεις όπου η ανάπτυξη τεχνολογιών αναγνώρισης προσώπου σε άτομα που συμμετέχουν σε επίδειξη μπορεί να είναι απαραίτητη και αναλογική.

Οι δημόσιες αρχές βασίζονται συνήθως σε ιδιωτικές εταιρείες για την προμήθεια και την ανάπτυξη της τεχνολογίας. Η βιομηχανία και η επιστημονική ερευνητική κοινότητα μπορούν να διαδραματίσουν σημαντικό ρόλο στην ανάπτυξη τεχνικών λύσεων που προάγουν τον σεβασμό των θεμελιωδών δικαιωμάτων, συμπεριλαμβανομένης της προστασίας των προσωπικών δεδομένων. Για αυτό, ωστόσο, τα ζητήματα θεμελιωδών δικαιωμάτων πρέπει να ενσωματωθούν σε τεχνικές προδιαγραφές και συμβάσεις.

- Η οδηγία της ΕΕ για τις δημόσιες συμβάσεις (2014/24/ΕΕ) ενίσχυσε τη δέσμευση των κρατών μελών της ΕΕ για μια κοινωνικά υπεύθυνη δημόσια προμήθεια κατά την αγορά ενός προϊόντος ή μιας υπηρεσίας. Σύμφωνα με το πνεύμα της οδηγίας του 2014, η ΕΕ και τα κράτη μέλη

της θα μπορούσαν να εφαρμόσουν παρόμοια προσέγγιση κατά την προμήθεια τεχνολογίας αναγνώρισης προσώπου ή την ανάθεση καινοτόμων ερευνών. Η τοποθέτηση θεμελιωδών δικαιωμάτων και, ειδικότερα, των απαιτήσεων προστασίας δεδομένων και απαγόρευσης των διακρίσεων στο επίκεντρο όλων των τεχνικών προδιαγραφών, θα εξασφαλίσει ότι ο κλάδος θα δώσει τη δέουσα προσοχή σε αυτά.

- Τα πιθανά μέτρα θα μπορούσαν να περιλαμβάνουν μια δεσμευτική απαίτηση για τη συμμετοχή εμπειρογνομόνων προστασίας δεδομένων και ειδικών για τα ανθρώπινα δικαιώματα στις ομάδες που εργάζονται για την ανάπτυξη της τεχνολογίας, προκειμένου να διασφαλιστεί η συμμόρφωση των θεμελιωδών δικαιωμάτων από το σχεδιασμό. Επιπλέον, οι τεχνικές προδιαγραφές θα μπορούσαν να κάνουν αναφορά σε πρότυπα υψηλής ποιότητας για να ελαχιστοποιήσουν τα ψευδή ποσοστά αναγνώρισης και τις αρνητικές επιπτώσεις στο φύλο, την εθνικότητα και την ηλικία.
- Πολύ σημαντική πρωτοβουλία στα πλαίσια της Ευρωπαϊκής Ένωσης είναι η καμπάνια «Reclaim Your Face», η οποία προτρέπει την Ευρωπαϊκή Επιτροπή να προτείνει νομική πράξη, η οποία θα βασίζεται στις γενικές απαγορεύσεις που προβλέπονται στο γενικό κανονισμό για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου και θα τις σέβεται, προκειμένου να διασφαλιστεί ότι απαγορεύεται ρητά και η συγκεκριμένα η μαζική βιομετρική παρακολούθηση στην ΕΕ¹⁷⁸.
- Οι πολιτικές αρχές, όπως το Ευρωπαϊκό Κοινοβούλιο, η Ευρωπαϊκή Επιτροπή και το Συμβούλιο θα μπορούσαν να παράσχουν διατάξεις soft law σχετικά με τις διακυβευόμενες από την τεχνητή νοημοσύνη αξίες και τρόπους προστασίας τους. Σε αυτό το πλαίσιο κινείται και η Λευκή Βίβλος της Επιτροπής για την Τεχνητή νοημοσύνη¹⁷⁹.
- Οι αρχές προστασίας δεδομένων, και ιδίως το Συμβούλιο Προστασίας Δεδομένων, θα πρέπει να παρέχουν στους υπεύθυνους επεξεργασίας κατάλληλη καθοδήγηση σχετικά με τα θέματα, για τα οποία δεν μπορεί

¹⁷⁸ Βλ. περισσότερα <https://reclaimyourface.eu/el/>. Ανάκτηση: Απρίλιος 2021.

¹⁷⁹ Διαθέσιμο στο https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf. Ανάκτηση: Απρίλιος 2021.

να βρεθεί ακριβής απάντηση στον Κανονισμό. Οι Εθνικές Αρχές Προστασίας Δεδομένων θα πρέπει επίσης να παρέχουν καθοδήγηση, ιδίως όταν πρόκειται να συμβουλευθούν τους υπεύθυνους επεξεργασίας ή απαντούν σε ερωτήματα των υποκειμένων των δεδομένων.

Συμπερασματικά, οι υπεύθυνοι επεξεργασίας που ασχολούνται με την επεξεργασία με βάση την τεχνητή νοημοσύνη θα πρέπει να εγκρίνουν τις αξίες του Κανονισμού και να υιοθετήσουν μια υπεύθυνη και προσανατολισμένη στον κίνδυνο προσέγγιση, καθώς και θα πρέπει να μπορούν να το κάνουν με τρόπο συμβατό με τις διαθέσιμες τεχνολογίες και με την οικονομική αποδοτικότητα (ή τη βιώσιμη επίτευξη δημοσίων συμφερόντων). Ωστόσο, δεδομένης της πολυπλοκότητας του θέματος και των κενών, της ασάφειας και των αμφισημιών που υπάρχουν στον Κανονισμό, οι υπεύθυνοι επεξεργασίας δεν πρέπει να μένουν μόνοι σε αυτήν την άσκηση.

Τα ιδρύματα πρέπει να προωθήσουν μια ευρεία κοινωνική συζήτηση για τις εφαρμογές τεχνητής νοημοσύνης και θα πρέπει να παρέχουν ενδείξεις υψηλού επιπέδου. Οι αρχές προστασίας δεδομένων πρέπει να ξεκινήσουν ενεργά διάλογο με όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των υπευθύνων επεξεργασίας, των εκτελούντων την επεξεργασία και της κοινωνίας των πολιτών, για την ανάπτυξη κατάλληλων απαντήσεων, βάσει κοινών αξιών και αποτελεσματικών τεχνολογιών. Η συνεπής εφαρμογή των αρχών προστασίας δεδομένων, όταν συνδυάζεται με την ικανότητα αποτελεσματικής χρήσης της τεχνολογίας ΤΝ, μπορεί να συμβάλει στην επιτυχία των εφαρμογών ΤΝ, δημιουργώντας εμπιστοσύνη και αποτρέποντας τους κινδύνους.

Βιβλιογραφία

- Βλαχάβας Ι., Κεφαλάς Π., Βασιλειάδης Ν., Κόκκορας Φ., Σακελλαρίου Η. (2011). Τεχνητή Νοημοσύνη (Τόμ. ΙΙΙ). Εκδόσεις Πανεπιστημίου Μακεδονίας.
- Γεωργούλη, Α. (2015). Τεχνητή νοημοσύνη: θεωρητική προσέγγιση της επίλυσης προβλημάτων με τη βοήθεια μεθόδων τεχνητής νοημοσύνης. Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.
- Ιγγλεζάκης, Ι. (2003). Ευαίσθητα προσωπικά δεδομένα. Αθήνα: Σάκκουλας.
- Ιγγλεζάκης, Ι. (2020). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Τόμ. ΙΙΙ). Interactive Books.
- Κουσουνή-Πανταζοπούλου, Α. (2019). Νομικές διαστάσεις της τεχνητής νοημοσύνης (παρόν και μέλλον) σε ΕλλΔνη 1/2019. Ανάκτηση Φεβρουάριος 2021, από Sak Koulas Online: <https://www.sakkoulas-online.gr/reader/492bbd0fc687934eccbd/>
- Μαντζούφας, Π. (2010). Βιοπολιτική και βιομετρία. Ανάκτηση από Όμιλος "Αριστόβουλος Μάνεσης": <https://www.constitutionalism.gr/1828-biopolitiki-kai-biometria/>
- Μήτρου, Λ. (2017). Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (νέο δίκαιο-νέες υποχρεώσεις-νέα δικαιώματα) (Τόμ. Ι). Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη.
- Παναγοπούλου-Κουτνατζή, Φ. (2013). Βιομετρικές μέθοδοι και προστασία ιδιωτικότητας: σκέψεις με αφορμή την απόφαση ΔΕΕ Michael Schwarz κατά κρατιδίου Bochum (C-291/2012). ΔίΜΜΕ, σσ. 482-492.
- Παναγοπούλου-Κουτνατζή, Φ. (2017). Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2019/ΕΕ. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα.
- Παναγοπούλου-Κουτνατζή, Φ. (2017). Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: μια πρώτη αποτίμηση και συνταγματική αξιολόγηση. ΕφημΔΔ(1), σσ. 81-98.
- Σκόνδρα, Μ. (2020). Αναγνώριση προσώπου (Face recognition) και προσωπικά δεδομένα. Ανάκτηση από LAWSPOT: <https://www.lawspot.gr/nomika->

blogs/magdalini_skondra/anagnorisi-prosopoy-face-recognition-kai-prosopika-dedomena

Τάσσης, Σ. (2019, May 31). Το Δίκαιο στην Εποχή της Τεχνητής Νοημοσύνης. Ανάκτηση March 2021, από Lawspot: https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis

Albrecht, J. (2016). How the GDPR will change the world. EDPL.

Andreessen, M. (2011, August 20). Why Software Is Eating The World. Ανάκτηση April 2021, από The Wall Street Journal: <https://www.wsj.com/articles/SB10001424053111903480904576512250915629460>

Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework,. Computer Law & Securtiy Review: The International Journal of Technology Law and Practice, 260.

C. Dwork, M. Naor, T. Pitassi, G. N. Rothblum. (2010, June). Differential privacy under continual observation. Proceedings of the forty-second ACM symposium on Theory of computing, σσ. 715-724.

Calo, M. R. (2012). Against notice skepticism in privacy (and elsewhere). Notre Dame Law Review, LXXXVII(3), σσ. 1027-1072.

Cate F. H., Cullen P., Mayer-Schönberger V. (2014). Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines. Oxford Internet Institute.

Conger K., Fausset R., Kovaleski S. F. (2019). San Francisco bans facial recognition technology. Ανάκτηση από The New York Times: <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>

Conrad, S. (2017, 12). Künstliche Intelligenz – Die Risiken für den Datenschutz. Datenschutz und Datensicherheit, σ. 743.

Crawford, K. (2019, August 29). Regulate facial-recognition technology. Nature, 572, σσ. 565-565.

- Datatilsynet. (2018). Artificial Intelligence and Privacy. Datatilsynet (The Norwegian Data Protection Authority), Oslo, Norway.
- Hacker, P. (2018). Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law. *Common Market Law Review*, IV(55).
- Hymas, C. (2019). AI used for first time in job interviews in UK to find best applicants. Ανάκτηση από The Telegraph: <https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/?fbclid=IwAR2YAjJpQqpSI dhNyZebyxrSvA xg-8SlSqEGbNK12kJoag5I1OewPUQ3Bk>
- I. Kamara, P. De Hert. (2018). Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach. *Brussels Privacy Hub*, IV(12).
- J. P. Achara, G. Acs, C. Castelluccia. (2015, October). On the unicity of smartphone applications. *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, σσ. 27-36.
- Jasserand, C. (2016). Legal nature of biometric data: From generic personal data to sensitive data. *Eur. Data Prot. L. Rev.*(2), σσ. 297-311.
- Kindt, E. (2016, October). Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer Law & Security Review*, 32(5), σσ. 729-748.
- Mitrou, L. (2018). Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? Ανάκτηση από https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914
- Mozur, P. (2019). How China Is Using A.I. to Profile a Minority. Ανάκτηση από The New York Times: <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>
- Norvig, P., & Russel, S. (2005). Τεχνητή Νοημοσύνη: Μία σύγχρονη προσέγγιση. Κλειδάριθμος.

- Oppermann, A. (2019, November 12). What is Deep Learning and How does it work? Ανάκτηση December 2020, από Towards Data Science: <https://towardsdatascience.com/what-is-deep-learning-and-how-does-it-work-2ce44bb692ac>
- R. Kitchin, M. Dodge. (2014). Code/space: Software and everyday life. Mit Press.
- Simonite, T. (2017). Facebook Can Now Find Your Face, Even When It's Not Tagged. Ανάκτηση από Wired: <https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/>
- Smith, A. (2019). More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. Ανάκτηση από Pew Research Center: <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/>
- Swanson, B.-M. (2017, August 10). What is Deep Learning? Ανάκτηση 2020 December, από Oracle AI and Data Science Blog: <https://blogs.oracle.com/datascience/what-is-deep-learning>
- Sweeney, L. (2000). Simple demographics often identify people uniquely. Health (San Francisco)(671), σσ. 1-34.

Νομοθετικά – Νομικά κείμενα

- ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΫ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
- ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2018/1807 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 14ης Νοεμβρίου 2018 σχετικά με ένα πλαίσιο για την

ελεύθερη ροή των δεδομένων μη προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση.

ΟΔΗΓΙΑ 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Ομάδα εργασίας του άρθρου 29. (2003). Έγγραφο εργασίας σχετικά με τα στοιχεία βιομετρίας.

Ομάδα εργασίας του άρθρου 29. (2007). Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα».

Ομάδα Εργασίας του άρθρου 29. (2012). Γνώμη 3/2012 σχετικά με τις εξελίξεις στις βιομετρικές τεχνολογίες.

Ομάδα εργασίας του άρθρου 29. (2020). Κατευθυντήριες γραμμές για την συγκατάθεση υπό το πρίσμα του Κανονισμού 2016/679.

Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Νομολογία

Υπόθεση C-434/16, Peter Nowak v. Data Protection Commissioner. (2017).

Υπόθεση ΕΔΔΑ 37138/14 Szabó and Vissy κατά Ουγγαρίας.

Συνεκδικασθείσες υποθέσεις ΕΔΔΑ 1874/13 και 8567/13, López Ribalda και λοιποί κατά Ισπανίας, παρ. 87.

Συνεκδικασθείσες υποθέσεις ΔΕΚ C-141/12 και C-372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel. (2014).

Συνεκδικασθείσες υποθέσεις ΔΕΕ C-92/09 και C-93/09, Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen, παρ. 71.

Διπλωματικές – Πτυχιακές εργασίες

Βιαννιτάκη, Β. (2014). Τεχνητή Νοημοσύνη, Ευφυείς Πράκτορες και Εφαρμογές στην Πληροφορική υγείας, Πτυχιακή εργασία, ΤΕΙ Πελοποννήσου.

Παναγιωτίδου, Μ. Ε. (2020). Τεχνητή Νοημοσύνη και Δίκαιο: τεχνολογικά, νομικά και ηθικά ζητήματα, Διπλωματική εργασία, Διδρυματικό Πρόγραμμα Μεταπτυχιακών Σπουδών, Πανεπιστήμιο Μακεδονίας και Δημοκρίτειο Πανεπιστήμιο Θράκης, σελ. 18-20.

Παπαδόπουλος, Γ. Κ. (2006). Πληροφοριακή Ιδιωτικότητα και ΜΜΕ, Διπλωματική εργασία, Νομική Σχολή ΕΚΠΑ, σελ. 28.

Χριστάκου, Α. (2020). Οι νομικές επιπτώσεις των αλγορίθμων στον εργασιακό χώρο. Διπλωματική εργασία, Νομική Σχολή ΕΚΠΑ.

Ηλεκτρονικές Πηγές

Bhatt, B. (2018). Data is the new oil, Medium. Διαθέσιμο στο <https://medium.com/@BhaskarBhatt/data-is-the-new-oil-dcad95dd25e6>.
Ανάκτηση: Μάρτιος 2021.

Conger, K., Fausset, R., & Kovaleski, S. F. (2019). San Francisco bans facial recognition technology, The New York Times. Διάθεσιμο στο <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>. Ανάκτηση: Απρίλιος 2021.

Consultive Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data. (2019). Report on Artificial Intelligence and Data Protection: Challenges and Possible Remedies. Διαθέσιμο στο <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>. Ανάκτηση: Ιανουάριος 2021.

Datatilsynet. (2018). Artificial Intelligence and Privacy. Διαθέσιμο στο <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

Ανάκτηση: Απρίλιος 2021.

European Commission. (2021). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. Διαθέσιμο στο <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>. Ανάκτηση: Ιούνιος 2021.

European Court of Human Rights. (2020). Guide on Article 8 of the European Convention on Human Rights – Right to respect for private and family life, home and correspondence. Διαθέσιμο στο https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Ανάκτηση: Απρίλιος 2021.

European Parliament - EPRS. (2020) The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Scientific Foresight Unit. Διαθέσιμο στο [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf). Ανάκτηση: Απρίλιος 2021.

European Union Agency for Fundamental Rights. (2018). #BigData: Discrimination in data-supported decision making. Διαθέσιμο στο <https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making>. Ανάκτηση: Ιανουάριος 2021.

FRA, Council of Europe and EDPS. (2018). Handbook on European data protection law. Publications Office. Διαθέσιμο σε

- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Ανάκτηση: Μάρτιος 2021.
- Glancy, D. J. (2012). Privacy in autonomous vehicles. *Santa Clara L. Rev.*, 52, 1171.
- Hildebrandt, M. (2016). Law as Information in the Era of Data-driven Agency. *The Modern Law Review*, 79(1), 1-30. Διαθέσιμο στο <https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-2230.12165>. Ανάκτηση: Ιούνιος 2021.
- High Level Expert Group on Artificial Intelligence. (2018). A definition of AI: Main capabilities and scientific disciplines. Διαθέσιμο στο <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Ανάκτηση: Απρίλιος 2021.
- Homo Digitalis. (2019). Προ των πυλών η χρήση τεχνολογίας αναγνώρισης προσώπου από την αστυνομία στην Ελλάδα. Διαθέσιμο στο <https://www.homodigitalis.gr/posts/4662>. Ανάκτηση: Μάρτιος 2021.
- Homy, M. (2019). Police Use of Facial Recognition Tech Approved in Sweden, *Bloomberg Law*. Διαθέσιμο στο <https://news.bloomberglaw.com/tech-and-telecom-law/police-use-of-facial-recognition-tech-approved-in-sweden>. Ανάκτηση: Απρίλιος 2021.
- Hymas, Ch. (2019). AI used for first time in job interviews in UK to find best applicants, *The Telegraph*. Διαθέσιμο στο <https://www.telegraph.co.uk/news/2019/09/27/ai-facial-recognition-used-first-time-job-interviews-uk-find/?fbclid=IwAR2YAjJpQqpSI dhNyZebyxrSvA xg-8SlSqEGbNK12kJoag5I1OoewPUQ3Bk>. Ανάκτηση: Μάρτιος 2021.

Information Commissioner Office – ICO (2014). Big data and data protection.

Διαθέσιμο στο <https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220>. Ανάκτηση: Ιανουάριος 2021.

Information Commissioner Office – ICO (2017). Big data, artificial intelligence, machine learning and data protection. Διαθέσιμο στο

<https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Ανάκτηση: Μάρτιος 2021.

Information Technology Gartner Glossary. Διαθέσιμο στο <https://www.gartner.com/en/information-technology/glossary/big-data>.

Ανάκτηση: Ιανουάριος 2021.

Mayhew, S. (2019). Expanded use of facial recognition at Prague international airport approved, BIMOETRIC UPDATE.COM. Διαθέσιμο στο

<https://www.biometricupdate.com/201903/expanded-use-of-facial-recognition-at-prague-international-airport-approved>. Ανάκτηση: Απρίλιος 2021.

Microsoft, The Future Computed. Διαθέσιμο στο <https://news.microsoft.com/uploads/2018/01/The-Future-Computed.pdf>.

Ανάκτηση: Μάρτιος 2021.

Mozur, P. (2019). How China Is Using A.I. to Profile a Minority, The New York Times.

Διαθέσιμο στο <https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html>. Ανάκτηση: Απρίλιος 2021.

Oppermann, A. (2019). What is Deep Learning and How does it work?, Towards Data Science. Διαθέσιμο στο <https://towardsdatascience.com/what-is-deep-learning-and-how-does-it-work-2ce44bb692ac>.

Ανάκτηση: Απρίλιος 2021.

- Sample, I. (2019). Watchdog criticises 'chaotic' police use of facial recognition, The Guardian. Διαθέσιμο στο <https://www.theguardian.com/uk-news/2019/jun/27/watchdog-criticises-chaotic-police-use-of-facial-recognition>. Ανάκτηση: Φεβρουάριος 2021.
- Simonite, T. (2017). Facebook Can Now Find Your Face, Even When It's Not Tagged, Wired. Διαθέσιμο στο <https://www.wired.com/story/facebook-will-find-your-face-even-when-its-not-tagged/>. Ανάκτηση: Απρίλιος 2021.
- Smith, A. (2019). More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly, Pew Research Center. Διάθεσιμο στο <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/>. Ανάκτηση: Μάρτιος 2021.
- Swanson, B.-M. (2017). What is Deep Learning?, Oracle AI and Data Science Blog. Διαθέσιμο στο <https://blogs.oracle.com/datascience/what-is-deep-learning>. Ανάκτηση: Μάρτιος 2021.
- UK-RAS NETWORK – Robotics & Autonomous Systems. (2017). Artificial Intelligence and Robotics, UK-RAS White papers. Διαθέσιμο στο https://www.ukras.org/wp-content/uploads/2021/01/UKRASWP_ArtificialIntelligence2017_online.pdf. Ανάκτηση: Μάρτιος 2021.
- Vass, Á. (2019). CCTV: Is It Big Brother or the Eye of Providence?, HUNGARY today. Διαθέσιμο στο <https://hungarytoday.hu/cctv-is-it-big-brother-or-the-eye-of-providence/>. Ανάκτηση: Απρίλιος 2021.
- Wiles, P. (2019). Commissioner for the retention and use of biometric material, Annual Report 2018. Διαθέσιμο στο

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf)

[001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/825106/CCS001_CCS0319869991-001_Biometrics_Commissioner_AR_2018_Web_Accessible.pdf). Ανάκτηση: Μάρτιος 2021.

Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή. (2019). Η ΕΟΚΕ προτείνει τη θέσπιση ενωσιακού συστήματος πιστοποίησης για αξιόπιστα προϊόντα τεχνητής νοημοσύνης. Διαθέσιμο στο <https://www.eesc.europa.eu/el/news-media/eesc-info/112019/articles/74868>. Ανάκτηση: Απρίλιος 2021.

Ευρωπαϊκό Κοινοβούλιο. (2020). Τί είναι η Τεχνητή Νοημοσύνη και πώς χρησιμοποιείται;. Διαθέσιμο στο <https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai>. Ανάκτηση: Ιανουάριος 2021.

Κουσουνή-Πανταζοπούλου, Α. (2019). Νομικές διαστάσεις της τεχνητής νοημοσύνης (παρόν και μέλλον), ΕλλΔνη 1/2019, Sakkoulas Online. Διαθέσιμο στο <https://www.sakkoulas-online.gr/reader/492bbd0fc687934eccbd/>. Ανάκτηση: Μάρτιος 2021.

Μαντζούφας, Π. (2010). Βιοπολιτική και βιομετρία, Όμιλος "Αριστόβουλος Μάνεσης". Διαθέσιμο στο <https://www.constitutionalism.gr/1828-biopolitiki-kai-biometria/>. Ανάκτηση: Μάρτιος 2021.

Ομάδα Εργασίας του ΣΕΒ για τα Προσωπικά Δεδομένα. (2018) Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Διαθέσιμο στο https://www.sev.org.gr/Uploads/Documents/51628/meleti_sev_GDPR_final.pdf. Ανάκτηση: Ιανουάριος 2021.

Τάσσης, Σπ. (2019). Το Δίκαιο στην Εποχή της Τεχνητής Νοημοσύνης, Lawspot,
Διαθέσιμο στο https://www.lawspot.gr/nomika-blogs/spiros_tassis/dikaio-stin-epohi-tis-tehnitis-noimosynis. Ανάκτηση: Μάρτιος 2021.