



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
Εθνικόν και Καποδιστριακόν  
Πανεπιστήμιον Αθηνών  
— ΙΔΡΥΘΕΝ ΤΟ 1837 —

## ΝΟΜΙΚΗ ΣΧΟΛΗ

---

Π.Μ.Σ.: ΑΣΤΙΚΟ ΔΙΚΑΙΟ

ΕΙΔΙΚΕΥΣΗ: ΑΣΤΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΕΤΟΣ: 2019-2020

### ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Αλεξάνδρας Νικολάου Τσινόρεμα

A.M.: 7340010219020

## Η επεξεργασία Προσωπικών Δεδομένων από συστήματα Τεχνητής Νοημοσύνης

### Επιβλέποντες:

- α) Χριστοδούλου Κωνσταντίνος
- β) Αυγουστιανάκης Μιχαήλ
- γ) Κονδύλη Ιωάννα

Αθήνα, Νοέμβριος 2020

Copyright © [Αλεξάνδρα Τσινόρεμα, Νοέμβριος 2020]

Με επιφύλαξη παντός δικαιώματος. All rights reserved. Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας 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.

Οι απόψεις και θέσεις που περιέχονται σε αυτήν την εργασία εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

## **ΕΥΧΑΡΙΣΤΙΕΣ**

Πριν την ανάπτυξη της παρούσας διπλωματικής εργασίας, θα ήθελα να αποδώσω θερμές ευχαριστίες στον Καθηγητή Κωνσταντίνο Χριστοδούλου για την επίβλεψη και την εν γένει στήριξη του κατά την εκπόνηση της παρούσας εργασίας.

Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου για την συνεχή ψυχολογική υποστήριξη που μου προσέφεραν καθ' όλη την διάρκεια ολοκλήρωσης αυτής.

## ΠΕΡΙΕΧΟΜΕΝΑ

<b>I. ΠΡΟΛΟΓΟΣ.....</b>	<b>σελ.1</b>
<b>II. ΚΕΦΑΛΑΙΟ Α : ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ.....</b>	<b>σελ.2</b>
<b>1. ΕΙΣΑΓΩΓΙΚΑ.....</b>	<b>σελ.2</b>
1.1. Ορισμός .....	σελ.2
1.2. Η χρήση της τεχνητής νοημοσύνης στην επεξεργασία προσωπικών δεδομένων.....	σελ.3
<b>III. ΚΕΦΑΛΑΙΟ Β: ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ.....</b>	<b>σελ.6</b>
<b>1. Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ.....</b>	<b>σελ.6</b>
1.1. Γενικά.....	σελ.6
1.2. Η Τεχνητή Νοημοσύνη στο πλαίσιο προστασίας του Κανονισμού.....	σελ.7
<b>2. Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ.....</b>	<b>σελ.9</b>
2.1. Ορισμός προσωπικών δεδομένων.....	σελ.9
2.2. Οι έννοιες του ταυτοποιημένου και ταυτοποιήσιμου φυσικού προσώπου.....	σελ.9
2.3. Ανώνυμα δεδομένα.....	σελ.10
2.4. Ανωνυμοποίηση.....	σελ.11
2.5. Ψευδωνυμοποίηση.....	σελ.12
2.6. Επαναονομαστικοποίηση.....	σελ.13
<b>3. Η ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ.....</b>	<b>σελ.15</b>
3.1. Ορισμός.....	σελ.15
3.2. Αυτοματοποιημένη και μη αυτοματοποιημένη επεξεργασία.....	σελ.15
3.3. Ιδιαίτερως η αυτοματοποιημένη επεξεργασία.....	σελ.16
3.4. Τρόποι επεξεργασίας.....	σελ.17
<b>IV. ΚΕΦΑΛΑΙΟ Γ: Η ΔΥΣΧΕΡΕΙΑ ΤΗΡΗΣΕΩΣ ΤΩΝ ΓΕΝΙΚΩΝ ΑΡΧΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ.....</b>	<b>σελ.18</b>
<b>1. Η ΑΡΧΗ ΤΗΣ ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΤΗΣ ΛΟΓΟΔΟΣΙΑΣ.....</b>	<b>σελ.18</b>
1.1. Η αρχή της Διαφάνειας.....	σελ.18
1.2. Η ενημέρωση του υποκειμένου σχετικά με την αυτοματοποιημένη λήψη αποφάσεων.....	σελ.19
1.3. Η αρχή της Λογοδοσίας .....	σελ.21
1.4. Η μελέτη εκτίμησης αντικτύπου.....	σελ.22
1.4.1. Γενικά.....	σελ.22

1.4.2. Ειδικά σχετικά με τα συστήματα τεχνητής νοημοσύνης.....	σελ.23
<b>2. ΤΟ ΖΗΤΗΜΑ ΤΗΣ ΑΔΙΑΦΑΝΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ.....</b>	<b>σελ.24</b>
2.1. Το πρόβλημα των “Black Boxes” .....	σελ.24
2.2. Λόγοι της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης.....	σελ.25
2.2.1. Ο τεχνικός αναλφαριθμητισμός.....	σελ.25
2.2.2. Η υπολογιστική πολυπλοκότητα.....	σελ.26
2.2.3. Η προγνωστική ανάλυση .....	σελ.27
2.2.4. Η εκούσια αδιαφάνεια για λόγους εταιρικού ή κρατικού απορρήτου.....	σελ.28
<b>3. Η ΑΡΧΗ ΠΕΡΙΟΡΙΣΜΟΥ ΤΟΥ ΣΚΟΠΟΥ.....</b>	<b>σελ.29</b>
<b>4. Η ΑΡΧΗ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ.....</b>	<b>σελ.31</b>
<b>5. Η ΑΡΧΗ ΤΗΣ ΑΚΡΙΒΕΙΑΣ.....</b>	<b>σελ.32</b>
<b>6. Η ΑΡΧΗ ΠΕΡΙΟΡΙΣΜΟΥ ΤΗΣ ΠΕΡΙΟΔΟΥ ΑΠΟΘΗΚΕΥΣΗΣ.....</b>	<b>σελ.32</b>
<b>7. Η ΑΡΧΗ ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΑΙ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ.....</b>	<b>σελ.33</b>

## **V. ΚΕΦΑΛΑΙΟ Δ: Η ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ ΑΠΟ ΣΥΣΤΗΜΑΤΑ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ.....σελ.35**

<b>1. Η ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ (PROFILING).....</b>	<b>σελ.35</b>
1.1. Ορισμός.....	σελ.35
1.2. Υποκατηγορίες και χρησιμότητα της καταρτίσεως προφίλ.....	σελ.36
1.3. Το profiling ως τρόπος επεξεργασίας.....	σελ.37
1.4. Η χρήση αλγορίθμων τεχνητής νοημοσύνης για την κατάρτιση προφίλ.....	σελ.38
<b>2. ΟΙ ΚΙΝΔΥΝΟΙ ΤΗΣ ΚΑΤΑΡΤΙΣΕΩΣ ΠΡΟΦΙΛ.....</b>	<b>σελ.39</b>
2.1. Αδιαφάνεια και παραβίαση ιδιωτικότητας.....	σελ.39
2.1.1. Η υπόθεση Cambridge Analytica – Facebook.....	σελ.40
2.2. Το πρόβλημα της μεροληψίας των συστημάτων τεχνητής νοημοσύνης.....	σελ.41
2.2.1. Η θεμελιώδης σημασία του θεμιτού της επεξεργασίας.....	σελ.41
2.2.2. Το πρόβλημα σχετικά με τα συστήματα τεχνητής νοημοσύνης.....	σελ.42
2.2.2.1. Διακρίσεις εξαιτίας των δεδομένων.....	σελ.43
2.2.2.2. Διακρίσεις εξαιτίας του σχεδιαστή και του σχεδιασμού του αλγορίθμου.....	σελ.44
<b>3. Η ΕΝΑΝΤΙΩΣΗ ΣΤΗΝ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΣ.....</b>	<b>σελ.46</b>
3.1. Γενικά τα δικαιώματα των υποκειμένων.....	σελ.46
3.2. Ειδικότερα το δικαίωμα του άρθρου 22 παράγραφος 1.....	σελ.47
3.2.1. Οι δικαιολογητικοί λόγοι θεσπίσεως του.....	σελ.47
3.2.2. Η φύση του δικαιώματος.....	σελ.48
3.2.3. Το περιεχόμενό του.....	σελ.48
3.2.3.1. Η αποκλειστικώς αυτοματοποιημένη λήψη αποφάσεως.....	σελ.49
3.2.3.2. Έννομα αποτελέσματα.....	σελ.51

3.2.3.3. Σημαντική επιρροή προς τα υποκείμενα.....σελ.51	
3.3. Οι εξαιρέσεις της παραγράφου 2.....σελ.52	
3.3.1. Σύναψη ή εκτέλεση σύμβασης.....σελ.52	
3.3.2. Πρόβλεψη από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.....σελ.53	
3.3.3. Ρητή συγκατάθεση υποκειμένου.....σελ.53	
3.3.3.1. Το πρόβλημα της συγκατάθεσης στο πλαίσιο της επεξεργασίας δεδομένων από συστήματα τεχνητής νοημοσύνης.....σελ.54	
3.4. Το περιεχόμενο των παραγράφων 3 και 4.....σελ.55	

**VI. ΚΕΦΑΛΑΙΟ Ε: ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ.....σελ.57**

**VII. ΒΙΒΛΙΟΓΡΑΦΙΑ.....σελ.58**

## ΠΡΟΛΟΓΟΣ

Η ραγδαία εξέλιξη της τεχνολογίας εισέβαλλε στην ανθρώπινη καθημερινότητα μεταβάλλοντας τον τρόπο ζωής των ατόμων. Στο πλαίσιο αυτό κυρίαρχο ρόλο διαδραματίζει η εξέχουσα ανάπτυξη της τεχνητής νοημοσύνης και ιδιαίτερα της μηχανικής εκμάθησης, οι οποίες δικαιολογημένα χαρακτηρίζονται ως οι τεχνολογίες του μέλλοντος. Παράλληλα με το πλήθος των πλεονεκτημάτων μιας τέτοιας τεχνολογικής ανάπτυξης και της συμβολής της στην οικονομική, πολιτισμική και κοινωνική πρόοδο, ερχόμαστε αντιμέτωποι και με πληθώρα προκλήσεων αναφορικά με την ιδιωτικότητα, τον πληροφοριακό αυτοκαθορισμό, τα προσωπικά δεδομένα και τα δικαιώματα των προσώπων. Η τεχνητή νοημοσύνη από την μία πλευρά παρουσιάζει ευεργετική επίδραση σχετικά με την επεξεργασία των προσωπικών δεδομένων, καθώς καθιστά ταχύτερη, αποτελεσματικότερη, ακριβέστερη και ευχερέστερη την επεξεργασία τεράστιου όγκου δεδομένων. Από την άλλη πλευρά ωστόσο ελλοχεύουν πολυποίκιλοι κίνδυνοι και προβληματισμοί σχετικά με τα προσωπικά δεδομένα και την συνύπαρξη της τεχνητής νοημοσύνης με τον Γενικό Κανονισμό για την προστασία δεδομένων προσωπικού χαρακτήρα 679/2016.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων καθιερώνει πλήθος αρχών που πρέπει να τηρούνται κατά την επεξεργασία προσωπικών δεδομένων προκειμένου να διασφαλιστούν τα συμφέροντα και τα δεδομένα των υποκειμένων. Η τεχνητή νοημοσύνη δημιουργεί ανασφάλεια σχετικά με την τήρηση των εν λόγω αρχών. Οι κυριότεροι κίνδυνοι εντοπίζονται στο γεγονός της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης, τα οποία χαρακτηρίζονται ως black boxes, καθώς δεν είναι πλήρως κατανοητός και προβλέψιμος ο τρόπος λειτουργίας τους, αλλά υφίσταται και πληθώρα άλλων προβλημάτων, που δυσχεραίνουν την εφαρμογή των γενικών αρχών επεξεργασίας του Κανονισμού.

Τέλος στο πλαίσιο της παρούσας διπλωματικής θα γίνει λόγος για την επονομαζόμενη κατάρτιση προφίλ, η διενέργεια της οποίας πραγματοποιείται συχνά με την χρησιμοποίηση αλγορίθμων και συστημάτων τεχνητής νοημοσύνης. Σε αυτό το γεγονός, πέραν της αδιαφάνειας των εν λόγω αλγορίθμων και της προσβολής της ιδιωτικότητας των προσώπων, συμπεριλαμβάνεται και ο κίνδυνος μεροληπτικών και λανθασμένων αποτελεσμάτων. Για τους λόγους αυτούς και της ανασφάλειας που δημιουργούν τα συστήματα, που λειτουργούν χωρίς ανθρώπινη συμβολή, καθιερώθηκε στον Κανονισμό και το δικαίωμα των υποκειμένων να μην υπόκεινται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, με απώτερο σκοπό την αποτελεσματική προστασία τους.

# ΚΕΦΑΛΑΙΟ Α: ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

## 1. ΕΙΣΑΓΩΓΙΚΑ

### 1.1. Ορισμός

Η Τεχνητή Νοημοσύνη αποτελεί κλάδος της πληροφορικής, που ασχολείται με την δημιουργία ευφυών υπολογιστικών συστημάτων, δηλαδή συστημάτων που μιμούνται την ανθρώπινη συμπεριφορά και ευφυΐα.<sup>1</sup> Αναφερόμαστε, δηλαδή, σε μια νοημοσύνη “μη βιολογική”, που δεν προέρχεται από έμβια όντα.<sup>2</sup> Ο όρος τεχνητή νοημοσύνη θεμελιώθηκε τυπικά το 1956 κατά την διάρκεια της συνάντησης επιφανών Αμερικανών επιστημόνων (John McCarthy, Marvin Minsky, Claude Shannon και Nathaniel Rocheste).<sup>3</sup> Ο επιστήμονας John McCarthy, μάλιστα, όρισε ως τεχνητή νοημοσύνη «την επιστήμη της δημιουργίας έξυπνων μηχανών και ιδιαιτέρως έξυπνων προγραμμάτων υπολογιστών».<sup>4</sup> Παρατήρησε ότι σχετίζεται με την χρήση υπολογιστών με σκοπό την κατανόηση της ανθρώπινης νοημοσύνης, όμως η τεχνητή νοημοσύνη δεν περιορίζεται σε μεθόδους που είναι βιολογικά παρατηρήσιμοι.<sup>5</sup> Ωστόσο, το πρώτο δείγμα τεχνητής νοημοσύνης παρατηρείται μετά τον Δεύτερο Παγκόσμιο πόλεμο, ήδη από το 1950, με την πρόταση του επιφανούς μαθηματικού Άλαν Τούρινγκ για την εφαρμογή του Turing Test, μιας δοκιμασίας, η οποία σύμφωνα με τον Τούρινγκ είναι ικανή να εξακριβώσει αν μια μηχανή διαθέτει ευφυΐα.<sup>6</sup>

Μερικά χαρακτηριστικά παραδείγματα εφαρμογής της τεχνητής νοημοσύνης είναι η αναγνώριση προσωπικών προτιμήσεων με σκοπό την παροχή εξατομικευμένων συστάσεων και διαφημίσεων, η αναγνώριση προσώπου και φωνής, οι επονομαζόμενοι εικονικοί προσωπικοί βοηθοί (Siri, Google Now), τα έξυπνα αυτόνομα αυτοκίνητα, τα έξυπνα σπίτια και οι έξυπνες πόλεις κ.α.<sup>7</sup> Γενικά αναγνωρίζεται ότι η χρήση της εν λόγω τεχνολογίας έχει πράγματι αλλάξει ριζικά την ανθρώπινη καθημερινότητα προς το καλύτερο, βελτιώνοντας την ποιότητα ζωής, ωστόσο δεν μπορούμε να παραβλέψουμε τους κινδύνους ηθικής και νομικής φύσεως που ανακύπτουν.

Στην σύγχρονη εποχή η παρουσία και χρησιμότητα της τεχνητής νοημοσύνης είναι ιδιαίτερα εμφανής και παρατηρείται σε όλους σχεδόν τους επιχειρηματικούς κλάδους. Μέσω της μηχανικής εκμάθησης, η οποία χρησιμοποιείται από τα συστήματα τεχνητής νοημοσύνης, καθίσταται δυνατή μία άκρως ταχεία και αποτελεσματική επίτευξη των εκάστοτε στόχων. Με τον όρο μηχανική εκμάθηση, πιο συγκεκριμένα, εννοούμε το πεδίο μελέτης που δίνει στους υπολογιστές την

<sup>1</sup> [https://el.wikipedia.org/wiki/Τεχνητή\\_νοημοσύνη](https://el.wikipedia.org/wiki/Τεχνητή_νοημοσύνη)

<sup>2</sup> Χριστοδούλου Κ., Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, Μηνιαίο Επιστημονικό Περιοδικό, ΙΘ/2019, Εκδόσεις Π. Ν. Σάκκουλας, σελ. 329

<sup>3</sup> [https://el.wikipedia.org/wiki/Τεχνητή\\_νοημοσύνη](https://el.wikipedia.org/wiki/Τεχνητή_νοημοσύνη)

<sup>4</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, σελ. 3

<sup>5</sup> Kamarinou D., Millard C., and Singh J., ο.π., σελ. 3

<sup>6</sup> [https://el.wikipedia.org/wiki/Τεχνητή\\_νοημοσύνη](https://el.wikipedia.org/wiki/Τεχνητή_νοημοσύνη)

<sup>7</sup> <https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoietai>



ικανότητα να μαθαίνουν, χωρίς να έχουν ρητά και σχετικώς προγραμματιστεί για αυτό. Κατασκευάζονται αλγόριθμοι τέτοιου είδους, που μαθαίνουν από τα δεδομένα και κάνουν σχετικές προβλέψεις σύμφωνα με αυτά.<sup>8</sup>

Η μηχανική εκμάθηση διαχωρίζεται σε δύο κατηγορίες την επιβλεπόμενη και την μη επιβλεπόμενη. Στην επιβλεπόμενη μηχανική εκμάθηση χαρακτηρίζονται δεδομένα βάσει άλλων δεδομένων εκπαίδευσης.<sup>9</sup> Με αυτόν τον τρόπο εκπαιδεύεται ο αλγόριθμος και καθίσταται ικανός να προβλέψει μελλοντικά αποτελέσματα. Αντιθέτως, στην μη επιβλεπόμενη μηχανική εκμάθηση ο αλγόριθμος μαθαίνει μόνος του και δεν του παρέχεται κάποια εμπειρία σχετικά με την δομή των δεδομένων εισόδου. Είναι, λοιπόν, εμφανές ότι οι προγραμματιστές διευκολύνονται στο έργο τους και στην επίβλεψη και πρόβλεψη της ανάπτυξης του αλγορίθμου στο πεδίο της επιβλεπόμενης μηχανικής εκμάθησης, επιτρέποντάς τους να τροφοδοτήσουν τον αλγόριθμο με τα κατάλληλα δεδομένα με σκοπό την βελτίωσή του.<sup>10</sup>

Φυσικά η επίδραση της τεχνητής νοημοσύνης και της μηχανικής εκμάθησης παρατηρείται έντονα και στην συλλογή και επεξεργασία προσωπικών δεδομένων, γεγονός που προβληματίζει έντονα τους νομικούς ανά τον κόσμο. Οι ανησυχίες τους εντοπίζονται κυρίως στη πιθανότητα παραβίασης του Γενικού Κανονισμού Προστασίας Δεδομένων, στους κινδύνους που ελλοχεύει το profiling γενικά και ειδικά όταν διενεργείται από αλγοριθμικά συστήματα τεχνητής νοημοσύνης, λαμβανομένης φυσικά υπόψιν και της αδιαφάνειας που χαρακτηρίζει τα συστήματα τεχνητής νοημοσύνης κατά την δράση τους.

## **1.2. Η χρήση της τεχνητής νοημοσύνης στην επεξεργασία προσωπικών δεδομένων**

Η σχέση της τεχνητής νοημοσύνης με τα προσωπικά δεδομένα αναγνωρίζεται ως μια σχέση διπλής κατεύθυνσης, κατά την οποία τα προσωπικά δεδομένα τροφοδοτούν την τεχνητή νοημοσύνη με πληροφορίες και δεδομένα, η οποία με την σειρά της οδηγεί και καταλήγει στην παραγωγή περισσότερων δεδομένων και πληροφοριών.<sup>11</sup> Με την συλλογή των δεδομένων ενισχύεται η γνωστική διαδικασία των συστημάτων τεχνητής νοημοσύνης. Στην πραγματικότητα τα προσωπικά δεδομένα έχουν εναρμονιστεί με την σύγχρονη ψηφιακή πραγματικότητα σε έναν μεγάλο βαθμό και παρότι εγκυμονεί πληθώρα κινδύνων, κυρίως σχετικών με τον πληροφοριακό αυτοκαθορισμό των ατόμων, ταυτόχρονα εμφανίζεται πλήθος πλεονεκτημάτων σε αυτό το πλαίσιο.

Πιο συγκεκριμένα με την εκμετάλλευση της τεχνολογίας της τεχνητής νοημοσύνης είναι δυνατή η επεξεργασία τεράστιου όγκου δεδομένων με ταχύτατους ρυθμούς, καθιστώντας δυνατή και ευκολότερη την επεξεργασία των επονομαζόμενων «Μεγάλων Δεδομένων» (Big Data).<sup>12</sup> Με τον όρο Big Data εννοούνται τα δεδομένα, τα οποία είναι τόσο μεγάλα σε ποσότητα, αναπτύσσονται και παράγονται με ταχύτατους ρυθμούς ή διακρίνονται από τεράστια

<sup>8</sup> [https://el.wikipedia.org/wiki/Μηχανική\\_μάθηση](https://el.wikipedia.org/wiki/Μηχανική_μάθηση)

<sup>9</sup> [https://el.wikipedia.org/wiki/Επιβλεπόμενη\\_μάθηση](https://el.wikipedia.org/wiki/Επιβλεπόμενη_μάθηση)

<sup>10</sup> *Humerick M.*, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, Volume 34/ Issue 4, 2018, σελ. 398

<sup>11</sup> *Mitrou L.*, Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, University of the Aegean Data Protection, 2019, σελ. 19

<sup>12</sup> *Βόρρας Α./Μήτρον Α.*, Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, ΔΙΤΕ(π. ΔΙΜΕΕ), Τεύχος 4/2018, σελ. 460-466

πολυπλοκότητα, ώστε η επεξεργασία τους δεν είναι δυνατή χρησιμοποιώντας παραδοσιακές βάσεις και τρόπους επεξεργασίας δεδομένων. Πλέον βέβαια, ο ορισμός αυτός έχει επεκταθεί και αναφέρεται εκτός από την ιδιότητα των ίδιων των δεδομένων και στις ποικίλες τεχνολογίες που χρησιμοποιούνται για τις ανωτέρω διεργασίες επεξεργασίας.

Τα στοιχεία, λοιπόν, που χαρακτηρίζουν τα Big Data είναι ο όγκος, η ταχύτητα και η ποικιλία (τα λεγόμενα 3Vs : Volume, Velocity, Variety).<sup>13</sup> Ως όγκο εννοούμε κυρίως την ποσότητα των δεδομένων, το μέγεθος της οποίας οφείλεται κυρίως στην προέλευση και παραγωγή τους από τεράστια ποικιλία πηγών (φυσικά πρόσωπα, επιχειρήσεις, διοικητικές αρχές κ.α.), ενώ με τον όρο ταχύτητα αναφερόμαστε στην ταχύτητα συλλογής και επεξεργασίας τους σε πραγματικό χρόνο. Τέλος ως ποικιλία εννοούμε κυρίως τις ποικίλες μορφές (κείμενο, ήχος, βίντεο), τις οποίες μπορούν να λάβουν τα δεδομένα. Μέσω της τεχνητής νοημοσύνης επιτεύχθηκε λοιπόν η ευχερέστερη, ταχύτερη και αποτελεσματικότερη συλλογή, επεξεργασία και αποθήκευση Μεγάλων Δεδομένων, εφόσον αναλογιστούμε ότι αυτού του είδους η επεξεργασία δεν θα ήταν δυνατόν να επιτευχθεί από ένα φυσικό πρόσωπο. Ακόμα, όμως, και αν ήταν εφικτή δεν θα ήταν οικονομικά συμφέρουσα, διότι θα απαιτείτο η εκμετάλλευση ιδιαιτέρως αυξημένου ανθρώπινου δυναμικού. Χωρίς, δηλαδή, την ύπαρξη συστημάτων τεχνητής νοημοσύνης, η επεξεργασία τόσο μεγάλου όγκου προσωπικών δεδομένων θα απαιτούσε την συμβολή πολλών εργαζομένων και την αφιέρωση πολλών εργατικών ωρών, πράγμα όχι μόνο εξαντλητικό για τους εργαζομένους αλλά και επιβλαβές για την οικονομία της εκάστοτε επιχείρησης. Φυσικά η ανθρώπινη συμβολή παραμένει απαραίτητη στην επεξεργασία των προσωπικών δεδομένων, αλλά έχει πλέον μειωθεί δραματικά.

Μέσω των συστημάτων τεχνητής νοημοσύνης είναι, επίσης, δυνατόν να αναγνωριστούν ορισμένα πρότυπα των δεδομένων και να προβλεφθεί το πιθανό μελλοντικό αποτέλεσμα.<sup>14</sup> Με αυτόν τον τρόπο επιτρέπεται, κυρίως στις επιχειρήσεις, να σχεδιάζουν πιο μακροπρόθεσμες και αποτελεσματικές στρατηγικές. Ταυτόχρονα δημιουργούνται και καινούργιοι τρόποι επεξεργασίας δεδομένων, οι οποίοι δεν ήταν εφικτοί στην προ τεχνητής νοημοσύνης εποχή.

Άλλο ένα χαρακτηριστικό των συστημάτων τεχνητής νοημοσύνης είναι ότι δεν δρουν μόνο βάσει του αρχικού προγραμματισμού τους, αλλά όσο τροφοδοτούνται με καινούργια δεδομένα, αποκτούν περαιτέρω γνώση, “μαθαίνουν”, προσαρμόζοντας κατά αυτόν τον τρόπο το αποτέλεσμα και τον τρόπο επεξεργασίας τους στην καινούργια αυτή πραγματικότητα και στις εκάστοτε ανάγκες. Αυτό, φυσικά, δημιουργεί ανασφάλεια δικαίου, λόγω της αδυναμίας προβλεψιμότητας του εκάστοτε αποτελέσματος. Ταυτόχρονα, όμως, βάσει αυτού του είδους της επεξεργασίας, καταλήγουμε σε πιο αληθινά, δίκαια, και ακριβή συμπεράσματα.

Η εξέλιξη των τεχνολογιών τεχνητής νοημοσύνης, από την χρήση της μηχανικής εκμάθησης και ανεπτυγμένων μορφών μηχανικής εκμάθησης, μέχρι το σημείο της δημιουργίας του επονομαζόμενου deep learning, οδήγησε επίσης στην επίλυση περίπλοκων προβλημάτων και στην επίτευξη σημαντικών στόχων. Μέσω της τεχνολογίας του deep learning (βαθιά εκμάθηση), η οποία χρησιμοποιώντας νευρώνες προσπαθεί να μιμηθεί σε μεγάλο βαθμό τις λειτουργίες του ανθρώπινου εγκεφάλου, είναι πλέον δυνατή, μέσω αναγνώρισης ορισμένων προτύπων και ανάλυσης δεδομένων, η διενέργεια διαδικασιών, όπως η πρόβλεψη του καιρού, η ανίχνευση περιπτώσεων φορολογικής απάτης κ.α. Έτσι συλλέγονται, κατηγοριοποιούνται και τροφοδοτούνται δεδομένα στον αλγόριθμο, κατά τέτοιο τρόπο, ώστε αυτός να μαθαίνει να

<sup>13</sup> [https://www.sas.com/el\\_gr/insights/big-data/what-is-big-data.html](https://www.sas.com/el_gr/insights/big-data/what-is-big-data.html)

<sup>14</sup> <https://ncube.com/blog/big-data-and-ai>

δημιουργεί συσχετισμούς δεδομένων ακόμα και θεωρητικά άσχετων μεταξύ τους. Ο αλγόριθμος, δηλαδή, συνεχίζει να μαθαίνει και να γίνεται περισσότερο αποδοτικός και αποτελεσματικός όσο τροφοδοτείται με μεγάλες ποσότητες δεδομένων. Αντίθετα στην περίπτωση της τεχνικής του shallow learning χρησιμοποιείται μικρός αριθμός δεδομένων καθιστώντας δυσχερή την εξέλιξη του αλγορίθμου.<sup>15</sup>

Η τεχνητή νοημοσύνη δρα άλλοτε αντικαθιστώντας τελείως την ανθρώπινη συμβολή και άλλοτε παράλληλα με αυτήν, διευκολύνοντας τις ενέργειες των υποκειμένων, ενισχύοντας την ανθρώπινη δημιουργικότητα και έμπνευση και κυρίως αντιμετωπίζοντας ταχύτερα, αποτελεσματικότερα και ιδιαίτερα λεπτομερώς τα εκάστοτε προβλήματα. Πιο συγκεκριμένα στον τομέα των δεδομένων, μέσω της μηχανικής εκμάθησης, πολλαπλασιάζονται οι δυνατότητες εξόρυξης γνώσης μέσα από τεράστιες βάσεις δεδομένων και επακολούθως η πραγματοποίηση έγκυρων προβλέψεων βάσει αυτών των πληροφοριών.

---

<sup>15</sup> *Humerick M.*, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, ο.π., σελ. 398

## ΚΕΦΑΛΑΙΟ Β: ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

### 1. Ο ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

#### 1.1. Γενικά

Η ταχύτατη ανάπτυξη της τεχνολογίας κατέστησε εφικτή την δυνατότητα συλλογής και επεξεργασίας τεράστιου αριθμού προσωπικών δεδομένων, κάνοντας με αυτόν τρόπο ακόμα πιο επιτακτική την ανάγκη δημιουργίας ενός σύγχρονου νομοθετήματος, το οποίο θα ανταποκρίνεται στις αυξημένες ανάγκες της εποχής και θα προστατεύει αποτελεσματικά από τους κινδύνους, που διατρέχει η ιδιωτική ζωή και τα προσωπικά δεδομένα των υποκειμένων. Η Ελλάδα, στην προσπάθεια της να αντιμετωπίσει τους εκάστοτε κινδύνους, ψήφισε τον νόμο 2472/1997, εναρμονίζοντας το εθνικό της δίκαιο με την κοινοτική οδηγία 95/46/ΕΟΚ, με τον οποίο ρύθμισε τα σημαντικότερα για την προστασία των προσωπικών δεδομένων, τους δικαιούχους, το επιτρεπτό ή μη της επεξεργασίας, τις πιθανές διοικητικές και ποινικές κυρώσεις κ.α.

Οι όλο και αυξανόμενες προκλήσεις της εποχής μας, ωστόσο, έκαναν φανερή την αδυναμία του προισχύσαντος θεσμοθετημένου νομοθετικού πλαισίου να ανταποκριθεί στις σύγχρονες ανάγκες και σε συνδυασμό με την αναποτελεσματικότητά του, οδήγησαν στην τροποποίησή του. Στις 25 Μαΐου του 2018 τέθηκε σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων (Κανονισμός 2016/679), (στο εξής ΓΚΠΔ ή Κανονισμός), και θεωρείται δεσμευτικός ως προς όλα τα μέρη του.<sup>16</sup> Με τον συγκεκριμένο Κανονισμό, πέρα από την παροχή αποτελεσματικότερης προστασίας, αποσαφηνίστηκαν και πολλά “τυφλά” σημεία της προηγούμενης νομοθεσίας και δόθηκε ιδιαίτερη προσοχή στην πρόληψη εναντίον των κινδύνων και των παρανομιών της επεξεργασίας προσωπικών δεδομένων, αντί για την μετέπειτα καταστολή και τιμώρησή τους.<sup>17</sup> Αυτό επιτεύχθηκε μέσω της πρόβλεψης προληπτικών μέτρων, όπως είναι η μελέτη εκτίμησης αντικτύπου.

Ο ΓΚΠΔ βασίζεται στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων, καθώς και στο άρθρο 16}1 της Συνθήκης για την Λειτουργία της Ευρωπαϊκής Ένωσης,<sup>18</sup> οι οποίες αποτελούν τις νομικές βάσεις για την προστασία των προσωπικών δεδομένων.<sup>19</sup> Υιοθετήθηκε, λοιπόν, ένας Κανονισμός από τα κράτη μέλη, ο οποίος κατισχύει έναντι των εθνικών δικαίων των κρατών μελών και ρυθμίζει κατά συνεκτικό και ομοιόμορφο τρόπο τα προσωπικά δεδομένα των πολιτών. Στο άρθρο 1 του Κανονισμού ορίζεται ως αντικείμενό του η προστασία των φυσικών προσώπων από την επεξεργασία των προσωπικών δεδομένων τους. Ένα από τα σημαντικότερα επιτεύγματα μάλιστα του Κανονισμού ήταν η πρόβλεψη ρυθμίσεων για την προστασία σημαντικών κατηγοριών δεδομένων, όπως τα δεδομένα θέσης, τα επιγραμμικά αναγνωριστικά ταυτότητας

<sup>16</sup> Άρθρο 99 του Κανονισμού

<sup>17</sup> Παναγόπουλου – Κουτνατζή Φ., Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, Εκδόσεις Σάκκουλα, 2017

<sup>18</sup> Ιγγλεζάκης Ι., Δίκαιο Πληροφορικής, 3η Έκδοση, Εκδόσεις Σάκκουλα, 2018

<sup>19</sup> Αιτιολογική Σκέψη 1 του Προοιμίου του Κανονισμού

κ.α.<sup>20</sup>

Όπως αναφέρεται και στις Αιτιολογικές Σκέψεις 6 και 7 του Προοιμίου του Κανονισμού «*οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα*». Πλέον μέσω της τεχνολογίας είναι εφικτή η χρήση και η εκμετάλλευση προσωπικών δεδομένων σε πολύ μεγαλύτερη κλίμακα σε σχέση με το παρελθόν, τόσο από ιδιωτικές επιχειρήσεις, όσο και από δημόσιες αρχές, ενώ και τα ίδια τα υποκείμενα συμβάλλουν σε αυτό το γεγονός μέσω της δημοσιοποίησης τεράστιας ποσότητας προσωπικών πληροφοριών σε παγκόσμια κλίμακα. Στο πλαίσιο αυτό καθίσταται σαφές ότι απαιτείται ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας των δεδομένων, μέσα στο οποίο θα τηρείται αυστηρώς η εφαρμογή της νομοθεσίας και τα υποκείμενα θα διαθέτουν τον έλεγχο των προσωπικών τους δεδομένων, ενισχύοντας την ασφάλεια δικαίου και την ασφάλεια των προσώπων.

Ο στόχος του Κανονισμού είναι να συμβαδίσει με τις σύγχρονες κοινωνικοοικονομικές εξελίξεις, δεδομένου ότι η προισχύσασα Οδηγία 95/46/ΕΟΚ εφαρμοζόταν στην προ της συνταρακτικής και τεράστιας αναπτύξεως του διαδικτύου και των επακόλουθων αλλαγών που επήλθαν στην ανθρωπότητα, περίοδο.<sup>21</sup> Με την ανάπτυξη της τεχνολογίας, λοιπόν, τα αρχαία αντικαταστάθηκαν από σύγχρονες υπολογιστικές συσκευές και συστήματα, όπως αποτελεί και η αποθήκευση δεδομένων στις υπηρεσίες υπολογιστικού νέφους, τα σύγχρονα συστήματα εξόρυξης δεδομένων και εξαγωγής γνώσεως και το λεγόμενο Διαδίκτυο των Πραγμάτων (Internet of Things), καθιστώντας επιτακτική την ανάγκη δημιουργίας και υιοθέτησης ενός νομοθετικού πλαισίου ικανού να εξασφαλίσει την ασφάλεια και προστασία των προσωπικών δεδομένων.

## **1.2. Η Τεχνητή Νοημοσύνη στο πλαίσιο προστασίας του Κανονισμού**

Η Τεχνητή Νοημοσύνη δεν αναφέρεται ρητώς στον Γενικό Κανονισμό Προστασίας Δεδομένων, γίνονται ωστόσο νομοθετικές προτάσεις από την Ευρωπαϊκή Ένωση για να προβλεφθεί ειδικώς, καθώς η έννοια της τεχνητής νοημοσύνης εντάσσεται στο πεδίο εφαρμογής του Κανονισμού.<sup>22</sup> Παρά το γεγονός ότι η τεχνητή νοημοσύνη βρίσκεται πλέον στο επίκεντρο της Ψηφιακής Ενιαίας Αγοράς δεν προβλέπεται σχετική ρύθμιση στο υφιστάμενο νομοθετικό πλαίσιο, πράγμα που ερείδεται στην αδυναμία ρύθμισης των όλο μεταβαλλόμενων, αναπτυσσόμενων και καινοτόμων σχέσεων που δημιουργούνται από τις μεθόδους τεχνητής νοημοσύνης.<sup>23</sup> Το πεδίο εφαρμογής του Κανονισμού επεκτάθηκε από τον Ευρωπαϊκό νομοθέτη περιλαμβάνοντας σε αυτό παρόχους υπηρεσιών νέφους, μηχανές αναζήτησης κ.α., με σκοπό να συμβαδίσει με τις σύγχρονες τεχνολογικές εξελίξεις.<sup>24</sup>

Οι ιδιαιτερότητες του τεχνολογικού περιβάλλοντος ελήφθησαν υπόψιν κατά το σχεδιασμό

---

<sup>20</sup> Γιαννόπουλος Γ., Γενικός Κανονισμός Προστασίας Δεδομένων : Οι νέες υποχρεώσεις και η ευθύνη του Υπεύθυνου Επεξεργασίας, ΕφημΔΔ 2/2017

<sup>21</sup> Μήτρον Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, Εκδόσεις Σάκκουλα, 2017

<sup>22</sup> Humerick M., Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, ο.π., σελ.401

<sup>23</sup> Βόρρας Α./ Μήτρον Α., Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, ο.π., σελ. 460-466

<sup>24</sup> Μήτρον Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ 51-54

της ρυθμιστικής στρατηγικής προστασίας των δεδομένων, ενώ ο ΓΚΠΔ συνειδητά επέλεξε να ακολουθήσει την οδό της τεχνολογικής ουδετερότητας, πράγμα το οποίο διαφαίνεται από την αυστηρή τεχνολογική ορολογία που διαθέτει.<sup>25</sup> Ο Κανονισμός τυγχάνει εφαρμογής, τόσο κατά το στάδιο της ανάπτυξης της τεχνητής νοημοσύνης, όσο και κατά το στάδιο της χρήσης της. Σε όλη την έκτασή του διαφαίνεται η προσπάθεια για προστασία των δεδομένων των υποκειμένων και της ιδιωτικότητας τους γενικά, αλλά και ειδικά από τις εφαρμογές της τεχνητής νοημοσύνης, είτε μέσω της αναγνώρισης σε αυτά πληθώρας δικαιωμάτων (π.χ. ενημέρωσης, εναντίωσης, λήθης κ.α.), είτε με την επιβολή υποχρεώσεων στους υπεύθυνους επεξεργασίας (π.χ. υποχρέωση λογοδοσίας). Πιο συγκεκριμένα οι διατάξεις που αναφέρονται στις αρχές και την νόμιμη βάση της επεξεργασίας, καθώς και στην αυτοματοποιημένη λήψη αποφάσεων εντοπίζονται και στο πλαίσιο εφαρμογής της τεχνητής νοημοσύνης.

Επιπλέον, η επεξεργασία των προσωπικών δεδομένων και τα ίδια τα προσωπικά δεδομένα είναι διατυπωμένα κατά ιδιαιτέρως ευρύ και γενικό τρόπο, ώστε να δεχτούμε ότι μπορεί να συμπεριληφθεί και η επεξεργασία που πραγματοποιείται από συστήματα τεχνητής νοημοσύνης.<sup>26</sup> Ιδιαίτερως, το πεδίο εφαρμογής του άρθρου 2}1 του Κανονισμού, όπου αναφέρεται ότι «*Ο παρών κανονισμός εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης*», προφανώς συμπεριλαμβάνει την επεξεργασία προσωπικών δεδομένων, που πραγματοποιείται από συστήματα τεχνητής νοημοσύνης.<sup>27</sup> Κυριότερα μάλιστα το άρθρο 22 του Κανονισμού και ειδικότερα η αναφορά του σε «*δικαίωμα του υποκειμένου να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας*» είναι εμφανές ότι αναφέρεται σε επεξεργασία, η οποία πραγματοποιείται με την βοήθεια και χρήση τεχνολογιών τεχνητής νοημοσύνης.

Σχετικά με τον προβληματισμό της ένταξης της τεχνητής νοημοσύνης στο πεδίο του Κανονισμού τέθηκε, μάλιστα, ερώτηση στην Ευρωπαϊκή Επιτροπή με θέμα «*Ρύθμιση της τεχνητής νοημοσύνης και πεδίο εφαρμογής του ΓΚΠΔ*». Στην απάντηση, που δόθηκε, προσδιορίστηκε ότι επιδιώκεται, τόσο η συμμόρφωση της τεχνητής νοημοσύνης με τα ανθρώπινα δικαιώματα και τα προσωπικά δεδομένα, όσο και η ανάπτυξη της τεχνολογίας.<sup>28</sup> Προχώρησε μάλιστα η Επιτροπή αναφέροντας ότι παρότι ο Κανονισμός είναι τεχνολογικά ουδέτερος και δεν αφορά ειδικώς την τεχνητή νοημοσύνη, εφαρμόζεται σε πολλές εφαρμογές της τεχνητής νοημοσύνης, ενώ αυτές πρέπει παράλληλα να είναι σύμφωνες με τις αρχές προστασίας των δεδομένων του Κανονισμού.

---

<sup>25</sup> *Mitrou L., Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”*, ο.π., σελ. 26-28

<sup>26</sup> *Mitrou L., ο.π., σελ. 28*

<sup>27</sup> *Genderen R., Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics, 2017*

<sup>28</sup> [https://www.europarl.europa.eu/doceo/document/E-9-2019-002411-ASW\\_EL.html](https://www.europarl.europa.eu/doceo/document/E-9-2019-002411-ASW_EL.html)

## 2. Η ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ

### 2.1. Ορισμός προσωπικών δεδομένων

Στο άρθρο 4 του Κανονισμού ορίζεται η έννοια των δεδομένων προσωπικού χαρακτήρα «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».

Τα προσωπικά δεδομένα τυγχάνουν της διάκρισης σε «απλά» και «ειδικής κατηγορίας» ή αλλιώς «ευαίσθητα» δεδομένα. Ο ορισμός των ευαίσθητων δεδομένων δίδεται στο άρθρο 9 του ΓΚΠΔ και πρόκειται για τα δεδομένα προσωπικού χαρακτήρα, «που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό». Η διάκριση σε απλά και ευαίσθητα δεδομένα έχει πρακτική σημασία, καθώς τα ευαίσθητα δεδομένα πρέπει να λαμβάνουν μεγαλύτερη προστασία και να υφίστανται αυστηρότερες προϋποθέσεις για την επεξεργασία τους, γιατί αφορούν θεμελιώδη δικαιώματα και ελευθερίες των ατόμων.

### 2.2. Οι έννοιες του ταυτοποιημένου και ταυτοποιήσιμου φυσικού προσώπου

Σε αυτό το σημείο είναι απαραίτητη μια σύντομη ανάλυση των όρων ταυτοποιημένο και ταυτοποιήσιμο φυσικό πρόσωπο. Τα δεδομένα, για να είναι δυνατόν να τύχουν προστασίας του Κανονισμού, πρέπει να είναι προσωπικά. Αυτό σημαίνει, ότι πρέπει να είμαστε σε θέση να τα συνδέσουμε είτε με πρόσωπο, το οποίο είναι εξ αρχής ορισμένο, είτε με πρόσωπο του οποίου η ταυτότητα μπορεί να προσδιορισθεί από επιπρόσθετα αναγνωριστικά της ταυτότητας στοιχεία, είναι δηλαδή οριστό.<sup>29</sup> Φυσικά ως πρόσωπα θεωρούνται μόνο τα φυσικά και όχι τα νομικά πρόσωπα.

Όσον αφορά το οριστό, για να μπορέσουμε να προσδιορίσουμε αν ένα πρόσωπο είναι ταυτοποιήσιμο, πρέπει να λάβουμε υπόψιν μας κάθε μέσο, το οποίο μπορεί να χρησιμοποιήσει ο υπεύθυνος επεξεργασίας ή κάποιος τρίτος για να ανακαλύψει την ταυτότητα του υποκειμένου των δεδομένων, κατά άμεσο ή έμμεσο τρόπο.<sup>30</sup> Η έννοια του ταυτοποιήσιμου προσώπου δεν ταυτίζεται απαραίτητως με την δυνατότητα ανεύρεσης του ονόματός του, αλλά και δεδομένα όπως η διεύθυνση e-mail, τα δεδομένα θέσης, η τοποθεσία αλλά και βιομετρικά δεδομένα<sup>31</sup>, όπως η

<sup>29</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2013, Εκδόσεις Νομική Βιβλιοθήκη, σελ. 17-18

<sup>30</sup> Αιτιολογική Σκέψη 26 του Προοιμίου του Κανονισμού

<sup>31</sup> Άρθρο 4}14 του Κανονισμού, Βιομετρικά θεωρούνται «τα δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν

αναγνώριση φωνής και προσώπου, υπάγονται στην έννοια των προσωπικών δεδομένων του Κανονισμού.

Το όνομα αποτελεί μόνο ένα από τα προσδιοριστικά στοιχεία της ταυτότητας του ατόμου και δεν θα πρέπει να παραμερίζουμε και άλλα παρόμοιας σημασίας, όπως οι πολιτικοοικονομικές και κοινωνικές απόψεις, αλλά και τα εξωτερικά χαρακτηριστικά, μέσω των οποίων μπορεί να εξακριβωθεί η ταυτότητα του υποκειμένου. Γίνεται δηλαδή δεκτή μία ευρεία σύλληψη της έννοιας του προσώπου.<sup>32</sup> Σημαντικό είναι να αναφέρουμε, επίσης, ότι η έννοια του ταυτοποιήσιμου αποτελεί μια ευρεία και μεταβλητή έννοια, η οποία προσαρμόζεται και μεταβάλλεται ανάλογα με την τεχνολογία που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας, με τις εξελίξεις της, καθώς και με άλλους αντικειμενικούς παράγοντες, όπως ο χρόνος και το κόστος που απαιτείται για την ταυτοποίηση, παραμέτρους τις οποίες υποχρεούται να λάβει υπόψιν του ο υπεύθυνος επεξεργασίας.<sup>33</sup>

Θεμελιώδης σημασία, λοιπόν, δίδεται στο γεγονός ότι το υποκείμενο των δεδομένων πρέπει να είναι φυσικό πρόσωπο ταυτοποιημένο ή ταυτοποιήσιμο. Είναι σαφές, ότι η έννοια των προσωπικών δεδομένων είναι τόσο ευρεία, ώστε μπορεί να τύχει εφαρμογής και το πεδίο της τεχνητής νοημοσύνης. Σε αυτό προστίθεται και το γεγονός ότι στην έννοια του ταυτοποιήσιμου φυσικού προσώπου εντάσσεται και το πρόσωπο, του οποίου η ταυτότητα μπορεί να προσδιοριστεί αναφορικά με επιγραμμικά αναγνωριστικά. Χαρακτηριστικό επιγραμμικό αναγνωριστικό είναι τα αυτοεγκαθιστώμενα αρχεία cookies, μέσω των οποίων καθίσταται εφικτή η κατάρτιση προφίλ των υποκειμένων και η ανακάλυψη της ταυτότητας και των χαρακτηριστικών της προσωπικότητάς τους. Με την θέσπιση λοιπόν του ΓΚΠΔ ορίστηκε ρητώς ότι επιγραμμικά αναγνωριστικά ταυτότητας (online identifiers), όπως είναι επίσης οι διευθύνσεις διαδικτυακού πρωτοκόλλου (IP address), αποτελούν προσωπικά δεδομένα.<sup>34</sup> Αυτή η καινοτομία ήταν πράγματι απαραίτητη, διότι και μέσω της επεξεργασίας των IP address είναι δυνατή η ανεύρεση της ταυτότητας των υποκειμένων.

### **2.3. Ανώνυμα δεδομένα**

Στην Αιτιολογική Σκέψη 26 του Προοιμίου του Κανονισμού προβλέπεται ότι δεν προστατεύονται οι ανώνυμες πληροφορίες, όσες δηλαδή δεν σχετίζονται προς ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, καθώς και τα δεδομένα προσωπικού χαρακτήρα, που έχουν καταστεί ανώνυμα κατά τρόπο ώστε η ταυτότητα του υποκειμένου των δεδομένων να μην μπορεί να εξακριβωθεί. Το ταυτοποιήσιμο ή όχι του προσώπου με λίγα λόγια αποτελεί προϋπόθεση για την δυνατότητα εφαρμογής του Κανονισμού.

Στα ανώνυμα δεδομένα εντάσσονται και τα απρόσωπα συγκεντρωτικά στοιχεία για στατιστικούς ή ερευνητικούς σκοπούς.<sup>35</sup> Ο όρος «στατιστικοί σκοποί» σημαίνει κάθε πράξη

---

*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 δακτυλосκοπικά δεδομένα»*

<sup>32</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, Εκδόσεις Νομική Βιβλιοθήκη, ο.π., σελ. 26-27

<sup>33</sup> Αιτιολογική Σκέψη 26 του Προοιμίου του Κανονισμού

<sup>34</sup> Μήτρου Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ. 38-47

<sup>35</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 27



συλλογής και επεξεργασίας δεδομένων που απαιτείται για την πραγματοποίηση στατιστικών ερευνών ή για την παραγωγή στατιστικών αποτελεσμάτων. Εξαιτίας του στατιστικού σκοπού, το αποτέλεσμα της εν λόγω επεξεργασίας δεν είναι δεδομένα προσωπικού χαρακτήρα αλλά συγκεντρωτικά δεδομένα και το αποτέλεσμα αυτό ή τα δεδομένα προσωπικού χαρακτήρα δεν χρησιμοποιούνται προς υποστήριξη μέτρων ή αποφάσεων που αφορούν συγκεκριμένο φυσικό πρόσωπο.<sup>36</sup>

#### **2.4. Ανωνυμοποίηση**

Τα ανώνυμα δεδομένα ενδέχεται είτε να είναι ανώνυμα εξ αρχής, να μην αναφέρονται δηλαδή σε κάποιο συγκεκριμένο ταυτοποιήσιμο πρόσωπο, είτε προσωπικά δεδομένα να μετατρέπονται σε ανώνυμα μέσω της τεχνικής της ανωνυμοποίησης.<sup>37</sup> Με τον όρο ανωνυμοποίηση εννοούμε μια ειδική κατηγορία επεξεργασίας προσωπικών δεδομένων, κατά την οποία τα δεδομένα τροποποιούνται με τέτοιο τρόπο, ώστε να παρεμποδιστεί η ταυτοποίηση του υποκειμένου άμεσα ή έμμεσα. Με την χρήση της τακτικής της ανωνυμοποίησης διαγράφεται από τα δεδομένα οποιοδήποτε στοιχείο μπορεί να οδηγήσει στην εξακρίβωση της ταυτότητας των προσώπων (π.χ. όνομα, διεύθυνση κ.α.), αλλά παραμένουν τα υπόλοιπα δεδομένα ώστε να είναι δυνατή η επεξεργασία τους. Με αυτόν τον τρόπο προστατεύεται η ιδιωτικότητα των προσώπων, ενώ παράλληλα διατηρείται και η δυνατότητα εκμετάλλευσης των δεδομένων για οικονομικούς και άλλους σκοπούς. Όπως αναφέραμε και παραπάνω, τα ανώνυμα δεδομένα δεν θεωρούνται προσωπικά δεδομένα και δεν εντάσσονται στο πεδίο εφαρμογής του Κανονισμού.

Τα ανωνυμοποιημένα δεδομένα χρησιμοποιούνται ιδιαίτερα στον τομέα της υγείας για την δυνατότητα διενέργειας κυρίως επιδημιολογικών μελετών, αλλά διαδραματίζουν πολύ σημαντικό ρόλο και στον τομέα της τεχνητής νοημοσύνης. Η ανωνυμοποίηση διευκολύνει τις επιχειρήσεις να αποφύγουν την εφαρμογή του Κανονισμού και να συνεχίσουν να επεξεργάζονται δεδομένα τροφοδοτώντας τα συστήματα τεχνητής νοημοσύνης.<sup>38</sup> Με αυτόν τον τρόπο, αποφεύγεται ο κίνδυνος της παραβίασης του Κανονισμού και των σοβαρών κυρώσεων που αυτός προβλέπει, ενώ προωθείται και η εξέλιξη της τεχνολογίας της τεχνητής νοημοσύνης. Αυτό είναι εύλογο, διότι η ποσότητα των δεδομένων που χρησιμοποιούν τα συστήματα τεχνητής νοημοσύνης επηρεάζει και την αποτελεσματικότητά τους. Βέβαια τα δεδομένα πρέπει να έχουν ανωνυμοποιηθεί επαρκώς και η ταυτοποίηση του υποκειμένου να μην είναι δυνατή, διότι διαφορετικά καλείται σε εφαρμογή ο ΓΚΠΔ. Σημαντικό είναι να τονίσουμε ότι και η ανωνυμοποίηση αποτελεί τρόπο επεξεργασίας και πρέπει να συμβαδίζει με τις γενικές αρχές και ειδικότερα την αρχή του σκοπού.<sup>39</sup>

Η ανωνυμοποίηση και η ψευδωνυμοποίηση, όπως θα δούμε στην συνέχεια, μπορούν να επιτευχθούν με διάφορους τρόπους. Μερικοί από αυτούς είναι η γενίκευση των δεδομένων, η απόκρυψη κ.α. Συγκεκριμένα ως γενίκευση ορίζουμε την τεχνική κατά την οποία τα δεδομένα που αποκαλύπτονται είναι γενικότερα σε σχέση με τα αρχικά προσωπικά δεδομένα καθιστώντας δυσχερή την ταυτοποίηση του προσώπου.<sup>40</sup> Για παράδειγμα, αντί να αναφερθεί ότι ο ασθενής

<sup>36</sup> Αιτιολογική Σκέψη 162 του Προοιμίου του Κανονισμού

<sup>37</sup> <https://www.isico-datenschutz.de/en/ai-gdpr-anonymisation-and-pseudonymisation/>

<sup>38</sup> Ο.π.

<sup>39</sup> *Jougleux P.*, Ευρωπαϊκό δίκαιο του διαδικτύου, Εκδόσεις Σάκκουλα, 2016, σελ. 56-58

<sup>40</sup> <https://www.record-evolution.de/en/data-anonymization-techniques-and-best-practices-a-quick-guide/>

(υποκείμενο των δεδομένων) προέρχεται από μια συγκεκριμένη πόλη, όπου η ταυτοποίηση είναι πιο πιθανή, θα αναφερθεί απλώς η χώρα. Στην απόκρυψη, αντίθετα, αφαιρούνται ολοκληρωτικά τα δεδομένα με την βοήθεια των οποίων μπορεί να επιτευχθεί η εξακρίβωση της ταυτότητας του προσώπου.

Η εξέλιξη της τεχνολογίας, ωστόσο, και ιδιαίτερος η τεχνητή νοημοσύνη φέρνουν προσκόμματα στις προσπάθειες αυτές ανωνυμοποίησης των δεδομένων, κατορθώνοντας σε πολλές περιπτώσεις να ταυτοποιήσουν τα ανώνυμα δεδομένα. Παρότι λαμβάνονται τεχνικά μέτρα από τις επιχειρήσεις, όπως τα κλειδιά κρυπτογράφησης ή η έρευνα της πιθανότητας αποκρυπτογράφησης, για να αποφευχθεί η επανανομαστικοποίηση των δεδομένων, αυτά δεν εμφανίζονται πάντοτε επαρκή για την αντιμετώπιση αυτού του κινδύνου.

## **2.5. Ψευδωνυμοποίηση**

Ο ορισμός της ψευδωνυμοποίησης δίδεται στο άρθρο 4 στοιχείο 5 του Κανονισμού ως «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο». Αντικαθίσταται, δηλαδή, ένα ή περισσότερα αναγνωριστικά της ταυτότητας στοιχεία με ψευδώνυμα, όμως η σύνδεση ανάμεσα στο ψευδώνυμο και τα αναγνωριστικά στοιχεία είναι δυνατόν να επανέλθει με την βοήθεια επιπρόσθετων ξεχωριστών πληροφοριών π.χ. κλειδιών κρυπτογράφησης.

Η ψευδωνυμοποίηση, λοιπόν, διαφέρει από την ανωνυμοποίηση στο γεγονός ότι στην περίπτωση της ψευδωνυμοποίησης δεν αναιρείται τελείως η δυνατότητα εξακρίβωσης της ταυτότητας του υποκειμένου των δεδομένων, απλώς αυτή μπορεί να επιτευχθεί μόνο με την βοήθεια πρόσθετων πληροφοριών. Η σημαντικότερη διαφορά, ωστόσο, έγκειται στο γεγονός ότι τα ψευδωνυμοποιημένα δεδομένα παραμένουν πληροφορίες, που σχετίζονται με ορισμένο ταυτοποιήσιμο πρόσωπο και για αυτόν τον λόγο εντάσσονται στο πεδίο εφαρμογής του Κανονισμού.<sup>41</sup>

Μια χαρακτηριστική τεχνική ψευδωνυμοποίησης αποτελεί η κρυπτογράφηση, κατά την οποία τα δεδομένα μετατρέπονται σε μορφή, η οποία δεν είναι πλέον αναγνώσιμη. Η κρυπτογράφηση γίνεται με την βοήθεια αλγορίθμων κρυπτογράφησης, κατάλληλων για την κάθε περίπτωση ή συνδυασμού πολλών αλγορίθμων μαζί.

Η τεχνητή νοημοσύνη εισήγαγε καινοτομίες στον τομέα της ψευδωνυμοποίησης και ειδικώς στην εξασφάλιση ενισχυμένης προστασίας με την χρήση εξελιγμένων μηχανισμών κρυπτογράφησης και αποκρυπτογράφησης. Μέσω συστημάτων τεχνητής νοημοσύνης είναι πλέον δυνατόν οι επιστήμονες δεδομένων να λάβουν χρήσιμες πληροφορίες από κρυπτογραφημένα δεδομένα, χωρίς να είναι απαραίτητη η αποκρυπτογράφηση τους. Φυσικά αυτή η καινούργια τεχνική είναι ιδιαίτερα χρήσιμη για την επεξεργασία ευαίσθητων δεδομένων, όπως είναι τα δεδομένα υγείας αλλά και τα οικονομικά δεδομένα. Χαρακτηριστικό παράδειγμα αυτής της

---

<sup>41</sup> Λουκάς Η. Ν., Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) - Κρυπτογράφηση και Ψευδωνυμοποίηση, Περιοδικό Συνήγορος, τεύχος 123/2017

καινοτομίας αποτελεί η ομομορφική κρυπτογράφηση. Η ομομορφική κρυπτογράφηση δημιουργήθηκε χάριν της επανάστασης της τεχνητής νοημοσύνης και της μηχανικής εκμάθησης. Με αυτήν την τεχνική οι αλγόριθμοι μηχανικής εκμάθησης τροφοδοτούνται με κρυπτογραφημένα δεδομένα και στην συνέχεια εξάγουν κρυπτογραφημένες πληροφορίες, η αποκρυπτογράφηση των οποίων είναι εφικτή μόνο από τον αρχικό ιδιοκτήτη τους.<sup>42</sup>

## **2.6. Επαναονομαστικοποίηση**

Τα ανώνυμα δεδομένα για να θεωρούνται ως τέτοια και να αποκλίνουν από το πεδίο εφαρμογής του Κανονισμού, θα πρέπει όχι μόνο να μην συνδέονται με ορισμένο πρόσωπο, αλλά η εν λόγω σύνδεση να μην είναι εφικτή, με άλλα λόγια να μην υπάρχει περίπτωση επαναονομαστικοποίησής τους.<sup>43</sup> Με τον όρο επαναονομαστικοποίηση δεδομένων εννοούμε την περίπτωση, κατά την οποία προσωπικές πληροφορίες ανωνυμοποιημένων δεδομένων αποκαλύπτονται και είναι πλέον αναγνώσιμες κατά τέτοιον τρόπο, ώστε να είναι εφικτή άμεσα ή έμμεσα η ταυτοποίηση του υποκειμένου των δεδομένων. Με την χρησιμοποίηση άμεσων αναγνωριστικών αποκαλύπτεται κατευθείαν η ταυτότητα του προσώπου, ενώ με τα έμμεσα απλά αποκαλύπτονται πληροφορίες σχετικά με το άτομο (π.χ. τα ενδιαφέροντά του, τα πιστεύω του κ.α.), βάσει των οποίων αποκαλύπτεται έμμεσα η ταυτότητά του.<sup>44</sup> Το πρόβλημα έγκειται κυρίως στο γεγονός της πρόσθετης πληροφόρησης, κατά πόσον δηλαδή είναι εφικτό κάποιος να κατορθώσει να συνδέσει ανώνυμα δεδομένα με συγκεκριμένο πρόσωπο.<sup>45</sup>

Στην Αιτιολογική Σκέψη 9 του Προοιμίου του Κανονισμού 2018/1807 προβλέπεται ότι «εάν οι τεχνολογικές εξελίξεις καταστήσουν δυνατή τη μετατροπή ανωνυμοποιημένων δεδομένων σε δεδομένα προσωπικού χαρακτήρα, τότε αυτά τα δεδομένα θα αντιμετωπίζονται ως δεδομένα προσωπικού χαρακτήρα και θα εφαρμόζεται αναλόγως ο κανονισμός (ΕΕ) 2016/679». Συγχρόνως αναφέρεται ότι μεγάλες πηγές δεδομένων μη προσωπικού χαρακτήρα είναι το επεκτεινόμενο διαδίκτυο των πραγμάτων, η τεχνητή νοημοσύνη και η εκμάθηση μηχανής. Παρατηρούμε, λοιπόν, ότι αυτό που συμβαίνει στην ουσία είναι ταυτοποιήσιμα χαρακτηριστικά να συνδέονται με μη ταυτοποιήσιμα δεδομένα μετατρέποντάς τα σε προσωπικά δεδομένα.

Κρίσιμο είναι να αναφερθεί ότι για να επιτευχθεί η εν λόγω σύνδεση δεν είναι απαραίτητο να επιτυγχάνεται πλήρης και με απόλυτη βεβαιότητα ταυτοποίηση του υποκειμένου, αλλά αρκεί η ύπαρξη μιας σχετικής πιθανότητας, η οποία μπορεί να οδηγήσει σε διαφορετική και εξατομικευμένη μεταχείριση του ίδιου υποκειμένου.<sup>46</sup> Κατανοούμε, λοιπόν, ότι η έννοια των ανώνυμων δεδομένων είναι σχετική, διότι προκειμένου να διαπιστώσουμε την σύνδεση μιας πληροφορίας με ένα συγκεκριμένο πρόσωπο θα πρέπει να την κρίνουμε *in concreto* και εφαρμόζοντας ουσιαστικά την αρχή της αναλογικότητας, προβαίνοντας σε μια ανάλυση κινδύνου σχετικά με την ταυτοποίηση του υποκειμένου και λαμβάνοντας υπόψιν μας διάφορα κριτήρια,

---

<sup>42</sup> <https://ntokas.gr/anonymous-data/>

<sup>43</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 27

<sup>44</sup> Lubarsky B., Re-identification of “Anonymized data”, 2017, σελ. 208-209

<sup>45</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 28

<sup>46</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit, (STOA), June 2020, σελ. 37

όπως το κόστος και το όφελος της διαδικασίας ονομαστικοποίησης, τα μέτρα ασφαλείας και την κρισιμότητά της για το υποκείμενο.<sup>47</sup>

Διχογνωμία εντοπίζεται αναφορικά με το αν κριτήριο σχετικά με την δυνατότητα εξακριβωσιμότητας του υποκειμένου θα συνιστούν οι ικανότητες και γνώσεις του συγκεκριμένου υπευθύνου επεξεργασίας ή η γενικότερη και αντικειμενική αντίληψη των συναλλαγών.<sup>48</sup> Ωστόσο, αν και αυτή κρίση αποτελεί ζήτημα ερμηνείας, που θα κριθεί στην εκάστοτε περίπτωση, το άρθρο 11}2 του Κανονισμού ορίζει ότι σε περίπτωση που ο υπεύθυνος επεξεργασίας αδυνατεί να εξακριβώσει την ταυτότητα του υποκειμένου απαλλάσσεται από τα καθήκοντα ενημέρωσης του, μετακυλίνοντας το βάρος επίκλησης στο ίδιο το υποκείμενο. Το υποκείμενο, δηλαδή αποστερείται των δικαιωμάτων των άρθρων 15-22 του Κανονισμού, εκτός αν αυτό παράσχει συμπληρωματικές πληροφορίες με σκοπό την εξακρίβωση της ταυτότητάς του.

Η επανανομαστικοποίηση αποτελεί τεράστια απειλή για την ιδιωτικότητα και τα προσωπικά δεδομένα των υποκειμένων, ιδιαίτερα όταν αποκαλύπτονται προσωπικές πληροφορίες και δεδομένα προσώπων από μεγάλες βάσεις δεδομένων. Η εξέλιξη της τεχνολογίας και ιδιαιτέρως η τεχνητή νοημοσύνη διευκόλυνε σε πολύ σημαντικό βαθμό την δυνατότητα επανανομαστικοποίησης ανωνυμοποιημένων δεδομένων, επιτρέποντας σε μη ταυτοποιήσιμα δεδομένα να συνδεθούν με ορισμένα υποκείμενα. Η τεχνητή νοημοσύνη έχει δηλαδή την δυνατότητα ακόμα και σε περιπτώσεις, που η ανωνυμοποίηση των δεδομένων έχει γίνει επαρκώς και με αποτελεσματικό τρόπο να ταυτοποιήσει τα υποκείμενα των δεδομένων.<sup>49</sup> Η ιδιωτική φύση των προσωπικών δεδομένων δεν λογίζεται πλέον ξεχωριστά αλλά θεωρείται ως ένα εννοιολογικό, συγκυριακό χαρακτηριστικό που εντάσσεται σε ένα ευρύτερο πλαίσιο συσχετισμών.

Η επανανομαστικοποίηση των δεδομένων συνήθως επιτυγχάνεται μέσω στατιστικών συσχετισμών μεταξύ μη ταυτοποιημένων δεδομένων και προσωπικών δεδομένων που προέρχονται από τα ίδια υποκείμενα.<sup>50</sup> Μια χαρακτηριστική τεχνική με την οποία κατορθώνεται αυτός ο στόχος είναι ο συνδυασμός δύο διαφορετικών βάσεων δεδομένων.<sup>51</sup> Όταν συνδεθούν δυο βάσεις δεδομένων, τότε είναι δυνατόν να χρησιμοποιηθούν για να εξαχθούν πληροφορίες που θα οδηγήσουν στην ταυτοποίηση των προσώπων. Μία τέτοια περίπτωση καταγράφηκε το 2006 όταν επιστήμονες κατόρθωσαν να επανανομαστικοποιήσουν μια τεράστια ποσότητα ανώνυμων δεδομένων, που περιλαμβάνονταν στην βάση δεδομένων του Netflix συνδυάζοντάς τα με τα δεδομένα, που ήταν αποθηκευμένα στην βάση δεδομένων του Imdb.<sup>52</sup> Στην εν λόγω περίπτωση οι ανώνυμες αξιολογήσεις ταινιών των χρηστών της διαδικτυακής σελίδας της Netflix συνδυάστηκαν με τις επώνυμες αξιολογήσεις, που είχαν πραγματοποιήσει οι χρήστες στην ιστοσελίδα της Imdb, καταλήγοντας στην ταυτοποίηση των προσώπων. Μέσω, δηλαδή, των επώνυμων αξιολογήσεων των χρηστών ήταν εφικτός ο εντοπισμός των αξιολογήσεων των ίδιων χρηστών στην ανώνυμη βάση δεδομένων.

---

<sup>47</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 28

<sup>48</sup> Χριστοδούλου Κ., ο.π., σελ. 29

<sup>49</sup> House of Lords, Select Committee on Artificial Intelligence, AI in the UK: ready, willing and able?, 2018, σελ. 31

<sup>50</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 36-37

<sup>51</sup> Lubarsky B., Re-identification of “Anonymized data”, ο.π., σελ. 211

<sup>52</sup> Lubarsky B., ο.π., σελ. 211- 212

### 3. Η ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΑΝΟΝΙΣΜΟ

#### 3.1. Ορισμός

Η επεξεργασία προσωπικών δεδομένων θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο.<sup>53</sup> Ο ορισμός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα διατυπώνεται στο άρθρο 4 στοιχείο 2 του Κανονισμού ως εξής, επεξεργασία είναι «*κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*». Η διατύπωση του Κανονισμού παρατηρείται ιδιαίτερος ευρεία εκθέτοντας την επιθυμία του νομοθέτη να καλύψει κάθε δυνατή επεξεργασία, που μπορούν να δεχτούν τα δεδομένα από την συλλογή τους μέχρι την καταστροφή τους. Σε έναν τόσο ευρύ, λοιπόν, κατάλογο τρόπων επεξεργασίας δεδομένων συγκαταλέγεται αδιαμφισβήτητα και η επεξεργασία δεδομένων, η οποία πραγματοποιείται από συστήματα τεχνητής νοημοσύνης. Σε περίπτωση υπολογιστικού περιβάλλοντος ως επεξεργασία θεωρείται μάλιστα και η διατύπωση και εκτέλεση ερωτημάτων σε βάσεις και αρχεία δεδομένων, η κατασκευή αντίστοιχων αλγορίθμων αλλά και οι βασικοί τρόποι επεξεργασίας, όπως η αποθήκευση, η διαγραφή δεδομένων, η διασύνδεση κ.α.<sup>54</sup>

Στο άρθρο 2}2 προβλέπεται ρητά ότι από το ουσιαστικό πεδίο εφαρμογής του Κανονισμού εξαιρείται η επεξεργασία δεδομένων προσωπικού χαρακτήρα: «*α) στο πλαίσιο δραστηριότητας η οποία δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της Ένωσης β) από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του κεφαλαίου 2 του τίτλου V της ΣΕΕ γ) από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας, δ) από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, συμπεριλαμβανομένης της προστασίας και πρόληψης έναντι κινδύνων που απειλούν τη δημόσια ασφάλεια*».

Επιπλέον το άρθρο 2, ορίζοντας το πεδίο εφαρμογής του Κανονισμού, προβαίνει σε μία διάκριση μεταξύ αυτοματοποιημένης και μη αυτοματοποιημένης επεξεργασίας. Συγκεκριμένα αναφέρεται, ότι ο Κανονισμός περιλαμβάνει «*την εν όλη ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και τη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης*».<sup>55</sup>

#### 3.2. Αυτοματοποιημένη και μη αυτοματοποιημένη επεξεργασία

Η συμπερίληψη αυτοματοποιημένης και μη αυτοματοποιημένης επεξεργασίας προβλέπεται, όπως αναφέραμε, στο άρθρο 2 του Κανονισμού. Στο άρθρο αυτό προβλέπεται ότι στην περίπτωση

<sup>53</sup> Αιτιολογική Σκέψη 4 του Προοιμίου του Κανονισμού

<sup>54</sup> Παπακωνσταντίνου Ε., Δίκαιο Πληροφορικής, Εκδόσεις Σάκκουλα, 2010, σελ. 78-80

<sup>55</sup> Άρθρο 2 του Κανονισμού

που πραγματοποιείται αυτοματοποιημένη επεξεργασία, αυτό και μόνο αρκεί για να τεθεί σε εφαρμογή ο Κανονισμός προστασίας προσωπικών δεδομένων. Αντίθετα, όταν μιλάμε για μη αυτοματοποιημένη επεξεργασία απαιτείται και άλλο ένα χαρακτηριστικό. Πρέπει τα δεδομένα, τα οποία θα υποστούν μη αυτοματοποιημένη επεξεργασία να περιλαμβάνονται ή να πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Η έννοια της μη αυτοματοποιημένης επεξεργασίας δεν θα μας απασχολήσει στο πλαίσιο της παρούσας εργασίας, για αυτό το λόγο θα δοθεί ένας πολύ σύντομος ορισμός του συστήματος αρχειοθέτησης. Η έννοια του συστήματος αρχειοθέτησης δίδεται στο άρθρο 4 του Κανονισμού στοιχείο 6 ως *«κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατακευματισμένο σε λειτουργική ή γεωγραφική βάση»*. Απαιτείται δηλαδή ένα δομημένο σύνολο ή αρχείο και τα μη διαρθρωμένα στοιχεία δεν επαρκούν.<sup>56</sup> Η ενταξιμότητα σε αρχείο αποτελεί δηλαδή ουσιαστική προϋπόθεση για να είναι δυνατή η εφαρμογή του Κανονισμού στην περίπτωση της μη αυτοματοποιημένης επεξεργασίας.<sup>57</sup> Το διαδίκτυο, μάλιστα έχει κριθεί ότι δεν αποτελεί αρχείο.

### **3.3. Ιδιαίτερος η αυτοματοποιημένη επεξεργασία**

Ως αυτοματοποιημένη επεξεργασία ορίζεται η επεξεργασία, η οποία πραγματοποιείται χωρίς ουσιαστική ανθρώπινη συμβολή με εν μέρει ή πλήρως αυτοματοποιημένα μέσα. Απαιτείται, δηλαδή, η απουσία ουσιαστικής ανθρώπινης παρουσίας, ενώ η συμβολική ανθρώπινη συμβολή δεν αρκεί για να χαρακτηριστεί η επεξεργασία ως μη αυτοματοποιημένη.<sup>58</sup> Η αυτοματοποιημένη επεξεργασία πραγματοποιείται σε ηλεκτρονικό αρχείο.<sup>59</sup> Στην συγκεκριμένη περίπτωση επεξεργασίας δηλαδή εννοούμε ότι η επεξεργασία πραγματοποιείται με την χρήση τεχνολογικών μέσων, όπου η μη αυτοματοποιημένη επεξεργασία μπορεί να αντικατασταθεί. Αυτοματοποιημένα ή τέτοια τεχνολογικά μέσα μπορεί να είναι ένας προσωπικός υπολογιστής, ένα ρούτερ κ.α. Δυστυχώς ο όρος της αυτοματοποιημένης επεξεργασίας δεν αναλύεται επαρκώς στον Κανονισμό, γεγονός που δημιουργεί ανασφάλειες σχετικές με την ορθή εφαρμογή του, αλλά δέχεται και έντονη κριτική.

Στην Αιτιολογική Σκέψη 71 του Προοιμίου αναφέρεται ότι *«σε κάθε περίπτωση, η επεξεργασία αυτή θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνουν ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης, το δικαίωμα διατύπωσης της άποψής του, το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης και το δικαίωμα αμφισβήτησης της απόφασης»*. Η πρόβλεψη αυτής της αιτιολογικής σκέψης αναφέρεται στην αυτοματοποιημένη επεξεργασία και ιδιαίτερα στην κατάρτιση προφίλ. Με αυτήν την διάταξη τονίζεται η ανάγκη παροχής εγγυήσεων ασφαλείας για τα υποκείμενα των δεδομένων και η ανάγκη προστασίας τους.

Ο τρόπος αυτός επεξεργασίας, ο οποίος αναπτύχθηκε μαζί με την εξέλιξη της τεχνολογίας

<sup>56</sup> Jougleux P., Ευρωπαϊκό δίκαιο του διαδικτύου, ο.π., σελ. 47-49

<sup>57</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2013, ο.π., σελ. 28-29

<sup>58</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017

<sup>59</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2013, ο.π., σελ. 28-29

έχει πλήθος πλεονεκτημάτων τόσο στον οικονομικό τομέα, όσο και στον τομέα της αποτελεσματικότητας των τυχόν εργασιών. Πιο συγκεκριμένα μέσω της αυτοματοποιημένης επεξεργασίας ελαχιστοποιούνται τα κόστη των επιχειρήσεων, αλλά περιορίζεται και το ανθρώπινο δυναμικό, το οποίο αντικαθίσταται από τεχνολογικά δημιουργήματα και κατάλληλους αλγορίθμους, που προβαίνουν στην επεξεργασία. Επίσης, στην εποχή των Big Data και της εξόρυξης καθημερινά τεράστιας ποσότητας δεδομένων από υπερμεγέθεις βάσεις δεδομένων, ο αυτοματοποιημένος τρόπος επεξεργασίας καθιστά την επεξεργασία δυνατή και πιο αποτελεσματική.

### **3.4. Τρόποι Επεξεργασίας**

Οι πράξεις που αναφέρονται στο άρθρο 4 είναι ενδεικτικές και περιλαμβάνονται σε ένα «τεχνολογικά ουδέτερο» πεδίο, το οποίο μπορεί να ενταχθεί στις ρυθμίσεις του Κανονισμού.<sup>60</sup> Με τον όρο επεξεργασία, λοιπόν, ενδέχεται να εννοούμε την συλλογή των δεδομένων, η οποία αποτελεί το πρώτο στάδιο της επεξεργασίας και περιλαμβάνει την εύρεση και συγκέντρωση των προσωπικών δεδομένων, την οργάνωση, δηλαδή την κατηγοριοποίηση και ομαδοποίησή τους και την μετέπειτα αποθήκευσή τους σε οποιοδήποτε αποθηκευτικό μέσο. Θεμελιώδους σημασίας είναι η τροποποίηση των δεδομένων, ως τρόπος επεξεργασίας, διότι στην έννοια αυτή περιλαμβάνονται η ανωνυμοποίηση και η ψευδωνυμοποίηση.

Μερικά παραδείγματα επεξεργασίας προσωπικών δεδομένων είναι η αποθήκευση διευθύνσεων IP, η μαγνητοσκόπηση (CCTV), η αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, η δημοσίευση φωτογραφίας ενός ατόμου σε ιστότοπο, η ανάρτηση προσωπικών δεδομένων στο διαδίκτυο κ.α.<sup>61</sup>

---

<sup>60</sup> Μήτρου Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ 38-47

<sup>61</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing\\_el](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_el)

## ΚΕΦΑΛΑΙΟ Γ : Η ΔΥΣΧΕΡΕΙΑ ΤΗΡΗΣΕΩΣ ΤΩΝ ΓΕΝΙΚΩΝ ΑΡΧΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΗΣ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

### 1. Η ΑΡΧΗ ΤΗΣ ΔΙΑΦΑΝΕΙΑΣ ΚΑΙ ΤΗΣ ΛΟΓΟΛΟΣΙΑΣ

#### 1.1. Η αρχή της Διαφάνειας

Η αρχή της διαφάνειας προβλέπεται στο άρθρο 5 } 1α του Κανονισμού, όπου αναφέρεται ότι η επεξεργασία των προσωπικών δεδομένων πρέπει να γίνεται με νόμιμο, θεμιτό και διαφανή τρόπο σε σχέση με το υποκείμενο. Η έννοια της διαφανούς επεξεργασίας διαδραματίζει θεμελιώδη ρόλο στην εξασφάλιση νόμιμης και δίκαιης επεξεργασίας των δεδομένων των υποκειμένων και στην εν γένει προστασία τους. Ο ΓΚΠΔ διαθέτει ποικίλες προκαθορισμένες διατάξεις, που ενσωματώνουν την αρχή της διαφάνειας και οι οποίες είναι στενά συνδεδεμένες με τις έννοιες της πληροφοριακής αυτοδιάθεσης και το κράτος δικαίου.<sup>62</sup>

Η αρχή της διαφάνειας αποτελεί πρωτεύων κανόνας και προκειμένου να ικανοποιηθεί συνδυάζεται με την τήρηση των καθηκόντων ενημέρωσης και πρόσβασης των άρθρων 12 έως 15 του Κανονισμού, στα οποία προβλέπεται το καθήκον του υπευθύνου επεξεργασίας να ενημερώνει το υποκείμενο των δεδομένων σχετικά με το γεγονός της επεξεργασίας.<sup>63</sup> Ο υπεύθυνος επεξεργασίας, δηλαδή, προκειμένου να εξασφαλίσει την τήρηση της αρχής της διαφάνειας, οφείλει να ενημερώσει το υποκείμενο των δεδομένων σχετικά με την πράξη της επεξεργασίας και τον σκοπό της, αλλά να παράσχει και κάθε χρήσιμη και απαραίτητη περαιτέρω πληροφορία, που θεωρείται σημανίσιμη για την συγκεκριμένη περίπτωση και τις ειδικές συνθήκες που ενδέχεται να επικρατούν, για την κατάρτιση προφίλ και τις συνέπειές του κ.α.<sup>64</sup> Οι πληροφορίες αυτές αποσκοπούν στην προστασία του υποκειμένου και την εξασφάλιση μιας δίκαιης και νόμιμης επεξεργασίας και πρέπει να παρέχονται με συνοπτικό, εύκολα προσβάσιμο τρόπο και σε κατανοητή γλώσσα.<sup>65</sup> Αυτή η πρόβλεψη του Κανονισμού καθίσταται εύλογη, διότι είναι αρκετά σύνηθες το υποκείμενο να μην γνωρίζει ότι τα δεδομένα του υπόκεινται σε κάποια μορφή επεξεργασία, ενώ η ανάγκη αυτή εντείνεται στο πλαίσιο της αυτοματοποιημένης επεξεργασίας, εξαιτίας της δυσκολίας ικανοποίησης αυτής της απαίτησης, σε αυτό το πεδίο.

Το υποκείμενο έχει δικαίωμα να πληροφορηθεί μεταξύ άλλων για την κοινολόγηση των δεδομένων του σε άλλους αποδέκτες, ή την τροποποίηση του σκοπού σε περίπτωση που η επεξεργασία γίνεται πλέον για σκοπό διαφορετικό από αυτόν που ίσχυε κατά την συλλογή τους και για κάθε περαιτέρω χρήσιμη πληροφορία. Επίσης πρέπει να λαμβάνει γενικές πληροφορίες, σε περίπτωση που δεν είναι δυνατή η γνωστοποίηση της προέλευσης των δεδομένων, καθώς αυτά προέρχονται από διάφορες πηγές. Όλες αυτές οι πληροφορίες πρέπει να παρασχεθούν κατά την συλλογή των δεδομένων τους ή εντός εύλογης προθεσμίας αν προέρχονται από διαφορετική πηγή

<sup>62</sup> Bayamlioglu E., Transparency of Automated Decisions in the GDPR: An Attempt for systemisation, Tilburg University/ TILT, 2018, σελ. 23

<sup>63</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 110

<sup>64</sup> Αιτιολογική Σκέψη 60 του Προοιμίου του Κανονισμού

<sup>65</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679



πέραν του υποκειμένου των δεδομένων.<sup>66</sup>

Προβλέπεται, βέβαια, εξαίρεση από αυτή την υποχρέωση ενημέρωσης στις περιπτώσεις που η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια (π.χ. σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, επιστημονικής ή ιστορικής έρευνας, στατιστικούς σκοπούς), αλλά και όταν αυτή η ενημέρωση είναι δυνατόν να καταστήσει αδύνατη ή να βλάψει την ικανοποίηση των σκοπών της επεξεργασίας.<sup>67</sup> Επίσης, στις περιπτώσεις που τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά εξαιτίας λόγων επαγγελματικού απορρήτου ή επειδή το υποκείμενο έχει ήδη πληροφορηθεί σχετικώς, είναι δυνατόν να μην εφαρμοστεί αυτή η υποχρέωση ενημέρωσης.<sup>68</sup> Αυτές οι εξαιρέσεις ισχύουν για τις περιπτώσεις που τα δεδομένα δεν έχουν συλλεγεί από το υποκείμενο, ωστόσο μια τέτοια διάκριση δεν φαίνεται εύλογη και θα έπρεπε να εφαρμόζονται και στην περίπτωση, που έχουν συλλεγεί από αυτό.<sup>69</sup>

## **1.2. Η ενημέρωση του υποκειμένου σχετικά με την αυτοματοποιημένη λήψη αποφάσεως**

Ο ΓΚΠΔ προβλέπει, όπως αναφέραμε, γενικώς το δικαίωμα ενημέρωσης των υποκειμένων στα άρθρα 13 και 14 αναλόγως αν τα δεδομένα έχουν συλλεγεί από το υποκείμενο των δεδομένων ή όχι. Πιο ειδικώς ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώνει τα υποκείμενα σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας, τους σκοπούς της επεξεργασίας, τους αποδέκτες, το χρονικό διάστημα αποθήκευσης των δεδομένων, την ύπαρξη δικαιώματος πρόσβασης, διόρθωσης και διαγραφής των δεδομένων τους, την νομική βάση της επεξεργασίας, αν δηλαδή πρόκειται για συμβατική ή νομική υποχρέωση, τις συνέπειες για το υποκείμενο μη παροχής δεδομένων, το δικαίωμα ανάκλησης της συγκατάθεσης, τις κατηγορίες των δεδομένων, την πηγή από όπου προέρχονται τα δεδομένα κ.α.

Σχετικά με την αυτοματοποιημένη επεξεργασία προβλέπεται στο άρθρο 13}2στ και στο άρθρο 14}2ζ, ότι ο υπεύθυνος επεξεργασίας, κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα, παρέχει στο υποκείμενο των δεδομένων πληροφορίες για *«την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων»*.

Διαβλέπουμε, λοιπόν, ότι στην περίπτωση της αυτοματοποιημένης επεξεργασίας, προκειμένου αυτή να επιτευχθεί με νόμιμο και δίκαιο τρόπο, πρέπει ο υπεύθυνος επεξεργασίας κατά την στιγμή της λήψης των δεδομένων να ενημερώσει το υποκείμενο σχετικά με τρία ζητήματα.<sup>70</sup> Πρώτον οφείλει να παράσχει ενημέρωση σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφά-

<sup>66</sup> Αιτιολογική Σκέψη 61 του Προοιμίου του Κανονισμού

<sup>67</sup> Άρθρο 14}5β του Κανονισμού

<sup>68</sup> Άρθρο 14}5α, δ του Κανονισμού

<sup>69</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ 53-54

<sup>70</sup> *Noto La Diega G.*, Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, 2018, σελ. 22-23

σεως και δεύτερον για την λογική που ακολουθείται. Ενώ τέλος, πρέπει να «αναλυθεί» ο αλγόριθμος και να παρασχεθούν πληροφορίες σχετικά με τη σημασία και τις συνέπειες της αυτοματοποιημένης επεξεργασίας. Ο υπεύθυνος υποχρεούται να ενημερώνει ενεργώς και να εφιστά την προσοχή του υποκειμένου και όχι απλά να κάνει διαθέσιμες τις πληροφορίες. Όταν τα δεδομένα δεν συλλέγονται από το υποκείμενο η ανωτέρω περιγραφείσα ενημέρωσή πρέπει να πραγματοποιηθεί εντός εύλογου χρονικού διαστήματος από την συλλογή τους, το οποίο δεν θα ξεπερνά τον ένα μήνα ή την στιγμή της πρώτης επικοινωνίας με το υποκείμενο ή εφόσον προβλέπεται γνωστοποίηση σε άλλον αποδέκτη το αργότερο όταν τα δεδομένα γνωστοποιηθούν για πρώτη φορά.<sup>71</sup>

Ο υπεύθυνος επεξεργασίας έχει καθήκον να ενημερώσει το υποκείμενο, λαμβάνοντας υπόψιν το γεγονός ότι στην πλειονότητα των περιπτώσεων δεν αποτελεί επιστήμονας υπολογιστικών συστημάτων ή ειδικός και επομένως δεν ενδιαφέρεται για τις καθαρώς τεχνικές πληροφορίες, τις λεπτομέρειες και τους μαθηματικούς όρους. Είναι εύλογη, λοιπόν, η πληροφόρηση του υποκειμένου σχετικά με τον αλγόριθμο, την λογική που ακολουθήθηκε και των κριτηρίων που ελήφθησαν υπόψιν, χωρίς την χρήση τεχνικών όρων, αλλά σε απλή και κατανοητή γλώσσα, προσιτή σε αυτό. Στις κατευθυντήριες γραμμές της Ομάδας του άρθρου 29 σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ αναφέρεται ότι δεν είναι πάντοτε απαραίτητη η αποκάλυψη πλήρως του αλγορίθμου ή μια περίπλοκη επεξήγηση των αλγορίθμων που χρησιμοποιήθηκαν, ωστόσο αποσκοπώντας αρχικά στην καλύτερη και πληρέστερη κατανόηση της απόφασεως αλλά και στην δυνατότητα αμφισβητήσεώς της εκ μέρους του υποκειμένου θεωρείται μια τέτοια επεξήγηση και ανάλυση του αλγορίθμου χρήσιμη, ώστε να ικανοποιηθεί το έννομο συμφέρον των υποκειμένων.<sup>72</sup>

Η έννοια των «σημαντικών πληροφοριών» του άρθρου 14}2ζ εκλαμβάνεται σε σχέση με το υποκείμενο των δεδομένων.<sup>73</sup> Η παρέχουσα πληροφόρηση πρέπει να είναι σημαίνουσα και κατανοητή για το υποκείμενο, το οποίο πιθανότατα δεν διαθέτει τις τεχνικές γνώσεις κάποιου ειδήμονα. Το «σημαντικό» των παρεχόμενων πληροφοριών εξαρτάται και από τον βαθμό λειτουργικότητάς τους.<sup>74</sup> Οι πληροφορίες δηλαδή πρέπει να είναι αρκετά λειτουργικές, ώστε να επιτρέπουν και να διευκολύνουν τα υποκείμενα των δεδομένων στην άσκηση των δικαιωμάτων, που τους παρέχει ο Κανονισμός. Αυτή η σκέψη απορρέει από το άρθρο 5 του Κανονισμού, όπου προβλέπονται οι αρχές της επεξεργασίας αλλά και από το άρθρο 12, όπου αναφέρεται ότι ο υπεύθυνος επεξεργασίας πρέπει να διευκολύνει την άσκηση των δικαιωμάτων των υποκειμένων, που προβλέπονται στα άρθρα 15 έως 22. Σημαντικό είναι επίσης να αναφέρουμε ότι η ερμηνεία της συγκεκριμένης έννοιας των «σημαντικών» πληροφοριών πρέπει να είναι ευέλικτη και να μην προβάλλονται αυστηροί μεθοδολογικοί κανόνες, που ενδέχεται να περιορίσουν την έρευνα και την τεχνολογική ανάπτυξη και ειδικότερα την δυνατότητα καινοτομιών και εξελίξεων στους τομείς της μηχανικής εκμάθησης και της τεχνητής νοημοσύνης.<sup>75</sup>

Διαλαμβανομένης της δυσκολίας κατανόησης των περίπλοκων και τεχνικών χαρακτηριστικών της τεχνητής νοημοσύνης, ο υπεύθυνος επεξεργασίας οφείλει να καταβάλλει κάθε εύλογη

---

<sup>71</sup> Άρθρο 14}3α, β, γ, του Κανονισμού

<sup>72</sup> *Noto La Diega G.*, Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, ο.π., σελ. 23

<sup>73</sup> *Selbst D. A., Powles J*, Meaningful information and the right to explanation, Volume 7/ Issue 4, 2017, σελ. 235-236

<sup>74</sup> *Selbst D. A., Powles J*, ο.π., σελ. 236

<sup>75</sup> *Selbst D. A., Powles J*, ο.π., σελ. 236

προσπάθεια προκειμένου να πληροφορήσει όσο το δυνατόν επαρκέστερα και εύληπτα το υποκείμενο των δεδομένων. Τα αλγοριθμικά συστήματα μηχανικής εκμάθησης χαρακτηρίζονται από αδιαφάνεια και λειτουργούν κατά τέτοιο τρόπο ενσωματώνοντας μια ευρεία ροή εργασιών, που ενδέχεται να περιλαμβάνει τη χρήση δεδομένων διαφορετικής προελεύσεως, κυμαινόμενης και επισφαλούς αξιοπιστίας, καθιστώντας απαραίτητη την ανάγκη ευρέσεως λύσεων προκειμένου να αντιμετωπιστούν τα εγγενή προβλήματα τους.<sup>76</sup> Στα προβλήματα αυτά συγκαταλέγεται και η δυσκολία του υπευθύνου επεξεργασίας να προβεί σε σύννομη και θεμιτή επεξεργασία ενημερώνοντας κατάλληλα το υποκείμενο και λογοδοτώντας σχετικά με τις πράξεις του.

### **1.3. Η αρχή της Λογοδοσίας**

Η αρχή της λογοδοσίας απορρέει από την αρχή της διαφάνειας ή μπορεί να θεωρηθεί και ταυτόσημη αυτής και αποτελείται από την υποχρέωση του υπευθύνου επεξεργασίας να λογοδοτεί οποιαδήποτε στιγμή σχετικά με τις πράξεις του και να είναι σε θέση να αποδείξει ότι σέβεται και δεν παραβιάζει τον νόμο, όχι μόνο απέναντι στα υποκείμενα αλλά και απέναντι στην εποπτική αρχή.<sup>77</sup>

Αναφορικά με τα συστήματα τεχνητής νοημοσύνης συναντάμε τον προβληματισμό, δεδομένης της αδιαφάνειας που τα χαρακτηρίζουν, σχετικά με την δυνατότητα των σχεδιαστών και των υπευθύνων επεξεργασίας να λογοδοτούν για τις ενέργειές τους. Με τον όρο της λογοδοσίας, εδώ, εννοείται η ικανότητα να προσδιοριστεί, κατά πόσον η απόφαση και η διαδικασία λήψης της πληροί τα απαραίτητα διαδικαστικά και ουσιαστικά κριτήρια, καθώς και η δυνατότητα απόδοσης ευθύνης στον υπεύθυνο επεξεργασίας, εφόσον αυτά δεν τηρήθηκαν.<sup>78</sup> Οι υπεύθυνοι επεξεργασίας πρέπει να λάβουν υπόψιν τους την σοβαρότητα και την πιθανότητα συνεπειών από την χρήση συστημάτων τεχνητής νοημοσύνης για την επεξεργασία προσωπικών δεδομένων, καθώς δεν μπορεί να θεωρηθεί το ίδιο το σύστημα υπόλογος για την ενδεχόμενη παραβίαση του Κανονισμού, λόγω των αποτελεσμάτων του.<sup>79</sup>

Η αρχή της λογοδοσίας προβλέπεται στο άρθρο 5}2 του Κανονισμού, όπου αναφέρεται, «*ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές που προβλέπονται στην παράγραφο 1 του άρθρου («λογοδοσία»)*» και αποτελεί ιδιαιτέρως σημαντικό στοιχείο, τόσο για την ιδιωτική, όσο και για την δημόσια διακυβέρνηση. Κατανοούμε, λοιπόν, ότι η υποχρέωση λογοδοσίας συνδέεται απαρεγκλίτως με την υποχρέωση του υπευθύνου να ενημερώσει το υποκείμενο σχετικά με την επεξεργασία και την αυτοματοποιημένη λήψη αποφάσεων αλλά και να καταρτίσει μελέτη αντικτύπου.

---

<sup>76</sup> *Noto La Diega G.*, Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, ο.π., σελ. 10

<sup>77</sup> *Χριστοδούλου Κ.*, Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 110

<sup>78</sup> *Doshi-Velez F., Kortz M., Budish R., Bavitz C., Gershman S., O'Brien D., Scott K., Shieber S., Waldo J., Weinberger D., Weller A., Wood A.*, Accountability of AI Under the Law: The Role of Explanation, 2017, σελ. 2

<sup>79</sup> *Hunton Andrews Kurth*, Artificial Intelligence and Data Protection, How the GDPR Regulates AI, Centre for Information Policy Leadership, 2020, σελ. 6-7

## **1.4. Η μελέτη εκτίμησης αντικτύπου**

### **1.4.1. Γενικά**

Στον Κανονισμό εισάγεται ένα ακόμη καθήκον λογοδοσίας και διαφάνειας του υπευθύνου επεξεργασίας, το οποίο περιγράφεται στο άρθρο 35 και ορίζεται ως εκτίμηση αντικτύπου. Με τον όρο αυτόν εννοείται η εκπόνηση μιας μελέτης για την εκτίμηση των επιπτώσεων, που πιθανόν να επέλθουν από τις προβλεπόμενες πράξεις επεξεργασίας. Η εν λόγω μελέτη πραγματοποιείται σαφώς πριν την διενέργεια της επεξεργασίας και κατευθύνεται κυρίως στην προστασία των δικαιωμάτων και των ελευθεριών των ατόμων, τα οποία τίθενται σε υψηλό κίνδυνο από ορισμένα είδη επεξεργασίας. Χαρακτηριστική τέτοια περίπτωση αποτελεί η επεξεργασία, η οποία διενεργείται με την χρήση νέων τεχνολογιών, ενώ πρέπει να ληφθεί υπόψιν και η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας. Η μελέτη εκτίμησης αντικτύπου πρέπει να πραγματοποιείται με την συνδρομή έμπειρων νομικών εξαιτίας της πολυπληθούς αναφοράς νομικών εννοιών.<sup>80</sup>

Το περιεχόμενο της μελέτης αντικτύπου περιγράφεται στην παράγραφο 7 του προαναφερθέντος άρθρου. Μεταξύ άλλων αναφέρεται ότι η μελέτη πρέπει να περιλαμβάνει πληροφορίες σχετικά με τις πράξεις, τους σκοπούς επεξεργασίας, τις πηγές του κινδύνου, καθώς και το έννομο συμφέρον του υπευθύνου επεξεργασίας. Επίσης πρέπει να περιγράφονται τα προβλεπόμενα μέτρα και οι κατάλληλες εγγυήσεις αντιμετώπισης των κινδύνων, καθώς και να εκτιμώνται οι κίνδυνοι των προσωπικών δεδομένων των ατόμων σε μία προσπάθεια ικανοποίησης και σεβασμού των διατάξεων του Κανονισμού. Τέλος αναφέρεται ότι πρέπει να λαμβάνει χώρα εκτίμηση κατά πόσον η συγκεκριμένη επεξεργασία είναι ανάλογη και αναγκαία για την επίτευξη των στόχων της.

Η επεξεργασία αυτή θεωρείται απαραίτητη στις περιπτώσεις που πραγματοποιείται επεξεργασία σε δεδομένα μεγάλης κλίμακας, καθώς τέτοιου είδους δεδομένα συνήθως αποσκοπούν στην επεξεργασία σημαντικής ποσότητας δεδομένων σε εθνικό ή υπερεθνικό επίπεδο, επηρεάζοντας μεγάλο αριθμό υποκειμένων και επιφυλάσσουν πολλούς κινδύνους. Το ίδιο συμβαίνει και στις περιπτώσεις που μία νέα τεχνολογία χρησιμοποιείται σε ευρεία κλίμακα, λαμβανομένων υπόψιν των ολοένα και προοδευτικών τεχνολογικών εξελίξεων, αλλά και όταν παρατηρείται αυτοματοποιημένη επεξεργασία που οδηγεί σε εκτενή και συστηματική αξιολόγηση προσωπικών πτυχών των υποκειμένων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που τα επηρεάζουν σημαντικά ή παράγουν έννομα αποτελέσματα.<sup>81</sup>

Η εν λόγω μελέτη είναι απαραίτητη και στις περιπτώσεις επεξεργασίας μεγάλης κλίμακας δεδομένων «ειδικής κατηγορίας», δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφαλείας, καθώς και για δεδομένα που χρησιμοποιούνται για την παρακολούθηση δημόσια προσπελάσιμων χώρων σε μεγάλη κλίμακα.<sup>82</sup> Η τελευταία κατηγορία αναφέρεται κυρίως στην χρήση οπτικοηλεκτρικών συσκευών ή άλλων εργασιών, που δυσκολεύουν τα υποκείμενα

---

<sup>80</sup> Γιαννόπουλος Γ., Γενικός Κανονισμός Προστασίας Δεδομένων: οι νέες υποχρεώσεις και η ευθύνη του Υπευθύνου Επεξεργασίας, ο.π.

<sup>81</sup> Άρθρο 35}3α του Κανονισμού

<sup>82</sup> Άρθρο 35}3β,γ του Κανονισμού

των δεδομένων στην άσκηση των δικαιωμάτων τους, ή σε επεξεργασία που πραγματοποιείται συστηματικά και σε μεγάλη κλίμακα.

#### **1.4.2. Ειδικά σχετικά με τα συστήματα τεχνητής νοημοσύνης**

Αρχικά πρέπει να γίνει αναφορά στην πρόβλεψη του άρθρου 35 ότι ιδιαίτερος στις περιπτώσεις που πραγματοποιείται επεξεργασία με την χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πραγματοποιεί μελέτη εκτίμησης αντικτύπου. Βέβαια η τεχνητή νοημοσύνη δεν αποτελεί εντελώς νέα τεχνολογία καθώς η έννοια της έχει ανακαλυφθεί ήδη από την δεκαετία του 1950. Ωστόσο, αναλόγως της περιπτώσεως και λαμβάνοντας υπόψιν τον σκοπό, την φύση και το πλαίσιο της επεξεργασίας ενδέχεται να χρησιμοποιείται ορισμένο σύστημα μηχανικής εκμάθησης, για το οποίο κρίνεται κρίσιμο από τον υπεύθυνο επεξεργασίας να διενεργηθεί μελέτη εκτίμησης αντικτύπου προκειμένου να προστατευθούν καταλλήλως και αποτελεσματικώς τα δικαιώματα των υποκειμένων.<sup>83</sup> Το Γραφείο της Επιτρόπου του Ηνωμένου Βασιλείου, Information Commissioner's Office ("ICO"), βέβαια, συγκαταλέγει την τεχνητή νοημοσύνη, την μηχανική εκμάθηση και την βαθιά εκμάθηση, στις καινοτόμες τεχνολογίες, για τις οποίες μπορεί να απαιτηθεί η κατάρτιση μελέτης αντικτύπου.<sup>84</sup> Επιπλέον ρητά προβλέπεται ότι επιβάλλεται μελέτη εκτίμησης αντικτύπου στις περιπτώσεις που υφίσταται αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης και της καταρτίσεως προφίλ, όπου λαμβάνεται μια απόφαση με αντίκτυπο στα έννομα ή άλλα συμφέροντα του υποκειμένου, ύστερα από συστηματική και εκτενή αξιολόγηση των προσωπικών πτυχών του.<sup>85</sup>

Στην περίπτωση που υφίσταται αυτοματοποιημένη επεξεργασία από συστήματα μηχανικής εκμάθησης είναι δυνατόν ο υπεύθυνος επεξεργασίας να δυσκολεύεται να συμμορφωθεί με τον Κανονισμό και να εφαρμόσει τα κατάλληλα οργανωτικά και τεχνικά μέτρα, όπως αυτά προβλέπονται και από το άρθρο 35}7δ του ΓΚΠΔ.<sup>86</sup> Αυτό, μεταξύ άλλων, οφείλεται στο γεγονός, ότι μερικές πτυχές ενός συστήματος μηχανικής εκμάθησης είναι πολύ πιθανόν να μην έχουν σχεδιαστεί ή προβλεφθεί από τον υπεύθυνο επεξεργασίας, πράγμα που επιτείνει την ήδη αδιαφάνεια που τα χαρακτηρίζει. Άλλο ενδεχόμενο είναι ότι τα δεδομένα εισόδου ενδεχομένως προέρχονται από πολλές και διαφορετικές πηγές, ή ότι η όλη διαδικασία λαμβάνει χώρα στο πλαίσιο ενός περιβάλλοντος υπολογιστικού νέφους, όπου περιλαμβάνεται πλήθος παρόχων υπηρεσιών.<sup>87</sup>

Σε αυτήν την προβληματική της αδιαφάνειας εντάσσεται και η δυσκολία του υπευθύνου επεξεργασίας να προσδιορίσει τον εκάστοτε σκοπό της επεξεργασίας. Με αυτόν τρόπο υφίσταται αδυναμία ικανοποίησεως τόσο του άρθρου 35}7α, βάσει του οποίου ο υπεύθυνος επεξεργασίας οφείλει να συμπεριλάβει στην μελέτη εκτίμησης αντικτύπου τους σκοπούς της επεξεργασίας, αλλά και γενικότερα του καθήκοντος ενημέρωσης των άρθρων 13}1γ, 14}1γ, όπου ο υπεύθυνος επεξεργασίας παρέχει πληροφορίες στο υποκείμενο σχετικά με τους σκοπούς της επεξεργασίας.

<sup>83</sup> *Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 13*

<sup>84</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when4>

<sup>85</sup> Άρθρο 35}3α του Κανονισμού

<sup>86</sup> *Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 13-14*

<sup>87</sup> *Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 13-14*

Στην περίπτωση αυτή θα μπορούσαμε να κάνουμε δεκτή την προσπάθεια μιας σταδιακής ειδικότερης ενημέρωσης του υποκειμένου, ανάλογα με την γνώση του υπευθύνου σχετικά με τον μεταβαλλόμενο σκοπό.<sup>88</sup> Εναλλακτικά θα μπορούσαμε να αναλογιστούμε την εφαρμογή της μηδενικής λύσης του περιορισμού της επεξεργασίας (άρθρο 18), εφόσον φυσικά εφαρμόζεται κατά περίπτωση η αρχή της αναλογικότητας, σταθμίζοντας τα κόστη και τα οφέλη της επεξεργασίας.<sup>89</sup> Με αυτόν τον τρόπο θα ζητείται ο περιορισμός της επεξεργασίας που πραγματοποιείται με εφαρμογές τεχνητής νοημοσύνης.

Μερικά μέτρα, τα οποία μπορούν να προβλέπονται στην μελέτη εκτίμησης αντικτύπου για την διασφάλιση της προστασίας των προσωπικών δεδομένων στην συγκεκριμένη περίπτωση, μπορεί να περιλαμβάνουν κατάλληλες συμβατικές υποχρεώσεις των σχεδιαστών των συστημάτων τεχνητής νοημοσύνης και των παρόχων υπηρεσιών, που θα αποκλείουν την χρήση των δεδομένων των υποκειμένων, εκτός αν αυτό είναι απαραίτητο και σύμφωνο με τον Κανονισμό.<sup>90</sup> Επιπλέον, μέσω της μελέτης εκτίμησης αντικτύπου μπορεί να ερευνηθεί και να διασφαλιστεί ότι τα άτομα, που είναι υπεύθυνα για την ανάπτυξη και τον έλεγχο των συστημάτων τεχνητή νοημοσύνης, είναι καταλλήλως εκπαιδευμένα και καταρτισμένα και έχουν προβλέψει ορθώς τις επιπτώσεις της επεξεργασίας, ώστε να αποφευχθούν οι κίνδυνοι και η ανακρίβεια των συστημάτων μηχανικής εκμάθησης.

Βέβαια δεν πρέπει να παραγνωρίζουμε και το γεγονός ότι η τεχνητή νοημοσύνη αποτελεί στην ουσία της μέτρο ασφαλείας, διαφάνειας και λογοδοσίας. Αυτό το γεγονός απορρέει από την σκέψη ότι στην ουσία, μέσω της τεχνητής νοημοσύνης, είναι εφικτή μια πιο ακριβής «*εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων*» του άρθρου 35} 7 γ του Κανονισμού, καθιστώντας την ίσως τον πιο ενδεδειγμένο τρόπο πραγματοποίησης της μελέτης αντικτύπου.<sup>91</sup>

## **2. ΤΟ ΖΗΤΗΜΑ ΤΗΣ ΑΔΙΑΦΑΝΕΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ**

### **2.1. Το πρόβλημα των “Black Boxes”**

Η εφαρμογή της αρχής της διαφάνειας στο πλαίσιο της επεξεργασίας δεδομένων που επιτυγχάνεται με την βοήθεια συστημάτων τεχνητής νοημοσύνης, αποτελεί ένα από τα σημαντικότερα ζητήματα που ανακύπτουν από την χρήση της τεχνητής νοημοσύνης σχετικά με την προστασία των προσωπικών δεδομένων. Ειδικότερα η «αυτόνομη» τεχνητή νοημοσύνη, η οποία είναι αδύνατον να προβλεφθεί ακόμα και από τους πιο εξειδικευμένους επιστήμονες και τους ίδιους τους δημιουργούς της, κατορθώνει σε πολλές περιπτώσεις να ξεπεράσει τους τιθέμενους προγραμ-

---

<sup>88</sup> Χριστοδούλου Κ., Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, ο.π., σελ. 333

<sup>89</sup> Χριστοδούλου Κ., ο.π., σελ. 333

<sup>90</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 13-14

<sup>91</sup> Χριστοδούλου Κ., Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, ο.π., σελ. 332-333

ματισμένους στόχους και να διασπάσει την αιτιώδη σχέση ανάμεσα στον άνθρωπο και στο σύστημα τεχνητής νοημοσύνης.<sup>92</sup>

Πιο συγκεκριμένα στα συστήματα Τεχνητής Νοημοσύνης αποδίδεται ο όρος Black Boxes (Μαύρα Κουτιά), διότι ο τρόπος λειτουργίας τους και το γεγονός ότι για την λήψη απόφασης στηρίζονται σε αλγορίθμους και στατιστικούς συσχετισμούς δεδομένων, καθιστούν ιδιαίτερα δυσχερή έως και ακατόρθωτη την κατανόησή τους, τόσο από τα υποκείμενα, όσο και από τους ίδιους τους δημιουργούς της.<sup>93</sup> Στα νευρωνικά δίκτυα τα δεδομένα εισόδου είναι εφικτό να υποστούν πολύπλοκους και πολλαπλούς μετασχηματισμούς, καθιστώντας το σύστημα ιδιαίτερα περίπλοκο και ικανό να συμπεριφέρεται με απρόβλεπτους τρόπους. Ορισμένοι αλγόριθμοι μηχανικής εκμάθησης έχουν μάλιστα σχεδιαστεί για να συνεχίσουν να μαθαίνουν από νέα δεδομένα κατά τη χρήση, ενώ παράλληλα προβλέπουν και λαμβάνουν υπόψιν τους άγνωστους συσχετισμούς και μεταβλητές.

Έχει διατυπωθεί η διαίρεση της έννοιας των μαύρων κουτιών σε τρεις υποκατηγορίες : στο οργανωτικό πεδίο, στο τεχνικό και στο νομικό.<sup>94</sup> Το οργανωτικό μαύρο κουτί αναφέρεται στην υλοποίηση των αλγορίθμων από ιδιωτικές και κερδοσκοπικές οντότητες, οι οποίες τηρούν ελάχιστες υποχρεώσεις προκειμένου να διασφαλίσουν την αρχή της διαφάνειας. Αναφορικά με το τεχνικό μαύρο κουτί, αναγνωρίζεται η δυσκολία σύλληψης και κατανόησης της λογικής που χρησιμοποιούν τα αλγοριθμικά συστήματα τεχνητής νοημοσύνης και καταλήγουν στην λήψη ορισμένης απόφασης με ακατάληπτο και αδιαφανή τρόπο. Τέλος το νομικό μαύρο κουτί προσδιορίζεται αναφορικά με την προστασία της διανοητικής ιδιοκτησίας.

## **2.2. Λόγοι της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης**

Ύστερα από την αναγνώριση του προβλήματος της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης οφείλουμε να κατευθυνθούμε προς την διερεύνηση των αιτιών της. Μερικοί, λοιπόν, λόγοι, οι οποίοι συμβάλλουν στον χαρακτηρισμό των συστημάτων τεχνητής νοημοσύνης ως Black Boxes, αναφέρονται κατωτέρω και οφείλονται, είτε στον τεχνικό αναλφαβητισμό και την υπολογιστική πολυπλοκότητα των εν λόγω συστημάτων, είτε στον επεμβατικό χαρακτήρα των συστημάτων που χρησιμοποιούν τεχνικές προγνωστικής ανάλυσης, είτε στην εκούσια αδιαφάνεια για λόγους εταιρικού ή κρατικού απορρήτου.<sup>95</sup>

### **2.2.1. Ο τεχνικός αναλφαβητισμός**

Το πρόβλημα αυτό έγκειται αρχικά στο γεγονός ότι τα εγγενή χαρακτηριστικά της τεχνητής

---

<sup>92</sup> Χριστοδούλου Κ., ο.π., σελ. 329

<sup>93</sup> Βόρρας Α. / Μήτρου Α., Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, ο.π., σελ. 460-466

<sup>94</sup> Noto La Diega G., Against the Dehumanisation of Decision-Making /Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, ο.π., σελ. 9-10

<sup>95</sup> Burrell J., How the machine ‘thinks’: Understanding opacity in machine learning algorithms, 2016, σελ. 3-5

νοημοσύνης και των προηγμένων τεχνολογιών που χρησιμοποιεί, την καθιστούν ιδιαίτερος δυσνόητη για τα υποκείμενα των δεδομένων. Αποτελεί πραγματική πρόκληση η παροχή πληροφοριών για την εσωτερική κατάσταση και λειτουργία ενός αλγορίθμου τεχνητής νοημοσύνης στα άτομα σε έναν επαρκώς κατανοητό βαθμό, προκειμένου να επιτύχουν και την προστασία των δεδομένων τους.

Έτσι, βασική αιτία της αδιαφάνειας των αυτοματοποιημένων συστημάτων τεχνητής νοημοσύνης είναι ότι ο σχεδιασμός των εν λόγω συστημάτων και η δημιουργία των αλγοριθμικών κωδίκων τους αποτελεί μια εξειδικευμένη ιδιότητα και γνώση, που είναι ακατάληπτη και άγνωστη για την πλειονότητα του πληθυσμού.<sup>96</sup> Για τον σχεδιασμό ενός αλγορίθμου απαιτείται η γνώση πολυπληθών και πολύπλοκων γλωσσών προγραμματισμού, οι οποίες απαιτούν την εφαρμογή αυστηρών λογικών κανόνων και ιδιαίτερης ακρίβειας, προκειμένου να επιτευχθεί η λειτουργία τους. Όλοι αυτοί οι κώδικες και κανόνες προφανώς είναι ακατανόητοι για τα υποκείμενα των δεδομένων, τα οποία αδυνατούν να κατανοήσουν το πλαίσιο, την έκταση και τα αποτελέσματα της επεξεργασίας των δεδομένων τους.

### **2.2.2. Η υπολογιστική πολυπλοκότητα**

Το πρόβλημα της δυσκολίας διαφάνειας των αυτοματοποιημένων συστημάτων εντείνεται από το γεγονός της λεγόμενης υπολογιστικής πολυπλοκότητας.<sup>97</sup> Οι διαδικασίες που ακολουθούν αυτού του είδους τα συστήματα είναι ιδιαίτερα απρόβλεπτες και χαρακτηρίζονται από μια σημαντικού βαθμού ικανότητα αυτορρύθμισης. Αν και ο σχεδιασμός αυτών των αλγοριθμικών συστημάτων αποτελεί δημιούργημα του ανθρώπινου εγκεφάλου, αυτό δεν εξασφαλίζει την ερμηνεία και την κατανόηση των τρόπων λειτουργίας τους, εξαιτίας της έκτασης και της φύσεως αυτής της ανθρώπινης συμβολής.

Σε αυτό το σημείο, πρέπει να αναφερθεί επίσης το γεγονός ότι οι δημιουργοί των εν λόγω συστημάτων τροποποιούν τακτικά τις ήδη περίπλοκες αυτοματοποιημένες διαδικασίες λήψεως αποφάσεων π.χ. αλλάζοντας τους κανόνες φιλτραρίσματος της ανεπιθύμητης αλληλογραφίας ή των αλγορίθμων των ιστοτόπων που επιλέγουν διαφημίσεις ανάλογα με την συμπεριφορά των εκάστοτε καταναλωτών.<sup>98</sup>

Το ζήτημα της αδιαφανούς επεξεργασίας επιτείνεται, όταν λάβουμε υπόψιν μας ότι υφίστανται συστήματα μηχανικής εκμάθησης, που τροποποιούν και ενημερώνουν το μοντέλο προβλέψεών τους, έπειτα από κάθε ερώτηση, καθιστώντας το εξαιρετικά δύσκολο να διατυπώσουμε έγκυρες και αποτελεσματικές προβλέψεις και να κατανοήσουμε τον τρόπο λειτουργίας του συστήματος, πόσο μάλλον όταν αυτές οι ενημερώσεις πραγματοποιούνται από το ίδιο το σύστημα μηχανικής εκμάθησης.<sup>99</sup>

---

<sup>96</sup> Burrell J., ο.π., σελ. 4

<sup>97</sup> Bayamlioglu E., Transparency of Automated Decisions in the GDPR: An Attempt for systemisation, ο.π., σελ. 17-18

<sup>98</sup> Kroll A. J., Huey J., Barocas S., Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., Accountable Algorithms, University of Pennsylvania Law Review, Vol. 165:633, 2017, σελ. 24-25

<sup>99</sup> Kroll A. J., Huey J., Barocas S., Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., ο.π., σελ. 24-25



Σε αυτήν την κατηγορία εντάσσονται οι αλγόριθμοι διαδικτυακής μάθησης.<sup>100</sup> Ακόμη δηλαδή και αν καταστεί δυνατή η γνώση και κατανόηση του πηγαιού κώδικα και τρόπου λειτουργίας του συστήματος, καθώς και των δεδομένων που το τροφοδότησαν, αυτό δεν αρκεί για την επαρκή πρόβλεψη της συμπεριφοράς του και των αποτελεσμάτων που θα εξάγει. Με τέτοιου είδους συστήματα, λοιπόν, κατανοούμε ότι προστίθεται ένας ακόμα κίνδυνος. Αυτός έγκειται στο ότι η γνώση του αρχικού κώδικα ενδέχεται να είναι ξεπερασμένη και ανακριβής κατά τον χρόνο που θα χρειαστεί αυτός να αναλυθεί, ώστε να μπορέσουμε να ερευνήσουμε την συμπεριφορά του και τα πιθανά αποτελέσματα της επεξεργασίας. Καθώς λοιπόν η «έξυπνη συσκευή» τροποποιεί από μόνη της, χωρίς ανθρώπινη συμβολή, τις παραμέτρους ή ακόμα και τον σκοπό της επεξεργασίας, καθίσταται αδύνατη η ενημέρωση του υποκειμένου από τον υπεύθυνο επεξεργασίας, καθώς και η κατάρτιση «μελέτης αντικτύπου», διότι ακόμα και ο ίδιος αγνοεί τον σκοπό και τα χαρακτηριστικά του συστήματος.<sup>101</sup> Στο πλαίσιο αυτό, χρήσιμη είναι επίσης η αναφορά του γεγονότος, ότι σε πολλές περιπτώσεις οι αλγόριθμοι τεχνητής νοημοσύνης περιλαμβάνουν στον σχεδιασμό τους στοιχεία τυχαιότητας, τα οποία καθιστούν την επεξεργασία και τα αποτελέσματά της ακόμα πιο απρόβλεπτα και ακατάληπτα.<sup>102</sup>

Τα αυτοματοποιημένα συστήματα, λοιπόν, που βασίζονται σε δεδομένα, χαρακτηρίζονται από περίπλοκα, αυτόνομα και ευμετάβλητα στοιχεία, τα οποία μετατρέπουν την τεχνική τους διάσταση και τις εσωτερικές τους λειτουργίες σε ένα πεδίο ακατάληπτο για τους ανθρώπινους χρήστες.<sup>103</sup> Βέβαια στις περιπτώσεις, όπου οι εν λόγω αλγόριθμοι βασίζονται σε ανεπτυγμένες μορφές μηχανικής εκμάθησης είναι πολλές φορές ακατάληπτοι και μη αναγνώσιμοι, όχι μόνο από τα υποκείμενα των δεδομένων, αλλά και από τους ίδιους τους υπευθύνους επεξεργασίας, οι οποίοι δυσκολεύονται ολοένα και συχνότερα να αποκωδικοποιήσουν τους τρόπους λειτουργίας τους και την λογική που ακολουθούν.<sup>104</sup> Ως επακόλουθο αυτής της αδυναμίας κατανόησης, ελέγχου του τρόπου λειτουργίας των εν λόγω συστημάτων και πρόβλεψης των αποτελεσμάτων τους, τα συστήματα αυτά γίνονται απρόσιτα ακόμα και για τον πιο εξειδικευμένο παρατηρητή, δημιουργώντας ιδιαίτερες δυσκολίες αναφορικά με την υποχρέωση λογοδοσίας του υπεύθυνου επεξεργασίας.<sup>105</sup>

### **2.2.3. Η προγνωστική ανάλυση**

Ειδικότερη περίπτωση και σημαντικός παράγοντας που οδήγησε στην επίταση της αδιαφάνειας των συστημάτων αυτοματοποιημένης λήψης αποφάσεων, αποτελεί η εξέλιξη της εξόρυξης δεδομένων (data mining) και της προγνωστικής ανάλυσης (predictive analytics).<sup>106</sup> Στις περιπτώσεις αυτές το πρόβλημα έγκειται στο γεγονός ότι ο ανθρώπινος έλεγχος περιορίζεται μόνο στις

---

<sup>100</sup> Kroll A. J., Huey J., Barocas S., Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H, ο.π., σελ. 24-25

<sup>101</sup> Χριστοδούλου Κ., Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, ο.π., σελ. 333

<sup>102</sup> Kroll A. J., Huey J., Barocas S., Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., Accountable Algorithms, ο.π., σελ. 24

<sup>103</sup> Bayamlioğlu E., Transparency of Automated Decisions in the GDPR: An Attempt for systemisation, ο.π., σελ.17-19

<sup>104</sup> Malgieri G., Comandé G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law, Volume 7/ Issue 4, 2017, σελ. 1-2

<sup>105</sup> Χριστοδούλου Κ., Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, ο.π., σελ. 329

<sup>106</sup> Sloan H. R and Warner R., When Is an Algorithm Transparent?: Predictive Analytics, Privacy, and Public Policy,

αποφάσεις σχεδιασμού, που είναι ενσωματωμένες στον αλγόριθμο προγνωστικής ανάλυσης και σε οποιαδήποτε διαδικασία επανεξέτασης, που ενδεχομένως προκύψει μετά την απόφαση, με αποτέλεσμα ο άμεσος ανθρώπινος έλεγχος να απομακρύνεται από την λήψη της απόφασης.<sup>107</sup>

Η τεχνική της προγνωστικής ανάλυσης αποτελεί μια μορφή προχωρημένης ανάλυσης, η οποία χρησιμοποιεί αλγόριθμους, δεδομένα, τεχνικές μηχανικής εκμάθησης και εξόρυξης δεδομένων και άλλα τεχνικά μορφώματα, προκειμένου να πραγματοποιήσει προβλέψεις για το μέλλον ή για άλλα άγνωστα γεγονότα, κάνοντας χρήση και αναλύοντας ιστορικά και τρέχοντα δεδομένα.<sup>108</sup> Χρησιμοποιείται ευρέως σε διάφορους τομείς, όπως στον τραπεζικό κλάδο με την πρόβλεψη πιστωτικών κινδύνων, στο μάρκετινγκ και στο λιανικό εμπόριο με την πρόβλεψη ενδεχόμενης ζήτησης συγκεκριμένων προϊόντων, στην ασφάλιση και στις τηλεπικοινωνίες κ.α., προβλέποντας τάσεις και πρότυπα συμπεριφοράς, μέσω των εξαγόμενων, από τα δεδομένα, πληροφοριών.

Παρά το πλήθος πλεονεκτημάτων, που απορρέουν από την χρήση τέτοιων τεχνικών, ωστόσο, παρατηρούνται και ορισμένοι κίνδυνοι. Ένας σημαντικός κίνδυνος, εδώ, εντοπίζεται στο γεγονός ότι τα αλγοριθμικά συστήματα προγνωστικής ανάλυσης διαθέτουν επεμβατικό χαρακτήρα κατά μία έννοια. Αυτό συμβαίνει, διότι ακολουθούνται προληπτικές στρατηγικές, κατά τις οποίες τα άτομα οδηγούνται σε συγκεκριμένη συμπεριφορά μέσω της εξάλειψης των ανεπιθύμητων επιλογών, προσβάλλοντας την αυτονομία και τον πληροφοριακό αυτοκαθορισμό των ατόμων.<sup>109</sup>

#### **2.2.4. Η εκούσια αδιαφάνεια για λόγους εταιρικού ή κρατικού απορρήτου**

Τέλος, άλλη μία αιτία της αδιαφάνειας των εν λόγω συστημάτων αποτελεί η ανάγκη μυστικότητας και εμπιστευτικότητας του τρόπου λειτουργίας τους, χάριν της επίτευξης του απώτερου σκοπού των εκάστοτε επιχειρήσεων ή οργανισμών.<sup>110</sup> Δικαιολογείται, δηλαδή, κάποιος βαθμός απόκρυψης των εσωτερικών λειτουργιών των συστημάτων ή άλλων σχετικών οικονομικών, πολιτικών ή νομικών στοιχείων, προκειμένου να διατηρηθεί η ακεραιότητά τους. Έτσι διατηρούν οι εταιρείες τα εμπορικά τους μυστικά και το ανταγωνιστικό πλεονέκτημα, που ενδεχομένως διαθέτουν. Για παράδειγμα, αν ήταν γνωστοί οι παράγοντες και τα στοιχεία, που λαμβάνονται υπόψη για την έρευνα των υπόπτων για τρομοκρατικές επιθέσεις στα αεροδρόμια, τότε οι ύποπτοι θα μετέβαλλαν ακολούθως την στρατηγική και την συμπεριφορά τους. Επίσης χαρακτηριστική περίπτωση αποτελούν οι εφαρμογές διασφάλισης δικτύου, που με την βοήθεια τεχνολογιών μηχανικής εκμάθησης εντοπίζουν περιπτώσεις απάτης (scam), ανεπιθύμητης αλληλογραφίας (spam) κ.α. και για να είναι αποτελεσματικές πρέπει να είναι αδιαφανείς.<sup>111</sup>

Είναι, λοιπόν πολύ συχνή έως και απαραίτητη η απόκρυψη, είτε στοιχείων της διαδικασίας λήψεως της απόφασης, είτε των υπολογιστικών συστημάτων που την ακολουθούν, των κλειδιών

---

vol.16, May/June 2018, σελ. 1-4

<sup>107</sup> Sloan H. R and Warner R., ο.π., σελ. 1-4

<sup>108</sup> [https://en.wikipedia.org/wiki/Predictive\\_analytics](https://en.wikipedia.org/wiki/Predictive_analytics)

<sup>109</sup> Bayamlioğlu E., Transparency of Automated Decisions in the GDPR: An Attempt for systemisation, ο.π., σελ. 18

<sup>110</sup> Bayamlioğlu E., ο.π., σελ. 18

<sup>111</sup> Burrell J., How the machine 'thinks': Understanding opacity in machine learning algorithms, ο.π., σελ.3-4

εισόδου ή των τελικών αποτελεσμάτων.<sup>112</sup> Πέρα από την προσπάθεια αυτή διατήρησης και προφύλαξης του επιχειρησιακού απορρήτου, αντίστοιχη είναι και η προσπάθεια προστασίας έννομων συμφερόντων και μορφωμάτων, μέσω της τήρησης στοιχείων αδιαφάνειας αυτών των συστημάτων, όπως είναι η προστασία των δικαιωμάτων πνευματικής και γενικότερα διανοητικής ιδιοκτησίας.<sup>113</sup>

Η προβληματική που καλούμαστε να επιλύσουμε στο συγκεκριμένο σημείο είναι η εύρεση μιας ενδιάμεσης λύσης αντιμετώπισης του προβλήματος, με την οποία θα εξισορροπούνται τα συμφέροντα της ανάπτυξης της τεχνητής νοημοσύνης και των ιδιαίτερων πλεονεκτημάτων της, αλλά και η τήρηση των αρχών της λογοδοσίας και διαφάνειας.

### 3. Η ΑΡΧΗ ΠΕΡΙΟΡΙΣΜΟΥ ΤΟΥ ΣΚΟΠΟΥ

Η αρχή περιορισμού του σκοπού είναι συνώνυμη με την αρχή της αναλογικότητας, καθώς κρίσιμο στοιχείο για το επιτρεπτό της επεξεργασίας κρίνεται η ύπαρξη ενός σκοπού και η αναλογικότητα της επεξεργασίας προς αυτόν.<sup>114</sup> Η εν λόγω αρχή περιγράφεται στο άρθρο 5 } 1β του Κανονισμού και ορίζει ότι τα προσωπικά δεδομένα πρέπει να «*συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς*». Κατά την συλλογή των δεδομένων πρέπει να υφίσταται ένας προκαθορισμένος και συγκεκριμένος σκοπός επεξεργασίας, ο οποίος να αποκαλύπτεται στα υποκείμενα, προκειμένου να κατορθώσουν τα ίδια να ασκήσουν τα δικαιώματά τους και να προστατεύσουν την ιδιωτικότητά τους. Συνδέεται, μάλιστα, απαρεγκλίτως με την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας, διότι ο υπεύθυνος επεξεργασίας γνωστοποιώντας στα υποκείμενα των δεδομένων τον σκοπό και τους λόγους της επεξεργασίας και μη παρεκκλίνοντας από αυτόν τον σκοπό ικανοποιεί και την υποχρέωση λογοδοσίας του, ενώ συνήθως η παραβίαση της μίας αρχής σημαίνει και την παραβίαση της άλλης.<sup>115</sup>

Παρόλα αυτά ο Κανονισμός εισάγει σημαντικές εξαιρέσεις στην αρχή του περιορισμού του σκοπού, επιτρέποντας αρχικά στον υπεύθυνο επεξεργασίας να προχωρήσει σε περαιτέρω επεξεργασία, εφόσον αυτή γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, χωρίς αυτή η επεξεργασία να θεωρείται ασύμβατη με τους αρχικούς σκοπούς της επεξεργασίας σύμφωνα με το άρθρο 89 } 1.<sup>116</sup> Επιπλέον είναι δυνατή η απομάκρυνση από τον αρχικό σκοπό και η περαιτέρω επεξεργασία για άλλους σκοπούς, εφόσον ληφθούν υπόψιν ορισμένα κριτήρια, τα οποία ελέγχουν την συμβατότητα του αρχικού σκοπού συλλογής των δεδομένων και του περαιτέρω σκοπού. Τέτοια κριτήρια θεωρούνται η σύνδεση μεταξύ των σκοπών, το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα, η σχέση μεταξύ του υποκειμένου και του υπευθύνου, η φύση των δεδομένων, οι πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα, η ύπαρξη κατάλληλων

<sup>112</sup> Kroll A. J., Huey J., Barocas S., Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., *Accountable Algorithms*, ο.π., σελ. 23-24

<sup>113</sup> Bayamlioglu E., *Transparency of Automated Decisions in the GDPR: An Attempt for systemisation*, ο.π., σελ. 18

<sup>114</sup> Χριστοδούλου Κ., *Δίκαιο Προσωπικών Δεδομένων*, 2020, ο.π., σελ. 111

<sup>115</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>

<sup>116</sup> Άρθρο 5 } 1β του Κανονισμού

εγγυήσεων, όπως η κρυπτογράφηση και η ψευδωνυμοποίηση.<sup>117</sup> Τέλος, φυσικά, επιτρέπεται περαιτέρω επεξεργασία για διαφορετικό σκοπό από τον αρχικό, εφόσον έχει συγκατατεθεί το υποκείμενο καταλλήλως.

Στο πεδίο της τεχνητής νοημοσύνης εντοπίζονται αρκετές δυσχέρειες σχετικά με την αρχή του περιορισμού του σκοπού. Αρχικά είναι ιδιαίτερα συνήθης σε αυτό το πλαίσιο ο επανακαθορισμός και ο επαναπροσδιορισμός του σκοπού των δεδομένων.<sup>118</sup> Δεδομένα διαφορετικού τύπου, που έχουν συλλεχθεί για διαφορετικούς σκοπούς είναι δυνατόν να χρησιμοποιούνται από συστήματα τεχνητής νοημοσύνης για την ανάπτυξη και ικανοποίηση των απαιτήσεών της. Είναι δηλαδή δυνατόν, πληροφορίες σχετικές με την δραστηριότητα των υποκειμένων στην διαδικτυακή πλατφόρμα του Facebook να περιλαμβάνονται σε έναν αλγόριθμο, ο οποίος θα προσδιορίσει την πιστοληπτική τους ικανότητα.<sup>119</sup> Κρίσιμο κριτήριο εκτίμησης της νομιμότητας του εν λόγω επαναπροσδιορισμού του σκοπού αποτελεί η συμβατότητα του καινούργιου με τον αρχικό σκοπό συλλογής των δεδομένων.

Από τα κριτήρια αυτά συμβατότητας, που πέρα από το άρθρο 6)4 του Κανονισμού περιγράφονται και στην Αιτιολογική Σκέψη 50 του Προοιμίου, ιδιαίτερο ενδιαφέρον παρουσιάζει το στοιχείο των πιθανών συνεπειών στο υποκείμενο των δεδομένων, σχετικά μάλιστα με τις νέες τεχνολογίες της τεχνητής νοημοσύνης και της μηχανικής εκμάθησης. Αυτό προκύπτει από το γεγονός ότι οι συνέπειες αυτές στα υποκείμενα διαφοροποιούνται αναλόγως αν τα δεδομένα χρησιμοποιούνται ως δεδομένα εισόδου σε ένα σύνολο δεδομένων εκμάθησης ενός αλγορίθμου (training set), ή ως δεδομένα εισόδου σε αλγορίθμους που διενεργούν κατάρτιση προφίλ του συγκεκριμένου ατόμου (profiling algorithms).<sup>120</sup> Στην περίπτωση των δεδομένων που συμπεριλαμβάνονται σε ένα σύνολο δεδομένων εκμάθησης ενός αλγορίθμου, τα αποτελέσματα δεν επηρεάζουν σε σημαντικό βαθμό το συγκεκριμένο υποκείμενο, καθώς αυτά δεν θα έχουν μεγάλη επίδραση σε αυτό στο πλαίσιο ενός αλγορίθμου που περιλαμβάνει μια τεράστια ποσότητα τέτοιων δεδομένων διαφόρων προσώπων. Συνεπώς, εφόσον το υποκείμενο δεν επηρεάζεται άμεσα από την εκμετάλλευση των προσωπικών του δεδομένων και δεν υφίσταται κατάχρηση αυτών, η συμβατότητα μεταξύ του αρχικού και του περαιτέρω σκοπού δεν πρέπει να θεωρείται με μεγάλη αυστηρότητα. Δεν ισχύει όμως το ίδιο στις περιπτώσεις που τα δεδομένα χρησιμοποιούνται ως δεδομένα εισόδου σε ένα αλγοριθμικό μοντέλο, το οποίο θα προβεί σε κατάρτιση προφίλ του υποκειμένου, καταλήγοντας σε συμπεράσματα σχετικά με το ίδιο το υποκείμενο των δεδομένων. Προφανώς σε μια τέτοια περίπτωση το υποκείμενο των δεδομένων επηρεάζεται άμεσα και επομένως τα κριτήρια συμβατότητας πρέπει να ληφθούν υπόψιν πιο σοβαρά και αυστηρά. Βέβαια σε πολλές περιπτώσεις παρατηρείται συνδυασμός της χρησιμοποίησης των δεδομένων για τους εκατέρωθεν προαναφερθέντες σκοπούς.

---

<sup>117</sup> Άρθρο 6)4 του Κανονισμού

<sup>118</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 45-46

<sup>119</sup> Datalisynet, The Norwegian Data Protection Authority, Artificial intelligence and privacy, January 2018, σελ. 16-17

<sup>120</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 45-47

#### 4. Η ΑΡΧΗ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Στο άρθρο 5}1γ του Κανονισμού προβλέπεται ότι τα δεδομένα «είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)». Είναι δηλαδή αναγκαία η χρήση όσο το δυνατόν μικρότερης ποσότητας δεδομένων για την ικανοποίηση του εκάστοτε σκοπού. Η αρχή αυτή σε συνδυασμό με την αρχή περιορισμού του χρόνου επεξεργασίας καθιερώνουν ρητώς την αρχή της αναγκαιότητας ή φειδούς, κατά την οποία η επεξεργασία πρέπει να είναι η απολύτως αναγκαία και λιγότερο επαχθής για το υποκείμενο που μπορεί να οδηγήσει στην επίτευξη του συγκεκριμένου σκοπού, στην εκάστοτε περίπτωση.<sup>121</sup> Εφόσον μάλιστα ο Κανονισμός δεν δίδει σαφείς ορισμούς των σχετικών εννοιών καλούμαστε να κρίνουμε κατά περίπτωση την εφαρμογή της εν λόγω αρχής, πάντοτε σε συνδυασμό με τον σκοπό για τον οποίο συλλέχθηκαν και χρησιμοποιούνται τα δεδομένα.<sup>122</sup> Ο υπεύθυνος επεξεργασίας δεν πρέπει να συλλέγει περισσότερα δεδομένα από αυτά που χρειάζεται, καθώς φέρει ο ίδιος το βάρος απόδειξης της τήρησης της αρχής της αναγκαιότητας.<sup>123</sup>

Όπως έχει ήδη αναφερθεί, η αποτελεσματικότητα και η εξέλιξη των συστημάτων τεχνητής νοημοσύνης εξαρτώνται από την ποσότητα των δεδομένων που έχουν στην διάθεσή τους για επεξεργασία, καθώς μεταξύ άλλων κατορθώνουν με αυτό τον τρόπο να εντοπίσουν διαφορετικούς και νέους συσχετισμούς μεταξύ των δεδομένων. Από μια πρώτη ματιά κατανοούμε, λοιπόν, ότι η αρχή της ελαχιστοποίησης έρχεται σε αντίθεση με τους σκοπούς και την εξέλιξη των μηχανών τεχνητής νοημοσύνης, διότι περιορίζουν την ποσότητα των δεδομένων που τα ίδια διαθέτουν. Επιπλέον οι υπεύθυνοι επεξεργασίας αντιμετωπίζουν δυσχέρειες στην προσπάθειά καθορισμού του σκοπού της επεξεργασίας, εξαιτίας της αδιαφάνειας και του απρόβλεπτου χαρακτήρα των συστημάτων τεχνητής νοημοσύνης, καθώς δεν μπορούν να προβλέψουν πάντοτε τι θα «μάθει» ο αλγόριθμος.<sup>124</sup>

Βέβαια πρέπει να αναλογιστούμε και ορισμένα στοιχεία, τα οποία θα μας βοηθήσουν να εξισορροπήσουμε την εν λόγω αρχή με τα συμφέροντα των μηχανών τεχνητής νοημοσύνης. Αρχικά, όπως αναφέραμε, η αρχή της ελαχιστοποίησης αποτελεί εκδήλωση της αρχής της αναγκαιότητας, η οποία φυσικά συγκροτεί, σε συνδυασμό με την αρχή της *stricto sensu* αναλογικότητας και την αρχή της καταλληλότητας, την αρχή της αναλογικότητας. Κριτήριο δηλαδή αποτελεί κατά πόσον το όφελος από την επεξεργασία υπερτερεί σχετικά με τους κινδύνους που ελλοχεύουν για τα υποκείμενα.<sup>125</sup> Αν λοιπόν αυτό επιτυγχάνεται, τότε η συμπερίληψη πρόσθετων δεδομένων στην συγκεκριμένη επεξεργασία δεν αποκλείεται. Επιτρέπεται μάλιστα, εφόσον τηρούνται ορισμένα μέτρα ασφαλείας των δεδομένων, όπως οι τεχνικές ψευδωνυμοποίησης, και η διατήρηση των δεδομένων για μελλοντική επεξεργασία. Εφόσον ο υπεύθυνος επεξεργασίας μπορεί να το δικαιολογήσει, δικαιούται να διατηρήσει πληροφορίες για ένα επερχόμενο γεγονός, το οποίο ωστόσο μπορεί να μην επέλθει ποτέ.<sup>126</sup>

<sup>121</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 112-113

<sup>122</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>

<sup>123</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 112-113

<sup>124</sup> Mitrou L., Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, ο.π., σελ. 49-50

<sup>125</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 47-48

<sup>126</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>

## 5. Η ΑΡΧΗ ΤΗΣ ΑΚΡΙΒΕΙΑΣ

Η αρχή της ακρίβειας περιγράφεται στο άρθρο 5}1δ του Κανονισμού, κατά την οποία τα δεδομένα «είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· 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». Ο υπεύθυνος επεξεργασίας, δηλαδή, πρέπει να είναι σε θέση να αποδείξει ότι τα δεδομένα που υπάγονται σε επεξεργασία ανταποκρίνονται στην πραγματικότητα.<sup>127</sup> Η αρχή της ακρίβειας εμφανίζεται εξαιρετικά απαραίτητη την σημερινή εποχή, που παρατηρείται ιδιαίτερα αυξημένη συχνότητα και ποσότητα επεξεργασίας προσωπικών δεδομένων, με την δημιουργία παράλληλα πολλών νέων τρόπων επεξεργασίας, αναλογιζόμενοι ότι οι συνέπειες επεξεργασίας πληθώρας ανακριβών δεδομένων θα ήταν καταστροφικές.

Η ακρίβεια των δεδομένων είναι απαραίτητο στοιχείο για την ορθή τροφοδότηση των συστημάτων τεχνητής νοημοσύνης, ιδιαίτερος στις περιπτώσεις, που τα δεδομένα χρησιμοποιούνται για την εξαγωγή συμπερασμάτων σχετικά με τα υποκείμενα, διότι ανακριβή δεδομένα ενδέχεται να βλάψουν σοβαρά τα πρόσωπα.<sup>128</sup> Χαρακτηριστική περίπτωση ανακριβείας των δεδομένων έγκειται, όταν τα δεδομένα, που τροφοδοτούν τον αλγόριθμο, διακρίνονται από μεροληπτικά στοιχεία ή ακόμα και αν αυτά είναι ακριβή, δεν εξασφαλίζουν μια ακριβή επεξεργασία, διότι τα πρόσωπα «υποεκπροσωπούνται» σε ορισμένες περιπτώσεις καταλήγοντας σε ανακριβή συμπεράσματα.<sup>129</sup> Οι υπεύθυνοι επεξεργασίας, λοιπόν, υποχρεούνται να προσέχουν ιδιαίτερος, ώστε το σύνολο των δεδομένων να μην καταστρέφεται από δεδομένα κακής ποιότητας, διότι με αυτόν τον τρόπο τα συμπεράσματα της επεξεργασίας, που πραγματοποιήθηκε από συστήματα τεχνητής νοημοσύνης, θα είναι λανθασμένα και ανακριβή.<sup>130</sup> Δεν πρέπει ωστόσο να αγνοήσουμε το γεγονός ότι η τεχνητή νοημοσύνη μπορεί σε πολλές περιπτώσεις να χρησιμοποιηθεί για την βελτίωση της ακρίβειας των δεδομένων.

## 6. Η ΑΡΧΗ ΠΕΡΙΟΡΙΣΜΟΥ ΤΗΣ ΠΕΡΙΟΔΟΥ ΑΠΟΘΗΚΕΥΣΗΣ

Η αρχή του περιορισμού του χρόνου επεξεργασίας επιβάλλει στον υπεύθυνο επεξεργασίας να προσδιορίζει ακριβώς το χρονικό διάστημα, κατά το οποίο θα αποθηκευτούν τα προσωπικά δεδομένα και εφόσον αυτό δεν είναι δυνατόν, τουλάχιστον τα κριτήρια που καθορίζουν αυτό το διάστημα (άρθ. 13}2α, 14}2α, 15}1δ).<sup>131</sup> Αυτή η αρχή προβλέπεται κυρίως στο άρθρο 5}1ε, κατά

---

gdpr/principles/data-minimisation/

<sup>127</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ.109

<sup>128</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 48

<sup>129</sup> Mitrou L., Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, ο.π., σελ. 51-53

<sup>130</sup> Hunton Andrews Kurth, Artificial Intelligence and Data Protection, How the GDPR Regulates AI, Centre for Information Policy Leadership, 2020, σελ.6

<sup>131</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 112-113

το οποίο τα δεδομένα προσωπικού χαρακτήρα «διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Μετά από αυτό το διάστημα δηλαδή ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα δεδομένα και να σταματήσει την οποιαδήποτε περαιτέρω επεξεργασία και χρησιμοποίησή τους.<sup>132</sup>

Τα προβλήματα εδώ σχετικά με την τεχνητή νοημοσύνη είναι παρόμοια με αυτά της αρχής ελαχιστοποίησης των δεδομένων, καθώς και σε αυτήν την περίπτωση δεν είναι δυνατή περαιτέρω επεξεργασία και είναι σαφές ότι η ποσότητα των δεδομένων βελτιώνει την λειτουργία του αλγορίθμου. Καθώς, λοιπόν, οι αλγόριθμοι μηχανικής εκμάθησης αποκτούν γνώση βάσει των δεδομένων που διαθέτουν και «εκπαιδεύονται» βάσει αυτών, μια ενδεχόμενη διαγραφή επιδρά στην αποτελεσματικότητά τους. Το μειονέκτημα αυτό εκλείπει ωστόσο στις περιπτώσεις, όπου η επεξεργασία πραγματοποιείται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.<sup>133</sup> Στις περιπτώσεις αυτές και εφόσον τηρούνται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων, είναι δυνατόν η αποθήκευση να πραγματοποιηθεί για μεγαλύτερο χρονικό διάστημα.

## 7. Η ΑΡΧΗ ΑΚΕΡΑΙΟΤΗΤΑΣ ΚΑΙ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ

Τα δεδομένα προσωπικού χαρακτήρα βρίσκονται σε ένα ιδιαίτερα επισφαλές περιβάλλον, μέσα στο οποίο ενδέχεται να παραβιαστούν οποιαδήποτε στιγμή, σκόπιμα ή μη. Για τον λόγο αυτό, έχει καθιερωθεί η αρχή της ακεραιότητας και εμπιστευτικότητας στο άρθρο 5}1στ του Κανονισμού, βάσει της οποίας τα δεδομένα «υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων». Οι κίνδυνοι που διατρέχουν τα δεδομένα είναι πολυποίκιλοι, π.χ. πλαστοπροσωπία, και δεν εντοπίζονται αποκλειστικά στο πλαίσιο της κυβερνοασφάλειας.<sup>134</sup> Στο πλαίσιο αυτό κινείται και το άρθρο 32 του Κανονισμού, που προβλέπει ότι ο υπεύθυνος επεξεργασίας οφείλει να υιοθετεί κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να παράσχει ένα επαρκές και κατάλληλο επίπεδο προστασίας και ασφάλειας απέναντι στους εκάστοτε κινδύνους.

Για τους λόγους αυτούς, οι υπεύθυνοι επεξεργασίας και όσοι ασχολούνται με την χρήση τεχνητής νοημοσύνης οφείλουν να λάβουν υπόψιν τους, τους ιδιαίτερους κινδύνους που ελλοχεύουν από την εκμετάλλευση αυτού του είδους της επεξεργασίας και να ανακαλύψουν λύσεις και τρόπους αντιμετώπισης ή μείωσής τους.<sup>135</sup> Η επίταση του κινδύνου, σε αυτές τις περιπτώσεις, έγκειται στο γεγονός ότι, πέραν της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας, είναι δυνα-

<sup>132</sup> Χριστοδούλου Κ., ο.π., σελ. 112-113

<sup>133</sup> Άρθρο 5}1ε του Κανονισμού

<sup>134</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>

<sup>135</sup> Hunton Andrews Kurth, Artificial Intelligence and Data Protection, How the GDPR Regulates AI, ο.π., σελ. 6

τόν τρίτα μέρη, χωρίς να έχουν εξουσιοδοτηθεί σχετικά, να κατορθώσουν να αποκτήσουν πρόσβαση στον αλγόριθμο, μεταβάλλοντας την λογική και τα αποτελέσματά του, με αποτέλεσμα ιδιαίτερα σοβαρές συνέπειες στα υποκείμενα των δεδομένων.<sup>136</sup>

---

<sup>136</sup> *Hunton Andrews Kurth*, ο.π., σελ. 6



## ΚΕΦΑΛΑΙΟ Δ : Η ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ ΑΠΟ ΣΥΣΤΗΜΑΤΑ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ

### 1. Η ΚΑΤΑΡΤΙΣΗ ΠΡΟΦΙΛ (PROFILING)

#### 1.1. Ορισμός

Ο Γενικός Κανονισμός Προστασίας Δεδομένων επιφυλάσσει σε δύο σημεία του σημαντικές διατάξεις σχετικά με την κατάρτιση προφίλ. Αρχικά στο άρθρο 4 στοιχείο 4, όπου περιλαμβάνεται ο ορισμός της έννοιας του profiling και στο άρθρο 22, όπου αναγράφεται η δυνατότητα εναντίωσης του υποκειμένου στην αυτοματοποιημένη λήψη αποφάσεων και ειδικότερα στην κατάρτιση προφίλ.

Στο άρθρο 4 στοιχείο 4 συγκεκριμένα προβλέπεται ότι «κατάρτιση προφίλ»: αποτελεί οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου». Η κατάρτιση προφίλ, λοιπόν, συνίσταται σε δύο στοιχεία: πρέπει να πρόκειται για αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων και με την χρήση των προσωπικών δεδομένων πρέπει να αξιολογούνται ορισμένες προσωπικές πτυχές, που σχετίζονται με ένα φυσικό πρόσωπο. Στην Αιτιολογική Σκέψη 72 του Προοιμίου του Κανονισμού αναφέρεται ρητώς ότι η κατάρτιση προφίλ υπόκειται σε όλους του κανόνες που προβλέπονται στον Κανονισμό, όπως είναι οι νόμιμοι λόγοι επεξεργασίας και οι αρχές προστασίας δεδομένων.

Επίσης στο άρθρο 22 παράγραφος 1 αναφέρεται ότι «το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο». Η αυτοματοποιημένη λήψη αποφάσεως, συμπεριλαμβανομένης της κατάρτισης προφίλ συνδέεται άρρηκτα πλέον με την Τεχνητή Νοημοσύνη, καθώς την σημερινή εποχή αυτού του είδους η επεξεργασία επιτυγχάνεται κατά κύριο λόγο, άλλοτε λιγότερο και άλλοτε περισσότερο, με τη βοήθεια συστημάτων τεχνητής νοημοσύνης.

Η Ομάδα εργασίας του άρθρου 29 της οδηγίας 95/46 έχει δώσει κατευθυντήριες γραμμές σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ, για τους σκοπούς του Κανονισμού 2016/679. Η Ομάδα εργασίας του άρθρου 29 αποτελούσε ένα συμβουλευτικό σώμα, που ενεργούσε με σκοπό την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των προσώπων στην Ευρωπαϊκή Ένωση και διέθετε ανεξαρτησία.<sup>137</sup> Ο στόχος της, μέσω αυτών των κατευθυντήριων γραμμών, ήταν να διευκρινίσει τις σχετικές με την αυτοματοποιημένη λήψη

<sup>137</sup> [https://en.wikipedia.org/wiki/Article\\_29\\_Data\\_Protection\\_Working\\_Party](https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party)

αποφάσεων και την κατάρτιση προφίλ, διατάξεις του Κανονισμού. Συγκροτείται από έναν εκπρόσωπο της Αρχής Προστασίας Δεδομένων κάθε κράτους μέλους της ΕΕ, του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων και της Ευρωπαϊκής Επιτροπής. Πλέον έχει αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB).

Σε μια προσπάθεια επεξήγησης της έννοιας της καταρτίσεως προφίλ, οι κατευθυντήριες αυτές γραμμές προχωρούν σε μία ευρεία διατύπωση του profiling ως αρχικά τη συλλογή πληροφοριών σχετικών με ένα πρόσωπο. Βάσει αυτών των πληροφοριών γίνεται στην συνέχεια προσπάθεια συναγωγής συμπερασμάτων και εκτίμησης χαρακτηριστικών, η οποία μπορεί να οδηγήσει στην κατηγοριοποίηση του προσώπου σε μια συγκεκριμένη ομάδα. Μέσω της κατάρτισης προφίλ θα είναι δυνατή η πιθανή πρόβλεψη της συμπεριφοράς του ατόμου, των προτιμήσεών του και των ενδιαφερόντων του.

## **1.2. Υποκατηγορίες και χρησιμότητα της καταρτίσεως προφίλ**

Το profiling μπορεί να διακριθεί σε περισσότερες υποκατηγορίες αναλόγως του αν είναι ατομικό ή ομαδικό, άμεσο ή έμμεσο.<sup>138</sup> Το ομαδικό profiling αναγνωρίζει μια ομάδα ατόμων, τα οποία συνήθως μοιράζονται ένα ή μερικά κοινά χαρακτηριστικά. Αντίθετα, στο ατομικό profiling συλλέγονται πληροφορίες γύρω από ένα συγκεκριμένο πρόσωπο, οι οποίες χρησιμοποιούνται για τον σκοπό της πρόβλεψης άλλων άγνωστων χαρακτηριστικών ή μελλοντικών συμπεριφορών του ατόμου.

Το ομαδικό και το ατομικό profiling μπορούν εξ ίσου να διενεργηθούν με άμεσο ή έμμεσο τρόπο. Αναφορικά με το άμεσο profiling, αυτό στηρίζεται στην επεξεργασία δεδομένων, τα οποία συλλέχθηκαν από το υποκείμενο και αποσκοπεί στην εξαγωγή συμπερασμάτων σχετικά με αυτό και στη διατύπωση μελλοντικών προβλέψεων. Αντίθετα, στο έμμεσο profiling χρησιμοποιούνται δεδομένα, τα οποία προέρχονται από μεγαλύτερο εύρος πληθυσμών και ατόμων και βασίζεται στα χαρακτηριστικά που έχουν εξαχθεί από αυτούς τους πληθυσμούς. Ένα χαρακτηριστικό παράδειγμα αυτής της περίπτωσης είναι τα συστήματα που προτείνουν στα υποκείμενα αγαθά (π.χ. προτάσεις μουσικής, ταινιών κ.α.) βασιζόμενο στις προτιμήσεις και στο ιστορικό αγορών και ενδιαφερόντων άλλων προσώπων.<sup>139</sup>

Η κατάρτιση προφίλ εμφανίζεται χρήσιμη σε πληθώρα τομέων, παράγοντας γνώση και εξάγοντας συμπεράσματα σχετικά με τα υποκείμενα και την συμπεριφορά τους.<sup>140</sup> Μερικοί τομείς, στους οποίους διαδραματίζει εξέχοντα ρόλο είναι ο οικονομικός τομέας, όπου το profiling χρησιμοποιείται για τον εντοπισμό ύποπτων οικονομικών συναλλαγών, ξεπλύματος χρήματος και φορολογικής απάτης, αλλά και στο marketing (προώθηση αγαθών), όπου κατορθώνουν οι επιχειρήσεις να δημιουργούν στοχευμένες διαφημίσεις αναλόγως του καταναλωτικού κοινού στο οποίο απευθύνονται, αυξάνοντας την αποτελεσματικότητα των δραστηριοτήτων τους. Κυρίαρχη εμφανίζεται η θέση του profiling και στον τομέα της υγείας, καθώς επιτυγχάνεται αυξημένη αποτελεσματικότητα στις ιατρικές θεραπείες και κυρίως στον τομέα της προληπτικής ιατρικής. Τέλος στον τομέα της εργασίας, μπορεί να χρησιμοποιηθεί για την ανάπτυξη της αποτελεσματικότητας της

<sup>138</sup> Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y., Defining profiling, 2013, σελ. 6-7

<sup>139</sup> Data is power: Profiling and Automated Decision-Making in GDPR, (privacyinternational.org), 2017, σελ. 3

<sup>140</sup> Ferraris V., Bosco F., Cafiero G., D'Angelo E., Suloyeva Y., Defining profiling, ο.π., σελ. 21-31

δράσης των εργαζομένων και την πρόληψη παράνομων συμπεριφορών τους.

### **1.3. Το profiling ως τρόπος επεξεργασίας**

Οι κατευθυντήριες γραμμές του άρθρου 29, μεταξύ άλλων, αναφέρουν ότι «η κατάρτιση προφίλ αποτελείται από τρία στοιχεία : πρέπει να είναι αυτοματοποιημένη μορφή επεξεργασίας, πρέπει να αφορά δεδομένα προσωπικού χαρακτήρα και ο στόχος της κατάρτισης προφίλ πρέπει να είναι η αξιολόγηση προσωπικών πτυχών ενός φυσικού προσώπου». Συνεχίζει μάλιστα, προβλέποντας ότι «το άρθρο 4 στοιχείο 4 του Κανονισμού αναφέρεται σε οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας αντί σε «αποκλειστικά» αυτοματοποιημένη επεξεργασία (αναφέρεται στο άρθρο 22)». Σύμφωνα με το άρθρο 4}4 λοιπόν το profiling δεν απαιτείται να γίνεται αποκλειστικά με αυτοματοποιημένο τρόπο, αλλά πρέπει να διαθέτει κάποια μορφή αυτοματοποιημένης επεξεργασίας, χωρίς να αποκλείεται η παρουσία ανθρώπινης συμβολής. Στο πλαίσιο της παρούσας διπλωματικής θα επικεντρωθούμε στην αυτοματοποιημένη επεξεργασία που πραγματοποιείται από συστήματα τεχνητής νοημοσύνης.

Το profiling στην πραγματικότητα αποτελεί μια προσπάθεια εξεύρεσης συσχετισμών μεταξύ δεδομένων.<sup>141</sup> Αν επιτευχθεί αυτή η προσπάθεια, τότε δημιουργούνται μορφότυποι - δηλαδή προφίλ- οι οποίοι μπορούν να συσχετισθούν με άλλα δεδομένα και να οδηγήσουν στην κατάταξη του συγκεκριμένου υποκειμένου των δεδομένων σε μια κατηγορία.<sup>142</sup> Μέσω αυτής της αυτοματοποιημένης επεξεργασίας, αντιστοιχείται το συγκεκριμένο προφίλ, που δημιουργήθηκε, με ένα πρόσωπο, με απώτερο σκοπό την ανάλυση της συμπεριφοράς του και την εξαγωγή συμπερασμάτων.

Είναι κατανοητό, λοιπόν, ότι η κατάρτιση προφίλ αποτελεί μια μορφή επεξεργασίας προσωπικών δεδομένων και μπορεί να περιλαμβάνει διάφορους στόχους.<sup>143</sup> Αρχικά, ενδέχεται να διεξάγεται profiling για να εξαχθούν πληροφορίες από τα δεδομένα, οι οποίες θα σχετίζονται με τα ενδιαφέροντα, την προσωπικότητα του υποκειμένου κ.α. Χαρακτηριστικό παράδειγμα αποτελεί η εξαγωγή πληροφοριών σχετικά με την κοινωνικοοικονομική κατάσταση των υποκειμένων από τα δεδομένα των κινητών τους τηλεφώνων (αρχεία κλήσεων, τοποθεσία κ.α.). Επιπλέον είναι εφικτό μέσω του profiling να βαθμολογηθούν, καταταχθούν ή αξιολογηθούν τα υποκείμενα, καθώς και να ληφθούν αποφάσεις σχετικές με αυτά. Τα υποκείμενα, δηλαδή, κατηγοριοποιούνται μέσω του profiling με βάση συγκεκριμένα πρότυπα συμπεριφοράς και ελέγχεται κατά πόσον αποκλίνουν από αυτά τα πρότυπα. Τα σημεία αναφοράς που θα επιτύχουν την εν λόγω κατάταξη ενδέχεται να ελέγχονται και σιωπηρά μέσα από τεχνολογίες ανίχνευσης ανωμαλιών. Τέλος, μπορεί να διενεργείται κατάρτιση προφίλ για να ληφθούν αποφάσεις που θα προσωποποιούν το περιβάλλον ενός υποκειμένου.

Στην πράξη στην περίπτωση της κατάρτισης προφίλ χρησιμοποιούνται κατά κόρον οι σύγχρονες μέθοδοι της τεχνητής νοημοσύνης και της εξόρυξης δεδομένων. Θα μπορούσαμε μάλιστα να διακρίνουμε την διαδικασία του profiling σε τρία στάδια, όπου ένα θα αποτελεί η συλλογή των δεδομένων των εκάστοτε προσώπων, ένα θα αφορά την δημιουργία και ανάπτυξη του μοντέλου

---

<sup>141</sup> Μήτρου Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ. 128-131

<sup>142</sup> Μήτρου Α., ο.π., σελ. 128-131

<sup>143</sup> Data is power: Profiling and Automated Decision-Making in GDPR, σελ. 4-6

επεξεργασίας, το οποίο θα λειτουργεί με την χρήση αλγορίθμων τεχνητής νοημοσύνης και το τελευταίο θα είναι η αυτοματοποιημένη λήψη της απόφασης.<sup>144</sup>

#### **1.4. Η χρήση αλγορίθμων τεχνητής νοημοσύνης για την κατάρτιση προφίλ**

Η τεχνητή νοημοσύνη σε συνδυασμό με τα Big Data έχουν αυξήσει σε τεράστιο βαθμό την ευχέρεια καταρτίσεως προφίλ. Η γνώση και οι πληροφορίες που εξάγουμε μέσω της κατάρτισης προφίλ μπορεί να προκύψουν από δεδομένα, που έχουν τύχει επεξεργασίας μέσα σε ένα τεράστιο πλαίσιο αυτοματοποιημένων τεχνικών, όπως είναι η προηγμένη μορφή επεξεργασίας των υπολογιστικών αλγορίθμων μηχανικής εκμάθησης.

Συγκεκριμένα οι τεχνικές μηχανικής εκμάθησης, επεξεργάζοντας δεδομένα προσωπικού χαρακτήρα, μπορούν να οδηγήσουν στην εξαγωγή συμπερασμάτων, προβλέψεων και αποφάσεων.<sup>145</sup> Στην πραγματικότητα αυτό που επιτυγχάνεται είναι η δημιουργία ενός συστήματος, το οποίο λειτουργεί βάσει ενός αλγοριθμικού μοντέλου, που πραγματοποιεί συσχετισμούς βάσει των δεδομένων που διαθέτει, συνδέοντας τα δεδομένα με συγκεκριμένα χαρακτηριστικά και προβλέποντας με αυτόν τον τρόπο μελλοντικούς τρόπους συμπεριφοράς, είτε του ίδιου ατόμου, είτε άλλων ατόμων με παρόμοια χαρακτηριστικά συμπεριφοράς.

Στο σημείο αυτό χρήσιμο είναι ένα παράδειγμα για να κατανοήσουμε πως λειτουργεί ένα αλγοριθμικό μοντέλο μηχανικής εκμάθησης στην κατάρτιση προφίλ. Ας υποθέσουμε, για παράδειγμα, ένα σύστημα το οποίο «μαθαίνει» βάσει συσχετισμών ανάμεσα στις δραστηριότητες του ατόμου (π.χ. τις αγορές του) και του προφίλ του ως συγκεκριμένου τύπου καταναλωτή.<sup>146</sup> Με την δημιουργία αυτού του συσχετισμού κατανοούμε ότι αυτή η συγκεκριμένη κατηγορία καταναλωτή ενδιαφέρεται για συγκεκριμένα προϊόντα και είναι πιθανόν να αντιδράσει σε διαφημίσεις αυτού του τύπου. Συνεπώς κατανοούμε ότι ένα άτομο, που διαθέτει τα ίδια χαρακτηριστικά, είναι πολύ πιθανόν να αντιδράσει με αντίστοιχο τρόπο σε διαφημίσεις αυτού του είδους, προβαίνοντας σε ανάλογη καταναλωτική συμπεριφορά.

Οι αλγόριθμοι τεχνητής νοημοσύνης τροφοδοτούνται αρχικά με δεδομένα και έπειτα προβαίνουν στην κατάλληλη επεξεργασία τους. Όσο μεγαλύτερη εισροή δεδομένων παρατηρείται, τόσο πιο αποτελεσματική είναι η επεξεργασία τους και σε τόσο πιο ακριβή και ορθά συμπεράσματα καταλήγουμε. Μέσω αυτών των δεδομένων, τα οποία παρέχονται, είτε από τον υπεύθυνο επεξεργασίας, είτε από τρίτο μέρος, εφοδιάζονται κατάλληλα οι εν λόγω αλγόριθμοι οδηγώντας στην δημιουργία ενός προφίλ. Σε αυτό το πλαίσιο η τεχνητή νοημοσύνη έχει συμβάλει δραστικά, μεγιστοποιώντας την ικανότητα συλλογής προσωπικών δεδομένων, με την χρήση κατάλληλων αισθητήρων.<sup>147</sup> Υπάρχουν πολλά τέτοια παραδείγματα, κατά τα οποία μέσω συστημάτων μηχανικής εκμάθησης συλλέγονται πληροφορίες για τα ενδιαφέροντα και την συμπεριφορά των υποκει-

<sup>144</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 8-11

<sup>145</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 39-40

<sup>146</sup> European Parliament, ο.π., σελ. 39-40

<sup>147</sup> <https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoietai>

μένων. Μερικά από αυτά είναι πληροφορίες που εξάγονται από βιντεοκάμερες και κάμερες παρακολούθησης, σήματα GPS, το Wifi, κινητά τηλέφωνα, κ.α.<sup>148</sup>

Η όλο και αυξανόμενη χρήση καμερών βιντεοσκοπήσης, στο πλαίσιο της βιντεοεπιτήρησης, για την παρακολούθηση των ατόμων και των συμπεριφορών τους, αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα.<sup>149</sup> Οι κάμερες παρακολούθησης (CCTV cameras), δηλαδή, χρησιμοποιούν αισθητήρες, ικανούς να συλλέξουν τεράστια ποσότητα δεδομένων, ανιχνεύοντας συμπεριφορές και κινήσεις ατόμων και καταλήγοντας σε συμπεράσματα βάσει αυτών. Το ογκώδες και αυξανόμενο σε καθημερινή βάση υλικό και τα δεδομένα, τα οποία συλλέγονται από τις εν λόγω βιντεοκάμερες αναλύεται και επεξεργάζεται από κατάλληλες υπολογιστικές μηχανές, που χρησιμοποιούν τεχνικές τεχνητής νοημοσύνης και ειδικώς τεχνολογίες βαθιάς μηχανικής εκμάθησης. Αυτό είναι κατανοητό, αν δεχτούμε ότι οι απαιτήσεις σε χρόνο διεκπεραίωσης και σε ποσότητα υλικού δεδομένων είναι τόσο μεγάλη, που καθιστά σχεδόν αδύνατο την συγκεκριμένη επεξεργασία να την υλοποιήσουν άτομα ή ομάδες ατόμων, προκειμένου μάλιστα να προβούν στην εξαγωγή συμπερασμάτων συμπεριφοράς και χαρακτηριστικών των ατόμων, στην αναγνώριση προτύπων και στην διατύπωση μελλοντικών προβλέψεων.

Η ολοένα και αυξανόμενη διενέργεια καταρτίσεως προφίλ με τη βοήθεια συστημάτων τεχνητής νοημοσύνης καθιστά αναγκαία την πρόβλεψη ορισμένων εχέγγυων προστασίας των υποκειμένων με σκοπό την αποσόβηση των ενδεχόμενων κινδύνων. Φυσικά κατά την διενέργεια καταρτίσεως προφίλ απαιτείται η τήρηση των γενικών αρχών επεξεργασίας του Κανονισμού, καθώς αυτή πρέπει να γίνεται κατά νόμιμο, θεμιτό και διαφανή σε σχέση με το υποκείμενο τρόπο.<sup>150</sup> Τα σημαντικότερα προσκόμματα εντοπίζονται στο στοιχείο της διαφάνειας, καθώς η κατάρτιση προφίλ και γενικότερα η αυτοματοποιημένη λήψη αποφάσεων χαρακτηρίζεται από αδιαφάνεια όταν διενεργείται από συστήματα τεχνητής νοημοσύνης, αλλά και του θεμιτού της επεξεργασίας, λόγω της ενδεχόμενης μεροληψίας των αλγοριθμικών συστημάτων τεχνητής νοημοσύνης.

## **2. ΟΙ ΚΙΝΔΥΝΟΙ ΤΗΣ ΚΑΤΑΡΤΙΣΕΩΣ ΠΡΟΦΙΛ**

### **2.1. Αδιαφάνεια και παραβίαση ιδιωτικότητας**

Στην σύγχρονη εποχή της τεχνολογικής εξέλιξης είναι αδύνατον τα υποκείμενα να γνωρίζουν και να ελέγχουν την ποσότητα των δεδομένων τους, που τυγχάνει επεξεργασίας από πλήθος διαφορετικών οντοτήτων.<sup>151</sup> Ένας τεράστιος όγκος προσωπικών δεδομένων αποθηκεύεται, κοινοποιείται, χρησιμοποιείται με την εκμετάλλευση ολοένα και πιο εξελιγμένων τεχνολογικών μέσων με σκοπό την κατάρτιση προφίλ των ατόμων. Τα υποκείμενα, μέσα σε αυτό το πλαίσιο, αγνοούν εντελώς ότι υφίστανται profiling, τις ενδεχόμενες συνέπειές του ή το μέγεθος και το είδος των πληροφοριών που μπορούν να αποκαλυφθούν μέσω αυτού, θέτοντας σε κίνδυνο την ιδιωτικότητα

<sup>148</sup> Yang Q., Activity Recognition: Linking Low-level Sensors to High-level Intelligence, Department of Computer Science and Engineering, Hong Kong University of Science and Technology, 2009, σελ. 20-21

<sup>149</sup> Sreenu G, Saleem Durai M. A., Intelligent video surveillance: a review through deep learning techniques for crowd analysis, Journal of Big Data, volume 6, Article number: 48, 2019, σελ. 9-10

<sup>150</sup> Άρθρο 5) 1α του Κανονισμού

<sup>151</sup> Data is power: Profiling and Automated Decision-Making in GDPR, ο.π., σελ. 8

και την προστασία του απορρήτου τους. Το ήδη αυτό επισφαλές πεδίο επιδεινώνεται με την χρήση της τεχνητής νοημοσύνης, η οποία αυξάνει τις δυνατότητες καταρτίσεως προφίλ, καθιστώντας κάθε είδος προσωπικών δεδομένων, ακόμα και τις θεωρούμενες “άχρηστες” πληροφορίες, αντικείμενα ανάλυσης και πρόβλεψης αλλά και επιδρώντας και επιτηρώντας τα υποκείμενα σε πολύ μεγαλύτερη ένταση και σε πληθώρα περισσότερων περιπτώσεων.<sup>152</sup>

Στο πλαίσιο αυτό προστίθεται και το γεγονός της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης, που μπορούν να χρησιμοποιηθούν για την διενέργεια της καταρτίσεως προφίλ των υποκειμένων, καθιστώντας την ενημέρωση των ατόμων ιδιαίτερα δυσχερή και την προστασία τους αβέβαιη. Το ζήτημα της αδιαφάνειας των συστημάτων τεχνητής νοημοσύνης αναλύθηκε διεξοδικώς στο προηγούμενο κεφάλαιο, συνεπώς στο συγκεκριμένο σημείο απλώς θα αναφερθούμε στο γεγονός ότι, στην περίπτωση της καταρτίσεως προφίλ, το υποκείμενο των δεδομένων πρέπει να πληροφορείται κυρίως σχετικά με την λογική που ακολουθήθηκε από τα αλγοριθμικά συστήματα, τις κατηγορίες δεδομένων που χρησιμοποιήθηκαν και τους κινδύνους και τις συνέπειες που εγκυμονούν.<sup>153</sup>

### **2.1.1. Η υπόθεση Cambridge Analytica – Facebook**

Μία περίπτωση που χρησιμοποιήθηκαν τεχνολογίες τεχνητής νοημοσύνης για την κατάρτιση προφίλ και στην οποία διαφάνηκαν οι κίνδυνοι που εγκυμονεί το profiling σχετικά με την ιδιωτικότητα των προσώπων, παρουσιάστηκε εντόνως στο σκάνδαλο που αποκαλύφθηκε το 2018 με εμπλεκόμενους, την εταιρεία ανάλυσης δεδομένων Cambridge Analytica και του μέσου κοινωνικής δικτύωσης επ’ ονόματι Facebook.<sup>154</sup> Η συγκεκριμένη υπόθεση αφορά την διαρροή προσωπικών δεδομένων, εκατομμυρίων χρηστών του Facebook, χωρίς την συγκατάθεσή τους, από την εταιρεία Cambridge Analytica, αποσκοπώντας κυρίως στην διενέργεια πολιτικών διαφημίσεων.

Αυτό που συνέβη ουσιαστικά στην εν λόγω υπόθεση ήταν η δημιουργία ψυχολογικών και πολιτικών προφίλ ενός τεράστιου αριθμού Αμερικανών ψηφοφόρων, με στόχο την μεταβολή της εκλογικής τους συμπεριφοράς. Αυτό επιδιώχθηκε μέσω της αποστολής εξατομικευμένων πολιτικών διαφημίσεων και άλλων μηνυμάτων, που μέσω της επίδρασης στα συναισθήματα και στις αντιλήψεις τους, θα επηρέαζε ή και θα μετέβαλλε την ψήφο τους. Η διαδικασία για την επίτευξη αυτού του στόχου αναφέρεται κατωτέρω.<sup>155</sup>

Αρχικά διάφοροι πολίτες, ψηφοφόροι των ΗΠΑ, προσκλήθηκαν να συμμετάσχουν σε μία έρευνα επί πληρωμή, που θα διεξαγόταν για ακαδημαϊκή χρήση, τα αποτελέσματα της οποίας όμως για να τους κατασταθούν γνωστά, θα έπρεπε αυτοί να παραχωρήσουν πρόσβαση στην προσωπική τους σελίδα στην διαδικτυακή πλατφόρμα του Facebook. Μέσω αυτής της πρόσβασης, ωστόσο, παρασχέθηκαν προσωπικές πληροφορίες, που εξάγονταν από τα ιδιωτικά τους προφίλ (likes, αναρτήσεις κ.α.), όχι μόνο των ίδιων των ατόμων που έλαβαν μέρος στην έρευνα, αλλά και όλων όσων περιλαμβάνονταν στις λίστες φίλων αυτών των ατόμων, αγγίζοντας προφανώς ένα

---

<sup>152</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 22-23

<sup>153</sup> Bygrave A. L., Minding the machine: art 15 of the EC Data Protection Directive and automated profiling, 2000

<sup>154</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 23-25

<sup>155</sup> European Parliament, ο.π., σελ. 23-25

τεράστιο αριθμό προσωπικών δεδομένων.

Η εταιρία μέσω αυτής της τεράστιας ποσότητας δεδομένων που πλέον διαθέτετε, δημιούργησε ένα σύστημα που κατήρτισε το προφίλ εκατομμυρίων χιλιάδων προσώπων. Συγκεκριμένα η Cambridge Analytica χρησιμοποιώντας αλγορίθμους μηχανικής εκμάθησης κατόρθωσε να αξιοποιήσει τα δεδομένα και τις πληροφορίες των υποκειμένων, συσχετίζοντάς τις και αποκαλύπτοντας στοιχεία σχετικά με τις πολιτικές προτιμήσεις, τις τάσεις συμπεριφοράς και διάφορα άλλα χαρακτηριστικά της προσωπικότητας των ατόμων.<sup>156</sup>

## **2.2. Το πρόβλημα της μεροληψίας των συστημάτων τεχνητής νοημοσύνης**

### **2.2.1. Η θεμελιώδης σημασία του θεμιτού της επεξεργασίας**

Το άρθρο 5 του Κανονισμού, στην παράγραφο 1 στοιχείο α, προβλέπει ρητώς ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να επεξεργάζονται κατά σύννομο, θεμιτό και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»). Οι προϋποθέσεις αυτές λειτουργούν σωρευτικά και επομένως μια επεξεργασία που τηρεί τα εχέγγυα νομιμότητας αλλά είναι αθέμιτη, θεωρείται παράνομη. Τα κριτήρια της νομιμότητας και του θεμιτού της επεξεργασίας κρίνονται αντικειμενικά και ανεξάρτητα από την νομιμότητα του σκοπού της επεξεργασίας.<sup>157</sup> Σε αυτήν την περίπτωση, δηλαδή, μας απασχολεί η ίδια η επεξεργασία και όχι οι σκοποί της, οι οποίοι παρότι μπορεί να κριθούν ως θεμιτοί, αυτό δεν καθιστά και την επεξεργασία ως τέτοια.

Το θεμιτό της επεξεργασίας εξαρτάται από πολλούς παράγοντες και είναι μια έννοια δύσκολα προσδιορίσιμη. Για να κατανοήσουμε τον όρο της αθέμιτης επεξεργασίας πρέπει να λάβουμε υπόψιν μας κυρίως τον βαθμό επίδρασης της επεξεργασίας στο υποκείμενο των δεδομένων. Συνεπώς μια επεξεργασία που διαθέτει έντονη κοινωνική απαξία κρίνεται κατά βάση ως αθέμιτη. Ο υπεύθυνος επεξεργασίας υποχρεούται να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση προφίλ και να υιοθετεί κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να μειώνεται ο κίνδυνος σφαλμάτων και ανακρίβειών και να προλαμβάνονται τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής κ.α.<sup>158</sup> Οφείλει, επίσης, να επεξεργάζεται τα δεδομένα κατά τρόπο εύλογα προσδιορισμένο από τα υποκείμενα, χωρίς να τους επιβάλλει αδικαιολόγητες και μη αναμενόμενες αρνητικές επιπτώσεις και σεβόμενος τα εύλογα ενδιαφέροντά τους. Το γεγονός, βέβαια, ότι κάποιο υποκείμενο επηρεάζεται αρνητικά από την επεξεργασία (π.χ. ως αποτέλεσμα της επεξεργασίας είναι η επιβολή κάποιου προστίμου) δεν σημαίνει ότι η επεξεργασία είναι αθέμιτη, εφόσον η ζημία του ήταν δικαιολογημένη.<sup>159</sup>

---

<sup>156</sup> European Parliament, ο.π., σελ. 24

<sup>157</sup> Παπακωνσταντίνου Ε., Δίκαιο Πληροφορικής, 2010, σελ. 78-80

<sup>158</sup> Αιτιολογική Σκέψη 71 του Προοιμίου του Κανονισμού.

<sup>159</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>

## **2.2.2. Το πρόβλημα σχετικά με τα συστήματα τεχνητής νοημοσύνης**

Η εξέλιξη της τεχνητής νοημοσύνης εισήγαγε καινοτομίες στο πεδίο της επεξεργασίας προσωπικών δεδομένων επιτρέποντας την αυτοματοποιημένη λήψη αποφάσεων ακόμα και σε πεδία που περιλαμβάνουν περίπλοκες αποφάσεις και πολλαπλούς παράγοντες και κριτήρια, που πρέπει να ληφθούν υπόψιν. Ταυτόχρονα, όμως, με τις καινοτομίες εισήγαγε και διάφορους κινδύνους, ένας από τους οποίους είναι ο κίνδυνος ανάδειξης μεροληπτικών αποτελεσμάτων και αποφάσεων από την αλγοριθμική επεξεργασία δεδομένων.

Παρότι πολλοί μελετητές ανακάλυψαν ότι η αυτοματοποιημένη επεξεργασία αποδεικνύεται ταχύτερη, πιο αποτελεσματική και αντικειμενική σε σχέση με αυτή που διενεργείται από ανθρώπους, δεν εκμηδενίζεται ο κίνδυνος να υποπέσει σε λάθη. Πολλοί παράγοντες επιδρούν πάνω στους ανθρώπους, όπως η ψυχολογία τους (π.χ. υπερβολική αυτοπεποίθηση ή γενικευμένη αναστάτωση που οδηγεί σε απροσεξία κατά την εκτέλεση της εργασίας), η ύπαρξη εγγενώς ή επίκτητων στοιχείων προκατάληψης (π.χ. φύλο, φυλή, εθνικότητα, κοινωνικό υπόβαθρο, θρησκευτικές αντιλήψεις κ.α.), αλλά και η γενικότερη ανθρώπινη αδυναμία στην επεξεργασία στατιστικών δεδομένων, επιδρούν αρνητικά στην διαδικασία επεξεργασίας των δεδομένων καταλήγοντας πολλές φορές σε λανθασμένα και άδικα αποτελέσματα.<sup>160</sup> Όπως θα αναλύσουμε στην συνέχεια, όμως, ακόμα και αν οι αλγόριθμοι τεχνητής νοημοσύνης δεν επηρεάζονται από τέτοια στοιχεία, είναι δυνατόν να υποπέσουν σε λάθη και επηρεάζονται από πεπλανημένα και διακριτικά στοιχεία να οδηγήσουν σε αθέμιτη επεξεργασία, επηρεάζοντας πολλές φορές δυσμενώς και αδικαιολόγητα ορισμένες ομάδες ανθρώπων σε σχέση με άλλες.

Η έννοια της θεμιτής επεξεργασίας διαδραματίζει, λοιπόν, πολύ σημαντικό ρόλο και αποτελεί μια προβληματική προϋπόθεση αναφορικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων και την κατάρτιση προφίλ με τη χρήση συστημάτων τεχνητής νοημοσύνης. Ο μεγαλύτερος κίνδυνος που εγκυμονεί σε αυτές τις περιπτώσεις είναι το γεγονός ότι οι διαδικασίες μηχανικής εκμάθησης μπορεί σε πολλές περιπτώσεις να λειτουργούν «μεροληπτικά».

Ο όρος των διακρίσεων, που πραγματοποιούν οι αλγόριθμοι, προφανώς αναφέρεται στην αυτοματοποιημένη επεξεργασία των δεδομένων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που οδηγεί σε διακριτική, άδικη και αθέμιτη αντιμετώπιση διαφορετικών κατηγοριών ανθρώπων, σε αντίθεση με μια ουδέτερη, θεμιτή, δίκαιη και αντικειμενική επεξεργασία.<sup>161</sup> Αυτή η επισήμανση είναι σημαντική, ώστε να επιτευχθεί διαχωρισμός μεταξύ της έννοιας διάκριση, ως προτεραιοποίηση ή διαφοροποίηση και της αθέμιτης διάκρισης. Οι αλγόριθμοι προβαίνουν συνεχώς σε διακρίσεις, δίνοντας έμφαση και προβάδισμα σε συγκεκριμένες πληροφορίες και δεδομένα, που οι ίδιοι θεωρούν χρήσιμα, εις βάρος άλλων. Αυτή η διάκριση, όμως, δεν είναι αθέμιτη, καθώς δεν επηρεάζει αρνητικά τα υποκείμενα, αλλά αντίθετα είναι απαραίτητη ώστε να εκπληρώσει ο αλγόριθμος τον σκοπό του ταχύτερα και πιο αποτελεσματικά.

Η μεροληπτική αντιμετώπιση των υποκειμένων, που μπορεί να προκαλέσει η αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, από συστήματα τεχνητής νοημοσύνης, πέραν της παραβίασης του Κανονισμού για θεμιτή επεξεργασία, οδηγεί και σε καταστρατήγηση του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Ο ΧΘΔ στο άρθρο 21 προβλέπει την απαγόρευση των διακρίσεων ιδίως λόγω φύλου, φυλής, χρώματος, εθνικής καταγωγής ή

<sup>160</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 20

<sup>161</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 16-18



κοινωνικής προέλευσης, γενετικών χαρακτηριστικών κ.α.

Η αθέμιτη διάκριση ενδέχεται να οφείλεται στον σχεδιασμό, τη λειτουργία και τη χρήση του αλγορίθμου μηχανικής εκμάθησης, στην ποσότητα και την ποιότητα των δεδομένων που έχουν τροφοδοτήσει τον αλγόριθμο, καθώς και στην αξιοπιστία των πηγών των δεδομένων. Όλα αυτά τα στοιχεία, εισάγοντας άμεσα ή έμμεσα στοιχεία προκατάληψης στην διαδικασία, μπορούν να επηρεάσουν σημαντικά την επεξεργασία των δεδομένων καταλήγοντας στην κατασκευή ενός συγκεκριμένου προφίλ βάσει αυτών.<sup>162</sup>

### 2.2.2.1. Διακρίσεις εξαιτίας των δεδομένων

Βασική περίπτωση αυτού του φαινομένου συναντάται όταν τα ίδια τα δεδομένα, τα οποία τροφοδοτούν τον αλγόριθμο της μηχανικής εκμάθησης, διαθέτουν μεροληπτικά στοιχεία.<sup>163</sup> Αυτή η περίπτωση συγκαταλέγεται στις περιπτώσεις έμμεσης προκατάληψης και έχει ως επακόλουθο ανακριβή και αναξιόπιστα αποτελέσματα, αλλά και διαιώνιση προκαταλήψεων. Σε πολλές περιπτώσεις τα δεδομένα, που τροφοδοτούν τα συστήματα μηχανικής εκμάθησης, δεν είναι πλήρη, είναι λανθασμένα ή δεν έχουν συλλεχθεί και επιλεγθεί καταλλήλως, καταλήγοντας στην εκδήλωση αλγοριθμικών λαθών και «προκαταλήψεων». Συνήθως αυτά τα μεροληπτικά στοιχεία προκύπτουν στα πολλαπλά στάδια προεπεξεργασίας, που ακολουθούνται σε μία αλγοριθμική επεξεργασία λήψης αποφάσεων, στα οποία στάδια περιλαμβάνονται μεταξύ άλλων ο καθαρισμός, η κατάταξη των δεδομένων κ.α.<sup>164</sup> Διακρίσεις, ωστόσο, είναι δυνατόν να εισαχθούν σε διάφορα στάδια της αλγοριθμικής επεξεργασίας.

Οι αλγόριθμοι, οι οποίοι λειτουργούν βάσει κάποιου συστήματος μηχανικής εκμάθησης, είναι δυνατόν να οδηγήσουν σε διακρίσεις, εάν έχουν «εκπαιδευθεί» με ιστορικά παραδείγματα, που αντικατοπτρίζουν παρελθούσες ή σιωπηρές προκαταλήψεις, ή με ανακριβή ή ανεπαρκή δεδομένα, ή με δεδομένα που παρουσιάζουν παραμορφωμένη εικόνα ομάδων που αποτελούν το συνολικό πληθυσμό.<sup>165</sup> Αυτό ενδέχεται να συμβαίνει στις περιπτώσεις που η επεξεργασία αφορά τα δεδομένα μιας μειονοτικής ομάδας, η οποία στο παρελθόν έχει πέσει θύμα διακρίσεων και προκαταλήψεων, με αποτέλεσμα σε άλλες περιπτώσεις να υποεκπροσωπείται και σε άλλες να υπερεκπροσωπείται.<sup>166</sup> Όταν παραδείγματος χάριν μια κοινωνική ομάδα εκπροσωπείται από ένα πολύ μικρό υποσύνολο των συνελεγμένων δεδομένων που θα χρησιμοποιηθούν για την επεξεργασία, είναι πολύ πιθανόν να τύχουν δυσμενούς διακριτικής μεταχείρισης, διότι μειώνεται η ακρίβεια των στοιχείων και των προβλέψεων για την συγκεκριμένη ομάδα.

Για παράδειγμα,<sup>167</sup> αν αναλογιστούμε έναν αλγόριθμο, ο οποίος θα καθοδηγεί την αστυνομία σχετικά με την δυνατότητα ελέγχου και σωματικής έρευνας πολιτών, τότε η τροφοδότηση

<sup>162</sup> Kamarinou D., Millard C., and Singh J, ο.π., σελ. 16-18

<sup>163</sup> Kamarinou D., Millard C., and Singh J, ο.π., σελ. 16

<sup>164</sup> Abiteboul S., Stoyanovich J., Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation, 2019, σελ. 15:5

<sup>165</sup> Kroll A. J., Huey J., Barocas S, Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., Accountable Algorithms, ο.π., σελ. 680-681

<sup>166</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ.16

<sup>167</sup> Kroll A. J., Huey J., Barocas S, Felten W. E., Reidenberg R. J., Robinson G. D. & Yu H., Accountable Algorithms, ο.π., σελ. 680-681

αυτού του αλγορίθμου με δεδομένα, τα οποία αντιπροσωπεύουν υπερβολικά τη συχνότητα εγκλήματος μεταξύ ορισμένων ομάδων, επειδή αυτές οι ομάδες ιστορικά είχαν στοχοποιηθεί από την δυσανάλογη αυτή επιβολή, αυτό θα έχει ως συνέπεια ανακριβή αποτελέσματα και διακρίσεις. Συγκεκριμένα η αστυνομία θα κατευθύνεται στην έρευνα αυτών των μειονοτικών ομάδων σε δυσανάλογο βαθμό σε σχέση με τις άλλες ομάδες. Αυτό το παράδειγμα, μάλιστα, δεν είναι τυχαίο αλλά έχει συναντηθεί στην πράξη, όταν το 2013 εκδόθηκε μια πολύ σημαντική απόφαση (Floyd et al. Vs the city of New York et al), κατά την οποία αποδείχθηκε ότι η αστυνομία της Νέας Υόρκης παραβίαζε συστηματικά δικαιώματα πολιτών μέσα από την εφαρμογή του δικαιώματος ελέγχου και σωματικής έρευνας («stop and frisk») σε πολίτες βάσει φυλετικών κριτηρίων. Αυτό διαφάνηκε από μια έρευνα που διεξήγαγε το Ινστιτούτο Συνταγματικών Δικαιωμάτων των Ηνωμένων Πολιτειών, το οποίο αποκάλυψε δεδομένα που παρουσίαζαν ότι σε σύνολο 685.724 πολιτών στους οποίους ασκήθηκε σωματικός έλεγχος από την Αστυνομία της Νέας Υόρκης, 84% ήταν Αφρικοαμερικανοί ή Ισπανόφωνοι και 9% Λευκοί.<sup>168</sup> Την περίοδο αυτή που διεξήχθη η έρευνα, συγκεκριμένα το 2010, ο πληθυσμός των κατοίκων της Νέας Υόρκης ανερχόταν 23% σε Αφρικοαμερικανούς, 29% σε Ισπανόφωνους και 33% σε Λευκούς.<sup>169</sup> Κατανοούμε, λοιπόν, ότι αυτό το γεγονός της υπερεκπροσώπησης ή υποεκπροσώπησης συγκεκριμένων ομάδων μπορεί να οδηγήσει τον αλγόριθμο σε λανθασμένα συμπεράσματα και φυλετικές και άλλες διακρίσεις.

Άλλο ένα παράδειγμα, που τα δεδομένα που τροφοδότησαν τον αλγόριθμο οδήγησαν σε διακρίσεις, αποτελεί η δημιουργία ενός αλγορίθμου της εταιρείας Amazon, ο οποίος με την χρήση της τεχνητής νοημοσύνης θα εξέταζε βιογραφικά των αιτούντων εργασία, ταξινομώντας τους κατάλληλα.<sup>170</sup> Δημιουργήθηκε, δηλαδή, ένα σύστημα ελέγχου των βιογραφικών (resume-screening), το οποίο ταξινόμησε τους υποψηφίους, στοχεύοντας στην εύρεση των πιο κατάλληλων εργαζομένων για μια ανοιχτή θέση εργασίας. Ενώ, όμως, αυτό το αλγοριθμικό σύστημα στόχευε να διευκολύνει και να κάνει αποτελεσματικότερη την διαδικασία, κατέληξε σε προκατειλημμένα κι αρνητικώς κείμενα προς τις γυναίκες αποτελέσματα. Αυτό οφειλόταν στο γεγονός ότι το σύστημα «εκπαιδεύτηκε» παρατηρώντας στοιχεία και πρότυπα από βιογραφικά που είχαν υποβληθεί στην εταιρία για μια δεκαετία, όμως η πλειοψηφία τους προέρχονταν από άνδρες, με αποτέλεσμα το σύστημα να «μάθει» από μόνο του ότι οι άντρες είναι προτιμητέοι, διακρίνοντας ταυτόχρονα δυσμενώς κατά των γυναικών.

#### **2.2.2.2. Διακρίσεις εξαιτίας του σχεδιαστή και του σχεδιασμού του αλγορίθμου**

Οι καινοτομίες στην τεχνολογική εξέλιξη της επεξεργασίας προσωπικών δεδομένων με την ανάπτυξη της τεχνητής νοημοσύνης κατέστησε σαφές ότι θα υπερκεραστούν οι ανθρώπινες αδυναμίες και προκαταλήψεις και θα δημιουργηθεί ένα μοντέλο επεξεργασίας δεδομένων αμερόληπτο, αντικειμενικό και πάνω από όλα αποτελεσματικό. Αυτές οι προβλέψεις, ωστόσο, δεν εκπληρώθηκαν ολοκληρωτικά, καθώς παραγνωρίστηκε το γεγονός ότι τα συστήματα τεχνητής νοημοσύνης κατασκευάζονται με ανθρώπινη συμβολή και ενδέχεται να διαθέτουν τις προκαταλήψεις

<sup>168</sup> <https://theartofcrime.gr/stop-frisk/>

<sup>169</sup> Rudovsky D., Rosenthal L., Debate: The Constitutionality of Stop-and-Frisk in New York City, 2013, σελ. 121

<sup>170</sup> <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>

του ίδιου του δημιουργού τους.<sup>171</sup>

Οι αλγόριθμοι αναπόφευκτα εκφράζουν τις ηθικές αξίες, τις ιδέες και τις απόψεις του σχεδιαστή τους, ενώ επιδιώκουν να πραγματοποιήσουν τον σκοπό, που αυτός επιδιώκει.<sup>172</sup> Δεν είναι ικανοί να δημιουργήσουν δικό τους σκοπό. Είναι, συνεπώς, ιδιαίτερα σημαντικό να σχεδιαστεί ο αλγόριθμος και να εξοπλιστεί με θεμελιώδεις και ηθικές αξίες, οι οποίες θα παραμείνουν όσο το δυνατόν σταθερές και αναλλοίωτες στο χρόνο και τις εξελίξεις τεχνολογικές και κοινωνικές.

Αναγνωρίζεται, λοιπόν, το φαινόμενο, ο αλγόριθμος να αναπαράγει τις ανθρώπινες προκαταλήψεις του δημιουργού του, διακρίνοντας τα άτομα και διαιωνίζοντας αυτές τις διακρίσεις. Συνεπώς, είναι ιδιαίτερα σημαντικό οι οργανισμοί που εκμεταλλεύονται εφαρμογές τεχνητής νοημοσύνης να γνωρίζουν τις επιδράσεις και τους κινδύνους που ενδέχεται να υποστούν τα υποκείμενα των δεδομένων αλλά και οι κοινωνικές ομάδες γενικότερα (π.χ. μειονότητες). Οφείλουν να καταβάλλουν κάθε προσπάθεια για να προσδιορίσουν και να ελέγξουν τυχόν προκαταλήψεις, τηρώντας την αρχή της θεμιτής επεξεργασίας κατά τον σχεδιασμό των συστημάτων μηχανικής εκμάθησης.

Κατανοούμε, επίσης, ότι είναι πιθανόν ο σχεδιαστής του αλγορίθμου να τον έχει ρυθμίσει κατά τέτοιο τρόπο, ώστε να υφίστανται στοιχεία διάκρισης στα κριτήρια ή στην τεχνική που χρησιμοποιείται από τον αλγόριθμο για την επίτευξη ενός συγκεκριμένου σκοπού. Είναι δυνατόν να έχει κατασκευαστεί ένα αλγοριθμικό μοντέλο με τέτοιο τρόπο, ώστε να κατηγοριοποιεί και φιλτράρει τους ανθρώπους με φυλετικά, οικονομικά κ.α. κριτήρια, τα οποία δεν απαιτούνται και δεν δικαιολογούνται στην συγκεκριμένη περίπτωση, ή να λαμβάνει υπόψιν του άσχετους και αχρείαστους παράγοντες, οδηγώντας σε προκατειλημμένα ή άδικα αποτελέσματα επεξεργασίας και αδικαιολόγητες διακρίσεις.<sup>173</sup> Για παράδειγμα, είναι δυνατόν να πραγματοποιηθούν διακρίσεις βάσει φυλής ή φύλου, μέσω της κατάρτισης προφίλ ατόμων, ανάλογα με τον ταχυδρομικό τους κώδικα ή των συνδρομών τους σε κάποιο περιοδικό.<sup>174</sup>

Ακόμα όμως και αν τα κριτήρια δεν είναι μεροληπτικά, αλλά απλώς άσχετα για το ζητούμενο αποτέλεσμα, ενδέχεται να οδηγήσουν σε διακρίσεις. Αν αναλογιστούμε, δηλαδή, έναν αλγόριθμο, που θα διαθέτει ως κριτήριο για την πρόσληψη ενός υποψηφίου εργαζομένου τις ώρες εργασίας/απασχόλησής του, θα οδηγήσει αναπόφευκτα σε δυσμενή διάκριση εις βάρος των γυναικών, οι οποίες συνήθως εργάζονται λιγότερες ώρες εξαιτίας των οικογενειακών τους υποχρεώσεων σε σχέση με τους άντρες.<sup>175</sup>

Παρά τα όσα αναφέρθηκαν δεν πρέπει να παραγνωρίζουμε την χρησιμότητα των αλγοριθμικών συστημάτων μηχανικής εκμάθησης στην αυτοματοποιημένη λήψη αποφάσεων και το γεγονός ότι σε μερικές περιπτώσεις είναι περισσότερο ελεγχόμενα από την ανθρώπινη επεξεργασία. Θεωρείται, μάλιστα, από μία πλευρά πιο εύκολη η εύρεση και επίλυση των ελαττωμάτων τους, καθώς μπορούν να βελτιωθούν ή να κατασκευαστούν εκ νέου προκειμένου να αποφευχθεί η διακριτική μεταχείριση ή τα λανθασμένα αποτελέσματα τους. Αυτό που εν τέλει απαιτείται είναι

---

<sup>171</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 20

<sup>172</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 17

<sup>173</sup> Kamarinou D., Millard C., and Singh J., ο.π., σελ. 16

<sup>174</sup> Kuner C., Svantesson D. J. B., Cate H. F., Lynskey O., Millard C., Machine learning with personal data: is data protection law smart enough to meet the challenge?, International Data Privacy Law, Volume 7/ Issue 1, February 2017, σελ. 1-2

<sup>175</sup> European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, ο.π., σελ. 21

ένας επιτυχής συνδυασμός της ανθρώπινης και της τεχνητής νοημοσύνης με σκοπό την αλληλοσυμπλήρωσή τους και την εξουδετέρωση των εκατέρωθεν αδυναμιών. Ταυτόχρονα είναι απαραίτητη και η προστασία των υποκειμένων από την προβληματική δράση της τεχνητής νοημοσύνης, η οποία μπορεί να επιτευχθεί με την παροχή μέτρων ασφαλείας, όπως είναι τα γενικότερα δικαιώματα των υποκειμένων που προβλέπονται από τον ΓΚΠΔ, αλλά και ειδικότερα το δικαίωμα της ανθρώπινης παρεμβάσεως και το δικαίωμα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων, το οποίο τελευταίο θα αναλυθεί στην συνέχεια.

### **3. Η ΕΝΑΝΤΙΩΣΗ ΣΤΗΝ ΑΥΤΟΜΑΤΟΠΟΙΗΜΕΝΗ ΛΗΨΗ ΑΠΟΦΑΣΕΩΣ**

#### **3.1. Γενικά τα δικαιώματα των υποκειμένων**

Η κατανόηση των κινδύνων της επεξεργασίας των προσωπικών δεδομένων οδήγησε τον νομοθέτη στην θεσμοθέτηση ορισμένων δικαιωμάτων των υποκειμένων με σκοπό την προστασία τους. Τα δικαιώματα αυτά περιγράφονται κατά βάση στα άρθρα 16, 17 και 18 του Γενικού Κανονισμού Προστασίας Δεδομένων και αποτελούν δικαιώματα αντίταξης κατά της παράνομης επεξεργασίας, αλλά και στα άρθρα 21, 22, που αποτελούν δικαιώματα εναντίωσης ακόμα και κατά της νόμιμης επεξεργασίας.<sup>176</sup> Το πλήθος αυτό δικαιωμάτων προφανώς εντάσσεται και στις περιπτώσεις που η επεξεργασία πραγματοποιείται με αυτοματοποιημένο τρόπο και από συστήματα τεχνητής νοημοσύνης.

Αρχικά, λοιπόν, το υποκείμενο σε περίπτωση τέτοιου είδους επεξεργασίας δικαιούται να επικαλεστεί κατά του υπευθύνου επεξεργασίας τα γενικά δικαιώματα αντίρρησης. Συγκεκριμένα μπορεί να ζητήσει την διόρθωση των δεδομένων του, δηλαδή την διόρθωση των ανακρίβειών των δεδομένων του, σύμφωνα με το άρθρο 16 του Κανονισμού αλλά και την ολοκληρωτική διαγραφή τους, βάσει του άρθρου 17}1δ, εφόσον κριθεί αυτού του είδους η επεξεργασία παράνομη στην συγκεκριμένη περίπτωση. Το δικαίωμα διαγραφής ή αλλιώς «δικαίωμα στην λήθη» (άρθρο 17 του Κανονισμού) αποτελεί την καθολικότερη εμφάνιση του δικαιώματος αντίρρησης, διότι το υποκείμενο αιτείται ουσιαστικά την ολοκληρωτική εξαφάνιση της επεξεργασίας.<sup>177</sup> Ιδιαίτερο ενδιαφέρον παρουσιάζει στην περίπτωση της αυτοματοποιημένης επεξεργασίας με την χρήση εφαρμογών τεχνητής νοημοσύνης, το δικαίωμα περιορισμού της επεξεργασίας, το οποίο περιγράφεται στο άρθρο 18 του Κανονισμού. Εφόσον, λοιπόν, η συγκεκριμένη επεξεργασία θεωρηθεί παράνομη, το υποκείμενο δικαιούται να αιτηθεί τον περιορισμό της επεξεργασίας (άρθρο 18}1β), το οποίο στην περίπτωση της επεξεργασίας με αυτοματοποιημένα μέσα τεχνητής νοημοσύνης, ενδέχεται να λάβει τη μορφή του αιτήματος να μην πραγματοποιείται πλέον η επεξεργασία με την χρήση τέτοιων μέσων.

Πέραν των γενικών δικαιωμάτων, όμως, διαλαμβανομένων και των σύγχρονων τεχνολογικών εξελίξεων ο νομοθέτης καθιέρωσε ένα δικαίωμα εναντίωσης κατά της αποκλειστικώς αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της καταρτίσεως προφίλ, το οποίο περιγράφεται στο άρθρο 22 του Κανονισμού και αναλύεται κατωτέρω.

<sup>176</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 128-134

<sup>177</sup> Χριστοδούλου Κ., ο.π., σελ. 132

### **3.2. Ειδικότερα το δικαίωμα του άρθρου 22 παράγραφος 1**

#### **3.2.1. Οι δικαιολογητικοί λόγοι θεσπίσεως του**

Στην παράγραφο 1 του άρθρου 22 του Κανονισμού ορίζεται ρητά 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 ένομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο*». Το άρθρο 22 είναι κατά τέτοιο τρόπο δομημένο, που περιλαμβάνει στην πρώτη παράγραφο το δικαίωμα που δίδεται στα πρόσωπα, στην συνέχεια προχωρά στην δεύτερη ορίζοντας τις περιπτώσεις που υφίσταται εξαίρεση στο προαναφερθέν δικαίωμα και στην παράγραφο 3 προσθέτει μέτρα για την προστασία των δικαιωμάτων των ατόμων σε δύο από τις εξαιρέσεις της παραγράφου 2. Τέλος στην τελευταία παράγραφο προβλέπει την απαγόρευση εφαρμογής των εξαιρέσεων της παραγράφου 2 στην περίπτωση των δεδομένων «ειδικής κατηγορίας».

Μεταξύ άλλων, παρατηρείται ότι συμπεριλαμβάνεται ρητώς η δυνατότητα του υποκειμένου να εναντιωθεί στην κατάρτιση προφίλ, καινοτομία σε σχέση με την Οδηγία 95/46/EK. Η καινοτομία αυτή αποδίδεται στην επιθυμία του κοινοτικού νομοθέτη να προστατέψει τα υποκείμενα των δεδομένων από τον απρόσωπο χαρακτήρα ενός «ηλεκτρονικού εγκεφάλου», ο οποίος αντικαθιστά τον ανθρώπινο παράγοντα.<sup>178</sup>

Οι προαναφερθέντες κίνδυνοι είχαν ληφθεί υπόψιν ήδη από την Οδηγία 95/46/EK, στην οποία στο άρθρο 15 προβλεπόταν το δικαίωμα των προσώπων να μη συμμορφωθούν με απόφαση που παράγει νομικά αποτελέσματα ή τους θίγει σημαντικά, εφόσον η εν λόγω απόφαση βασίζεται αποκλειστικώς σε αυτοματοποιημένη επεξεργασία που αξιολογεί ορισμένες πτυχές της προσωπικότητάς τους. Ο κυριότερος λόγος θέσπισης αυτού του άρθρου ήταν η αντιμετώπιση του κινδύνου της αποδυνάμωσης του ανθρώπινου παράγοντα και της ικανότητάς του να επιδράσει σε αποφάσεις που τον αφορούν, καθώς αυτός θα αντικαθίστατο από αυτοματοποιημένης μορφής επεξεργασίες.<sup>179</sup> Επιπλέον είχε διατυπωθεί και η ανησυχία σχετικά με την ποιότητα των αποφάσεων που ελήφθησαν ύστερα από αυτοματοποιημένη επεξεργασία.<sup>180</sup> Αυτός ο φόβος ενέκειτο κυρίως στο γεγονός ότι υπήρχε πιθανότητα τα άτομα να θεωρούσαν δεδομένη την εγκυρότητα των αποφάσεων αυτού του είδους, μειώνοντας ταυτόχρονα την δική τους συμβολή στον έλεγχό τους.

Αντίστοιχες ανησυχίες οδήγησαν και στην θέσπιση του άρθρου 22, όμως σε αυτό δόθηκε περισσότερο έμφαση στην σημασία της καταρτίσεως προφίλ, κάτι που διαφαίνεται ήδη από τον τίτλο του άρθρου, που ρητά αναφέρεται ο όρος κατάρτιση προφίλ.<sup>181</sup> Προβλέπεται πλέον το δικαίωμα εναντίωσης σε κάθε περίπτωση καταρτίσεως προφίλ και όχι μόνο σε συγκεκριμένα είδη αποφάσεων που προκύπτουν από το profiling. Ο ενωσιακός νομοθέτης, δηλαδή, θέλησε να εφοδιάσει τα υποκείμενα με ένα «δικαίωμα μη συμμόρφωσης», προκειμένου να μην μετατρέπονται σε αντικείμενα της αυτοματοποιημένης διαδικασίας, αλλά να εμπλέκονται σε αυτήν διατηρώντας

<sup>178</sup> Μήτρου Α., Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ. 128-131

<sup>179</sup> Mendoza I. and Bygrave A. L., The Right not to be Subject to Automated Decisions based on Profiling, University of Oslo, Faculty of Law, Legal Studies Research Paper Series No. 2017-20, σελ. 6-7

<sup>180</sup> Mendoza I. and Bygrave A. L., ο.π., σελ. 6-7

<sup>181</sup> Mendoza I. and Bygrave A. L., ο.π., σελ. 7-8

την ατομικότητά τους.<sup>182</sup>

### **3.2.2. Η φύση του δικαιώματος**

Υφίσταται διχογνωμία σχετικά με την φύση του δικαιώματος του υποκειμένου να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, του άρθρου 22. Ο προβληματισμός έγκειται στο αν πρόκειται για κάποιου είδους απαγόρευση ή για δικαίωμα αντιρρήσεως.<sup>183</sup> Η αποσαφήνιση αυτού του ζητήματος είναι ιδιαίτερα σημαντική, διότι επηρεάζει τον βαθμό προστασίας που επιφυλάσσεται για τα υποκείμενα. Αν δεχτούμε ότι πρόκειται για απαγόρευση, τότε ο υπεύθυνος επεξεργασίας απαγορεύεται να προβεί σε αυτοματοποιημένη μορφή επεξεργασίας και κατάρτιση προφίλ, εκτός αν πρόκειται για μία από τις εξαιρέσεις που προβλέπονται στην παράγραφο 2 του άρθρου 22. Αντίθετα, αν θεωρήσουμε αυτή την πρόβλεψη του νομοθέτη ως ένα δικαίωμα αντιρρήσεως, τότε είναι επιτρεπτή αυτή η μορφή επεξεργασίας, εκτός αν εναντιωθούν τα υποκείμενα.

Από την μία πλευρά το άρθρο 22 περιλαμβάνεται στο κεφάλαιο του Κανονισμού, που τιτλοφορείται ως «*Δικαιώματα του υποκειμένου των δεδομένων*», ενώ και το ίδιο το άρθρο κάνει λόγο για «*δικαίωμα*».<sup>184</sup> Αν θεωρήσουμε, ωστόσο, το δικαίωμα του άρθρου 22 ως δικαίωμα αντίρρησης, θα βασίζουμε την εφαρμογή του στην αντίδραση και ενέργεια του υποκειμένου των δεδομένων, αποδυναμώνοντας με αυτόν τον τρόπο τον βαθμό προστασίας της ιδιωτικότητας και των δεδομένων των προσώπων. Επιπλέον, αν έπρεπε το δικαίωμα της παραγράφου 1 να ασκηθεί από τα υποκείμενα, θα λειτουργούσε επαρκώς ως ένα δικαίωμα που θα εξασφάλιζε την ανθρώπινη παρέμβαση στην περίπτωση της αυτοματοποιημένης λήψης αποφάσεων, καθιστώντας περιττή την πρόβλεψη της παραγράφου 3 του άρθρου.<sup>185</sup>

Καθίσταται, λοιπόν, σαφές ότι, τόσο από λογική όσο και από τελεολογική σκοπιά, ίσως ορθότερο είναι να θεωρήσουμε ότι το δικαίωμα εναντιώσεως που προβλέπεται στο άρθρο 22, πρόκειται στην ουσία για απαγόρευση, αποσκοπώντας στην προστασία των υποκειμένων αποτελεσματικότερα και εξ ορισμού.<sup>186</sup> Με την θεώρηση του δικαιώματος ως απαγόρευσης καθιερώνεται αυτεπάγγελτος έλεγχος εκ μέρους της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Αυτή η πρόβλεψη επικράτησε, κυρίως, λόγω του γεγονότος ότι σε πολλές περιπτώσεις τα υποκείμενα δεν διαθέτουν καν γνώση ότι τα δεδομένα τους δέχονται επεξεργασία και μάλιστα με αυτοματοποιημένους τρόπους ή ότι καταρτίζονται προφίλ βάσει αυτών. Αυτό έχει ως αποτέλεσμα να αποστερούνται στην ουσία της δυνατότητας ενασκήσεως αυτού του δικαιώματος.

### **3.2.3. Το περιεχόμενό του**

---

<sup>182</sup> *Μήτρου Α.*, Ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο.π., σελ.128-131

<sup>183</sup> *Data is power: Profiling and Automated Decision-Making in GDPR*, ο.π., σελ. 10-11

<sup>184</sup> *Mendoza I. and Bygrave A. L.*, The Right not to be Subject to Automated Decisions based on Profiling, ο.π., σελ.9-10

<sup>185</sup> *Mendoza I. and Bygrave A. L.*, ο.π., σελ.10

<sup>186</sup> *Mendoza I. and Bygrave A. L.*, ο.π., σελ.10

Το δικαίωμα του άρθρου 22 αποτελεί ένα ιδιότυπο δικαίωμα εναντίωσης. Κατά την ανάγνωση της πρώτης παραγράφου του άρθρου διαπιστώνουμε ότι για να τύχει εφαρμογής πρέπει το υποκείμενο να αντιτίθεται σε απόφαση, που ελήφθη αποκλειστικώς με αυτοματοποιημένα μέσα επεξεργασίας, συμπεριλαμβανόμενης της καταρτίσεως προφίλ, και είτε να παράγονται έννομα αποτελέσματα που επιδρούν σε αυτό, είτε το υποκείμενο να επηρεάζεται σημαντικά με παρόμοιο τρόπο.

### **3.2.3.1. Η αποκλειστικώς αυτοματοποιημένη λήψη αποφάσεως**

Ως αυτοματοποιημένη λήψη αποφάσεως ορίζεται αυτή που λαμβάνεται από τεχνολογικά μέσα, χωρίς ανθρώπινη συμβολή. Η έννοια, ωστόσο, της αυτοματοποιημένης λήψης αποφάσεως δεν συνιστά μια ενιαία έννοια που αποτελείται μόνο από έναν συγκεκριμένο τύπο αποφάσεων, αλλά αντίθετα λαμβάνεται ευρέως και μπορεί να χωριστεί σε υποκατηγορίες. Μερικές από αυτές είναι η διάκριση ανάμεσα σε διαδικαστική και ουσιαστική αυτοματοποιημένη λήψη αποφάσεων, σε αλγοριθμική και μη αλγοριθμική και σε αυτή που βασίζεται σε κανόνες σε αντίθεση με αυτή που βασίζεται στο νόμο.<sup>187</sup>

Η διάκριση σε ουσιαστική και διαδικαστική αναφέρεται στο γεγονός ότι η αυτοματοποιημένη λήψη της απόφασης πρέπει να υιοθετηθεί κατά τέτοιο τρόπο, ώστε να εγγυάται διαδικαστική ή ουσιαστική δικαιοσύνη και ακρίβεια. Με τον όρο διαδικαστική δικαιοσύνη εννοείται ότι όλες οι αποφάσεις, που σχετίζονται με ίδια γεγονότα, έχουν ληφθεί με την ίδια αυτοματοποιημένη διαδικασία, ενώ ουσιαστική δικαιοσύνη σημαίνει ότι οι αποφάσεις δεν πρέπει να προβαίνουν σε οποιαδήποτε μεροληπτική διάκριση.

Αλγοριθμική αυτοματοποιημένη λήψη αποφάσεως καλείται αυτή που λαμβάνεται σαφώς με την βοήθεια ενός αλγορίθμου, κυρίως αλγορίθμου – υπολογιστή, δηλαδή μια σειρά ενεργειών, αυστηρά καθορισμένων και εκτελέσιμων, που στοχεύουν στην επίλυση ενός προβλήματος.<sup>188</sup> Οι σύγχρονες τεχνολογικές εξελίξεις και ιδιαίτερα η ανάπτυξη των Big Data και της τεχνητής νοημοσύνης έχουν καταστήσει σχεδόν απαραίτητη την αλγοριθμική αυτοματοποιημένη λήψη αποφάσεως, καθιστώντας την, τον κανόνα. Τέλος στην περίπτωση των αποφάσεων που βασίζονται σε κανόνες, ως κανόνας θεωρείται κατά βάση το αποτέλεσμα μιας επιχειρηματικής αποφάσεως π.χ. η στοχευμένη διαφήμιση μέσω της κατάρτισης προφίλ, σε αντίθεση με την απόφαση που στηρίζεται στον νόμο, η οποία βασίζεται σε κάποιον ακριβή νομικό κανόνα και είναι νομικά δεσμευτική.

Η προβληματική, που εντοπίζεται σε αυτό το σημείο, επικεντρώνεται στην έννοια της «αποκλειστικώς» αυτοματοποιημένης επεξεργασίας. Τα προσωπικά δεδομένα υφίστανται επεξεργασία μέσα από συστήματα αλγορίθμων, η οποία επεξεργασία καταλήγει σε μια σειρά αποφάσεων. Βέβαια αυτό δεν σημαίνει ότι δεν θα υφίσταται ανθρώπινη συμβολή σε κανένα στάδιο της επεξεργασίας. Στην πραγματικότητα ο άνθρωπος παράγοντας μπορεί να έχει χρησιμοποιηθεί σε διάφορα στάδια της. Αρχικά παρουσιάζεται στον σχεδιασμό του συστήματος μηχανικής εκμάθησης με την τροφοδότησή του με τα κριτήρια, τα οποία πρέπει να λάβει υπόψιν του ο αλγόριθμος

<sup>187</sup> Brkan M., Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond, Assistant Professor Faculty of Law, Maastricht University, 2018, σελ. 3-4

<sup>188</sup> <https://el.wikipedia.org/wiki/Αλγόριθμος>

για την λήψη της απόφασης. Ενδέχεται, όμως, επίσης να έχει πραγματοποιηθεί κάποιου είδους εκτίμηση του αποτελέσματος, που θα εξαχθεί από τον αλγόριθμο, πριν την λήψη της τελικής απόφασης.

Έχουν διατυπωθεί, ωστόσο, σχετικές αντιρρήσεις, που υποστηρίζουν ότι οποιαδήποτε μορφή ανθρώπινης συμβολής, ακόμα και ασήμαντης, αποκλείει την εφαρμογή του άρθρου 22.<sup>189</sup> Μια τέτοια στενή ερμηνεία, όμως, θα αμφισβητούσε την χρησιμότητα των γραπτών διατάξεων, καθιστώντας τις άσκοπες, ενώ ταυτόχρονα θα απέκλειε από το πεδίο εφαρμογής του άρθρου έναν τεράστιο αριθμό περιπτώσεων, εκθέτοντας τα υποκείμενα σε μια πληθώρα κινδύνων.<sup>190</sup> Χαρακτηριστικό παράδειγμα αποτελούν οι αλγόριθμοι, οι οποίοι αξιολογούν την πιστοληπτική ικανότητα των υποκειμένων.<sup>191</sup> Στην περίπτωση αυτή όλη η διαδικασία της αξιολόγησης πραγματοποιείται με την χρήση αυτοματοποιημένων αλγορίθμων και ο υπεύθυνος επεξεργασίας λαμβάνει μια απόφαση με παθητικό τρόπο, εφαρμόζοντας προκαθορισμένους όρους και οδηγίες και μη ασκώντας σχεδόν καμία κριτική στην τελική απόφαση. Σε αυτήν την περίπτωση λοιπόν, η οποία καταλήγει συχνά σε μεροληπτικά και λανθασμένα αποτελέσματα, αν δεχτούμε ότι δεν υφίσταται απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, τα υποκείμενα δεν μπορούν να προστατευθούν βάσει του άρθρου 22.

Εκτός, όμως του γεγονότος ότι αν ερμηνεύαμε αυστηρά την έννοια της «αποκλειστικώς» αυτοματοποιημένης επεξεργασίας, τότε το άρθρο 22 θα εφαρμοζόταν σε ελάχιστες περιπτώσεις, αναφέρεται ρητά στις κατευθυντήριες γραμμές της Ομάδας του άρθρου 29 για τις αυτοματοποιημένες λήψεις αποφάσεων, ότι ασήμαντη ανθρώπινη συμβολή δεν αρκεί. Για να θεωρήσουμε ότι δεν υφίσταται αποκλειστικώς αυτοματοποιημένη λήψη απόφασης, πρέπει η ανθρώπινη συμβολή να είναι ουσιαστική κατά τρόπο που να επηρεάζει σε σημαντικό βαθμό το αποτέλεσμα της αυτοματοποιημένης επεξεργασίας. Αν, για παράδειγμα, τα άτομα δεν αξιολογούν καταλυτικά το αποτέλεσμα του συστήματος, αλλά απλώς π.χ. σημειώνουν ένα κουτί σε μία φόρμα, δεν μπορούμε να πούμε ότι επηρεάζουν σημαντικά το αποτέλεσμα της επεξεργασίας και επομένως εξακολουθεί να υφίσταται λήψη απόφασης με αυτοματοποιημένο τρόπο.<sup>192</sup>

Επιπλέον είναι κατανοητό ότι προκειμένου να είναι δυνατή η επίδραση στο τελικό αποτέλεσμα και στην λήψη της απόφασης, προϋποτίθεται ότι τα άτομα γνωρίζουν και κατανοούν τον τρόπο λειτουργίας των αυτοματοποιημένων συστημάτων. Στην περίπτωση, όμως, των συστημάτων τεχνητής νοημοσύνης αυτό παρουσιάζεται ιδιαίτερα δυσχερές εξαιτίας της αδιαφάνειας και του πολύπλοκου τρόπου λειτουργίας τους, ώστε ακόμα και αν άνθρωποι έλαβαν την τελική απόφαση, αυτή θα έχει στην ουσία ληφθεί με αυτοματοποιημένα μέσα, διότι τα άτομα δεν θα είχαν την δυνατότητα να επηρεάσουν σε σημαντικό βαθμό το αποτέλεσμα.<sup>193</sup> Κατανοούμε, συνεπώς, ότι μόνο με μια πιο ευρεία ερμηνεία της έννοιας «αποκλειστικώς αυτοματοποιημένης επεξεργασίας», ως επεξεργασία, η οποία απαιτεί ουσιαστική ανθρώπινη συμβολή, μπορεί να οδηγήσει στην αποτελεσματική εφαρμογή του άρθρου 22 και στην ουσιαστική προστασία των υποκειμένων.

<sup>189</sup> *Selbst D. A., Powles J.*, Meaningful information and the right to explanation, 2017, Volume 7, No 4, σελ. 235

<sup>190</sup> *Malgieri G., Comandé G.*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, ο.π., σελ. 13

<sup>191</sup> *Malgieri G., Comandé G.*, ο.π., σελ.13-14

<sup>192</sup> *Kamarinou D., Millard C., and Singh J.*, Machine Learning with Personal Data, ο.π., σελ. 11-12

<sup>193</sup> Data is power: Profiling and Automated Decision-Making in GDPR, ο.π., σελ. 13-14



### 3.2.3.2. Έννομα αποτελέσματα

Όπως αναφέρεται στο άρθρο 22 του Κανονισμού, η απόφαση πρέπει να παράγει έννομα αποτελέσματα που αφορούν το υποκείμενο ή να το επηρεάζει σημαντικά με παρόμοιο τρόπο. Τα έννομα αποτελέσματα μπορούν να είναι τόσο υλικά, όσο και άυλα επηρεάζοντας π.χ. την φήμη του ατόμου κ.α., ενώ αμφισβητείται αν με τον όρο «έννομα» αποτελέσματα προϋποτίθεται ότι η απόφαση είναι δεσμευτική ή ότι δημιουργούνται νομικές υποχρεώσεις στο υποκείμενο.<sup>194</sup> Κατά μια άποψη, λήψη απόφασης ουσιαστικά σημαίνει ότι έχει ληφθεί μια στάση απέναντι σε κάποιο πρόσωπο και αυτή η στάση έχει κάποιο βαθμό δεσμευτικής επίδρασης πάνω του.<sup>195</sup> Φυσικά αυτή η διαδικασία λήψης της αποφάσεως μπορεί να συγκροτείται εξ ολοκλήρου από τις λειτουργίες ενός υπολογιστικού συστήματος.

Έννομα αποτελέσματα θεωρούνται αυτά που έχουν αντίκτυπο στα ανθρώπινα ή στα συμβατικά δικαιώματα του ατόμου. Για παράδειγμα, αν η απόφαση που ελήφθη βάσει αυτοματοποιημένης επεξεργασίας παραβιάζει δικαιώματα του υποκειμένου, όπως είναι το δικαίωμα του εκλέγειν ή η ελευθερία έκφρασης και επικοινωνίας αλλά και όταν υπόκεινται τα άτομα αδικαιολόγητα σε αυξημένα μέτρα επιτήρησης από τις αρμόδιες αρχές, έχουν το δικαίωμα εναντίωσης του άρθρου 22.<sup>196</sup>

### 3.2.3.3. Σημαντική επιρροή προς τα υποκείμενα

Προσοχή πρέπει να δοθεί και στην έννοια της «σημαντικής» επιρροής προς το υποκείμενο, που αναφέρεται στο άρθρο 22. Οι κατευθυντήριες οδηγίες του άρθρου 29 προβλέπουν ότι για να δεχτούμε ότι η επεξεργασία δεδομένων μπορεί να επηρεάσει σημαντικά κάποιον, πρέπει τα αποτελέσματα της να μην είναι ασήμαντα, αλλά να είναι επαρκώς σημαντικά και άξια προσοχής. Με άλλα λόγια η απόφαση πρέπει να έχει τη δυνατότητα να επηρεάσει σημαντικά τις περιστάσεις, τη συμπεριφορά ή τις επιλογές των ενδιαφερόμενων ατόμων ή ακόμα και να οδηγήσει στην διακριτική μεταχείρισή τους. Αν και δεν αναφέρεται ρητώς στο άρθρο ότι αυτή η επίδραση πρέπει να είναι ολοκληρωτικώς αρνητική προς το υποκείμενο, είναι λογικό όσο πιο αρνητική είναι τόσο μεγαλύτερη πιθανότητα υπάρχει να θεωρηθεί ως «σημαντική».<sup>197</sup>

Χαρακτηριστικά παραδείγματα τέτοιας περίπτωσης αναφέρονται στην Αιτιολογική Σκέψη 71 του Προοιμίου του Κανονισμού. Στο σημείο αυτό αναγνωρίζεται ότι η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή οι πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση, αποτελούν αποφάσεις με τις οποίες αξιολογούνται προσωπικές πτυχές που αφορούν το υποκείμενο και λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και οι οποίες παράγουν έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζουν σημαντικά κατά

<sup>194</sup> Kamarinou D., Millard C., and Singh J., Machine Learning with Personal Data, ο.π., σελ. 12

<sup>195</sup> Mendoza I. and Bygrave A. L., The Right not to be Subject to Automated Decisions based on Profiling, ο.π., σελ. 10-11

<sup>196</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

<sup>197</sup> Mendoza I. and Bygrave A. L., The Right not to be Subject to Automated Decisions based on Profiling, ο.π., σελ.12

ανάλογο τρόπο. Ο κατάλογος περιπτώσεων της Αιτιολογικής Σκέψης 71 του Κανονισμού, ωστόσο, είναι εξαιρετικά περιορισμένος οδηγώντας σε αμφισβητήσεις σχετικά με την φύση της εν λόγω σημαντικής επιρροής, στο κατά πόσο εξαρτάται από την υποκειμενική κρίση του υποκειμένου των δεδομένων ή του υπευθύνου επεξεργασίας, ή στην δυνατότητα καθιέρωσης ορισμένων αντικειμενικών κριτηρίων, που θα μας επιτρέπουν να θεωρήσουμε ορισμένες μορφές αυτοματοποιημένης επεξεργασίας ως έχουσες σημαντική επίδραση στο υποκείμενο.<sup>198</sup>

Οι κατευθυντήριες γραμμές του άρθρου 29 φαίνεται να κατευθύνονται προς μια υποκειμενική θεωρία, όπου κριτήριο αποτελεί το υποκείμενο των δεδομένων. Αυτό συνάγεται από το γεγονός ότι αναφέρεται πως «*Η επεξεργασία που μπορεί να έχει μικρή επιρροή στα άτομα γενικά μπορεί στην πραγματικότητα να έχει σημαντική επιρροή σε ορισμένες κοινωνικές ομάδες, όπως ομάδες μειονοτήτων ή ευάλωτους ενήλικες*». Συμπεραίνουμε, λοιπόν, ότι η έννοια της σημαντικής επιρροής είναι σχετική έννοια και εξαρτάται μεταξύ άλλων παραγόντων και από το υποκείμενο στο οποίο έχει άμεσο αντίκτυπο. Για παράδειγμα, συνεχείς διαφημίσεις για τυχερά παιχνίδια στο διαδίκτυο δεν έχουν τόσο σημαντική επιρροή σε έναν οποιοδήποτε καταναλωτή, αν όμως ο συγκεκριμένος καταναλωτής αντιμετωπίζει έντονα οικονομικές δυσχέρειες ή και εθισμό σε τέτοιου είδους παιχνίδια τότε μια τέτοια διαφήμιση ίσως θεωρηθεί επικίνδυνη.

Ο νομοθέτης, επιπλέον, στην Αιτιολογική Σκέψη 71 του Προοιμίου του Κανονισμού προβλέπει ότι ο υπεύθυνος επεξεργασίας οφείλει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ και να εφαρμόζει τεχνικά και οργανωτικά μέτρα με σκοπό την δίκαιη και διαφανή επεξεργασία, την ασφάλεια των δεδομένων, προλαμβάνοντας κινδύνους και διάφορα είδη διακρίσεων (φυλετικών, βάσει θρησκείας, πολιτικών φρονημάτων, πεποιθήσεων κ.α.) σε βάρος των προσώπων.

### **3.3. Οι εξαιρέσεις της παραγράφου 2**

Στην παράγραφο 2 του άρθρου 22 του Κανονισμού αναφέρονται εξαιρέσεις, κατά τις οποίες επιτρέπεται απόκλιση από το δικαίωμα εναντίωσης της παραγράφου 1 σε τρεις συγκεκριμένες περιπτώσεις. Αυτό συμβαίνει όταν η απόφαση «*α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων β) 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 γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων*». Οι τρεις αυτές εξαιρέσεις εντάσσονται σε ένα στενό πεδίο εφαρμογής και συναντώνται σε περιορισμένες περιπτώσεις.

#### **3.3.1. Σύναψη ή εκτέλεση σύμβασης**

Αν και η πρώτη εξαίρεση της σύμβασης ερμηνεύεται στενά από τις ρυθμιστικές αρχές, η έννοια του «αναγκαίου» της απόφασης για την εκτέλεση της σύμβασης δεν μπορεί να ερμηνευτεί

---

<sup>198</sup> Data is power: Profiling and Automated Decision-Making in GDPR, ο.π., σελ. 11-13

αυστηρά, αλλά πρέπει να μεταφράζεται κατά εύλογο τρόπο, ώστε να επιτρέπεται η λήψη απόφασης βάσει αυτοματοποιημένης επεξεργασίας, όπου δεν υπάρχουν άλλες πρακτικές λύσεις.<sup>199</sup> Αυτή η αναγκαιότητα μπορεί να εξαρτάται από τον μεγάλο αριθμό των περιπτώσεων, που επρόκειτο να εξεταστούν. Ένα τέτοιο παράδειγμα θα μπορούσε να είναι μια επιχείρηση που δέχεται χιλιάδες αιτήσεις δουλειάς για μια συγκεκριμένη θέση.<sup>200</sup> Στην περίπτωση αυτή, για να είναι εφικτός ο εντοπισμός και η απόρριψη των μη χρήσιμων αιτήσεων, ενδέχεται να είναι απαραίτητη η αυτοματοποιημένη λήψη αποφάσεων, προκειμένου να δημιουργηθεί ένας σύντομος κατάλογος πιθανών υποψηφίων με απώτερο σκοπό την σύναψη σύμβασης με το υποκείμενο των δεδομένων.

Ο σκοπός του κριτηρίου της αναγκαιότητας είναι να εμποδίσει τον υπεύθυνο της επεξεργασίας να διαφύγει του πεδίου εφαρμογής του άρθρου 22}1, αλλά επικαλούμενος την ύπαρξη μιας τυποποιημένης σύμβασης με το υποκείμενο. Ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει ότι αυτός ο τρόπος επεξεργασίας ήταν απαραίτητος στην συγκεκριμένη περίπτωση, αποκλείοντας την δυνατότητα εφαρμογής μιας λιγότερο επεμβατικής προς την ιδιωτικότητα των προσώπων, μεθόδου.<sup>201</sup> Αν αυτό δεν συμβαίνει, τότε η αλγοριθμική απόφαση δεν ήταν απαραίτητη και συνεπώς δεν επιτρέπεται.

### **3.3.2. Πρόβλεψη από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους**

Η διατύπωση του στοιχείου β του άρθρου 22 του Κανονισμού, σε συνδυασμό με την Αιτιολογική Σκέψη 71 του Προοιμίου, όπου αναφέρεται ότι «η λήψη απόφασης βάση αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ πρέπει να επιτρέπεται όταν προβλέπεται ρητώς από το δίκαιο της Ένωσης ή κράτους μέλους, στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, μεταξύ άλλων για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής», δημιουργεί την εντύπωση ότι τα κράτη μέλη και η ΕΕ μπορούν να επιτρέψουν την αλγοριθμική λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ για απεριόριστους λόγους και σκοπούς.<sup>202</sup> Αυτό δεν σημαίνει, ωστόσο, ότι όταν η νομοθεσία επιτρέπει την αυτοματοποιημένη λήψη αποφάσεων σε έναν συγκεκριμένο τομέα, θα μπορούμε να αποκλίνουμε τελείως από τον ΓΚΠΔ. Οι υπεύθυνοι επεξεργασίας οφείλουν να εξακολουθήσουν να σέβονται τις αρχές προστασίας του Κανονισμού και να εξοπλίζουν τα υποκείμενα των δεδομένων με τα απαραίτητα δικαιώματα προστασίας.

### **3.3.3. Ρητή συγκατάθεση υποκειμένου**

Η συγκατάθεση της παραγράφου 2γ ερμηνεύεται αντιστοίχως με τον γενικό ορισμό της συγκατάθεσης, που δίδεται στο άρθρο 4 του Κανονισμού. Στο πλαίσιο αυτό παρατηρούνται μερικά

---

<sup>199</sup> Hintze M., Automated Individual Decisions to Disclose Personal Data: Why GDPR Article 22 Should Not Apply, 2020, σελ. 7-8

<sup>200</sup> Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, As last Revised and Adopted on 6 February 2018

<sup>201</sup> Article 29 Data Protection Working Party, ο.π.

<sup>202</sup> Noto La Diega G., Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, ο.π., σελ. 19-21

προβλήματα σχετικά με την επεξεργασία που πραγματοποιείται με τη βοήθεια αυτοματοποιημένων μέσων και κυρίως με τη χρήση εφαρμογών τεχνητής νοημοσύνης. Το βασικότερο ζήτημα έγκειται στην δυσκολία εξασφάλισης μιας πλήρως ενημερωμένης συγκατάθεσης του υποκειμένου, καθώς αυτό στις περισσότερες περιπτώσεις, είτε αγνοεί τελείως ότι υφίστανται τα δεδομένα του αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της καταρτίσεως προφίλ ή ακόμα και αν το γνωρίζει δυσκολεύεται να κατανοήσει την σημασία του.

Ο Κανονισμός εισάγει ένα «σύστημα» opt-in, κατά το οποίο η επεξεργασία καταρχήν θεωρείται παράνομη και απαγορεύεται, εκτός και αν συγκατατεθεί σε αυτήν το υποκείμενο.<sup>203</sup> Ο ορισμός της συγκατάθεσης δίδεται στο άρθρο 4 και συγκεκριμένα στο στοιχείο 11, όπου αναφέρεται ότι συγκατάθεση του υποκειμένου αποτελεί «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». Ο θεσμός της συγκατάθεσης συνδέεται με το δικαίωμα του πληροφοριακού αυτοκαθορισμού και αποτελεί στην ουσία της άσκηση αυτού ακριβώς του δικαιώματος.

Η συγκατάθεση αποτελεί δικαιοπραξία, καθώς αποσκοπεί στην παραγωγή του εννόμου αποτελέσματος του επιτρεπτού της επεξεργασίας.<sup>204</sup> Πρέπει να δίδεται σε κατανοητή, εύκολα προσβάσιμη μορφή και με σαφή και απλή διατύπωση.<sup>205</sup> Αυτό μπορεί να επιτευχθεί, μεταξύ άλλων, είτε με ηλεκτρονικά μέσα είτε με προφορική δήλωση. Χαρακτηριστικό παράδειγμα συγκατάθεσης με ηλεκτρονικά μέσα αποτελεί η συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε κάποια διαδικτυακή ιστοσελίδα, όμως στις περιπτώσεις αυτές, όπου η συγκατάθεση επρόκειτο 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.<sup>206</sup> Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Πρέπει επίσης να έχει δοθεί ελεύθερα και εν πλήρει επιγνώσει του υποκειμένου. Αν και δεν αναφέρεται η δυνατότητα άρσης της συγκατάθεσης για μελλοντική αυτοματοποιημένη λήψη αποφάσεων, γίνεται δεκτό ότι ισχύει αναλογικά η παράγραφος 3 του άρθρου 7 και το υποκείμενο έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή.<sup>207</sup>

### **3.3.3.1. Το πρόβλημα της συγκατάθεσης στο πλαίσιο της επεξεργασίας δεδομένων από συστήματα τεχνητής νοημοσύνης**

Προκειμένου η συγκατάθεση να παράξει τα έννομα αποτελέσματά της, νομιμοποιώντας την επεξεργασία, θα πρέπει να έχει δοθεί με συγκεκριμένο τρόπο από το υποκείμενο και να τηρούνται ορισμένα κριτήρια, όπως αναφέρθηκε ανωτέρω. Ορισμένα από αυτά τα κριτήρια αντιμετωπίζουν δυσχέρεια εφαρμογής στο πλαίσιο επεξεργασίας που πραγματοποιείται από συστήματα τεχνητής νοημοσύνης.

<sup>203</sup> Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, 2020, ο.π., σελ. 71

<sup>204</sup> Χριστοδούλου Κ., ο.π., σελ. 82-83

<sup>205</sup> Άρθρο 7)2 του Κανονισμού

<sup>206</sup> Αιτιολογική Σκέψη 32 του Προοιμίου του Κανονισμού

<sup>207</sup> Mendoza I. and Bygrave A. L., The Right not to be Subject to Automated Decisions based on Profiling, ο.π., σελ. 18

Αρχικά στο πλαίσιο του Κανονισμού καθιερώνεται ένα μοντέλο ενημερωμένης συγκατάθεσης, βάσει του οποίου το υποκείμενο προχωρεί στην συγκατάθεση επεξεργασίας των δεδομένων του, εφόσον έχει ενημερωθεί πλήρως σχετικά με αυτήν. Φυσικά το πρόβλημα της επαρκούς ενημέρωσης του υποκείμενου σχετικά με την επεξεργασία των δεδομένων του από αλγοριθμικά συστήματα τεχνητής νοημοσύνης αναφέρθηκε στο προηγούμενο κεφάλαιο, κατανοώντας ότι στο πλαίσιο αυτό είναι ιδιαίτερα δυσχερές η συγκατάθεση εν πλήρει επιγνώσει.

Σε αυτό το πρόβλημα προστίθεται και το γεγονός ότι είναι αρκετά σύνηθες αυτού του είδους η επεξεργασία να καταλήγει στον επαναπροσδιορισμό του σκοπού της επεξεργασίας, μέσω της αναγνώρισης νέων συσχετισμών των δεδομένων ή την διαφορετική κατηγοριοποίησή τους ή άλλων γεγονότων, χωρίς μάλιστα αυτό να είναι πάντοτε προβλέψιμο από τον υπεύθυνο επεξεργασίας.<sup>208</sup> Είναι αρκετά σύνηθες μάλιστα, δεδομένα, τα οποία συλλέχθηκαν για έναν διαφορετικό σκοπό, να χρησιμοποιούνται περαιτέρω για την κατάρτιση προφίλ των υποκειμένων. Η συγκατάθεση του υποκειμένου, όμως, δεν περιλαμβάνει πιθανούς μελλοντικούς τρόπους και σκοπούς επεξεργασίας των δεδομένων τους. Όσα αναφέρθηκαν θα έρχονταν προφανώς σε αντίθεση με την αρχή της ειδικότητας, κατά την οποία η συγκατάθεση πρέπει να αφορά συγκεκριμένο σκοπό επεξεργασίας και συγκεκριμένα δεδομένα. Το γεγονός, ωστόσο, ότι το υποκείμενο των δεδομένων έχει συγκατατεθεί στην επεξεργασία των δεδομένων του για έναν συγκεκριμένο σκοπό δεν καθιστά απαραίτητα την επεξεργασία, που θα πραγματοποιηθεί για έναν διαφορετικό σκοπό οπωσδήποτε παράνομη, καθώς ενδέχεται αυτή να καλύπτεται από κάποια άλλη νομική βάση ή να υπάρχει συμβατότητα μεταξύ του αρχικού και του περαιτέρω σκοπού.<sup>209</sup>

Τέλος ζητήματα δημιουργούνται και σχετικά με το δικαίωμα ανάκλησης της συγκατάθεσης του υποκειμένου, η οποία προβλέπεται στο άρθρο 7}3 του Κανονισμού. Τα συστήματα τεχνητής νοημοσύνης δρουν αποτελεσματικότερα και εξελίσσονται αναλόγως της ποσότητας των δεδομένων που διαθέτουν. Όταν, λοιπόν δίδεται στο υποκείμενο το δικαίωμα ανάκλησης της συγκατάθεσής του στην επεξεργασία των δεδομένων του, όπως αντίστοιχα ισχύει και με το δικαίωμα διαγραφής, τα διαθέσιμα δεδομένα θα περιοριστούν και το σύστημα δεν θα μπορεί πλέον να τα χρησιμοποιήσει για να βελτιώσει τον αλγόριθμο του, με αποτέλεσμα να τίθεται ένας κίνδυνος στην ανάπτυξη της τεχνητής νοημοσύνης εν γένει.<sup>210</sup>

### **3.4. Το περιεχόμενο των παραγράφων 3 και 4**

Η παράγραφος 3 του άρθρου 22 συνεχίζει, καθιερώνοντας ένα minimum προστασίας των δικαιωμάτων των υποκειμένων, προβλέποντας ότι πρέπει να ληφθούν κατάλληλα μέτρα για την αντιμετώπιση του κινδύνου παραβίασης τους, τουλάχιστον εξασφαλίζοντας δικαίωμα ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης, όταν εφαρμόζονται οι εξαιρέσεις της σύμβασης ή της συγκατάθεσης του υποκειμένου της προηγούμενης παραγράφου. Ο κατάλογος αυτός των προαναφερόμενων μέτρων δεν

---

<sup>208</sup> *Mitrou L., Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, ο.π., σελ. 39-40*

<sup>209</sup> European Parliament, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, ο.π., σελ. 41-42

<sup>210</sup> *Mitrou L., Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, ο.π., σελ. 40*

είναι εξαντλητικός.

Στην παράγραφο 4 του άρθρου 22 του Κανονισμού προβλέπεται μια απαγόρευση στις εξαιρέσεις της παραγράφου 2, στις περιπτώσεις των δεδομένων «ειδικής κατηγορίας» του άρθρου 9}1. Παρόλα αυτά και σε αυτήν την περίπτωση διαφαίνονται δύο περιπτώσεις, κατά τις οποίες επιτρέπεται εξαίρεση από τον κανόνα. Αυτές είναι η ρητή συγκατάθεση της παραγράφου 2α του άρθρου 9 και η ύπαρξη ουσιαστικού δημόσιου συμφέροντος βάσει του δικαίου της Ένωσης ή κράτους μέλους, του άρθρου 9}2ζ. Η υποχρέωση της ύπαρξης κατάλληλων μέτρων για την προστασία των δικαιωμάτων υφίσταται και σε αυτήν την περίπτωση και θεωρείται ότι αυτά είναι αντίστοιχα με τα όσα προβλέπονται στην παράγραφο 3, κυρίως δηλαδή εξασφαλίζεται το δικαίωμα της ανθρωπίνης παρέμβασης.

## ΚΕΦΑΛΑΙΟ Ε: ΣΥΜΠΕΡΑΣΜΑΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ

Στο πλαίσιο της παρούσας διπλωματικής επικεντρωθήκαμε στους κινδύνους που επιφυλάσσει και στα προβλήματα που δημιουργεί, η ολοένα και εξελισσόμενη τεχνολογία της τεχνητής νοημοσύνης σχετικά με τα προσωπικά δεδομένα των υποκειμένων, καθώς και τα προσκόμματα που προκαλεί αναφορικά με την τήρηση του Γενικού Κανονισμού Προστασίας Δεδομένων.

Καθίσταται λοιπόν σαφές ότι υφίσταται έντονη ανάγκη διαφύλαξης της ιδιωτικότητας των προσώπων και προστασίας τους από τις υπεράριθμες τεχνολογικές εξελίξεις, οι οποίες παρέχουν πλήθος πλεονεκτημάτων αλλά και μειονεκτημάτων. Αυτό θα επιτευχθεί κυρίως με τον εκσυγχρονισμό του δικαίου και την προσπάθειά του να συμβαδίσει με τις νέες εξελίξεις. Όσο αναπτύσσεται η τεχνολογία και όσο μεγαλύτεροι κίνδυνοι και ανασφάλεια δικαίου δημιουργούνται, πρέπει να εξελίσσεται και το δίκαιο, ώστε να κατορθώσει να προστατεύσει τα πρόσωπα και τα δικαιώματά τους όσο το δυνατόν πιο αποτελεσματικά. Σε αυτή την προσπάθεια πρέπει να προστεθεί και η σημασία της προσωπικής συμβολής για επιμόρφωση, πληροφόρηση των ατόμων σχετικά με τις νέες τεχνολογίες, την τεχνητή νοημοσύνη, τους επιφυλασσόμενους κινδύνους, τις συνέπειες αλλά και τις ενδεχόμενες λύσεις στα εκάστοτε προβλήματα.

## ΒΙΒΛΙΟΓΡΑΦΙΑ

### I. ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΡΘΡΟΓΡΑΦΙΑ:

- *Βόρρας Κ. Απόστολος / Μήτρου Λίλιαν*, Τεχνητή νοημοσύνη και προσωπικά δεδομένα - Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679, ΔΙΤΕ(π. ΔΙΜΕΕ), Τεύχος 4/2018
- *Γιαννόπουλος Ν. Γεώργιος*, Γενικός Κανονισμός Προστασίας Δεδομένων: οι νέες υποχρεώσεις και η ευθύνη του Υπεύθυνου Επεξεργασίας, ΕφημΔΔ 2/2017
- *Ιγγλεζάκης Ιωάννης*, Δίκαιο Πληροφορικής, 3η Έκδοση, Εκδόσεις Σάκκουλα, 2018
- *Jougleux Philippe*, Ευρωπαϊκό δίκαιο του διαδικτύου, Εκδόσεις Σάκκουλα, 2016
- *Λουκάς Η. Νικόλαος*, Τεχνικά μέτρα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) - Κρυπτογράφηση και Ψευδωνυμοποίηση, Περιοδικό Συνήγορος, τεύχος 123/2017
- *Μήτρου Λίλιαν*, Ο Γενικός Κανονισμός Προστασίας Δεδομένων, Εκδόσεις Σάκκουλα, 2017
- *Παναγόπουλου – Κουτνατζή Φερηνίκη*, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, Εκδόσεις Σάκκουλα, 2017
- *Παπακωνσταντίνου Ευάγγελος*, Δίκαιο Πληροφορικής, Εκδόσεις Σάκκουλα, 2010
- *Χριστοδούλου Ν. Κωνσταντίνος*, Δίκαιο Προσωπικών Δεδομένων, Εκδόσεις Νομική Βιβλιοθήκη, 2013
- *Χριστοδούλου Ν. Κωνσταντίνος*, Δίκαιο Προσωπικών Δεδομένων, Εκδόσεις Νομική Βιβλιοθήκη, 2020
- *Χριστοδούλου Ν. Κωνσταντίνος*, Νομικά ζητήματα από την τεχνητή νοημοσύνη, Χρονικά Ιδιωτικού Δικαίου, Μηνιαίο Επιστημονικό Περιοδικό, ΙΘ/2019, Εκδόσεις Π. Ν. Σάκκουλας

### II. ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ - ΑΡΘΡΟΓΡΑΦΙΑ:

- Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 2017
- Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, As last Revised and Adopted on 6 February 2018
- *Abiteboul Serge, Stoyanovich Julia*, Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation, 2019
- *Bayamlioğlu Emre*, Transparency of Automated Decisions in the GDPR: An Attempt for systemisation, Tilburg University/ TILT, 2018
- *Brkan Maja*, Do algorithms rule the world? Algorithmic decision-making in the framework of the GDPR and beyond, Assistant Professor Faculty of Law, Maastricht University, 2018



- *Burrell Jenna*, How the machine ‘thinks’: Understanding opacity in machine learning algorithms, 2016
- *Bygrave A. Lee*, Minding the machine: art 15 of the EC Data Protection Directive and automated profiling, 2000
- Data is power: Profiling and Automated Decision-Making in GDPR (privacyinternational.org), 2017
- Datalisynet, The Norwegian Data Protection Authority, Artificial intelligence and privacy, January 2018
- *Doshi-Velez Finale, Kortz Mason, Budish Ryan, Bavitz Chris, Gershman Sam, O’Brien David, Scott Kate, Shieber Stuart, Waldo James, Weinberger David, Weller Adrian, Wood Alexandra*, Accountability of AI Under the Law: The Role of Explanation, 2017
- European Parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Study, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA), June 2020
- *Ferraris Valeria, Bosco Francesca, Cafiero G., D’Angelo Elena, Suloyeva Y.*, Defining profiling, 2013
- *Genderen Robert van den Hoven van*, Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics, 2017
- *Hintze Mike*, Automated Individual Decisions to Disclose Personal Data: Why GDPR Article 22 Should Not Apply, 2020
- House of Lords, Select Committee on Artificial Intelligence, AI in the UK: ready, willing and able?, 2018
- *Humerick Matthew*, Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, Volume 34/Issue 4, 2018
- *Hunton Andrews Kurth*, Artificial Intelligence and Data Protection, How the GDPR Regulates AI, Centre for Information Policy Leadership, March 2020
- *Kamarinou Dimitra, Millard Christopher, and Singh Jatinder*, Machine Learning with Personal Data, Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016
- *Kroll A. Joshua, Huey Joanna, Barocas Solon, Felten W. Edward, Reidenberg R. Joel, Robinson G. David & Yu Harlan*, Accountable Algorithms, University of Pennsylvania Law Review Vol. 165: 633, 2017
- *Kuner Christopher, Svantesson B. Dan Jerker, Cate H. Fred, Lynskey Orla, Millard Christopher*, Machine learning with personal data: is data protection law smart enough to meet the challenge?, International Data Privacy Law, Volume 7/Issue 1, February 2017
- *Lubarsky Boris*, Re- Identification of “anonymized data”, 2017
- *Malgieri Gianclaudio, Comandé Giovanni*, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law, Volume 7/Issue 4, November 2017
- *Manheim Karl and Kaplan Lyric*, Artificial Intelligence: Risks to Privacy and Democracy, 21 Yale J.L. & Tech. 106, 2019
- *Mendoza Isak and Bygrave A. Lee*, The Right not to be Subject to Automated Decisions based

on Profiling, University of Oslo, Faculty of Law, Legal Studies Research Paper Series No. 2017-20

- *Mitrou Lilian*, Artificial Intelligence and Cognitive Services / Is the General Data Protection Regulation (GDPR) “Artificial Intelligence proof”, University of the Aegean Data Protection, 2019
- *Noto La Diega Guido*, Against the Dehumanisation of Decision-Making Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information, 2018
- *Rudovsky David, Rosenthal Lawrence*, Debate: The Constitutionality of Stop-and-Frisk in New York City, 2013
- *Selbst D. Andrew, Powles Julia*, Meaningful information and the right to explanation, International Data Privacy Law, Volume 7/ Issue 4, November 2017
- *Sloan H. Robert and Warner Richard*, When Is an Algorithm Transparent?: Predictive Analytics, Privacy, and Public Policy, vol. 16, May/June 2018
- *Sreenu G, Saleem Durai M. A.*, Intelligent video surveillance: a review through deep learning techniques for crowd analysis, Journal of Big Data, volume 6, Article number: 48, 2019
- *Yang Qiang*, Activity Recognition: Linking Low-level Sensors to High-level Intelligence, Department of Computer Science and Engineering, Hong Kong University of Science and Technology, 2009

### III. ΙΣΤΟΤΟΠΟΙ

- [https://www.sas.com/el\\_gr/insights/big-data/what-is-big-data.html](https://www.sas.com/el_gr/insights/big-data/what-is-big-data.html)
- [https://el.wikipedia.org/wiki/Επιβλεπόμενη\\_μάθηση](https://el.wikipedia.org/wiki/Επιβλεπόμενη_μάθηση)
- [https://el.wikipedia.org/wiki/Τεχνητή\\_νοημοσύνη](https://el.wikipedia.org/wiki/Τεχνητή_νοημοσύνη)
- [https://el.wikipedia.org/wiki/Μηχανική\\_μάθηση](https://el.wikipedia.org/wiki/Μηχανική_μάθηση)
- [https://en.wikipedia.org/wiki/Article\\_29\\_Data\\_Protection\\_Working\\_Party](https://en.wikipedia.org/wiki/Article_29_Data_Protection_Working_Party)
- <https://el.wikipedia.org/wiki/Αλγόριθμος>
- [https://en.wikipedia.org/wiki/Predictive\\_analytics](https://en.wikipedia.org/wiki/Predictive_analytics)
- <https://ncube.com/blog/big-data-and-ai>
- <https://www.isico-datenschutz.de/en/ai-gdpr-anonymisation-and-pseudonymisation/>
- <https://www.record-evolution.de/en/data-anonymization-techniques-and-best-practices-a-quick-guide/>
- <https://ntokas.gr/anonymous-data/>
- [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing\\_el](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_el)
- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/>
- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>

- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when4>
- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>
- <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>
- <https://theartofcrime.gr/stop-frisk/>
- <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scrapes-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>
- <https://www.wikipedia.org/>
- <https://www.europarl.europa.eu/news/el/headlines/society/20200827STO85804/ti-einai-i-techniti-noimosuni-kai-pos-chrisimopoieitai>