ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
Τμήμα Οικονομικών Επιστημών

MSc law & economics
DEPARTMENT of ECONOMICS, UNIVERSITY of MACEDONIA and SCHOOL of LAW, ARISTOTLE UNIVERSITY of THESSALONIKI

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
Νομική Σχολή

ΔΙΪΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΚΑ

<u>Διπλωματική Εργασία</u>

ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΠΟΧΗ ΤΩΝ BIG DATA ANALYTICS

Της

ΠΑΝΑΓΙΩΤΑΣ – ΠΩΛΙΝΑΣ ΒΕΝΤΖΙΟΥ

Υποβλήθηκε ως απαιτούμενο για την απόκτηση του Μεταπτυχιακού Διπλώματος
Ειδίκευσης Δίκαιο και Οικονομικά
με εξειδίκευση στον τομέα: Δίκαιο και Οικονομικά στον τομέα των Επιχειρήσεων

Νοέμβριος, 2020

Τμήμα Οικονομικών Επιστημών

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
Νομική Σχολή

ΔΙΪΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΚΑ

Διπλωματική Εργασία

ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΕΠΟΧΗ ΤΩΝ BIG DATA ANALYTICS

PRIVACY AND PERSONAL DATA PROTECTION IN THE ERA OF BIG DATA ANALYTICS

Της

ΠΑΝΑΓΙΩΤΑΣ – ΠΩΛΙΝΑΣ ΒΕΝΤΖΙΟΥ

Εξεταστική επιτροπή

Ασπασία Τσαούση, Αναπληρώτρια Καθηγήτρια στον Τομέα Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου, Νομική Σχολή ΑΠΘ, Επιβλέπουσα

Ευμορφία Τζίβα, Αναπληρώτρια Καθηγήτρια στον Τομέα Εμπορικού και Οικονομικού Δικαίου, Νομική Σχολή ΑΠΘ

Άννα Δεσποτίδου, Λέκτορας στον Τομέα Εμπορικού και Οικονομικού Δικαίου, Νομική Σχολή ΑΠΘ

Ευχαριστίες

Αρχικά, θα ήθελα να ευχαριστήσω θερμά όλους, όσους αποτέλεσαν αρωγοί στην εκπόνηση της παρούσας διπλωματικής εργασίας, στο πλαίσιο του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Δίκαιο και Οικονομικά». Ιδιαίτερα δε, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου κ. Ασπασία Τσαούση, Αναπληρώτρια Καθηγήτρια της Νομικής Σχολής του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης, του Τμήματος Ιστορίας, Φιλοσοφίας και Κοινωνιολογίας του Δικαίου για τη συνεργασία, την υποστήριξη και την πολύτιμη καθοδήγηση που μου προσέφερε καθ' όλη τη διάρκεια του μεταπτυχιακού προγράμματος και της συγγραφής της διπλωματικής μου εργασίας. Επίσης, θα ήθελα να ευχαριστήσω όλα τα μέλη της εξεταστικής επιτροπής για την καθοδήγηση, τις συμβουλές και τις παρατηρήσεις τους.

Τέλος, θα ήθελα να αφιερώσω την εργασία μου στην οικογένειά μου, στους γονείς μου και στον αδελφό μου, που είναι πάντα δίπλα μου και με στηρίζουν σε κάθε μου απόφαση.

Παναγιώτα – Πωλίνα Βέντζιου,

Θεσσαλονίκη, 2020

Περίληψη

Η παρούσα διπλωματική εργασία αποσκοπεί αφενός στη διερεύνηση του φαινομένου της ανάλυσης μαζικών δεδομένων (Big Data Analytics), καθώς και των δυνατοτήτων και των κινδύνων που συνεπάγεται η χρήση τους και αφετέρου στην ανάλυση της νομικής αντιμετώπισης του φαινομένου αυτού, κυρίως μέσω του Γενικού Κανονισμού για την Προστασία των Δεδομένων (Κανονισμού 2016/679). Ειδικότερα, τα Big Data Analytics, τα οποία χρησιμοποιούνται σήμερα ευρέως τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα, αναφέρονται στη δυνατότητα επεξεργασίας και ανάλυσης τεράστιων ποσοτήτων δομημένων και αδόμητων δεδομένων, τα οποία παράγονται και ανανεώνονται διαρκώς από ένα πλήθος διαφορετικών πηγών, κυρίως χάρη στις δυνατότητες που προσφέρουν τα συστήματα τεχνητής νοημοσύνης και δη τα συστήματα μηχανικής μάθησης. Τα κέρδη από τη χρήση των Big Data Analytics είναι πολλά, εντούτοις δεν εκλείπουν και οι κίνδυνοι για τα θεμελιώδη δικαιώματα και τις ελευθερίες των ανθρώπων. Στο πλαίσιο αυτό, ο Γενικός Κανονισμός για την Προστασία των Δεδομένων αποτελεί σήμερα το σημαντικότερο νομοθετικό εργαλείο για την αντιμετώπιση των ανωτέρω κινδύνων, έτσι ώστε να καταστεί δυνατή η αξιοποίηση των Big Data Analytics στον μέγιστο δυνατό βαθμό, με σεβασμό στις ευρωπαϊκές αξίες, στα ανθρωπινά δικαιώματα και στις ελευθέριες. Ωστόσο, παρά το διευρυμένο πεδίο εφαρμογής του Κανονισμού και το καινοτόμο ρυθμιστικό πλαίσιο που εισάγει, φαίνεται, ότι υπάρχουν αρκετά ζητήματα κατά την εφαρμογή των διατάξεών του στην πράξη, με αποτέλεσμα να επιβαρύνονται σε μεγάλο βαθμό οι υπεύθυνοι επεξεργασίας που καλούνται να συμμορφωθούν με αυτές, καθώς και να μην επιτυγχάνεται εν τέλει η αποτελεσματική προστασία των δικαιωμάτων των υποκειμένων. Ο εντοπισμός των πρακτικών αυτών ζητημάτων αποτελεί το πρώτο βήμα για την αποτελεσματικότερη εφαρμογή του Κανονισμού και τη δημιουργία ενός κλίματος εμπιστοσύνης στις σύγχρονες ψηφιακές οικονομίες και κοινωνίες.

Λέξεις κλειδιά: Big Data Analytics, τεχνητή νοημοσύνη, μηχανική μάθηση, ΓΚΠΔ, προσωπικά δεδομένα, ιδιωτικότητα

Abstract

The present dissertation aims on one hand to investigate Big Data Analytics, as well as the potential and the risks that result from their use and on the other hand to analyze the legal treatment of this phenomenon, mainly by the General Data Protection Regulation (Regulation 2016/679). In particular, Big Data Analytics, which are widely used today in both the private and the public sector, refer to the ability of processing and analyzing huge amounts of structured and unstructured data, which are constantly generated and updated from several different sources, mainly because of the capabilities offered by artificial intelligence systems, i.e. machine learning systems. The benefits of Big Data Analytics are many, however, there are also risks for fundamental human rights and freedoms. In this context, the General Data Protection Regulation is today the most important legislative tool to address the aforementioned risks, in order to make the most of Big Data Analytics, with respect for European values, human rights and freedoms. However, despite the expanded scope of the Regulation and the innovative regulatory framework it introduces, it appears that there are a number of issues concerning the implementation of its provisions and as a result, the controllers who are required to comply with them are considered greatly burdened, while at the same time the effective protection of the subjects' rights is not ultimately achieved. Identifying these practical issues constitutes the first step towards the more effective implementation of the Regulation and the creation of a climate of trust in modern digital economies and societies.

Keywords: Big Data Analytics, artificial intelligence, machine learning, GDPR, personal data, privacy

Πίνακας Περιεχομένων

Συντομογραφίες

AI	Artificial Intelligence
Art. 29 WP	Article 29 Data Protection Working Party
CNIL	Commission nationale de l'informatique et des libertés
GDPR	General Data Protection Regulation
FRA	European Union Agency for Fundamental Rights
ICO	Information Commissioner’s Office
ΑΕΠ	Ακαθάριστο Εθνικό Προϊόν
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
βλ.	βλέπε
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία των Δεδομένων
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
Ε.Ε.	Ευρωπαϊκή Ένωση
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΗΠΑ	Ηνωμένες Πολιτείες της Αμερικής
κ.ά.	και άλλα
κ.τ. λ.	και τα λοιπά
ΟΕΥΕ για την ΤΝ	Ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
π.χ.	παραδείγματος χάρη
ΧΘΔ	Χάρτης των Θεμελιωδών Δικαιωμάτων

1. Εισαγωγή

Οι έννοιες της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων δεν είναι καινούργιες. Αντιθέτως, η προστασία του ιδιωτικού βίου και η εξασφάλιση της δυνατότητας να ελέγχει ο καθένας τις πληροφορίες που τον / την αφορούν αποτελούν διαχρονικά και διατοπικά ζητήματα. Το ενδιαφέρον για τα δικαιώματα αυτά έγινε ιδιαίτερα έντονο μετά τον Β' Παγκόσμιο Πόλεμο και ειδικότερα, σε ευρωπαϊκό επίπεδο έχουν και τα δύο αναχθεί σε θεμελιώδη. Συγκεκριμένα, το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής αναγνωρίσθηκε ήδη το 1950 με την υπογραφή της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (εφεξής ΕΣΔΑ), στο άρθρο 8 αυτής, ενώ ακολούθησε η έκδοση από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (εφεξής ΟΟΣΑ) το 1980 των Κατευθυντήριων Γραμμών για την προστασία του απορρήτου και των διασυνοριακών ροών προσωπικών δεδομένων, οι οποίες αν και δεν διαθέτουν νομικά δεσμευτική ισχύ, εντούτοις θέτουν μια σειρά από γενικές αρχές που διέπουν την επεξεργασία των δεδομένων (Πλατής, 2018). Εν συνεχεία, υπογράφηκε η από 28/01/1987 Σύμβαση 108 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, η οποία αποτελεί τη μοναδική νομικά δεσμευτική διεθνή πράξη στον τομέα της προστασίας δεδομένων. Τέλος, στον Χάρτη των Θεμελιωδών Δικαιωμάτων (εφεξής ΧΘΔ) περιλήφθηκαν τόσο το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής (άρθρο 7) όσο και το δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα (άρθρο 8).

Τα δύο αυτά δικαιώματα, αν και αυτοτελή, συνδέονται πολύ στενά και σε μεγάλο βαθμό αλληλεπικαλύπτονται, καθώς η ιδιωτικότητα αποτελεί τον πυρήνα της προστασίας των προσωπικών δεδομένων (Kokott & Sobotta, 2013). Όπως αναφέρει χαρακτηριστικά και ο Πλατής (2018): «η ιδιωτικότητα είναι η δικαιολογητική βάση για την απαγόρευση της κρατικής παρέμβασης στον ιδιωτικό και οικογενειακό βίο ενώ εμφανίζεται σαν το δικαιοπολιτικό θεμέλιο για την ελευθερία της σκέψης, τις προσωπικές επιλογές του ατόμου για κάθε πτυχή της ιδιωτικής του ζωής. Στο σημείο αυτό συνδέεται και με τον περιορισμό της χρήσης δεδομένων προσωπικού χαρακτήρα».

Με το τέλος του 20ου αιώνα και τη μετάβαση στην εποχή της πληροφορίας (ή αλλιώς ψηφιακή εποχή), όπου η οικονομία βασίζεται κατά κύριο λόγο σε τεχνολογίες της πληροφορίας και στην ψηφιοποίηση αυτής, τα ανωτέρω δικαιώματα έχουν δοκιμαστεί σε μεγάλο βαθμό (Πλατής, 2018). Με αποκορύφωμα τη δημιουργία του Διαδικτύου, το οποίο εισχώρησε ραγδαία σε όλους τους τομείς της καθημερινότητας των ανθρώπων, η ψηφιακή εποχή έχει φθάσει πλέον στο στάδιο της λεγόμενης «δεδομενοποίησης» των κοινωνιών, δηλαδή στην όλο και αυξανόμενη μετατροπή

διαφόρων πτυχών της ζωής των ανθρώπων σε δεδομένα (Fuster & Scherrer, 2015). Στο πλαίσιο αυτό, η παραγωγή και η δυνατότητα αποθήκευσης μεγάλου όγκου δεδομένων προερχόμενων από διαφορετικές πηγές έχουν αποκτήσει σήμερα ιδιαίτερο νόημα λόγω της ανάπτυξης τεχνολογιών, ικανών να "διαβάσουν" και να "κατανοήσουν" αυτήν την πληθώρα δεδομένων και να την αξιοποιήσουν καταλλήλως. Το φαινόμενο αυτό, το οποίο στη βιβλιογραφία αναφέρεται ως “Big Data Analytics”, έχει κατακλύσει τις σύγχρονες οικονομίες, υποστηρίζοντας δευτερευόντως τις παραδοσιακές αγορές αγαθών και υπηρεσιών, όπου στο πλαίσιο μιας συναλλαγής ενδέχεται να υπάρξει ανταλλαγή και επεξεργασία των προσωπικών δεδομένων του καταναλωτή αλλά και δημιουργώντας μια νέα αγορά προσωπικών δεδομένων, όπου αντικείμενο των συναλλαγών αποτελούν τα ίδια τα δεδομένα, ή όπου αγαθά και υπηρεσίες παρέχονται «δωρεάν» με αντάλλαγμα την αποκάλυψη προσωπικών δεδομένων (π.χ. μέσα κοινωνικής δικτύωσης, μηχανές αναζήτησης κ.τ.λ.) (Acquisti, 2014). Δεν είναι άλλωστε τυχαίο το γεγονός, ότι τα προσωπικά δεδομένα έχουν χαρακτηριστεί σήμερα ως το νέο πετρέλαιο του διαδικτύου και το νέο νόμισμα του ψηφιακού κόσμου (Hoofnagle, van der Sloot & Borgesius, 2019). Χαρακτηριστικά, ο κλάδος των μαζικών δεδομένων αυξάνεται κατά 40% ανά έτος (Ευρωπαϊκό Κοινοβούλιο, 2018), ενώ συλλογικά, οι μεγαλύτερες επιχειρήσεις στον τομέα της τεχνολογίας (Facebook, Amazon, Apple, Netflix και Google) έχουν καθαρή αξία 3,5 τρισεκατομμύρια δολάρια, περίπου ίση με το ΑΕΠ της Γερμανίας, της τέταρτης μεγαλύτερης οικονομίας στον κόσμο (Manheim & Kaplan, 2018).

Η παρουσία των Big Data Analytics σε όλο και περισσότερους τομείς της οικονομίας και της κοινωνίας παρά τις δυνατότητες που προσφέρουν, δημιουργούν παράλληλα νέους και σημαντικούς κινδύνους για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των ανθρώπων. Τα αλματώδη αυτά βήματα της τεχνολογίας και η ανάγκη ενίσχυσης της προστασίας των ανωτέρω θεμελιωδών δικαιωμάτων έγιναν αντιληπτά από την Ευρωπαϊκή Ένωση (εφεξής Ε.Ε.), η οποία σε επίπεδο δευτερογενούς πλέον δικαίου συνειδητοποίησε την ανάγκη εκσυγχρονισμού της Οδηγίας 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών», η οποία βρίσκονταν σε ισχύ από το 1995 και προχώρησε στην αντικατάσταση της από τον Γενικό Κανονισμό για την Προστασία Δεδομένων - Κανονισμό 2016/679 (εφεξής ΓΚΠΔ), ο οποίος βρίσκεται πλέον σε ισχύ από την 25η Μαΐου 2018.

Σκοπός της παρούσας εργασίας είναι αφενός να εξηγήσει τι είναι τα Big Data Analytics, τις δυνατότητες που ενδεχομένως να προσφέρουν για την οικονομία και γενικότερα για την κοινωνία αλλά και τους κινδύνους που ελλοχεύει η χρήση τους για τα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των προσωπικών δεδομένων και αφετέρου να προχωρήσει σε μια επισκόπηση των βασικότερων διατάξεων του πρόσφατου ΓΚΠΔ που αφορούν και επηρεάζουν την εφαρμογή των Big Data Analytics και να εξηγήσει κατά πόσο οι διατάξεις αυτές είναι ενδεχομένως σε θέση να διασφαλίσουν την τήρηση και τον σεβασμό των ανωτέρω θεμελιωδών δικαιωμάτων.

Αναλυτικότερα, στα κεφάλαια που ακολουθούν επιχειρείται να δοθεί ένας ορισμός των Big Data Analytics, καθώς και μια αναλυτική περιγραφή των κυριότερων χαρακτηριστικών του φαινομένου αυτού (βλ. κεφάλαιο 2). Εν συνεχεία, γίνεται μια συστηματοποίηση των κυριότερων περιπτώσεων θεμιτής χρήσης των Big Data Analytics που παρουσιάζουν πολλά οφέλη τόσο σε ατομικό, όσο και σε συλλογικό επίπεδο, καθώς και των σημαντικότερων κινδύνων που ενδέχεται να προκύψουν από τη χρήση τους (βλ. κεφάλαια 3 και 4) και συγκεκριμένα γίνεται λόγος για την αδιαφάνεια που χαρακτηρίζει τα συστήματα αυτά, για την έλλειψη ελέγχου και την αβεβαιότητα των χρηστών ως προς τα προσωπικά τους δεδομένα, για τυχόν διακρίσεις και άδικα αποτελέσματα που ενδέχεται να προκύψουν, καθώς και για τη χειραγώγηση των χρηστών.

Στο δεύτερο μέρος της εργασίας (βλ. κεφάλαιο 5), γίνεται μια συστηματική ανάλυση των σημαντικότερων διατάξεων του ΓΚΠΔ που επηρεάζουν τη λειτουργία των Big Data Analytics, στις οποίες περιλαμβάνονται τόσο κάποιες από τις αρχές που διέπουν την επεξεργασία των δεδομένων, όσο και διατάξεις που χορηγούν δικαιώματα στα υποκείμενα των δεδομένων και αντίστοιχα υποχρεώσεις στους υπεύθυνους επεξεργασίας. Παράλληλα, επιχειρείται ο εντοπισμός των σημαντικότερων προβλημάτων που δημιουργούνται κατά την εφαρμογή των διατάξεων αυτών στην πράξη, υποσκάπτοντας την αποτελεσματικότητά τους. Στο κεφάλαιο 6 γίνεται μια σύντομη αναφορά στην έννοια της συλλογικής ιδιωτικότητας που έχει κινήσει τον τελευταίο καιρό το νομικό ενδιαφέρον. Έπειτα, ακολουθεί η συζήτηση και τα συμπεράσματα που προέκυψαν από την παρούσα εργασία.

Στο τέλος της παρούσας διπλωματικής εργασίας, παρατίθεται το σύνολο των βιβλιογραφικών παραπομπών που χρησιμοποιήθηκαν για τη συγγραφή της, ελληνόγλωσσων και ξενόγλωσσων, καθώς και το σύνολο της νομολογίας και τις νομοθεσίας, στις οποίες γίνεται αναφορά καθ’ όλη τη διάρκεια αυτής.

2. Τι είναι τα Big Data Analytics;

Το φαινόμενο των Big Data Analytics ξεκίνησε να απασχολεί εντονότερα την ακαδημαϊκή κοινότητα από το 2011 και μετά, ωστόσο μέχρι και σήμερα δεν υπάρχει ένας κοινά αποδεκτός ορισμός. Σύμφωνα με το γλωσσάριο Gartner, που παρέχει έναν από τους πιο γνωστούς ορισμούς: «Τα Big Data είναι μεγάλου μεγέθους, υψηλής ταχύτητας και μεγάλης ποικιλίας πληροφορίες που απαιτούν οικονομικά αποδοτικές, καινοτόμες μορφές πληροφοριακής επεξεργασίας για την επίτευξη βελτιωμένης γνώσης και για τη λήψη αποφάσεων» ("Big Data", n.d.). Η έννοια, επομένως, των Big Data Analytics θα μπορούσε να χωριστεί σε δύο σκέλη: α) στην ύπαρξη άμεσων, ποικίλων δεδομένων σε τεράστιες ποσότητες και β) στη δυνατότητα που παρέχουν οι σύγχρονες τεχνολογίες να αναλύσουν τα δεδομένα αυτά και να τα αξιοποιήσουν καταλλήλως.

Το πρώτο σκέλος του ορισμού αφορά τα βασικά χαρακτηριστικά των δεδομένων που χρησιμοποιούνται στα Big Data Analytics. Στην ιστοσελίδα της Ευρωπαϊκής Επιτροπής (European Commission, 2020α) αναφέρεται σχετικά ότι: «Τα Big Data αφορούν μεγάλες ποσότητες δεδομένων που παράγονται πολύ γρήγορα από έναν μεγάλο αριθμό διαφορετικών πηγών». Τα βασικά επομένως γνωρίσματα των πληροφοριών που σχετίζονται με τα Big Data Analytics είναι τρία: το μέγεθος, η ποικιλία και η ταχύτητα, τα οποία αναφέρονται στη βιβλιογραφία και ως τα 3V's (*volume, variety, velocity*).

Όσον αφορά το μέγεθος (*volume*), η καθιέρωση του διαδικτύου σε πολλούς τομείς της καθημερινότητας έχει οδηγήσει σε δραματική αύξηση των παραγόμενων δεδομένων και στη δημιουργία γιγαντιαίων βάσεων δεδομένων, η επεξεργασία των οποίων απαιτεί εξελιγμένες υπολογιστικές δομές. Χαρακτηριστικά, μόνο από την πλατφόρμα κοινωνικής δικτύωσης Facebook παράγονται καθημερινά 4 petabytes δεδομένων (όπου 1 petabyte ισούται με 1.000^5 bytes) (Desjardins, 2019) ενώ κάθε δευτερόλεπτο πραγματοποιούνται 82.285 αναζητήσεις στη μηχανή αναζήτησης της Google (https://www.internetlivestats.com/one-second/#google-band). Συνολικά δε, ο ψηφιακός κόσμος αναμένεται να ανέλθει το έτος 2020 στα 44 zettabytes (όπου 1 zettabyte ισούται με 1.000^7 bytes) και το έτος 2025 στα 175 zettabytes (Desjardins, 2019· European Commission, 2020β).

Η ποικιλία (*variety*) αφορά αφενός την ετερογένεια των δεδομένων και αφετέρου το πλήθος των πηγών από τις οποίες αυτά προέρχονται. Συγκεκριμένα, τα δεδομένα μπορεί να είναι δομημένα (π.χ. όνομα, διεύθυνση, ηλικία) ή και αδόμητα (π.χ. εικόνα, ήχος, βίντεο), με αποτέλεσμα να χρειάζονται διαφορετικές τεχνικές για την επεξεργασία της κάθε κατηγορίας (Skiena, 2017). Επιπλέον, δεδομένα παράγονται

σήμερα από την περιήγηση στο διαδίκτυο, από διαδικτυακές συναλλαγές, από τη χρήση μηχανών αναζήτησης, από την ηλεκτρονική αλληλογραφία, από την παρουσία στα μέσα κοινωνικής δικτύωσης και γενικά από οποιαδήποτε δραστηριότητα πραγματοποιείται "online". Σημαντική πηγή δεδομένων αποτελεί και το λεγόμενο Διαδίκτυο των Πραγμάτων (*Internet of Things*), "έξυπνα" δηλαδή καθημερινά αντικείμενα ή συσκευές –εκτός από υπολογιστές, κινητά και τάμπλετ - τα οποία είναι συνδεδεμένα στο διαδίκτυο και ανταλλάσσουν πληροφορίες (Federal Trade Commission, 2015) (π.χ. αυτοκίνητα, ηλεκτρικές συσκευές, λάμπες).

Τα δεδομένα και οι πληροφορίες που παράγονται από όλες αυτές τις διαφορετικές πηγές μπορεί είτε να σχετίζονται με κάποιο συγκεκριμένο πρόσωπο είτε να είναι εντελώς απρόσωπα (π.χ. γεωλογικές μετρήσεις, δεδομένα καιρού). Ειδικότερα, αναφορικά με τα προσωπικά δεδομένα, η ομάδα εργασίας του άρθρου 29 στις κατευθυντήριες γραμμές της για την αυτοματοποιημένη ατομική λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του ΓΚΠΔ (Article 29 Data Protection Working Party [Art. 29 WP], 2017α) προβαίνει στην εξής διάκριση με βάση την πηγή προέλευσής τους:

- Δεδομένα που παρέχονται απευθείας από τα ενδιαφερόμενα άτομα (όπως απαντήσεις σε ερωτηματολόγιο ή η διεύθυνση και το ονοματεπώνυμο για την πραγματοποίηση μιας ηλεκτρονικής συναλλαγής).
- Δεδομένα που έχουν παρατηρηθεί σχετικά με τα άτομα (όπως τα δεδομένα τοποθεσίας που συλλέγονται μέσω μιας αίτησης, τα δεδομένα που συλλέγονται μέσω των cookies ή από το Διαδίκτυο των Πραγμάτων).
- Δεδομένα που έχουν εξαχθεί ή συναχθεί, όπως ένα προφίλ του ατόμου που έχει ήδη δημιουργηθεί.

Η ταχύτητα (*velocity*) αναφέρεται στον αυξανόμενο ρυθμό συλλογής των δεδομένων, επεξεργασίας αυτών, καθώς και εξαγωγής γνώσεων και απαντήσεων από αυτά σε πραγματικό χρόνο (Klous, 2016). Συγκεκριμένα, η ταχεία εξάπλωση των ψηφιακών συσκευών έχει οδηγήσει σε έναν πρωτοφανή ρυθμό δημιουργίας δεδομένων που έχει ως αποτέλεσμα τη δημιουργία μιας όλο και μεγαλύτερης ανάγκης για ανάλυση και εξαγωγή εφαρμόσιμων συμπερασμάτων από αυτά σε πραγματικό χρόνο (Gandomi & Haider, 2015).

Εκτός από τα τρία αυτά βασικά χαρακτηριστικά των Big Data, στη βιβλιογραφία αναφέρονται και δύο ακόμα, η εγκυρότητα (*veracity*) και η αξία (*value*), έτσι ώστε στην πραγματικότητα να γίνεται λόγος για τα 5 V's. Η εγκυρότητα αναφέρεται στην ανάγκη αντιμετώπισης ανακριβών και αβέβαιων δεδομένων, στην

ανάγκη δηλαδή να υπάρχει εμπιστοσύνη απέναντι στα δεδομένα, ενώ η αξία στη δυνατότητα εξαγωγής πολλών, σημαντικών και αξιοποιήσιμων πληροφοριών από τις μεγάλες ποσότητες δεδομένων. Στην προσπάθεια ορισμού του φαινομένου αυτού έχουν χρησιμοποιηθεί και άλλες, παρόμοιες περιγραφικές έννοιες (*exhaustivity, variability, complexity* κ.τ.λ.). Από την άλλη, έχει υποστηριχθεί, ότι ο ορισμός αυτός των Big Data δεν είναι ακριβής καθώς υπάρχουν διάφορες μορφές βάσεων δεδομένων, οι οποίες δεν μοιράζονται όλες τα ίδια χαρακτηριστικά (Kitchin & McArdle, 2016). Σε κάθε περίπτωση πάντως, ακόμα και αν εμφανίζονται κάποιες διαφοροποιήσεις μεταξύ των χαρακτηριστικών τους, τα Big Data Analytics αναφέρονται σε πολύ μεγάλες βάσεις ετερόκλητων δεδομένων που ανανεώνονται διαρκώς και σε πραγματικό χρόνο, περιέχοντας ενδεχομένως και ανακριβή ή αβέβαια δεδομένα και οι οποίες "κρύβουν" χρήσιμες και αξιοποιήσιμες πληροφορίες, που δεν μπορούν να εξαχθούν με τις παραδοσιακές μεθόδους ανάλυσης δεδομένων.

Στο πλαίσιο αυτό έρχεται το δεύτερο σκέλος του ορισμού των Big Data Analytics, η δυνατότητα δηλαδή συλλογής, αποθήκευσης, επεξεργασίας και ανάλυσης τεράστιων ποσοτήτων δεδομένων χάρη στην ύπαρξη μεγαλύτερης υπολογιστικής δύναμης. Πιο συγκεκριμένα, καθοριστική για την εξέλιξη των Big Data Analytics αποτέλεσε κατ' αρχάς η δυνατότητα αποθήκευσης και μετακίνησης των τεράστιων όγκων δεδομένων που παράγονται με χαμηλό κόστος, κυρίως χάρη στην τεχνολογία του υπολογιστικού νέφους (*cloud computing*), μέσω του οποίου η διάθεση των υπολογιστικών πόρων γίνεται από απόσταση και, ως εκ τούτου, τα δεδομένα εκφεύγουν από κάθε έλεγχο (Ιγγλεζάκης, 2020). Χαρακτηριστικά, στο άρθρο του Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (Information Commissioner's Office [ICO], 2017) αναφέρεται ότι: «τα Big Data είναι αυτό που συνέβη όταν το κόστος αποθήκευσης πληροφοριών έγινε μικρότερο από το κόστος του να τις ξεφορτωθείς».

Παράλληλα, μέσω της τεχνητής νοημοσύνης καθίσταται πλέον δυνατό να "ξεκλειδωθεί", να αποκωδικοποιηθεί η γνώση που είναι κρυμμένη μέσα σε αυτήν την πληθώρα δεδομένων που υπάρχει σήμερα. Η ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη (ΟΕΥΕ για την ΤΝ, 2019α) έχει δώσει τον εξής ορισμό για την τεχνητή νοημοσύνη: «Τα συστήματα τεχνητής νοημοσύνης (ΤΝ) είναι συστήματα λογισμικού (ή ενδεχομένως και υλισμικού) που σχεδιάζονται από ανθρώπους και, βάσει ενός δεδομένου σύνθετου στόχου, ενεργούν στην υλική ή ψηφιακή διάσταση με το να αντιλαμβάνονται το περιβάλλον τους μέσω της απόκτησης δεδομένων, να ερμηνεύουν τα δομημένα ή αδόμητα δεδομένα που έχουν συλλεχθεί, να

προβαίνουν σε συλλογισμούς με βάση τις γνώσεις ή να επεξεργάζονται τις πληροφορίες που εξάγονται από αυτά τα δεδομένα και να αποφασίζουν ποια είναι η βέλτιστη ενέργεια (ή οι βέλτιστες ενέργειες) που θα πρέπει να εκτελέσουν για να επιτύχουν τον δεδομένο στόχο. Τα συστήματα ΤΝ μπορεί είτε να χρησιμοποιούν συμβολικούς κανόνες είτε να μαθαίνουν ένα αριθμητικό μοντέλο και μπορεί επίσης να προσαρμόζουν τη συμπεριφορά τους με το να αναλύουν πώς επηρεάζεται το περιβάλλον από τις προηγούμενες ενέργειές τους». Τα συστήματα τεχνητής νοημοσύνης έχουν δηλαδή την ικανότητα να αντιλαμβάνονται τον κόσμο συλλέγοντας και ερμηνεύοντας δεδομένα, να προβαίνουν σε υπολογιστικούς συλλογισμούς και να εξάγουν πληροφορίες από αυτά προκειμένου να επιλύσουν ένα πρόβλημα και να λάβουν σχετικές αποφάσεις, δίνοντας έτσι στους υπολογιστές συμπεριφορές που θα θεωρούνταν ευφυείς / έξυπνες σε έναν άνθρωπο (ICO, 2017). Για την επίτευξη του σκοπού τους, τα συστήματα τεχνητής νοημοσύνης χρησιμοποιούν αλγορίθμους, ακολουθίες, δηλαδή, εντολών που δίνονται σε έναν υπολογιστή για τη μετατροπή μιας καταχώρησης (*input*) σε ένα αποτέλεσμα (*output*) (European Union Agency for Fundamental Rights [FRA], 2018).

Ειδικότερα, σήμερα γίνεται λόγος για τη στενή τεχνητή νοημοσύνη (*narrow artificial intelligence*), στα πλαίσια της οποίας δημιουργούνται συστήματα, τα οποία μπορούν να εκτελέσουν μόνο μια εργασία πολύ καλά, χωρίς να μπορούν να μεταφέρουν τη γνώση τους σε κάποιο άλλο έργο (Rellion, 2018). Στόχος – αν και ακόμη και σήμερα φαντάζει ανέφικτος, δεδομένου ότι υπάρχουν πολλές ανοιχτές ηθικές, επιστημονικές και τεχνολογικές προκλήσεις - είναι η επίτευξη της λεγόμενης δυνατής τεχνητής νοημοσύνης (*strong artificial intelligence*), όπου τα συστήματα εμφανίζουν ανθρώπινη νοημοσύνη, κοινή λογική και αυτογνωσία και μπορούν να θέτουν αυτόνομα (από μόνα τους) τους στόχους τους (Rellion, 2018· ΟΕΥΕ για την ΤΝ, 2019α).

Στα πλαίσια λοιπόν της στενής τεχνητής νοημοσύνης, ιδιαίτερα σημαντική για τα Big Data Analytics είναι η τεχνική της μηχανικής μάθησης (*machine learning*). Χάρη στη μηχανική μάθηση, ένα σύστημα τεχνητής νοημοσύνης μπορεί να μαθαίνει πώς να επιλύει προβλήματα που δεν είναι δυνατό να προσδιοριστούν επακριβώς ή η μέθοδος επίλυσης των οποίων δεν είναι δυνατό να περιγραφεί με συμβολικούς κανόνες συλλογιστικής, παράγοντας ένα αριθμητικό μοντέλο (δηλ. έναν μαθηματικό τύπο) που χρησιμοποιείται για τον υπολογισμό της απόφασης βάσει των δεδομένων (ΟΕΥΕ για την ΤΝ, 2019α). Η μηχανική μάθηση έχει εναλλακτικά οριστεί ως «οποιαδήποτε μεθοδολογία και σύνολο τεχνικών που βρίσκει νέα πρότυπα και γνώση στα δεδομένα

και δημιουργεί μοντέλα (π.χ. προφίλ) που μπορούν να χρησιμοποιηθούν για αποτελεσματικές προβλέψεις σχετικά με τα δεδομένα» (Ishii, 2017). Τα συστήματα δηλαδή της μηχανικής μάθησης, χρησιμοποιώντας ουσιαστικά ένα δείγμα των δεδομένων, τα αποκαλούμενα και «δεδομένα κατάρτισης», διαμορφώνουν τα δικά τους αριθμητικά μοντέλα επίλυσης προβλημάτων –χωρίς να απαιτείται η ανθρώπινη παρέμβαση, μέσω για παράδειγμα της περιγραφής του προβλήματος ή του τρόπου επίλυσής του- που τους επιτρέπουν να εκτελούν εργασίες, να πραγματοποιούν προβλέψεις και να λαμβάνουν αποφάσεις, εντοπίζοντας μοτίβα, στατιστικούς συσχετισμούς και κάνοντας γενικεύσεις. Έτσι λοιπόν, όταν χρησιμοποιούνται τεχνικές μηχανικής μάθησης μεσολαβεί ένα στάδιο μάθησης ή εκπαίδευσης, όπου το σύστημα χρησιμοποιεί τα δεδομένα κατάρτισης, ώστε να αναπτύξει το μοντέλο του για τη "λήψη των αποφάσεων", να "μάθει" δηλαδή πώς να επιλύει τα προβλήματα που ανακύπτουν, μοντέλο το οποίο βελτιώνεται αυτόματα και διαρκώς, όσο το σύστημα της μηχανικής μάθησης "αποκτά εμπειρία" και χρησιμοποιείται όλο και περισσότερο. Εν ολίγοις, η μηχανική μάθηση επιτρέπει ουσιαστικά στους υπολογιστές να "σκέφτονται" δημιουργώντας μαθηματικούς αλγορίθμους βάσει συσσωρευμένων δεδομένων (ICO, 2017). Στο πλαίσιο αυτό, πολλοί από τους αλγόριθμους που χρησιμοποιούνται στη μηχανική μάθηση είναι στατιστικές μέθοδοι και οι περισσότερες από αυτές βασίζονται στις αποκαλούμενες μεθόδους παλινδρόμησης, οι οποίες είναι οι πιο διαδεδομένες στατιστικές τεχνικές για τον υπολογισμό της επίδρασης ενός συνόλου δεδομένων σε ένα επιλεγμένο αποτέλεσμα (FRA, 2018).

Μια ιδιαίτερη κατηγορία μηχανικής μάθησης είναι αυτή των νευρωνικών δικτύων (*neural networks*). Εμπνευσμένα από τη λειτουργία του ανθρώπινου εγκεφάλου, τα συστήματα νευρωνικών δικτύων διαθέτουν ένα δίκτυο μονάδων επεξεργασίας (αντίστοιχα με τους ανθρώπινους νευρώνες), μεταξύ των οποίων υπάρχουν πολλές σταθμισμένες συνδέσεις, με αποτέλεσμα να δημιουργείται ένα σύνθετο δίκτυο αλληλεπιδράσεων με διαφορετικά επίπεδα (Reillon, 2018· ΟΕΥΕ για την ΤΝ, 2019α). Έτσι, στο πλαίσιο ενός τέτοιου συστήματος, δίνονται κάποια δεδομένα ως σήμα εισόδου (*input*) και παράγεται ένα σήμα εξόδου (*output*), το οποίο προκύπτει από τις αλληλεπιδράσεις στο δίκτυο. Κατά την ανάλυση των παραδειγμάτων αυτών, το σύστημα νευρικών δικτύων είναι σε θέση να προσαρμόζεται και να τροποποιεί τις αλληλεπιδράσεις στο δίκτυο έως ότου η δεδομένη είσοδος παράγει την αναμενόμενη έξοδο δεδομένων, αποκτώντας ουσιαστικά εμπειρία και ελαχιστοποιώντας την πιθανότητα σφάλματος (Reillon, 2018· ΟΕΥΕ για την ΤΝ, 2019α).

Εξέλιξη των νευρωνικών δικτύων αποτελούν τα συστήματα βαθιάς μάθησης (*deep learning*). Τα εν λόγω συστήματα στηρίζονται στον πολλαπλασιασμό των επιπέδων των νευρωνικών δικτύων και στη σύζευξη διαφορετικών τεχνικών μηχανικής μάθησης, που καθιστούν δυνατή τη μάθηση της συνολικότερης σχέσης εισόδου-εξόδου σε διαδοχικά βήματα (ΟΕΥΕ για την ΤΝ, 2019α). Ειδικότερα, τα σύνθετα επίπεδα νευρωνικών δικτύων της βαθιάς μάθησης δημιουργούνται από το ίδιο το σύστημα, μέσω αυτής της διαδικασίας μάθησης, με αποτέλεσμα να περιορίζεται στο ελάχιστο η ανάγκη ανθρώπινης καθοδήγησης (LeCun, Bengio & Hinton, 2015). Χαρακτηριστικό παράδειγμα εφαρμογής της βαθιάς μάθησης είναι οι στοχευμένες προτάσεις μεταξύ άλλων της Google και του Youtube (Ishii, 2017).

Τα συστήματα μηχανικής μάθησης και οι εξελίξεις αυτών (νευρωνικά δίκτυα, βαθιά μάθηση) χρειάζονται, επομένως, μεγάλες ποσότητες δεδομένων για να "εκπαιδευτούν", γι’ αυτό ακριβώς και έχουν "ανθίσει" στον σημερινό ψηφιακό κόσμο. Τα συστήματα που χρησιμοποιούν τέτοιου είδους τεχνικές χρειάζεται να έχουν πρόσβαση σε τεράστιες ποσότητες δεδομένων κατάρτισης για να μάθουν από αυτά και να αναπτύξουν το μοντέλο τους, βελτιώνοντας έτσι την αποτελεσματικότητα τους και μειώνοντας την πιθανότητα σφάλματος. Ο στόχος είναι η χρησιμοποίηση όσο το δυνατόν περισσότερων και αν είναι δυνατόν, όλων των δεδομένων, όπως αυτά θα μπορούσαν να συνοψιστούν με το «N = all», όπου το "N" αναφέρεται στο μέγεθος του δείγματος σύμφωνα με τη Στατιστική (Mayer-Schönberger & Cukier, 2013). Η σχέση επομένως των Big Data με τις σύγχρονες μεθόδους ανάλυσης δεδομένων είναι αμφίδρομη, καθώς αφενός μεν οι μεγάλες και ετερόκλητες βάσεις δεδομένων που υπάρχουν σήμερα μπορούν να αναλυθούν και να αξιοποιηθούν από τέτοιες τεχνικές και αφετέρου τα συστήματα μηχανικής μάθησης βελτιώνονται και γίνονται πιο ακριβή σε ένα τέτοιο περιβάλλον. Λόγω ακριβώς των μεγάλων ποσοτήτων δεδομένων που εμπλέκονται στις διαδικασίες της μηχανικής μάθησης, αυτή η νέα γενιά τεχνητής νοημοσύνης ονομάζεται στη βιβλιογραφία καθοδηγούμενη από δεδομένα τεχνητή νοημοσύνη (*data driven AI*), (Reillon, 2018).

Περαιτέρω, η μηχανική μάθηση διακρίνεται σε επιβλεπόμενη (*supervised*) και μη επιβλεπόμενη (*unsupervised*). Στις περιπτώσεις της επιβλεπόμενης μάθησης, το σύστημα εκπαιδεύεται, μέσα από επισημασμένα σύνολα δεδομένων (συγκεκριμένα παραδείγματα συμπεριφορών εισόδου-εξόδου) να πραγματοποιεί μια συγκεκριμένη εργασία, κάνοντας κάποιες γενικεύσεις, έτσι ώστε να είναι σε θέση να "συμπεριφερθεί" ανάλογα σε αντίστοιχες περιπτώσεις στο μέλλον (ΟΕΥΕ για την ΤΝ, 2019α). Έτσι, τουλάχιστον στο στάδιο της εκπαίδευσης του συστήματος, καθίσταται δυνατός ο

έλεγχος της ορθότητας των απαντήσεων που παρέχει το σύστημα (Reillon, 2018). Αντιθέτως, στις περιπτώσεις της μη επιβλεπόμενης μηχανικής μάθησης δεν δίνεται στο σύστημα κάποια συγκεκριμένη εργασία που πρέπει να εκτελέσει και τα δεδομένα δεν είναι επισημασμένα (Reillon, 2018). Το σύστημα είναι δηλαδή ελεύθερο να βρει τους δικούς του συσχετισμούς μεταξύ των δεδομένων, χωρίς ανθρώπινη επίβλεψη, με αποτέλεσμα να καθίσταται δύσκολο πολλές φορές να κατανοήσει κανείς πως προέκυψε η τελική απάντηση (π.χ. ποιοι συσχετισμοί έγιναν, σε ποια δεδομένα δόθηκε μεγαλύτερη βάση κ.τ.λ.) (Mittelstadt, Allo, Taddeo, Watcher & Floridi, 2016).

Στο πλαίσιο αυτό συνάγεται, ότι η διαφορά των παραδοσιακών μεθόδων ανάλυσης δεδομένων από τις σύγχρονες βρίσκεται ακριβώς στο ότι, ενώ οι παραδοσιακές μέθοδοι χρησιμοποιούνται για να βρουν απαντήσεις σε προκαθορισμένα ερωτήματα, στις σύγχρονες μορφές τεχνητής νοημοσύνης τα ερωτήματα ανακύπτουν από τα ίδια τα δεδομένα. Ειδικότερα, οι επιστημονικές μέθοδοι στηρίζονταν παραδοσιακά στη διατύπωση υποθέσεων, βάσει των οποίων σχεδιάζονταν πειράματα και συγκεντρώνονταν ακριβώς εκείνη η ποσότητα δεδομένων που χρειαζόταν για να απαντηθούν τα διερευνητικά ερωτήματα (Skiena, 2017). Αντίθετα, στην εποχή των Big Data Analytics προηγείται η συλλογή τεράστιων ποσοτήτων δεδομένων και μέσα από τον εντοπισμό απροσδόκητων και άγνωστων συνδέσεων και συσχετίσεων μεταξύ αυτών, που δημιουργούνται από χιλιάδες μεταβλητές, εντοπίζονται χρήσιμες, προηγουμένως άγνωστες πληροφορίες σχετικά με την ανθρώπινη συμπεριφορά, την ιδιωτική ζωή αλλά και τις κοινωνίες, ενώ εξάγονται σχετικά αποτελέσματα και συμπεράσματα. Όπως πολύ εύστοχα το θέτει η Moerel (2014), τα Big Data: «ψάχνουν για το "τι", χωρίς να γνωρίζουν το "γιατί"».

Συνεπώς, γίνεται κατανοητό, πως τα Big Data Analytics «αφορούν τη συλλογή, ανάλυση και διαρκή συσσώρευση μεγάλου όγκου δεδομένων συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα, από ένα ευρύ φάσμα πηγών, τα οποία υποβάλλονται σε αυτόματη επεξεργασία από υπολογιστικούς αλγορίθμους και προηγμένες τεχνικές επεξεργασίας δεδομένων, με τη χρήση αποθηκευμένων δεδομένων αλλά και δεδομένων συνεχούς ροής, με σκοπό τη δημιουργία ορισμένων συσχετισμών, τάσεων και προτύπων» (Ευρωπαϊκό Κοινοβούλιο, 2018). Η προσδοκία για τα Big Data Analytics είναι ακριβώς, ότι θα οδηγήσουν τελικά στη λήψη ορθότερων, πιο ενημερωμένων αποφάσεων (Art. 29 WP, 2013). Όπως περιγράφεται χαρακτηριστικά στο άρθρο του Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO, 2017): «Εν ολίγοις, τα Big Data μπορούν να θεωρηθούν ως ένα δύσκολα εκμεταλλεύσιμο περιουσιακό στοιχείο. Η τεχνητή νοημοσύνη μπορεί να θεωρηθεί ως

το κλειδί για να απελευθερωθεί η αξία των Big Data. Και η μηχανική μάθηση είναι ένας από τους τεχνικούς μηχανισμούς που στηρίζει και διευκολύνει την τεχνητή νοημοσύνη. Ο συνδυασμός και των τριών εννοιών μπορεί να ονομαστεί "Big Data Analytics"».

3. Θεμιτή χρήση των Big Data Analytics

Τα Big Data Analytics έχουν εισχωρήσει στην καθημερινότητα και χρησιμοποιούνται πλέον εκτεταμένα τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα, πραγματοποιώντας γρήγορα και αποτελεσματικά "εργασίες", οι οποίες για έναν άνθρωπο θα ήταν ιδιαίτερα δύσκολες και χρονοβόρες. Οι υπηρεσίες ανεπιθύμητης ηλεκτρονικής αλληλογραφίας (*spam filter*) αλλά και οι στοχευμένες προτάσεις που αναφέρονται ανωτέρω αποτελούν δύο χαρακτηριστικά παραδείγματα εφαρμογής τέτοιων μεθόδων που διευκολύνουν την καθημερινότητα εκατομμυρίων ανθρώπων. Τα Big Data Analytics προσφέρουν ατελείωτες δυνατότητες και παρουσιάζουν μια ισχυρή δυναμική στη σημερινή εποχή, δημιουργώντας προστιθέμενη αξία με πολλούς τρόπους, με πολλά θετικά παραδείγματα, που συνεπάγονται σημαντικές ευκαιρίες για τους πολίτες (Ευρωπαϊκό Κοινοβούλιο, 2018).

Ειδικότερα, όσον αφορά τον ιδιωτικό τομέα και ειδικότερα το κομμάτι του εμπορίου, τα Big Data Analytics προσφέρουν ένα εύρος δυνατοτήτων. Αρχικά, η εφαρμογή τους συμβάλλει στην αύξηση της παραγωγικότητας και στη μείωση των λειτουργικών δαπανών μιας επιχείρησης, καθιστώντας την αυτομάτως πιο αποτελεσματική (Raguseo, 2018). Πιο συγκεκριμένα, η ανάλυση μεγάλων ποσοτήτων δεδομένων είναι ιδιαίτερα χρήσιμη για τη βελτιστοποίηση των διαδικασιών παραγωγής, οι οποίες γίνονται πιο ευέλικτες και επεκτάσιμες, εξοικονομώντας πόρους και κόστος (Lenz, 2019). Οι Brynjolfsson, Hitt και Kim (2011) διαπίστωσαν, ότι οι επιχειρήσεις που υιοθετούν τη λήψη αποφάσεων βάσει δεδομένων (*data driven decision-making*), παρουσιάζουν 5 – 6% αύξηση στην απόδοση και την παραγωγικότητά τους. Επιπλέον, αξιοποιώντας τα δεδομένα που συγκεντρώνουν από τους καταναλωτές, οι επιχειρήσεις είναι σε θέση να αποκτήσουν μια ακριβή εικόνα των προτιμήσεων και των συμπεριφορών των πελατών τους. Με τον τρόπο αυτό μπορούν να εκτιμήσουν τη ζήτηση των προϊόντων/υπηρεσιών που παρέχουν και να ρυθμίσουν αντίστοιχα τη διανομή και την τιμή τους, να προσφέρουν εξατομικευμένα προϊόντα και υπηρεσίες για κάθε πελάτη αλλά και γενικότερα να βελτιώσουν την ποιότητα των προϊόντων και υπηρεσιών που παρέχουν.

Πιο αποτελεσματικές γίνονται και οι στρατηγικές μάρκετινγκ καθώς υπάρχει η δυνατότητα στοχευμένης-εξατομικευμένης διαφήμισης στον κάθε καταναλωτή, ενώ μειώνεται έτσι και το κόστος διαφήμισης (Acquisti, 2014). Ένα χαρακτηριστικό παράδειγμα χρήσης των Big Data Analytics στο λιανικό εμπόριο είναι η συνεργασία μεταξύ της Pantene, της Walgreens και του Weather Channel. Χρησιμοποιώντας τα δεδομένα που συλλέχθηκαν από το Weather Channel σχετικά με το επίπεδο υγρασίας

στον αέρα και το χρόνο κατά τον οποίο αυτό θα είναι υψηλότερο, η εταιρία προϊόντων περιποίησης μαλλιών Pantene και η μεγάλη αλυσίδα φαρμακείων Walgreens, χρησιμοποιώντας την έκφραση "haircast", ώθησαν τις γυναίκες να αναζητήσουν σχετικά προϊόντα στα τοπικά τους καταστήματα για να αποφύγουν προβλήματα στα μαλλιά τους προερχόμενα από την υγρασία. Αυτό είχε ως αποτέλεσμα την αύξηση κατά 10% των πωλήσεων της Pantene στην αλυσίδα Walgreens για τους μήνες Ιούλιο και Αύγουστο, καθώς και αύξηση των πωλήσεων κατά 4% σε ολόκληρη την κατηγορία μαλλιών στη Walgreens (Jagdev, 2019).

Επιπροσθέτως, στον αγροτικό τομέα κυριαρχεί τα τελευταία χρόνια η λεγόμενη "έξυπνη γεωργία" (*smart agriculture*). Χάρη στα Big Data Analytics καθίσταται δυνατή μια πιο αποτελεσματική χρήση των φυσικών πηγών ενέργειας, μέσω για παράδειγμα του αυτόματου κλιματισμού σύμφωνα με τις απαιτήσεις της συγκομιδής, της έγκαιρης και ελεγχόμενης άρδευσης και του ελέγχου της υγρασίας (Marjani et al., 2017). Έντονη είναι και η παρουσία των Big Data Analytics στον χρηματοπιστωτικό και τον ασφαλιστικό τομέα, όπου χρησιμοποιούνται για να καθοριστεί η πιστωτική ικανότητα (κατά πόσο ένας υποψήφιος πληροί τις προϋποθέσεις για τη χορήγηση πίστωσης) και ο ασφαλιστικός κίνδυνος (και κατ' επέκταση το ύψος του ασφαλίστρου) των καταναλωτών αντίστοιχα.

Από την άλλη, η ανάδειξη των "έξυπνων πόλεων" (*smart cities*) τα τελευταία χρόνια αποτελεί το πιο χαρακτηριστικό παράδειγμα αξιοποίησης των Big Data Analytics στον δημόσιο τομέα. Οι λεγόμενες "έξυπνες πόλεις" χρησιμοποιούν τις σύγχρονες μορφές ανάλυσης δεδομένων για να βελτιώσουν το επίπεδο της βιωσιμότητας, της ανθεκτικότητας και της διακυβέρνησής τους, να καλυτερεύσουν την ποιότητα ζωής των πολιτών τους, καθώς και να διαχειριστούν καλύτερα και αποτελεσματικότερα τις υποδομές και τους φυσικούς πόρους που διαθέτουν (Al Nuaimi, Al Neyadi, Mohamed & Al – Jaroodi, 2015), αξιοποιώντας σε μεγάλο βαθμό δεδομένα που προέρχονται από το Διαδίκτυο των Πραγμάτων. Για παράδειγμα, η Βαρκελώνη μεταξύ άλλων έχει υιοθετήσει ένα έξυπνο σύστημα διαχείρισης απορριμμάτων, χρησιμοποιώντας κάδους που "ρουφάνε" τα απόβλητα σε υπόγεια αποθήκη, ανιχνεύοντας το μέγεθος των απορριμμάτων στα διάφορα σημεία της πόλης, ώστε να βελτιστοποιηθεί η συλλογή τους και χρησιμοποιώντας την αποτέφρωση των αποβλήτων για την παραγωγή ενέργειας για συστήματα θέρμανσης (Zigurat Global Instituteof Technology, 2019). Γενικότερα άλλωστε, οι "έξυπνες πόλεις" σήμερα έχουν καταφέρει να μειώσουν τον αντίκτυπό τους στο περιβάλλον (π.χ. αποδοτικότερη ενεργειακή υποδομή και κατανάλωση), να διαχειριστούν την κυκλοφοριακή

συμφόρηση (π.χ. μέσω των έξυπνων φαναριών), καθώς και να ενισχύσουν τα Μέσα Μαζικής Μεταφοράς (π.χ. ελαχιστοποίηση της αναμονής, βελτιστοποίηση της δρομολόγησης, ενίσχυση της ανεξαρτησίας των ατόμων με προβλήματα όρασης). Στο πληροφοριακό δελτίο της στρατηγικής της Ευρωπαϊκής Επιτροπής για τα δεδομένα (European Commission, 2020β) αναφέρεται χαρακτηριστικά, ότι η πλοήγηση αποφυγής κίνησης σε πραγματικό χρόνο μπορεί να εξοικονομήσει έως 730 εκατομμύρια ώρες (έως 20 δισεκατομμύρια ευρώ σε κόστος εργασίας). Αντίστοιχα, οι έξυπνοι μετρητές αερίου και ηλεκτρικής ενέργειας που είναι εγκατεστημένοι στα σπίτια των ευρωπαίων πολιτών θα μπορούσαν να μειώσουν τις εκπομπές άνθρακα στην Ε.Ε. έως και 9%, καθώς και την ετήσια κατανάλωση ενέργειας των νοικοκυριών κατά παρόμοιο ποσοστό (Fuster & Scherrer, 2015). Παράλληλα, πολύ σημαντική είναι η χρήση των Big Data Analytics τόσο στον τομέα της εκπαίδευσης (π.χ. μέσω εξατομικευμένων εκπαιδευτικών προγραμμάτων, προσαρμοσμένων στην απόδοση και τις δυνατότητες των μαθητών) (ΟΕΥΕ για την ΤΝ, 2019β), όσο και για την αντιμετώπιση των φυσικών καταστροφών (π.χ. για τη γρήγορη εκκένωση των πληττόμενων περιοχών) (Ishii, 2017).

Βέβαια, η σημαντικότερη ίσως εφαρμογή των Big Data Analytics είναι στον τομέα της υγείας. Με την αξιοποίηση των μεθόδων αυτών καθίσταται δυνατή η εξατομικευμένη και αποτελεσματικότερη πρόβλεψη, ανίχνευση και θεραπεία των ασθενειών (Mehta & Pandit, 2018), ενώ πολύ σημαντική είναι η συμβολή τους και στο κομμάτι της έρευνας και της ανάπτυξης. Χαρακτηριστικό παράδειγμα αποτελεί μια ομάδα ερευνητών, η οποία χρησιμοποιώντας τεχνικές εξόρυξης σε μεγάλες βάσεις δεδομένων ανακάλυψε, ότι ο συνδυασμός δύο φαρμάκων - ενός αντικαταθλιπτικού και ενός φαρμάκου μείωσης της χοληστερόλης – μπορεί να οδηγήσει σε αύξηση των επιπέδων γλυκόζης στο αίμα των ασθενών σε επίπεδα διαβητικών, παρόλο που τα δύο φάρμακα από μόνα τους δεν προκαλούν παρόμοιες παρενέργειες (Tene & Polonetsky, 2012). Επιπλέον, η αξιοποίηση του IBM Watson (ενός υπερ-υπολογιστή που συνδυάζει τεχνητή νοημοσύνη και εξελιγμένο αναλυτικό λογισμικό για βέλτιστη απόδοση) στον τομέα της ογκολογίας έχει συμβάλλει στην παροχή εξατομικευμένων συστάσεων κλινικής θεραπείας βασισμένης σε ενδείξεις (*evidence based treatment recommendations*) και κατάλληλων κλινικών δοκιμών για κάθε ασθενή, καθώς και στην ανάλυση του γονιδιωματικού προφίλ του όγκου των ασθενών (Ishii, 2017). Τα Big Data Analytics μπορούν να χρησιμοποιηθούν και για την προστασία της δημόσιας υγείας, εντοπίζοντας για παράδειγμα την εμφάνιση μιας ασθένειας σε μια συγκεκριμένη περιοχή (Raghupathi, W. & Raghupathi, V., 2014), όπως έγινε στην περίπτωση της

Κένυας, όπου επιστήμονες από τη Σχολή Δημόσιας Υγείας του Χάρβαρντ χρησιμοποίησαν τα δεδομένα των κινητών τηλεφώνων για τη χαρτογράφηση της εξάπλωσης της ελονοσίας (Kalapesi, 2013), αλλά και με την πρόσφατη πανδημία του COVID – 19, όπου τα δεδομένα κινητικότητας της Google χρησιμοποιήθηκαν για τη συσχέτιση της κινητικότητας των πολιτών των διάφορων χωρών με την εξάπλωση του ιού και τον αριθμό των κρουσμάτων και των θανάτων (Yilmazkuday, 2020).

Τα Big Data Analytics ήρθαν, επομένως, για να μείνουν. Οι ευεργετικές ιδιότητες της αξιοποίησής τους για την οικονομία αλλά και για την κοινωνία γενικότερα είναι αναμφισβήτητες. Οι οικονομίες γίνονται αποτελεσματικότερες, ο δημόσιος τομέας πιο λειτουργικός και οι ζωές των πολιτών πιο εύκολες και ποιοτικές. Εντούτοις, εκτός από τις τεράστιες δυνατότητές τους, η καθιέρωση τους τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα έχει εγείρει έντονες ανησυχίες από την ακαδημαϊκή κοινότητα σχετικά με τις επιπτώσεις τους στην ιδιωτικότητα και στην προστασία των προσωπικών δεδομένων των ατόμων, όπως θα αναλυθεί στα κεφάλαια που ακολουθούν.

4. Οι Κίνδυνοι των Big Data Analytics

Στην εποχή των Big Data Analytics τεράστιες ποσότητες δεδομένων (προσωπικών και απρόσωπων) παράγονται καθημερινά, οι οποίες συλλέγονται, αποθηκεύονται, μετακινούνται και ανταλλάσσονται, συνδυάζονται μεταξύ τους και αναλύονται για την "εξαγωγή" σιωπηρών, προηγουμένως άγνωστων και δυνητικά χρήσιμων πληροφοριών, γεγονότων και μοτίβων, απαντώντας ουσιαστικά σε ερωτήσεις, που οι άνθρωποι δεν γνώριζαν ότι έχουν ευθύς εξαρχής (Kitchin, 2014). Τα Big Data Analytics έχουν οδηγήσει, δηλαδή, στη δημιουργία ενός ψηφιακού "οικοσυστήματος", στο οποίο η ανάλυση των δεδομένων καθιστά δυνατή την κατανόηση σε βαθύτερο επίπεδο του τρόπου με τον οποίο οι άνθρωποι ζουν, εργάζονται, ταξιδεύουν, μελετούν, τρώνε, κοιμούνται και καταναλώνουν (Fuster & Scherrer, 2015). Στο πλαίσιο αυτό, μία από τις πιο σημαντικές εφαρμογές των Big Data Analytics είναι η παρακολούθηση της ανθρώπινης συμπεριφοράς, τόσο σε συλλογικό όσο και σε ατομικό επίπεδο και η δυνατότητα πραγματοποίησης προγνώσεων σχετικά με συμπεριφορές και καταστάσεις (European Data Protection Supervisor, 2016), γι' αυτό το λόγο άλλωστε και χρησιμοποιούνται μεταξύ άλλων για να ενισχύσουν και να καταστήσουν πιο αποτελεσματικές δραστηριότητες όπως είναι η κατάρτιση προφίλ (*profiling*), η βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (*scoring*), η αυτοματοποιημένη λήψη αποφάσεων (π.χ. για τη χορήγηση δανείου και ασφάλισης ή για την πραγματοποίηση προσλήψεων), η στοχευμένη διαφήμιση (*targeted advertising*) και η ανάλυση προγνωστικών (*predictive analytics*).

Το όραμα πίσω από τις σύγχρονες αυτές τεχνολογίες ήταν η βελτιστοποίηση της διαδικασίας λήψης αποφάσεων, εξαλείφοντας τους περιορισμούς και την υποκειμενικότητα της ανθρώπινης νόησης, κάτι που ωστόσο δεν έχει επιτευχθεί μέχρι σήμερα. Τα Big Data Analytics στηρίζονται σε συσχετισμούς, οι οποίοι αν και δημιουργούν σίγουρα στατιστικούς συνδέσμους μεταξύ των δεδομένων, εντούτοις σε καμία περίπτωση δεν εξισώνονται με την αιτιότητα (Diakopoulos, 2016). Όπως άλλωστε αναφέρεται χαρακτηριστικά στο άρθρο της ΟΕΥΕ για την ΤΝ (2019α), σε όλες τις περιπτώσεις μηχανικής μάθησης υπάρχει πάντοτε ένα ορισμένο ποσοστό σφάλματος. Στο πλαίσιο αυτό, τα Big Data Analytics πέρα από τις αναμφισβήτητες δυνατότητες που προσφέρουν, ελλοχεύουν και πολλούς κινδύνους, οι βασικότεροι των οποίων – που θα αναλυθούν και κατωτέρω- είναι:

- Αδιαφάνεια
- Έλλειψη ελέγχου επί των δεδομένων και αβεβαιότητα
- Διακρίσεις και αδικία

- Χειραγώγηση

4.1. Αδιαφάνεια

Ένα από τα βασικά χαρακτηριστικά των Big Data Analytics είναι η αδιαφάνεια που διέπει τη λήψη των αποφάσεων, η οποία αναφέρεται στη βιβλιογραφία και ως το φαινόμενο του "μαύρου κουτιού". Το "μαύρο κουτί" της τεχνητής νοημοσύνης (*black-box AI*) αναφέρεται ακριβώς στην αδυναμία κατανόησης του τρόπου με τον οποίο λαμβάνονται οι αποφάσεις από τα συστήματα τεχνητής νοημοσύνης, στην αδυναμία δηλαδή να εντοπίσει κανείς τους λόγους στους οποίους βασίζονται ορισμένες αποφάσεις (ΟΕΥΕ για την ΤΝ, 2019α).

Ειδικότερα, η αδιαφάνεια οφείλεται αρχικά στην εγγενή πολυπλοκότητα των συστημάτων τεχνητής νοημοσύνης, η οποία είναι αποτέλεσμα της αλληλεπίδρασης των εξαιρετικά μεγάλων ποσοτήτων ετερόκλητων δεδομένων αφενός και αφετέρου του κώδικα, του μοντέλου ανάλυσης των δεδομένων (Burrell, 2016). Οι συσχετίσεις, δηλαδή, που εντοπίζονται μεταξύ των δεδομένων δημιουργούνται από χιλιάδες μεταβλητές σε τομείς εκατομμυρίων σημείων δεδομένων (*datapoints*) με τρόπους που δεν μπορούν να μεταφραστούν με κανένα διαισθητικά διαθέσιμο μοτίβο (Andrejevic & Gates, 2014). Ιδιαίτερα δε στις περιπτώσεις της μη επιβλεπόμενης μηχανικής μάθησης, τα συστήματα ενημερώνουν και αλλάζουν το μοντέλο τους μετά από κάθε απόφαση που λαμβάνουν, ενσωματώνοντας κάθε νέα παρατήρηση στα δεδομένα κατάρτισης, πράγμα που σημαίνει, ότι μετά από κάθε απόφαση, το μοντέλο που χρησιμοποιήθηκε για τη λήψη της είναι ήδη ξεπερασμένο (Kroll et al., 2016). Για αυτόν τον λόγο άλλωστε, η κατανόηση της λογικής των συστημάτων μη επιβλεπόμενης μηχανικής μάθησης είναι δύσκολη ακόμα και για τους ειδικούς του τομέα. Σε κάθε περίπτωση, για την κατανόηση του "τρόπου σκέψης" ενός συστήματος τεχνητής νοημοσύνης απαιτούνται τεχνικές γνώσεις και δεξιότητες προγραμματισμού και χρήσης υπολογιστή, με τις οποίες η πλειοψηφία των σύγχρονων πολιτών δεν είναι εξοικειωμένη (Burrell, 2016).

Επιπλέον, η αδιαφάνεια των Big Data Analytics είναι αποτέλεσμα των εμπορικών συμφερόντων και των δικαιωμάτων των επιχειρήσεων που επεξεργάζονται προσωπικά δεδομένα. Πρόκειται ουσιαστικά για μια μορφή αυτοπροστασίας των επιχειρήσεων με σκοπό να προστατεύσουν και να διατηρήσουν το ανταγωνιστικό τους πλεονέκτημα και τα δικαιώματα πνευματικής ιδιοκτησίας, όπως είναι τα εμπορικά μυστικά, τα οποία είναι εγγενώς ασυμβίβαστα με την πλήρη διαφάνεια (Burrell, 2016). Η ανάγκη προστασίας αυτών των δικαιωμάτων, ακόμα και αν η φύση τους είναι

καθαρά εμπορική τονίζεται και στο προοίμιο του ΓΚΠΔ, στην Αιτιολογική Σκέψη 63. Παράλληλα, υποστηρίζεται και η άποψη ότι η αλγοριθμική αδιαφάνεια αποτελεί κατ' ουσία μια νέα μορφή συγκάλυψης από τις επιχειρήσεις των παραβιάσεων των νομικών κανόνων, της χειραγώγησης των καταναλωτών και των διακρίσεων (Burrell, 2016). Από την άλλη υποστηρίζεται, ότι η διατήρηση ενός βαθμού αδιαφάνειας των συστημάτων εξασφαλίζει την αποτελεσματικότητά τους, καθώς αποφεύγεται με αυτόν τον τρόπο η υιοθέτηση στρατηγικών συμπεριφορών από τα υποκείμενα των δεδομένων, τα οποία γνωρίζοντας την εσωτερική λογική του συστήματος θα μπορούσαν να προσαρμόσουν τη συμπεριφορά τους ώστε να ελέγξουν και να επηρεάσουν την τελική απόφαση (Kroll et al., 2016).

Σε κάθε περίπτωση, η αδιαφάνεια αποτελεί αφενός ένα εγγενές χαρακτηριστικό των Big Data Analytics και αφετέρου έναν σκοπό που επιδιώκεται για διάφορους λόγους από τις επιχειρήσεις που χρησιμοποιούν τέτοιου είδους τεχνολογίες, εξαιτίας της οποίας δημιουργούνται σοβαρά προβλήματα. Το μεγαλύτερο πρόβλημα βρίσκεται ακριβώς στις προκλήσεις που δημιουργούνται στην ικανότητα των ατόμων αλλά και των αρχών να αξιολογούν τις διαδικασίες και τον σκοπό της συλλογής, της συγκέντρωσης, της ανάλυσης και της χρήσης των δεδομένων προσωπικού χαρακτήρα (Ευρωπαϊκό Κοινοβούλιο, 2018). Οι πολίτες των σύγχρονων ψηφιακών κοινωνιών αδυνατούν, δηλαδή, να κατανοήσουν και κατ' επέκταση να αντικρούσουν τις αποφάσεις που λαμβάνονται σχετικά με αυτούς, οι οποίες σε πολλές περιπτώσεις έχουν πολύ σοβαρές οικονομικές και κοινωνικές επιπτώσεις (Lenz, 2019). Πώς μπορεί κανείς να αντικρούσει μια λανθασμένη απόφαση (επειδή π.χ. στηρίχθηκε σε ανακριβή δεδομένα), όταν δεν μπορεί να κατανοήσει πώς και γιατί λήφθηκε η απόφαση αυτή; Η αδιαφάνεια που χαρακτηρίζει τα Big Data Analytics μπορεί, συνεπώς, να στερήσει εν τέλει από τους ανθρώπους τη δυνατότητα άσκησης των δικαιωμάτων που τους χορηγεί ο νόμος (Hirsch, 2019).

4. 2. Έλλειψη ελέγχου επί των δεδομένων και αβεβαιότητα

Το μέγεθος του ψηφιακού κόσμου σήμερα και η ευρεία χρησιμοποίηση των Big Data Analytics έχουν ως αποτέλεσμα να παρακολουθείται από ένα πλήθος διαφορετικών φορέων η διαδικτυακή συμπεριφορά εκατοντάδων εκατομμυρίων ανθρώπων και να δημιουργούνται λεπτομερή, εξατομικευμένα προφίλ για τον καθένα από αυτούς, χωρίς οι τελευταίοι να έχουν καμία επίγνωση του γεγονότος αυτού. Μία μόνο επίσκεψη σε έναν ιστότοπο μπορεί να οδηγήσει στη λήψη δεκάδων cookies παρακολούθησης και κατ' επέκταση στη συλλογή εκτενών ποσοτήτων προσωπικών

δεδομένων από τρίτους φορείς (που δεν σχετίζονται με την ιστοσελίδα που επισκέφθηκε ο χρήστης), η λεγόμενη διαφορετικά πρακτική του third party tracking (Robertson, 2020· Zuiderveen Borgesius, 2015). Εκτός από τα cookies, χρησιμοποιούνται σήμερα όλο και περισσότερο προηγμένες τεχνολογίες παρακολούθησης (π.χ. *webbeacons, digital fingerprinting*) (Ipsos, London Economics, Deloitte, 2018). Από την άλλη, ένας νέος τύπος εταιρειών, οι λεγόμενοι data brokers συλλέγουν από ένα πλήθος διαφορετικών πηγών δεδομένα των καταναλωτών, με σκοπό τη μεταπώληση τους (π.χ. σε εταιρείες μάρκετινγκ) (Tsesis, 2014· Μπούκης, 2019). Τα δεδομένα, δηλαδή, συλλέγονται, συγκεντρώνονται, αναλύονται, χρησιμοποιούνται και ανταλλάσσονται μέσα στη σύνθετη αγορά που έχει δημιουργηθεί γύρω από αυτά και στην οποία συμμετέχει ένα πλήθος διαφορετικών φορέων (Ipsos, London Economics, Deloitte, 2018).

Στο πλαίσιο αυτό και λαμβάνοντας υπόψη και την αδιαφάνεια που χαρακτηρίζει τα Big Data Analytics (βλ. ανωτέρω κεφάλαιο 4.1) καθίσταται ιδιαίτερα δυσχερές για έναν σύγχρονο πολίτη, να παρακολουθεί διαρκώς και να έχει μια πλήρη εικόνα των δεδομένων που παράγονται και κατέχουν οι τρίτοι για αυτόν, του τρόπου με τον οποίο θα χρησιμοποιηθούν τα δεδομένα του, των πιθανών αποτελεσμάτων της ανάλυσης τους αλλά και τις επιπτώσεις που θα έχει η επεξεργασία τους. Γενικότερα άλλωστε, η πορεία που ακολουθούν τα δεδομένα μετά τη συλλογή τους είναι πολύ περίπλοκη και αδιαφανής (van Ooijen & Vrabec, 2019). Ακόμα, δηλαδή κι αν οι λόγοι για τη συλλογή των δεδομένων είναι απλοί (π.χ. χρήση μιας πλατφόρμας κοινωνικών μέσων) και η επεξεργασία των δεδομένων φαίνεται αρχικά να είναι υπό έλεγχο, οι δευτερεύουσες χρήσεις των δεδομένων μπορεί να είναι πολύ αδιαφανείς (π.χ. κοινή χρήση δεδομένων χρηστών με data brokers), με αποτέλεσμα το υποκείμενο να μην γνωρίζει πότε ένας (τρίτος) φορέας έχει αποκτήσει πρόσβαση στα δεδομένα του και ποιες συνέπειες ενδέχεται να επέλθουν και να αποδυναμώνεται έτσι ο έλεγχος των υποκειμένων στα δεδομένα τους (Acquisti & Grossklags, 2007· van Ooijen & Vrabec, 2019).

Στην ειδική έρευνα 487α του Ευρωβαρόμετρου που δημοσιεύθηκε τον Ιούνιο του 2019 (European Commission, Directorate-General for Justice and Consumers, co-ordinated by the Directorate-General for Communication, 2019), στην ερώτηση για το μέγεθος του ελέγχου που νιώθουν ότι έχουν στις πληροφορίες που παρέχουν διαδικτυακά, μόνο το 14% των πολιτών απάντησε ότι έχει τον απόλυτο έλεγχο, το 30% απάντησε ότι δεν έχει καθόλου έλεγχο και το 51% ότι έχει μερικό μόνο έλεγχο, ενώ από τα άτομα που δήλωσαν ότι δεν έχουν καθόλου ή ότι έχουν μερικό έλεγχο, το 62% δήλωσε ότι ανησυχεί που δεν έχει τον απόλυτο έλεγχο, φανερώνοντας το αίσθημα της

αβεβαιότητας και της ανασφάλειας που έχουν οι πολίτες της Ευρωπαϊκής Ένωσης σχετικά με τη διαχείριση των δεδομένων τους στον ψηφιακό κόσμο.

Επιπλέον, τεχνικές όπως είναι η ανωνυμοποίηση και η ψευδωνυμοποίηση, οι οποίες στηρίζονται στην αποσύνδεση των δεδομένων από τα προσωπικά στοιχεία που παραπέμπουν στο υποκείμενο αυτών και υποδεικνύουν την ταυτότητά του (*personal identifiers*) και οι οποίες συνιστώνται και από τον ΓΚΠΔ σε πολλά σημεία του, δεν μπορούν πλέον να εγγυηθούν την ανωνυμία των υποκειμένων και την αυξημένη προστασία των δεδομένων τους. Ακριβώς χάρη στην ικανότητα των Big Data Analytics να βρίσκουν νέους συσχετισμούς και να ανακαλύπτουν νέες πληροφορίες στα δεδομένα που αναλύουν, καθίσταται σήμερα δυνατή η επαναταυτοποίηση (*re-identification*) των δεδομένων, η σύνδεση τους δηλαδή με το πρόσωπο που αφορούν, ακόμα και αν είχαν υποστεί ανωνυμοποίηση ή ψευδωνυμοποίηση, συνδυάζοντας πληροφορίες από διαφορετικές πηγές και συνδέοντας ανώνυμα δεδομένα (π.χ. οικονομικά αρχεία) με προσωπικά αναγνωρίσιμες πληροφορίες (π.χ. όνομα, διεύθυνση) (Organisation for Economic Cooperation and Development, Directorate for Financial and Enterprise Affair, Competition Committee [OECD, Directorate for Financial and Enterprise Affair, Competition Committee], 2016). Όσο περισσότερα δεδομένα και δη όσο περισσότερα λεπτομερή δεδομένα για ένα άτομο είναι διαθέσιμα, τόσο πιο εύκολος γίνεται ο επαναπροσδιορισμός του ατόμου είτε μέσω της αντίστροφης μηχανικής του συνόλου των δεδομένων, είτε συνδυάζοντάς τα με άλλα σύνολα δεδομένων που ενδεχομένως να περιλαμβάνουν και τα ονόματα των υποκειμένων (Froomkin, 2019). Σε μια πρόσφατη έρευνά τους οι Rocher, Hendrickx, και De Montjoye (2019) δημιούργησαν ένα μοντέλο, το οποίο μπορεί να εκτιμήσει με ακρίβεια την πιθανότητα επαναταυτοποίησης ενός ατόμου και διαπίστωσαν, ότι, χρησιμοποιώντας 15 δημογραφικά χαρακτηριστικά, το 99,98% των Αμερικανών πολιτών θα επαναπροσδιοριζόταν σωστά σε οποιοδήποτε σύνολο δεδομένων. Στο πλαίσιο αυτό, η διάκριση μεταξύ μη προσωπικών και προσωπικών δεδομένων δεν είναι τόσο εύκολη στην πράξη, καθιστώντας ουσιαστικά αδύνατη την επίτευξη της ανωνυμίας στη σύγχρονη ψηφιακή πραγματικότητα.

Ένα ακόμη χαρακτηριστικό των σύγχρονων συστημάτων ανάλυσης δεδομένων που έρχεται σε σύγκρουση με το δικαίωμα της ιδιωτικότητας είναι η ισχυρή τους "μνήμη", η δυνατότητα τους δηλαδή να διατηρούν τα δεδομένα που χρησιμοποιούν για μεγάλα, αόριστα χρονικά διαστήματα. Συγκεκριμένα, μια σημαντική πτυχή του δικαιώματος της ιδιωτικότητας είναι η δυνατότητα μιας δεύτερης ευκαιρίας, μιας νέας αρχής, χωρίς το άτομο να βαρύνεται από τις προηγούμενες επιλογές που έχει κάνει (Blanchette & Johnson, 2002). Εντούτοις, σήμερα είναι σχεδόν αδύνατο να ξεφύγει

κανείς από το παρελθόν, αφού κάθε status στο Facebook, φωτογραφία ή Tweet μπορεί να αντιγραφεί ή/και να σταλεί από άλλους χρήστες ή να αποθηκευτεί σε διαδικτυακές αρχειοθήκες, όπως το Wayback Machine και σε προαποθηκευμένες ιστοσελίδες (*cached pages*) (Ιγγλεζάκης, 2017). Στην εποχή των Big Data Analytics φαίνεται ακριβώς, ότι οι άνθρωποι ζούνε "στη σκιά των ίδιων τους των δεδομένων", καθώς τα δεδομένα αποθηκεύονται και διατηρούνται όσο παλιά και αν είναι, ακριβώς επειδή όλα τα δεδομένα έχουν αξία και μπορεί – αν όχι από μόνα τους, σε συνδυασμό και με άλλα δεδομένα- να οδηγήσουν σε σημαντικούς συσχετισμούς και προβλέψεις, ακόμη και αν η χρησιμότητά τους δεν ήταν εξ' αρχής εμφανής. Χαρακτηριστικό παράδειγμα των ανωτέρω αποτελεί η υπόθεση C-131/12 του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ), στην οποία ένας Ισπανός πολίτης στράφηκε κατά της Google, διότι η μηχανή αναζήτησης της, κάθε φορά που πραγματοποιούνταν αναζήτηση για το όνομα του, στην κορυφή των αποτελεσμάτων της εμφάνιζε δύο ανακοινώσεις για πλειστηριασμούς ακινήτων του κατόπιν κατάσχεσης που του είχε επιβληθεί λόγω κοινωνικοασφαλιστικών οφειλών, υποθέσεις όμως οι οποίες είχαν διευθετηθεί αρκετά χρόνια πριν τη δικαστική αυτή διαμάχη και δεν συνέτρεχε πλέον κανένας λόγος να συνδέονται με το όνομά του. Αξίζει να σημειωθεί, ότι στην προκειμένη περίπτωση, το ΔΕΕ - υπό το προϊσχύον καθεστώς της Οδηγίας 95/46/ΕΚ για την προστασία δεδομένων- δικαίωσε τον Ισπανό πολίτη, καθώς έκρινε ότι το υποκείμενο των δεδομένων μπορεί, υπό το πρίσμα των θεμελιωδών του δικαιωμάτων σύμφωνα με τα άρθρα 7 και 8 του ΧΘΔ, να ζητήσει οι εν λόγω πληροφορίες να μην είναι πλέον διαθέσιμες στο ευρύ κοινό με τη συμπερίληψή τους σε έναν τέτοιο κατάλογο αποτελεσμάτων.

Επιπροσθέτως, ένας από τους μεγαλύτερους κινδύνους στην εποχή της πληροφορίας έχει να κάνει με την ανάδυση θεσμών επιτήρησης. Τα Big Data Analytics έχουν μεταμορφώσει τον συστηματικό και στοχευμένο χαρακτήρα των πρακτικών επιτήρησης, με αποτέλεσμα να μην υπάρχει πλέον λειτουργική διάκριση μεταξύ στόχων και μη στόχων (υπόπτων και μη υπόπτων), καθόσον σκοπός πλέον είναι η συγκέντρωση όσο το δυνατόν περισσότερων πληροφοριών για ολόκληρους πληθυσμούς (Andrejevic & Gates, 2014). Άλλωστε, δεν είναι μόνο οι κυβερνητικοί φορείς που έχουν τελειοποιήσει την "πανταχού παρούσα" επιτήρηση των πολιτών, αλλά οι πρακτικές επιτήρησης χρησιμοποιούνται πλέον και στον ιδιωτικό τομέα για την αποκόμιση κέρδους, με αποτέλεσμα να έχει αναδυθεί σχετικά η έννοια του καπιταλισμού παρακολούθησης (*surveillance capitalism*) (Manheim & Kaplan, 2018). Στο πλαίσιο αυτό, οι σύγχρονες κοινωνίες έχουν αναδειχθεί σε κοινωνίες επιτήρησης, όπου το να

παρακολουθεί κάποιος και να τον παρακολουθούν έχει αποκτήσει ένα συγκεκριμένο νόημα, δίνοντας ώθηση σε νέες τεχνικές κοινωνικού ελέγχου, όπως είναι η συγκαλυμμένη αστυνόμευση, η παρακολούθηση μέσω ηλεκτρονικού υπολογιστή, η ανάλυση προφίλ και η εξόρυξη δεδομένων, η καταπολέμηση του ντοπαρίσματος, οι υπηρεσίες αναγνώρισης καλούντος, κ.ά. (Τσαούση, 2018).

Πέρα από τα ανωτέρω, κίνδυνοι για το δικαίωμα της ιδιωτικότητας δημιουργούνται στον ιδιωτικό τομέα και από διάφορες χρήσεις των Big Data Analytics. Συγκεκριμένα, οι τεράστιες ποσότητες δεδομένων που παράγονται σήμερα, σε συνδυασμό με τη δυνατότητα ανάλυσής τους, που παρέχουν οι σύγχρονες τεχνολογίες, έχουν επιτρέψει στις επιχειρήσεις να κατανοήσουν καλύτερα τη συμπεριφορά και τις ανάγκες των καταναλωτών τους και να αναπτύξουν διάφορες πρακτικές εξατομίκευσης. Οι κυριότερες πρακτικές, οι οποίες και δημιουργούν τα περισσότερα ζητήματα στην πράξη, είναι η στοχευμένη διαφήμιση (*targeted advertising*) και η διάκριση τιμών (*price discrimination*).

Πιο συγκεκριμένα, οι επιχειρήσεις έχουν πλέον την ικανότητα να προσαρμόζουν τις διαφημίσεις των προϊόντων / υπηρεσιών τους ανάλογα με τον χαρακτήρα του κάθε καταναλωτή, ώστε να επηρεάσουν στο μέγιστο τη συμπεριφορά του. Η λεγόμενη διαφορετικά και συμπεριφορική διαφήμιση αναφέρεται ακριβώς στην παρακολούθηση της διαδικτυακής συμπεριφοράς των ατόμων, προκειμένου να χρησιμοποιηθούν οι πληροφορίες που θα συγκεντρωθούν για να δείξουν στον καθένα εξατομικευμένες διαφημίσεις (Borgesius, 2015). Ο τρόπος, δηλαδή με τον οποίο παρουσιάζεται το εκάστοτε διαφημιζόμενο προϊόν διαφέρει από άτομο σε άτομο, ανάλογα με τις πληροφορίες που γνωρίζει το σύστημα τεχνητής νοημοσύνης για το καθένα (Susser, Roessler & Nissenbaum, 2018).

Ένα χαρακτηριστικό παράδειγμα προσβολής της ιδιωτικότητας εξαιτίας στοχευμένων διαφημίσεων αποτελεί η υπόθεση της Target Inc. Σύμφωνα με ένα άρθρο των New York Times, η εταιρεία Target –μια από τις μεγαλύτερες εταιρείες λιανικού εμπορίου– διαθέτει ένα σύστημα που της επιτρέπει να προβλέπει με ακρίβεια την εγκυμοσύνη των πελατισσών της και την ημερομηνία τοκετού τους. Αξιοποιώντας, συγκεκριμένα, τα δεδομένα από τις αγοραστικές συνήθειες των εγκύων πελατισσών της, η Target ανακάλυψε διάφορα μοτίβα (π.χ. την προτίμηση των γυναικών για λοσιόν χωρίς άρωμα, όταν άρχιζε το δεύτερο τρίμηνο της εγκυμοσύνης τους), κατορθώνοντας τελικά να συγκεντρώσει ένα σύνολο προϊόντων, τα οποία, αν συνδυαστούν από κάποια πελάτισσα φανερώνουν την εγκυμοσύνη της και το στάδιο αυτής. Στο πλαίσιο αυτό, η Target έστειλε προσφορές προϊόντων για εγκυμοσύνη σε μια έφηβη πελάτισσα της, η

οποία δεν είχε ακόμα ενημερώσει τον πατέρα της –με τον οποίο και διέμενε- για την εγκυμοσύνη της (Edwards & Veale, 2017· Tene & Polonetsky, 2012). Το ανωτέρω παράδειγμα αναδεικνύει ένα ακόμη πρόβλημα που δημιουργεί η χρήση των Big Data Analytics. Στην προκειμένη περίπτωση, η ανάλυση κοινών και "ακίνδυνων" δεδομένων (η αγορά μιας νέας λοσιόν από την Target) οδήγησε στην ανακάλυψη-πρόβλεψη ευαίσθητων πληροφοριών, που ανήκουν στην προσωπική σφαίρα του ατόμου (δεδομένα υγείας - εγκυμοσύνη) και που ενδεχομένως να μην επιθυμούσε να αποκαλύψει σε τρίτα πρόσωπα. Πολλές φορές, δηλαδή, το πρόβλημα δεν βρίσκεται στα δεδομένα που συλλέγονται για κάποιο υποκείμενο, αλλά στις πληροφορίες και στα συμπεράσματα που εξάγονται από αυτά τα δεδομένα (στα δεδομένα που έχουν εξαχθεί ή συναχθεί, όπως τα χαρακτηρίζει η ομάδα εργασίας του άρθρου 29 – βλ. ανωτέρω κεφάλαιο 2) και στις οποίες το ενδιαφερόμενο πρόσωπο δεν έχει πρόσβαση, ενδεχομένως δε να μην γνωρίζει καν την ύπαρξή τους. Ένα άλλο αντίστοιχο παράδειγμα αποτελεί η περίπτωση της μουσικής υπηρεσίας Pandora, η οποία συλλέγει τα δεδομένα για τις προτιμήσεις των χρηστών της προκειμένου αφενός να παρέχει προσαρμοσμένες προτάσεις μουσικής και αφετέρου να τις συσχετίζει με γεωγραφικά δεδομένα και τα τελευταία με μοτίβα ψηφοφορίας, προκειμένου να συνάγει πληροφορίες σχετικά με τις πολιτικές πεποιθήσεις των χρηστών της (Andrejevic & Gates, 2014). Η χρησιμοποίηση, δηλαδή, των Big Data Analytics δημιουργεί μια σύγχυση ως προς τον διαχωρισμό όχι μόνο προσωπικών και μη προσωπικών δεδομένων, αλλά και ως προς τον διαχωρισμό απλών και ευαίσθητων προσωπικών δεδομένων.

Εκτός, όμως από τις στοχευμένες διαφημίσεις, τα Big Data Analytics παρέχουν σήμερα στις επιχειρήσεις τη δυνατότητα να συνάγουν την προθυμία των καταναλωτών να πληρώσουν και να προσαρμόζουν τις τιμές των προϊόντων / υπηρεσιών τους στον καθένα από αυτούς. Η διάκριση τιμών αναφέρεται ακριβώς στην πρακτική της χρέωσης διαφορετικών τιμών σε διαφορετικούς αγοραστές για το ίδιο προϊόν ή υπηρεσία σύμφωνα με τη μέγιστη τιμή που ο κάθε αγοραστής είναι διατεθειμένος να πληρώσει για το συγκεκριμένο προϊόν/υπηρεσία (Woodcock, 2016). Τέτοιου είδους πρακτικές, παρά τα οφέλη που μπορεί να έχουν στην οικονομία γενικότερα (π.χ. περισσότερες συναλλαγές, καθώς παρέχεται η δυνατότητα να πραγματοποιηθούν συναλλαγές και με άτομα που διαφορετικά δεν θα αγόραζαν το εκάστοτε προϊόν/υπηρεσία, καθώς δεν θα ήταν διατεθειμένοι να πληρώσουν την ενιαία για όλους τιμή), εντούτοις ενισχύουν σε μεγάλο βαθμό τη θέση των επιχειρήσεων σε σχέση με τους καταναλωτές (Art. 29 WP, 2013). Σε μια ακραία περίπτωση, οι επιχειρήσεις θα είναι σε θέση να καθορίζουν με

απόλυτη ακρίβεια τη μέγιστη τιμή που είναι διατεθειμένος να πληρώσει ο κάθε καταναλωτής και να του κάνουν μια προσφορά take-it-or-leave-it, με αποτέλεσμα το σύνολο του πλεονάσματος που προκύπτει από μια συναλλαγή να καταλήγει στον πωλητή, με τον αγοραστή να μην διαθέτει στην περίπτωση αυτή καμία απολύτως διαπραγματευτική δύναμη (Bourreau & DeStreel, 2018· Woodcock, 2016). Ωστόσο, αξίζει να σημειωθεί, ότι οι πρακτικές της διάκρισης τιμών δεν είναι σήμερα ιδιαίτερα ανεπτυγμένες, αλλά οι επιχειρήσεις πειραματίζονται ακόμα με αυτές (OECD, Directorate for Financial and Enterprise Affair, Competition Committee, 2016).

Ταυτόχρονα, ιδιαίτερες ανησυχίες εγείρει και η αντίληψη των καταναλωτών σε σχέση με αυτές τις πρακτικές. Σε έρευνα που πραγματοποιήθηκε από την Ευρωπαϊκή Επιτροπή το 2018 (Ipsos, London Economics, Deloitte, 2018), μόλις το 44% των καταναλωτών απάντησε ότι γνωρίζει για τις πρακτικές της διάκρισης τιμών, ενώ το αντίστοιχο ποσοστό για τις πρακτικές της στοχευμένης διαφήμισης έφτανε το 67%. Εντούτοις, λιγότεροι από τους μισούς ερωτηθέντες μπόρεσαν να εντοπίσουν σωστά, πότε ήταν δέκτες στοχευμένων διαφημίσεων στο διαδίκτυο ή εξατομικευμένης τιμολόγησης (Ipsos, London Economics, Deloitte, 2018). Τα προβλήματα συνεπώς, ανακύπτουν αφενός μεν από τους κινδύνους που εν γένει ελλοχεύουν οι πρακτικές εξατομίκευσης για την ιδιωτικότητα των καταναλωτών και αφετέρου από την αδυναμία των τελευταίων να αντιληφθούν και να εντοπίσουν τις πρακτικές αυτές, προκειμένου να μπορέσουν να ασκήσουν τα προβλεπόμενα εκ του νόμου δικαιώματά τους.

Γίνεται, επομένως, κατανοητό, ότι τα Big Data Analytics δημιουργούν σήμερα ένα περιβάλλον αβεβαιότητας και ανασφάλειας σε ότι έχει να κάνει με την προστασία της ιδιωτικότητας των ατόμων. Ο σύγχρονος πολίτης αισθάνεται ότι δεν έχει τον έλεγχο των προσωπικών του δεδομένων και πρακτικά, αν αναλογιστεί κανείς το μέγεθος του ψηφιακού κόσμου και τις δυνατότητες των σύγχρονων τεχνολογιών σήμερα, είναι πολύ δύσκολο να έχει κανείς μια πλήρη και σαφή εικόνα αυτών. Η υπόσχεση δε της ανωνυμίας μέσα από τεχνικές ανωνυμοποίησης και ψευδωνυμοποίησης αλλά και της λήθης, μέσα από τη διαγραφή των παλαιότερων δεδομένων, οι οποίες θα μπορούσαν να ενισχύσουν την εμπιστοσύνη των υποκειμένων των δεδομένων και το αίσθημα ασφάλειας, φαίνεται ότι δεν είναι πλέον εφικτές. Αντιθέτως, η ενίσχυση των τεχνικών επιτήρησης μέσω ηλεκτρονικών επικοινωνιών, ως μια νέα μορφή άμεσου κοινωνικού ελέγχου, θέτει πρωτόφαντες απειλές στην ιδιωτικότητα και στις ατομικές ελευθερίες (Τσαούση, 2018). Παράλληλα, η δυνατότητα των σύγχρονων επιχειρήσεων να κατανοούν σε βάθος τον χαρακτήρα και την προσωπικότητα του κάθε καταναλωτή και να προσαρμόζουν τις παροχές τους ανάλογα, δημιουργεί ένα καθεστώς ασύμμετρης

πληροφόρησης και έχει ως αποτέλεσμα να πραγματοποιούνται συναλλαγές, οι οποίες ενδεχομένως δεν ανταποκρίνονται στην πραγματική βούληση του καταναλωτή ή στις οποίες ο καταναλωτής δεν έχει ούτε την ικανότητα αλλά ούτε και τη διαπραγματευτική δύναμη για να συμβληθεί, φέρνοντας εν τέλει τον καταναλωτή σε μειονεκτική θέση. Όπως το θέτει χαρακτηριστικά και ο Calo (2013): «Η ψηφιοποίηση του εμπορίου μεταβάλλει δραματικά την ικανότητα των επιχειρήσεων να επηρεάζουν τους καταναλωτές σε προσωπικό επίπεδο».

4. 3. Διακρίσεις και Αδικία

Η απαγόρευση των διακρίσεων αποτελεί έναν από τους βασικότερους πυλώνες των θεμελιωδών δικαιωμάτων και σε ενωσιακό επίπεδο έχουν γίνει πολύ μεγάλες προσπάθειες για την εξάλειψη τους. Συγκεκριμένα, σύμφωνα με το άρθρο 21 του ΧΘΔ απαγορεύονται οι διακρίσεις που βασίζονται σε χαρακτηριστικά, όπως: το φύλο, η φυλή, το χρώμα, η εθνοτική καταγωγή ή η κοινωνική προέλευση, τα γενετικά χαρακτηριστικά, η γλώσσα, η θρησκεία ή οι πεποιθήσεις, τα πολιτικά φρονήματα ή κάθε άλλη γνώμη, η ιδιότητα μέλους εθνικής μειονότητας, η περιουσία, η γέννηση, η αναπηρία, η ηλικία και ο γενετήσιος προσανατολισμός. Τα χαρακτηριστικά αυτά αποτελούν "ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα" και τυγχάνουν αυξημένης προστασίας και από τον ΓΚΠΔ.

Τα τελευταία χρόνια, χάρη στην ευρεία καθιέρωση των Big Data Analytics έχουν έρθει στο φως αρκετές περιπτώσεις άμεσων και έμμεσων διακρίσεων από τη χρήση τους, οι οποίες έχουν απασχολήσει ιδιαίτερα την ακαδημαϊκή κοινότητα και εγείρουν σοβαρές ανησυχίες. Ένα χαρακτηριστικό παράδειγμα αποτελεί το σύστημα COMPAS που χρησιμοποιείται από την ποινική δικαιοσύνη των ΗΠΑ, το οποίο μεταξύ άλλων βαθμολογεί τον κίνδυνο υποτροπής των κατηγορουμένων. Σύμφωνα με μια έρευνα που πραγματοποίησε μια ομάδα δημοσιογράφων, οι λευκοί κατηγορούμενοι εσφαλμένα χαρακτηρίζονταν πιο συχνά ως «χαμηλού κινδύνου» για την πιθανότητα της υποτροπής σε σύγκριση με τους μαύρους κατηγορούμενους, οι οποίοι χαρακτηρίζονταν συχνότερα ως «υψηλού κινδύνου» από το σύστημα αυτό (FRA, 2018). Αντίστοιχα διαπιστώθηκε, ότι η αναζήτηση στο διαδίκτυο ονομάτων που συνδέονται πιο στενά με έγχρωμους πληθυσμούς είχε ως αποτέλεσμα να στέλνονται στα άτομα αυτά πιο συχνά διαφημίσεις που αφορούσαν συλλήψεις σε σχέση με άτομα που αναζητούσαν στο διαδίκτυο ονόματα που έχουν συνδεθεί με λευκούς πληθυσμούς (ICO, 2017). Σε μια άλλη περίπτωση μια γυναίκα γιατρός κλειδώθηκε έξω από τα αποδυτήρια ενός

γυμναστηρίου, επειδή το αυτοματοποιημένο σύστημα ασφαλείας είχε συνδέσει τον τίτλο του "Δόκτορος" με το ανδρικό φύλο (ICO, 2017).

Συγκεκριμένα, η εξαγωγή ενός μεροληπτικού αποτελέσματος από ένα σύστημα μηχανικής μάθησης μπορεί να ανάγεται σε οποιοδήποτε στάδιο του σχεδιασμού ή της εκπαίδευσής του. Κατά τον σχεδιασμό ενός συστήματος επιβλεπόμενης μηχανικής μάθησης, οι προγραμματιστές καλούνται να ορίσουν τις μεταβλητές – στόχους (*target variables*) και να χαρακτηρίσουν τις κλάσεις (*class labels*). Αρχικά, πρέπει δηλαδή να οριστεί το ζητούμενο, ποιο είναι το επιδιωκόμενο αποτέλεσμα (η μεταβλητή στόχος), το οποίο δεν είναι πάντοτε αυτονόητο. Ο προγραμματιστής θα πρέπει να κατανοήσει τους στόχους του έργου που έχει αναλάβει και να τους μετατρέψει σε ένα πρόβλημα, σε μία ερώτηση που πρέπει τελικά να απαντηθεί από το σύστημα μηχανικής μάθησης (Barocas & Selbst, 2016). Στη συνέχεια, πρέπει να οριστούν όλες οι πιθανές "τιμές" της μεταβλητής – στόχου, όλα τα πιθανά ενδεχόμενα που μπορεί να προκύψουν, όλες δηλαδή οι απαντήσεις στην ερώτηση που έχει τεθεί και να διαιρεθούν σε αμοιβαία αποκλειόμενες κατηγορίες – κλάσεις (Barocas & Selbst, 2016). Οι κλάσεις αυτές, ανάλογα πάντοτε με το ζητούμενο, μπορεί να είναι είτε δύο (π.χ. στην περίπτωση της ανεπιθύμητης αλληλογραφίας, ένα email είτε είναι ανεπιθύμητο είτε όχι) είτε και περισσότερες (π.χ. στην περίπτωση των προσλήψεων από έναν εργοδότη, ένας υποψήφιος μπορεί να είναι καλός, μέτριος, κακός) (Barocas & Selbst, 2016). Στο πλαίσιο αυτό του σχεδιασμού ενός συστήματος μηχανικής μάθησης, οι προγραμματιστές μπορεί να εκφράσουν το πρόβλημα με τέτοιο τρόπο, που να φέρνει σε μειονεκτική θέση τις ανωτέρω προστατευόμενες ομάδες, ειδικά στις περιπτώσεις όπου χρειάζονται περισσότερες από δύο κλάσεις (οπότε το πρόβλημα δεν επιλύεται με το σύστημα "είναι ή δεν είναι") και αναγκαστικά εμπεριέχεται η κρίση του προγραμματιστή σε αυτές (π.χ. πότε ένας υποψήφιος εργαζόμενος δεν είναι καλός και είναι μέτριος, με βάση ποια κριτήρια;) (Barocas & Selbst, 2016).

Επιπλέον, οι υποκειμενικές επιλογές που γίνονται όταν διαλέγονται, συλλέγονται και προετοιμάζονται τα δεδομένα κατάρτισης μπορούν επίσης να διαμορφώσουν ένα σύστημα μηχανικής μάθησης που θα "παράγει" διακρίσεις και μεροληπτικά συμπεράσματα (FRA, 2018). Στο στάδιο της διαλογής και της συλλογής, ιδιαίτερη προσοχή πρέπει να δίνεται στην ποιότητα και την αντιπροσωπευτικότητα των δεδομένων. Όσον αφορά την ποιότητα, τα δεδομένα που χρησιμοποιούνται για την εκπαίδευση του συστήματος πρέπει να είναι ακριβή, να μην περιλαμβάνουν λάθη και ελλείψεις και να είναι ενημερωμένα (FRA, 2018). Η εξασφάλιση της ποιότητας των δεδομένων κατάρτισης καθίσταται σήμερα ιδιαίτερα δύσκολη, καθώς τα δεδομένα

παράγονται σε τεράστιες ποσότητες και με μεγάλη ταχύτητα, ενώ πολλές φορές το κόστος της εξασφάλισης μεγαλύτερης ακρίβειας στα δεδομένα που χρησιμοποιούνται, υπερβαίνει κατά πολύ τα οφέλη που θα αποκομίσει αυτός που τα επεξεργάζεται, για αυτό άλλωστε και σήμερα δεν γίνονται συχνά ποιοτικοί έλεγχοι των δεδομένων (Barocas & Selbst, 2016· FRA, 2018).

Σχετικά με την αντιπροσωπευτικότητα, όταν επιλέγονται τα δεδομένα κατάρτισης θα πρέπει να εξασφαλίζεται, ότι όλες οι κοινωνικές ομάδες αντιπροσωπεύονται επαρκώς σε αυτά. Αντιθέτως, παρατηρείται ότι ομάδες που δεν έχουν τόσο έντονη παρουσία στον ψηφιακό κόσμο (επειδή π.χ. δεν έχουν τη δυνατότητα ή την ικανότητα να αλληλεπιδράσουν με τις σύγχρονες τεχνολογίες) υπο-εκπροσωπούνται σε τέτοιου είδους δείγματα δεδομένων, με αποτέλεσμα να υφίστανται μεροληπτική αντιμετώπιση όταν λαμβάνονται αποφάσεις για αυτούς από συστήματα τεχνητής νοημοσύνης. Όπως αναφέρει χαρακτηριστικά και ο Muller (2017), η ανάπτυξη της τεχνητής νοημοσύνης συντελείται σε ένα ομοιογενές περιβάλλον αποτελούμενο κυρίως από νέους άνδρες της λευκής φυλής, γεγονός που οδηγεί (εσκεμμένα ή όχι) στην παγίωση στον κόσμο της τεχνητής νοημοσύνης των πολιτισμικών ανισοτήτων και των ανισοτήτων μεταξύ των φύλων, μεταξύ άλλων επειδή τα συστήματα τεχνητής νοημοσύνης μαθαίνουν βάσει δεδομένων εκπαιδευτικού χαρακτήρα.

Βέβαια, ακόμη και αν υποθέσουμε ότι τα δεδομένα κατάρτισης είναι άρτια, διαθέτουν δηλαδή και ποιότητα και αντιπροσωπευτικότητα, εντούτοις και πάλι δεν εξαλείφεται εντελώς ο κίνδυνος διακρίσεων. Τα προσωπικά δεδομένα που χρησιμοποιούνται για τη εκπαίδευση ενός συστήματος μηχανικής μάθησης αντιπροσωπεύουν ένα κοινωνικό σύνολο μια δεδομένη χρονική περίοδο, συνεπώς διακρίσεις και μεροληπτικές συμπεριφορές που εμφανίζονται σε μια κοινωνία - ακόμα και αν αντίκεινται στην κείμενη νομοθεσία - αντικατοπτρίζονται στα δεδομένα αυτά, πάνω σε αυτές θα "εκπαιδευτεί" το εκάστοτε σύστημα και μετέπειτα θα τις αναπαράγει. Ένα σύστημα μηχανικής μάθησης διαθέτει λογική, όχι όμως και ενσυναίσθηση, δεν είναι δηλαδή σε θέση να διακρίνει αν κάτι είναι ηθικό ή όχι.

Χαρακτηριστικό παράδειγμα αποτελεί το μοντέλο προσλήψεων της Amazon, το οποίο στηρίχθηκε σε παλαιότερες αιτήσεις υποψηφίων και στους λόγους που απορρίφθηκαν ή έγιναν αυτές δεκτές, προκειμένου να αναπτύξει το μοντέλο του. Η ανάλυση έδειξε, ότι τα στοιχεία των βιογραφικών που συνδέονται με το γυναικείο φύλο (π.χ. συμμετοχή σε ένα γυναικείο κολέγιο) σχετίζονταν με ανεπιτυχείς αιτήσεις, με αποτέλεσμα ο αλγόριθμος να "μάθει" να απορρίπτει τις αιτήσεις των γυναικών. Το

γεγονός αυτό οφείλεται πιθανότατα στην εδραιωμένη προκατάληψη υπέρ των ανδρών - εργαζομένων που υφίσταται στη βιομηχανία της τεχνολογίας και η οποία είχε διαμορφώσει τα δεδομένα κατάρτισης, δηλαδή τα βιογραφικά των επιτυχημένων και ανεπιτυχών υποψηφίων. Η Amazon αντιλήφθηκε έγκαιρα το φαινόμενο αυτό και τελικά δεν εφάρμοσε το συγκεκριμένο μοντέλο για τις προσλήψεις της (Hirsch, 2019).

Το στάδιο της προετοιμασίας των δεδομένων αφορά τα συστήματα επιβλεπόμενης μηχανικής μάθησης και συγκεκριμένα το στάδιο της επισήμανσης των δεδομένων κατάρτισης, όπου τα δεδομένα αυτά διανέμονται στις διάφορες κλάσεις (Barocas & Selbst, 2016). Στο στάδιο αυτό, όπως ακριβώς και στο στάδιο του σχεδιασμού του συστήματος, η ανθρώπινη παρεμβολή (από τον προγραμματιστή) και η εγγενής υποκειμενικότητα που εμπεριέχεται στην αντιστοιχία δεδομένων και κλάσεων μπορεί να έχει ως συνέπεια να "μάθει" το σύστημα να διακρίνει και να μεροληπτεί σε βάρος συγκεκριμένων κοινωνικών ομάδων. Επομένως, η εξασφάλιση της ποιότητας και η σωστή διαχείριση των δεδομένων κατάρτισης αποτελούν πολύ σημαντικά βήματα στη διαδικασία "κατασκευής" ενός συστήματος τεχνικής νοημοσύνης, ώστε να αποφευχθεί αυτό που με πολύ γλαφυρό τρόπο περιγράφει η φράση: "Σκουπίδια βάζεις, σκουπίδια παίρνεις" ("*garbage in, garbage out*").

Ακόμα βέβαια και στην περίπτωση, που αφαιρεθούν εντελώς από τα δεδομένα κατάρτισης εκείνες οι κατηγορίες ευαίσθητων προσωπικών δεδομένων, που αποτελούν το έναυσμα για την εμφάνιση μεροληπτικών συμπεριφορών και διακρίσεων, εντούτοις και πάλι δεν εξαλείφεται ο κίνδυνος αυτών, καθώς τα υπόλοιπα δεδομένα που θα χρησιμοποιηθούν για τη λήψη της απόφασης μπορεί να συνδέονται άμεσα με τα ευαίσθητα χαρακτηριστικά που έχουν παραλειφθεί, λειτουργώντας ως ενδείξεις αυτών[1]. Για παράδειγμα καθίσταται δυνατή η πρόβλεψη της φυλετικής καταγωγής ενός ανθρώπου με βάση τον ταχυδρομικό του κώδικα, όταν τα δύο αυτά χαρακτηριστικά συνδέονται μεταξύ τους (π.χ. σε περιπτώσεις διαχωρισμένων περιοχών στις πόλεις) (FRA, 2018). Μια απόφαση, επομένως, που στηρίζεται στην περιοχή που μένει ένας άνθρωπος, στηρίζεται ουσιαστικά και στη φυλετική του καταγωγή, αφού το ένα χαρακτηριστικό υποδεικνύει έμμεσα και την ύπαρξη του άλλου.

Στο πλαίσιο αυτό, οι Barocas και Selbst (2016) εντοπίζουν ίσως το πιο τρομακτικό σενάριο, τις εκούσιες διακρίσεις, όπου η εξαγωγή μεροληπτικών συμπερασμάτων είναι σκόπιμη και όλοι οι ανωτέρω μηχανισμοί χρησιμοποιούνται για να καλύψουν και να αιτιολογήσουν τις προθέσεις του προσώπου που επεξεργάζεται τα

[1]Για αυτού του είδους τα δεδομένα, που υποδεικνύουν δηλαδή κάποιες ευαίσθητες πληροφορίες για κάποιο πρόσωπο χρησιμοποιείται ο αγγλικός όρος "proxy".

δεδομένα. Ο κίνδυνος, επομένως, διακρίσεων και προκαταλήψεων στην εποχή των Big Data Analytics, όχι μόνο δεν εξαλείφεται, αλλά αντιθέτως αν δεν υπάρξει η δέουσα προσοχή, οι διακρίσεις θα επαναληφθούν, θα διαιωνιστούν και ενδεχομένως θα ενισχυθούν (FRA, 2018).

Σε κάθε περίπτωση, η χρησιμοποίηση των Big Data Analytics για τη λήψη αποφάσεων μπορεί να οδηγήσει σε προβληματικά και άδικα αποτελέσματα, ακόμα και όταν αυτά δεν στηρίζονται σε μια από τις προστατευόμενες κατά τα ανωτέρω κατηγορίες δεδομένων. Το φαινόμενο αυτό εμφανίζεται έντονα στον χρηματοπιστωτικό τομέα, όπου χρησιμοποιούνται σήμερα νέες μέθοδοι για την εκτίμηση της πιστοληπτικής ικανότητας των υποψήφιων δανειοληπτών. Ειδικότερα, η βαθμολόγηση της πιστοληπτικής ικανότητας (*credit scoring*) αναφέρεται ακριβώς στον συνδυασμό των πληροφοριών που λαμβάνονται παραδοσιακά υπόψη κατά τη διαδικασία χορήγησης πίστωσης (π.χ. τα εισοδήματα του υποψήφιου δανειολήπτη) με χιλιάδες σημεία δεδομένων που εξάγονται από τις διαδικτυακές και μη δραστηριότητες των καταναλωτών (Hurley & Adebayo, 2016). Για παράδειγμα, η Ομοσπονδιακή Επιτροπή Εμπορίου στις ΗΠΑ ανακάλυψε, ότι τα πιστωτικά όρια μιας ομάδας καταναλωτών μειώθηκαν με βάση το κακό ιστορικό αποπληρωμής άλλων καταναλωτών, που ψώνιζαν στα ίδια καταστήματα με τους πρώτους (ICO, 2017). Σε μια άλλη αντίστοιχη περίπτωση, τα τραπεζικά ιδρύματα στις ΗΠΑ διαφήμισαν τις πιστωτικές τους κάρτες σε άτομα που είχαν αγοράσει αντιολισθητικά μαξιλαράκια για τα έπιπλα, καθώς η αγορά αυτού του προϊόντος συνδέονταν, με βάση τα δεδομένα που κατείχαν από τους μέχρι τότε πελάτες τους, με χαμηλότερο κίνδυνο αδυναμίας πληρωμής της κάρτας στο μέλλον (Hirsch, 2019). Παράλληλα, η χορήγηση πιστώσεων εξαρτάται σε πολλές περιπτώσεις από την περιοχή που ζει ο κάθε υποψήφιος και από τη "φερεγγυότητα" που αποδίδεται σε κάθε μια από αυτές (Bennett & Bayley, 2016). Η πρόσβαση, δηλαδή στην πίστωση εξαρτάται σε πολλές περιπτώσεις από τις αδιαφανείς προβλέψεις των δανειστών σχετικά με τους φίλους των καταναλωτών, με τους γείτονες τους, καθώς και με άτομα με παρόμοια ενδιαφέροντα, εισοδήματα και υπόβαθρα (Hurley & Adebayo, 2016). Το ερώτημα, επομένως, που γεννάται είναι το εξής: Είναι σωστό, ή δίκαιο η πρόσβαση ενός ατόμου σε πίστωση να εξαρτάται όχι μόνο από τα οικονομικά του δεδομένα (π.χ. το εισόδημα του) αλλά και από διάφορα άλλα, όπως για παράδειγμα τις καταναλωτικές του συνήθειες ή την περιοχή στην οποία διαμένει, πόσο μάλλον όταν ο υποψήφιος δανειολήπτης δεν γνωρίζει, ότι οι πληροφορίες αυτές βρίσκονται στα χέρια του δανειστή του και ότι λαμβάνονται υπόψη για τη χορήγηση της πίστωσης;

Συνεπώς, υπάρχει έντονα ο κίνδυνος, τα Big Data Analytics αντί να οδηγήσουν στη λήψη αντικειμενικών, πληροφορημένων αποφάσεων, απαλλαγμένων από τις προκαταλήψεις και τους περιορισμούς της ανθρώπινης νόησης, να διαιωνίσουν και ενδεχομένως να επιδεινώσουν τις υπάρχουσες και εδραιωμένες προκαταλήψεις και τα στερεότυπα, δημιουργώντας έναν φαύλο κύκλο, όπου η ανατροφοδότηση που λαμβάνει το σύστημα μηχανικής μάθησης ενισχύει τις προκαταλήψεις που υπήρχαν εξ' αρχής (European Data Protection Supervisor, 2016). Οι διακρίσεις και τα άδικα αποτελέσματα μπορεί να ανάγονται σε οποιοδήποτε από τα διαφορετικά στάδια της δημιουργίας και της ανάπτυξης ενός συστήματος τεχνητής νοημοσύνης, ενώ παράλληλα μπορούν να εμφανιστούν οπουδήποτε χρησιμοποιούνται τέτοιου είδους τεχνολογίες (από το γυμναστήριο μέχρι και τα πιστωτικά ιδρύματα). Καθίσταται, επομένως, επιτακτική η ανάγκη να δοθεί ιδιαίτερη προσοχή τόσο στην πρόληψη τέτοιου είδους φαινομένων, κατά τον σχεδιασμό και την κατασκευή των συστημάτων τεχνητής νοημοσύνης, όσο και στην αντιμετώπιση αυτών, μέσα από τον ενδελεχή έλεγχο των αποτελεσμάτων και των συμπερασμάτων που προκύπτουν από την ανάλυση των δεδομένων.

4. 4. Χειραγώγηση

Στην εποχή των Big Data Analytics, η πληθώρα των διαθέσιμων προσωπικών δεδομένων αφενός και η δυνατότητα κατανόησης των δεδομένων αυτών σε ένα βαθύτερο επίπεδο αφετέρου έχουν ως αποτέλεσμα να γνωρίζουν τα συστήματα τεχνητής νοημοσύνης τα πάντα σχετικά με τις προτιμήσεις, τα ενδιαφέροντα και τις συνήθειες ενός ατόμου, τους φίλους και τους γνωστούς του, την εκπαίδευση και την απασχόλησή του, την υγεία και την οικονομική του κατάσταση και κατ' επέκταση να μπορούν να κατανοήσουν τι δίνει κίνητρο στο άτομο αυτό, ποιες είναι οι αδυναμίες του και πότε γίνεται ευάλωτος (Susser, Roessler & Nissenbaum, 2019). Με άλλα λόγια, όπως αναφέρουν χαρακτηριστικά οι Susser et al. (2018) τα συστήματα τεχνητής νοημοσύνης, μελετώντας τόσο τις ατομικές ιδιοσυγκρασίες ενός ατόμου όσο και τα μοτίβα που εμφανίζονται μεταξύ των δημογραφικών ομάδων στις οποίες ανήκει, αποκαλύπτουν αδυναμίες και διαθέσεις του, τις οποίες πολλές φορές ούτε το ίδιο το άτομο μπορούσε να διακρίνει. Ακριβώς η δυνατότητα αυτή των σύγχρονων τεχνολογιών να κατανοούν σε βάθος την προσωπικότητα και τον χαρακτήρα ενός ατόμου καθιστά πιο εύκολη και αποτελεσματική τη χειραγώγηση του σε συμπεριφορές που διαφορετικά δεν θα επεδείκνυε, μέσω της εκμετάλλευσης των αδυναμιών και των ευαίσθητων σημείων του.

Χαρακτηριστικό παράδειγμα αποτελεί η αξιοποίηση των Big Data Analytics από πολιτικές εκστρατείες, προκειμένου να ασκήσουν ουσιαστική επιρροή στη συμπεριφορά και στις αποφάσεις των ψηφοφόρων, με το σκάνδαλο της Cambridge Analytica να αποτελεί την πιο τρανταχτή και ανησυχητική περίπτωση. Η Cambridge Analytica, μια βρετανική συμβουλευτική εταιρεία στον τομέα της πολιτικής συγκέντρωσε -όπως φημολογείται- προσωπικές πληροφορίες για εκατομμύρια χρήστες της Facebook, τις οποίες στη συνέχεια και χρησιμοποίησε για να επηρεάσει τη συμπεριφορά τους. Συγκεκριμένα, χρησιμοποιώντας διαδικτυακά κουίζ προσωπικότητας σε χρήστες της Facebook, κατάφερε να εκμαιεύσει προσωπικές πληροφορίες τόσο των ίδιων, όσο και των διαδικτυακών τους φίλων, να "χαρτογραφήσει" την προσωπικότητα τους και να στείλει στον καθένα από αυτούς εξατομικευμένα πολιτικά μηνύματα τόσο στο δημοψήφισμα του 2016 στο Ηνωμένο Βασίλειο για την αποχώρηση από την Ευρωπαϊκή Ένωση όσο και στις προεδρικές εκλογές των ΗΠΑ το 2016 (Granville, 2018· Βέργου, 2019). Η Cambridge Analytica ουσιαστικά προσπάθησε, χρησιμοποιώντας τις πληροφορίες που διέθετε για κάθε ψηφοφόρο και εκμεταλλευόμενη τις αδυναμίες του καθενός, να πλαισιώσει τα πολιτικά μηνύματα που ήθελε να περάσει με τέτοιο τρόπο, που θα ήταν δύσκολο να "τους αντισταθεί" κανείς (Hirsch, 2019).

Οι σύγχρονες μορφές χειραγώγησης έχουν, επομένως, ως αποτέλεσμα την καταπάτηση της ιδιωτικής αυτονομίας, καθώς στρεβλώνουν τον τρόπο με τον οποίο οι άνθρωποι λαμβάνουν συνήθως αποφάσεις (Kilovaty, 2019). Στερούν από τους ανθρώπους, με έναν λανθάνοντα τρόπο, που δεν μπορεί να γίνει εύκολα αντιληπτός, τη δυνατότητα να είναι κύριοι του εαυτού τους, να κάνουν ελεύθερες και συνειδητές επιλογές για σημαντικές πτυχές της ζωής τους, με αποτέλεσμα να λαμβάνουν αποφάσεις που δεν εξυπηρετούν τα συμφέροντά τους, χωρίς καν να αντιλαμβάνονται το γεγονός αυτό. Από την περίπτωση δε της Cambridge Analytica κατέστη σαφές, ότι η χειραγώγηση αποτελεί έναν υπαρκτό κίνδυνο των Big Data Analytics, όχι μόνο για την ιδιωτική αυτονομία αλλά ενδεχομένως και για την ίδια τη δημοκρατία, καθώς, κατ’ εφαρμογή της έννοιας της οριακότητας που προέρχεται από την Οικονομική Επιστήμη, η στρέβλωση έστω και μιας ψήφου, ακόμα και αν αυτή δεν είναι ικανή να αλλάξει το τελικό εκλογικό αποτέλεσμα, από μόνη της αντίκειται στις θεμελιώδεις αρχές της δημοκρατίας και το αδιάβλητο της εκλογικής διαδικασίας, καθιστώντας με τον τρόπο αυτό τη χειραγώγηση τον μεγαλύτερο ίσως κίνδυνο των Big Data Analytics.

5. Τα Big Data Analytics υπό το νέο καθεστώς του ΓΚΠΔ

5. 1. Εισαγωγή

Αναμφισβήτητα, τα Big Data Analytics παρουσιάζουν μια ιδιαίτερη δυναμική, αποτελώντας πλέον έναν βασικό μοχλό της οικονομικής ανάπτυξης. Το εύρος των δυνατοτήτων τους επεκτείνεται από την εξασφάλιση μιας πιο εύκολης και ποιοτικής καθημερινότητας για κάθε πολίτη έως την ενίσχυση της οικονομίας, μέσω της αύξησης της παραγωγικότητας των ιδιωτικών επιχειρήσεων και της αναβάθμισης των δημοσίων υπηρεσιών. Το Παγκόσμιο Οικονομικό Φόρουμ, μάλιστα έχει χαρακτηρίσει τα δεδομένα ως έναν νέο συντελεστή παραγωγής μαζί με την εργασία και το κεφάλαιο (Schwab, Marcus, Oyola, Hoffman & Luizi, 2011). Παράλληλα όμως, όπως φαίνεται και από την ανωτέρω ανάλυση, η χρήση των Big Data Analytics εγείρει πολλά ηθικά και νομικά ζητήματα, με αποτέλεσμα να καθίσταται αναγκαία η εξεύρεση μιας ισορροπίας ανάμεσα αφενός στα συμφέροντα των οργανισμών (επιχειρήσεις και δημόσιους φορείς) που χρησιμοποιούν τέτοιες μεθόδους και αφετέρου στις πιθανές βλάβες που μπορεί να προκαλέσει η χρήση αυτών στους πολίτες.

Στο πλαίσιο αυτό, οι σύγχρονες αυτές τεχνολογικές εξελίξεις έχουν μονοπωλήσει το ενδιαφέρον της Ευρωπαϊκής Ένωσης τα τελευταία χρόνια. Συγκεκριμένα, τον Φεβρουάριο του 2020 η Ευρωπαϊκή Επιτροπή εξέδωσε την Ανακοίνωση για τη Διαμόρφωση του Ψηφιακού Μέλλοντος της Ευρώπης, η οποία περιλαμβάνει την ενωσιακή στρατηγική για τη μετάβαση σε μια νέα ψηφιακή πραγματικότητα. Η στρατηγική αυτή επικεντρώνεται σε τρεις βασικούς στόχους: τεχνολογία που λειτουργεί για τους ανθρώπους, μια δίκαιη και ανταγωνιστική οικονομία και μια ανοιχτή, δημοκρατική και βιώσιμη κοινωνία (European Commission, 2020γ). Στόχος της Ευρωπαϊκής Ένωσης είναι να παραμείνει στην πρώτη γραμμή των τεχνολογικών εξελίξεων, με σεβασμό πάντα των θεμελιωδών ευρωπαϊκών αξιών και με γνώμονα την ανθρώπινη ευημερία. Οι δύο βασικοί πυλώνες της στρατηγικής αυτής είναι τα δεδομένα και η τεχνητή νοημοσύνη (European Commission, 2020δ).

Όσον αφορά το κομμάτι των δεδομένων, η Ευρωπαϊκή Επιτροπή προχώρησε στην Ανακοίνωση για την Ευρωπαϊκή Στρατηγική για τα δεδομένα [COM(2020)66], με την οποία αναγνωρίζεται η καίρια σημασία που έχουν τα δεδομένα στις σύγχρονες ψηφιακές οικονομίες και προβλέπεται η δημιουργία μιας ενιαίας αγοράς δεδομένων στην οποία: τα δεδομένα θα μπορούν να ρέουν εντός της Ε.Ε. και μεταξύ τομέων, προς όφελος όλων, οι ευρωπαϊκοί κανόνες, ιδίως η προστασία της ιδιωτικής ζωής και των δεδομένων, καθώς και η νομοθεσία περί ανταγωνισμού θα τηρούνται πλήρως και οι κανόνες πρόσβασης και χρήσης δεδομένων θα είναι δίκαιοι, πρακτικοί και σαφείς.

Επιπλέον, σε ότι έχει να κάνει με την τεχνητή νοημοσύνη, δημοσιεύθηκε η Λευκή Βίβλος για την Τεχνητή Νοημοσύνη [COM(2020)65], με την οποία προβλέπονται δράσεις για τη διάκριση της Ευρωπαϊκής Ένωσης στον τομέα της τεχνητής νοημοσύνης, δημιουργώντας παράλληλα ένα περιβάλλον εμπιστοσύνης και ασφάλειας, έτσι ώστε η τεχνητή νοημοσύνη να είναι "αξιόπιστη".

Στο υπόβαθρο αυτής της νέας ψηφιακής στρατηγικής της Ευρωπαϊκής Ένωσης βρίσκεται μια πληθώρα δράσεων των προηγούμενων ετών. Συγκεκριμένα, ήδη από το 2014 η Επιτροπή είχε λάβει μέτρα για την ανάπτυξη μιας ευέλικτης οικονομίας δεδομένων (π.χ. μέσω του Κανονισμού για την ελεύθερη ροή μη προσωπικών δεδομένων), ενώ παράλληλα είχε αρχίσει να αναπτύσσεται η ιδέα της συνεργασίας των κρατών – μελών και της Ε.Ε. για μια ενιαία αγορά δεδομένων [όπως φαίνεται στην Ανακοίνωση της Ευρωπαϊκής Επιτροπής προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα - COM(2014)442, την οποία διαδέχθηκε η Ανακοίνωση για την οικοδόμηση μιας ευρωπαϊκής οικονομίας δεδομένων - COM(2017)9]. Το 2018, ακολουθώντας τη Διακήρυξη Συνεργασίας για την Τεχνητή Νοημοσύνη που είχε υπογραφεί από τα κράτη – μέλη, η Επιτροπή παρουσίασε μια στρατηγική για την τεχνητή νοημοσύνη [Ανακοίνωσή για την «Τεχνητή Νοημοσύνη για την Ευρώπη» - COM(2018)237] και συμφώνησε ένα συντονισμένο σχέδιο για τα κράτη μέλη [Συντονισμένο Σχέδιο για την Τεχνητή Νοημοσύνη - COM(2018)795]. Σημαντικό είναι και το έργο της Ομάδας Εμπειρογνωμόνων Υψηλού Επιπέδου για την Τεχνητή Νοημοσύνη, η οποία ιδρύθηκε τον Ιούνιο του 2018, με σκοπό την υποστήριξη της στρατηγικής της Ε.Ε. στον τομέα της τεχνητής νοημοσύνης, κυρίως μέσω συστάσεων σχετικά με ηθικά, νομικά και κοινωνικά ζητήματα που σχετίζονται με αυτήν (European Commission, 2019) και μεταξύ άλλων δημοσίευσε τον Απρίλιο του 2019 τις Κατευθυντήριες Γραμμές Δεοντολογίας για την Αξιόπιστη Τεχνητή Νοημοσύνη.

Κατόπιν των ανωτέρω, γίνεται κατανοητό, ότι η Ευρωπαϊκή Ένωση, αναγνωρίζοντας τόσο τις προοπτικές όσο και τους κινδύνους των Big Data Analytics έχει θέσει ως στόχο της τη δημιουργία μιας ανταγωνιστικής, αλλά βασισμένης στις ευρωπαϊκές αξίες ψηφιακής οικονομίας και κοινωνίας. Εντούτοις, όλες οι ανωτέρω δράσεις της Ευρωπαϊκής Ένωσης αποτελούν περιπτώσεις ηπίου δικαίου. Η νομοθεσία για την προστασία των προσωπικών δεδομένων, με κύριο όργανο τον ΓΚΠΔ αποτελεί το μοναδικό μέχρι στιγμής νομικά δεσμευτικό εργαλείο για την αντιμετώπιση των κινδύνων που εγείρει η χρήση των Big Data Analytics, αποτελώντας ουσιαστικά την οργανωτική αρχή των οικονομικών του διαδικτύου (Moerel, 2014). Η σημασία του ΓΚΠΔ, για τη δημιουργία ενός περιβάλλοντος εμπιστοσύνης και ασφάλειας στις

σύγχρονες ψηφιακές κοινωνίες έχει επισημανθεί και από την Ευρωπαϊκή Επιτροπή σε πολλές περιπτώσεις, ενώ η εφαρμογή των διατάξεων του ΓΚΠΔ στις περιπτώσεις που χρησιμοποιούνται τα Big Data Analytics, αλλά και γενικότερα συστήματα τεχνητής νοημοσύνης και μηχανικής μάθησης έχει τονιστεί από την ομάδα εργασίας του άρθρου 29.

5. 2. Ο ΓΚΠΔ

Στις 25 Μαΐου 2018 τέθηκε σε εφαρμογή ο νέος ΓΚΠΔ, αντικαθιστώντας την προϊσχύουσα Οδηγία 95/46/ΕΚ, η οποία βρισκόταν σε εφαρμογή από το 1995 και δεν συμβάδιζε πλέον με τις νέες τεχνολογικές εξελίξεις και τον νέο ρόλο των δεδομένων στην οικονομία και στην κοινωνία (Burri & Schär, 2016), ενώ παράλληλα, σε εθνικό επίπεδο, δημοσιεύθηκε πρόσφατα ο Νόμος 4624/2019, ο οποίος αφορά μεταξύ άλλων τη λήψη μέτρων εφαρμογής του Κανονισμού 2016/679 (ΓΚΠΔ/GDPR). Σκοπός του ΓΚΠΔ είναι ακριβώς να βρεθεί μια ισορροπία ανάμεσα στα συμφέροντα των επιχειρήσεων και στα θεμελιώδη ατομικά δικαιώματα στο πλαίσιο της σύγχρονης ψηφιακής πραγματικότητας, να εξασφαλισθεί δηλαδή αφενός η ελεύθερη ροή των δεδομένων προσωπικού χαρακτήρα εντός της Ε.Ε. και η αξιοποίηση των νέων τεχνολογιών ανάλυσης δεδομένων στο μέγιστο και αφετέρου η προστασία των ανθρώπων και των προσωπικών τους δεδομένων. Ακολουθώντας τη λογική της προϊσχύουσας Οδηγίας, ο Κανονισμός βασίζεται στην αρχή, ότι το κάθε άτομο πρέπει να ασκεί έλεγχο στην επεξεργασία που υφίστανται τα δεδομένα που το αφορούν (Bennett & Bayley, 2016). Στο πλαίσιο αυτό, ο ΓΚΠΔ διαμορφώνεται γύρω από τρεις πυλώνες: τη θέσπιση των θεμελιωδών αρχών της επεξεργασίας των δεδομένων, τη θέσπιση δικαιωμάτων και υποχρεώσεων για τα υποκείμενα των δεδομένων και τους υπεύθυνους επεξεργασίας αντίστοιχα και την εξασφάλιση της εφαρμογής και της τήρησης των διατάξεων (Ishii, 2017). Ο Κανονισμός αποτελεί κατά κανόνα ένα νομικό κείμενο και παρέχει πολύ μικρή τεχνική καθοδήγηση προς τους φορείς που είναι υποχρεωμένοι να συμμορφωθούν με αυτόν, επιδιώκοντας με αυτόν τον τρόπο την προσαρμοστικότητα των διατάξεών του σε μελλοντικές τεχνολογικές καινοτομίες (Politou, Alepis & Patsakis, 2018).

Πιο συγκεκριμένα, ο ΓΚΠΔ ρυθμίζει τις προϋποθέσεις της νόμιμης επεξεργασίας προσωπικών δεδομένων, διαμορφώνοντας τη σχέση (τα δικαιώματα και τις υποχρεώσεις) του υποκειμένου των δεδομένων αφενός και των προσώπων που επεξεργάζονται τα δεδομένα αφετέρου (τους υπεύθυνους της επεξεργασίας ή τους εκτελούντες την επεξεργασία). Ειδικότερα, στο άρθρο 4 περ. 7 του ΓΚΠΔ, ο υπεύθυνος

επεξεργασίας ορίζεται ως «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα», ενώ στην περ. 8 δίνεται ο ορισμός του εκτελούντος την επεξεργασίας ως «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας». Βέβαια, στο πλαίσιο των Big Data Analytics, η διάκριση μεταξύ υπεύθυνων και εκτελούντων την επεξεργασία δεν είναι πάντα εύκολη. Τα Big Data Analytics στηρίζονται στην εύρεση συσχετίσεων, στην πραγματοποίηση προβλέψεων και στη διευκόλυνση της λήψης αποφάσεων, με αποτέλεσμα να μην είναι πάντοτε ξεκάθαρο ποιος καθορίζει στην πραγματικότητα τους σκοπούς και τον τρόπο της επεξεργασίας, ιδιαίτερα δε όταν ένας οργανισμός έχει επιλέξει να αναθέσει την ανάλυση των δεδομένων σε εξωτερικούς συνεργάτες, που εξειδικεύονται στην τεχνητή νοημοσύνη (ICO, 2017).

Ως προς το εδαφικό πεδίο εφαρμογής του, ο Κανονισμός εφαρμόζεται τόσο όταν οι υπεύθυνοι ή οι εκτελούντες την επεξεργασία των δεδομένων είναι εγκατεστημένοι σε κράτος-μέλος της Ένωσης, όσο και όταν η εγκατάστασή τους βρίσκεται εκτός Ε.Ε. Ειδικότερα, στη δεύτερη αυτή περίπτωση, θα πρέπει η επεξεργασία δεδομένων προσωπικού χαρακτήρα να αφορά υποκείμενα των δεδομένων που βρίσκονται στην Ένωση και οι δραστηριότητες επεξεργασίας να σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης (άρθρο 3 του Κανονισμού).

Όσον αφορά το ουσιαστικό πεδίο εφαρμογής του, ο ΓΚΠΔ εφαρμόζεται όταν υπάρχει επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τόσο η έννοια της επεξεργασίας όσο και η έννοια των δεδομένων προσωπικού χαρακτήρα είναι υπό το καθεστώς του ΓΚΠΔ ιδιαίτερα ευρείες και ελαστικές, με αποτέλεσμα ο Κανονισμός να τυγχάνει εφαρμογής σε μια μεγάλη γκάμα περιπτώσεων. Συγκεκριμένα, ως δεδομένο προσωπικού χαρακτήρα θεωρείται κάθε πληροφορία που αφορά κάποιο ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, πρόσωπο δηλαδή του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα (άρθρο 4 περ. 1 ΓΚΠΔ). Έτσι, ‘προσωπικά δεδομένα’ θεωρούνται μεταξύ άλλων τα δεδομένα που έχουν υποστεί ψευδωνυμοποίηση, τα οποία θα μπορούσαν να αποδοθούν στο φυσικό πρόσωπο που αφορούν με τη χρήση συμπληρωματικών πληροφοριών, η διεύθυνση IP, τα cookies και τα δεδομένα θέσης. Επιπλέον, ως ‘επεξεργασία’ νοείται κάθε πράξη ή σειρά πράξεων που πραγματοποιείται

με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα (π.χ. η συλλογή, η αποθήκευση, η αναζήτηση πληροφοριών, η συσχέτιση ή ο συνδυασμός, η κοινολόγηση με διαβίβαση) (άρθρο 4 περ. 2 ΓΚΠΔ), με αποτέλεσμα, σχεδόν οτιδήποτε μπορεί να γίνει με προσωπικά δεδομένα να θεωρείται ως επεξεργασία αυτών (Hoofnagle et al., 2019). Στο πλαίσιο αυτό, τα Big Data Analytics εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ, όταν αντικείμενο της επεξεργασίας είναι δεδομένα προσωπικού χαρακτήρα (και όχι για παράδειγμα δεδομένα σχετικά με τον καιρό, ή την αγροτική παραγωγή) (Voigt & Von dem Bussche, 2017).

Ιδιαίτερα σημαντική διάταξη για τη ρύθμιση των Big Data Analytics είναι το άρθρο 22 του Κανονισμού σχετικά με την αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ, ακριβώς επειδή σκοπός των Big Data Analytics, της τεχνητής νοημοσύνης και της μηχανικής μάθησης είναι η διευκόλυνση της δημιουργίας προφίλ και της λήψης αυτοματοποιημένων αποφάσεων, οι οποίες ενδέχεται να επηρεάσουν σημαντικά τα δικαιώματα και τις ελευθερίες των εμπλεκόμενων ατόμων (Art. 29 WP, 2017α). Σε περίπτωση που δεν πληρείται κάποια από τις προϋποθέσεις του άρθρου αυτού, οπότε και αποκλείεται η εφαρμογή του, η νόμιμη επεξεργασία των δεδομένων διέπεται από τις γενικές διατάξεις του ΓΚΠΔ (άρθρα 6 επ.) (Art. 29 WP, 2017α). Σε κάθε περίπτωση, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, για να είναι σύννομη, πρέπει να είναι σύμφωνη και να συμπλέει με τις θεμελιώδεις αρχές της προστασίας των προσωπικών δεδομένων, όπως αυτές διατυπώνονται στο άρθρο 5 του Κανονισμού.

Κατόπιν των ανωτέρω, θα ακολουθήσει στα επόμενα κεφάλαια μια ανάλυση των βασικότερων διατάξεων και καινοτομιών του ΓΚΠΔ σε σχέση με τα Big Data Analytics, προκειμένου να διαπιστωθεί αν και σε ποιο βαθμό οι διατάξεις αυτές μπορούν να επιτύχουν τη σκοπούμενη ισορροπία ανάμεσα στα μαζικά δεδομένα αφενός και στην προστασία των προσωπικών δεδομένων αφετέρου. Ειδικότερα, στα κεφάλαια που ακολουθούν θα γίνει μια ανάλυση των σημαντικότερων αρχών που διέπουν την επεξεργασία των προσωπικών δεδομένων και επηρεάζουν τη λειτουργία των Big Data Analytics, του άρθρου 22 του Κανονισμού, καθώς και ορισμένων νέων διατάξεων που εισήχθησαν με τον Κανονισμό και αποσκοπούν ακριβώς στην αντιμετώπιση των σύγχρονων τεχνολογικών προκλήσεων, είτε χορηγώντας σχετικά δικαιώματα στα υποκείμενα των δεδομένων (δικαίωμα στη λήθη και δικαίωμα στη φορητότητα των δεδομένων) είτε γεννώντας υποχρεώσεις για τους υπεύθυνους επεξεργασίας (αρχή της

προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού και εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων).

5. 3. Η σχέση των Big Data Analytics με τις αρχές της επεξεργασίας των δεδομένων

Στην παράγραφο 1 του άρθρου 5 του ΓΚΠΔ περιλαμβάνονται οι έξι αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι οποίες αποτελούν τον πυρήνα τόσο του ΓΚΠΔ όσο και της προϊσχύουσας Οδηγίας. Οι αρχές αυτές, πάνω στις οποίες στηρίζεται όλο το οικοδόμημα της προστασίας των δεδομένων προσωπικού χαρακτήρα, είναι "απόγονος" των Κατευθυντήριων Γραμμών του ΟΟΣΑ για την προστασία του απορρήτου και των διασυνοριακών ροών προσωπικών δεδομένων. Με την υιοθέτηση και τη διατήρηση των θεμελιωδών αρχών για την προστασία των προσωπικών δεδομένων και υπό το νέο καθεστώς του Κανονισμού, η Ευρωπαϊκή Ένωση αποσκοπούσε στην ανάπτυξη και την ενίσχυση των νέων τεχνολογικών εξελίξεων, όπως είναι τα Big Data Analytics, μέσω της δημιουργίας και της διατήρησης ενός περιβάλλοντος εμπιστοσύνης, στο οποίο θα μπορούσαν να αναπτυχθούν οι επιχειρήσεις και μιας ανταγωνιστικής αγοράς (Art. 29 WP, 2014· Reding, 2012· Rouvroy, 2016).

Εντούτοις, ορισμένες από τις αρχές αυτές είναι ασύμβατες με τα Big Data Analytics (τουλάχιστον σύμφωνα με τον Zarsky, 2016), καθώς έρχονται σε σύγκρουση με τα βασικά χαρακτηριστικά τους, εμποδίζοντας, ουσιαστικά, την ανάπτυξη και την εκμετάλλευση στον μέγιστο βαθμό των δυνατοτήτων των Big Data Analytics και καθιστώντας ιδιαίτερα δύσκολη τη συμμόρφωση των υπεύθυνων επεξεργασίας με τις υποχρεώσεις τους που πηγάζουν από αυτές, ενώ παράλληλα δεν επιτυγχάνεται η εξασφάλιση της προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων. Όπως αναφέρουν και οι Hoofnagle et al. (2019), ο συνδυασμός των αρχών αυτών δημιουργεί εμπόδια στα μοντέλα των επιχειρήσεων που στηρίζονται στα Big Data Analytics. Πρόκειται, συγκεκριμένα, για την αρχή του περιορισμού του σκοπού (άρθρο 5 παρ. 1 περ. β του ΓΚΠΔ), την αρχή της ελαχιστοποίησης των δεδομένων (άρθρο 5 παρ. 1 περ. γ του ΓΚΠΔ), την αρχή της ακρίβειας των δεδομένων (άρθρο 5 παρ. 1 περ. δ του ΓΚΠΔ), καθώς και την αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας (άρθρο 5 παρ. 1 περ. α του ΓΚΠΔ).

5. 3. 1. Η αρχή του περιορισμού του σκοπού

Η αρχή του περιορισμού του σκοπού έχει χαρακτηριστεί ως ο ακρογωνιαίος λίθος της νομοθεσίας για την προστασία των προσωπικών δεδομένων, καθώς προβλέπεται τόσο από το πρωτογενές δίκαιο της Ε.Ε. όσο και από διεθνή κείμενα. Ειδικότερα, η συγκεκριμένη αρχή διαμορφώθηκε αρχικά από τη νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου σχετικά με την ερμηνεία της παραγράφου 2 του άρθρου 8 της ΕΣΔΑ -στην οποία, μεταξύ άλλων, προβλέπεται, ότι δεν επιτρέπεται να υπάρξει επέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος σεβασμού της ιδιωτικής και της οικογενειακής ζωής- ενώ προβλέφθηκε στη συνέχεια και ρητά στον ΧΘΔ της Ε.Ε. (άρθρο 8 παρ. 2, το οποίο προβλέπει, ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται για καθορισμένους σκοπούς). Επιπλέον, η αρχή του περιορισμού του σκοπού προβλέπεται τόσο στις Κατευθυντήριες γραμμές του ΟΟΣΑ για την προστασία του απορρήτου και των διασυνοριακών ροών προσωπικών δεδομένων, όσο και στο άρθρο 5 της Σύμβασης 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων.

Στο πλαίσιο αυτό, το άρθρο 5 παρ. 1 περ. β του ΓΚΠΔ, που διαδέχθηκε το προϊσχύον άρθρο 6 παρ. 1 περ. β της Οδηγίας προβλέπει, ότι τα δεδομένα προσωπικού χαρακτήρα «συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς». Η έννοια του περιορισμού του σκοπού έχει επομένως δύο κύρια δομικά στοιχεία: τον προσδιορισμό του σκοπού και τη συμβατή περαιτέρω χρήση (Art. 29 WP, 2013). Τα προσωπικά δεδομένα πρέπει δηλαδή να συλλέγονται μόνο για σκοπούς, οι οποίοι είναι εκ των προτέρων (πριν τη συλλογή ή το αργότερο μέχρι και τη στιγμή της συλλογής) επακριβώς καθορισμένοι, σαφείς και ρητοί (δηλαδή διατυπώνονται με τέτοιον τρόπο, ώστε όλοι οι ενδιαφερόμενοι να αντιλαμβάνονται με τον ίδιο τρόπο τους σκοπούς επεξεργασίας, ανεξάρτητα από κάθε πολιτισμική ή γλωσσική διαφοροποίηση) και να μην τυγχάνουν περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (Ιγγλεζάκης, 2018). Σκοπός δηλαδή, της εν λόγω αρχής είναι αφενός να αποτρέψει τη χρήση των δεδομένων κατά τρόπο που δεν ανταποκρίνεται στις προσδοκίες του υποκειμένου, διαμορφώνοντας ένα περιβάλλον εμπιστοσύνης και ασφάλειας δικαίου και αφετέρου να δώσει στους υπευθύνους επεξεργασίας τη δυνατότητα να αξιοποιήσουν τα δεδομένα που έχουν συλλέξει στο μέγιστο, εφόσον αυτά είναι χρήσιμα και για άλλους σκοπούς και εφόσον συντρέχει το κριτήριο της συμβατότητας (Art. 29 WP, 2013).

Στο πλαίσιο αυτό, μεγάλο μέρος της βιβλιογραφίας υποστηρίζει, ότι τα Big Data Analytics φαίνεται να βρίσκονται εξ' ορισμού σε αντίθεση και με τις δύο πτυχές της εν λόγω αρχής. Σε ότι έχει να κάνει ειδικότερα με τον προσδιορισμό του σκοπού, ο Zarsky (2016) αναφέρει, ότι τέτοιου είδους αναλύσεις δεδομένων περιλαμβάνουν συχνά μεθόδους και οδηγούν σε μοτίβα, τα οποία ούτε το υποκείμενο των δεδομένων αλλά ούτε και η ίδια η επιχείρηση που συνέλεξε τα δεδομένα μπορούσαν να σκεφτούν ή να φανταστούν τη στιγμή της συλλογής των δεδομένων. Ο σκοπός δηλαδή της επεξεργασίας προσδιορίζεται από το εκάστοτε αποτέλεσμα της ανάλυσης των δεδομένων και όχι το αντίστροφο (Voigt & Von dem Bussche, 2017). Καθίσταται, δηλαδή, ιδιαίτερα δύσκολο για τους υπεύθυνους επεξεργασίας που χρησιμοποιούν μεθόδους τέτοιου είδους να καθορίσουν τη στιγμή της συλλογής των δεδομένων με ακρίβεια τον σκοπό/τους σκοπούς της επεξεργασίας τους, καθώς δεν είναι σε θέση να γνωρίζουν το αποτέλεσμα της ανάλυσής τους (ιδίως στις περιπτώσεις της μη επιβλεπόμενης μηχανικής μάθησης). Το γεγονός αυτό οφείλεται ακριβώς στην επαγωγική δύναμη των σύγχρονων αυτών τεχνολογιών, στη δυνατότητα δηλαδή εύρεσης απρόσμενων συσχετισμών και μοτίβων μεταξύ των δεδομένων, η οποία προϋποθέτει ότι θα προκύψουν και νέοι σκοποί για τα δεδομένα αυτά (Bennett & Bayley, 2016). Το μεγαλύτερο μέρος της καινοτομίας και κατ' επέκταση της οικονομικής και κοινωνικής αξίας των Big Data Analytics βρίσκεται στις δευτερεύουσες χρήσεις των δεδομένων (Kalapesi, 2013), οι οποίες είναι ενδεχομένως αδιανόητες τη στιγμή της συλλογής τους.

Επιπλέον, τόσο οι Mayer-Schonberger και Padova (2016), όσο και ο Zarsky (2016) υποστηρίζουν, ότι ο ορισμός ενός γενικότερου και πιο αόριστου σκοπού που θα μπορούσε να καλύψει διάφορες μελλοντικές χρήσεις των δεδομένων, διευκολύνοντας με τον τρόπο αυτό τους υπεύθυνους επεξεργασίας, δεν θα ήταν συμβατός με τον ΓΚΠΔ. Βέβαια, η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2013) αναφέρει, ότι παρ' όλο που ασαφείς και γενικοί σκοποί (π.χ. μάρκετινγκ ή η βελτίωση της εμπειρίας του χρήστη) κατά κανόνα δεν συμβαδίζουν με την αρχή του περιορισμού του σκοπού, εντούτοις σε κάθε περίπτωση το πόσο συγκεκριμένος πρέπει να είναι ο σκοπός εξαρτάται από τις εκάστοτε συνθήκες και καταστάσεις (π.χ. διαφορετικά θα αντιμετωπιστεί ένα τοπικό μαγαζί, διαφορετικά μια επιχείρηση που προσφέρει τις υπηρεσίες της σε όλη την Ευρώπη και διαφορετικά μια κρατική ιστοσελίδα). Το πόσο δηλαδή λεπτομερής πρέπει να είναι η περιγραφή του σκοπού κρίνεται κατά περίπτωση, με βάση τις συγκεκριμένες συνθήκες της επεξεργασίας (Voigt & Von dem Bussche, 2017). Σε κάθε περίπτωση, πάντως, η συμμόρφωση των υπευθύνων επεξεργασίας με

την αρχή του περιορισμού του σκοπού και συγκεκριμένα με τον προσδιορισμό του σκοπού θα είναι ιδιαίτερα δύσκολη στην πράξη, χωρίς να περιοριστούν σε μεγάλο βαθμό οι δυνατότητες και οι προοπτικές που προσφέρουν τα Big Data Analytics.

Επιπροσθέτως, όσον αφορά τη συμβατή περαιτέρω χρήση, σύμφωνα με το άρθρο 5 παρ. 1 περ. β' σε συνδυασμό με το άρθρο 6 παρ. 4 του ΓΚΠΔ, η επεξεργασία των δεδομένων για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί επιτρέπεται μόνο στις εξής περιπτώσεις: όταν έχει δοθεί η συγκατάθεση του υποκειμένου για τη νέα επεξεργασία, όταν το προβλέπει ρητά διάταξη του εθνικού ή του ενωσιακού δικαίου ή όταν η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα. Ιδιαίτερα σε ότι αφορά την τρίτη περίπτωση, για να εξακριβωθεί η συμβατότητα μεταξύ του αρχικού και του μεταγενέστερου σκοπού πρέπει –σύμφωνα και με το άρθρο 6 παρ. 4 του ΓΚΠΔ- να πραγματοποιείται κάθε φορά ένας έλεγχος συμβατότητας, στα πλαίσια του οποίου θα πρέπει, μεταξύ άλλων, να λαμβάνεται υπόψη: «α) τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας, β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας, γ) η φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10, δ) οι πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων, ε) η ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση».

Στο πλαίσιο αυτό, ανακύπτουν διάφορα ζητήματα σχετικά με το ανωτέρω κριτήριο της συμβατότητας και τη χρήση των Big Data Analytics, καθώς τα τελευταία στηρίζονται στην ιδέα της χρησιμοποίησης των δεδομένων για διαφορετικούς σκοπούς από αυτόν για τον οποίο συλλέχθηκαν αρχικά, ακριβώς λόγω της ικανότητάς τους να βρίσκουν νέους, άγνωστους συσχετισμούς και μοτίβα στα δεδομένα που αναλύουν. Η σημασία, επομένως των Big Data Analytics, βρίσκεται στην κρυφή αξία των δεδομένων, τα οποία μπορούν σήμερα να αναλυθούν σε διαφορετικά πλαίσια και με διαφορετικούς τρόπους (Zarsky, 2016), με αποτέλεσμα να καθίσταται ιδιαίτερα δύσκολο για τους υπεύθυνους επεξεργασίας να εξασφαλίσουν τη συνδρομή όλων των ανωτέρω κριτηρίων και κατ' επέκταση τη συμβατότητα των σκοπών που προκύπτουν

από την ανάλυση των δεδομένων με τον αρχικό σκοπό για τον οποίο αυτά είχαν συλλεγεί.

Ιδιαίτερα, όσον αφορά τη συμβατότητα των σκοπών στην περίπτωση των Big Data Analytics, η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2013) κάνει λόγο για δύο σενάρια. *Στο πρώτο σενάριο*, όπου οι φορείς που επεξεργάζονται τα δεδομένα θέλουν να εντοπίσουν τάσεις και συσχετίσεις στα δεδομένα, η διασφάλιση του λειτουργικού διαχωρισμού είναι πολύ σημαντική για τη συμβατότητα των δύο σκοπών[2]. *Στο δεύτερο σενάριο*, όπου οι φορείς που επεξεργάζονται τα δεδομένα θέλουν συγκεκριμένα να αναλύσουν ή να προβλέψουν τις προσωπικές προτιμήσεις, τη συμπεριφορά και τη στάση των υποκειμένων και στη συνέχεια να ενημερώσουν «μέτρα ή αποφάσεις» που λαμβάνονται σχετικά με αυτά (π.χ. δημιουργία προφίλ για σκοπούς άμεσου μάρκετινγκ), για τη συμβατότητα των σκοπών είναι σχεδόν πάντα απαραίτητη η δωρεάν, συγκεκριμένη, ενημερωμένη και σαφής συγκατάθεση αυτών (*opt-in*). Εντούτοις, η λήψη της σύννομης συγκατάθεσης του υποκειμένου στη δεύτερη αυτή περίπτωση εμφανίζεται ιδιαίτερα δυσχερής, εξαιτίας ακριβώς της αδυναμίας των υπεύθυνων επεξεργασίας να προβλέψουν τα αποτελέσματα της επεξεργασίας και κατ' επέκταση να καθορίσουν εκ των προτέρων τους σκοπούς αυτής.

Επιπροσθέτως, ζήτημα δημιουργείται και σχετικά με την εφαρμογή της αρχής του περιορισμού του σκοπού στην πράξη. Συγκεκριμένα, η Rauhofer (2015) κατέληξε στο συμπέρασμα πως μέχρι σήμερα, δεν έχουν γίνει αποφασιστικά βήματα προς την επιβολή της εν λόγω αρχής, παρά και την έκδοση της Γνώμης 03/2013 της ομάδας εργασίας του άρθρου 29 σχετικά με αυτή. Χαρακτηριστικό παράδειγμα αυτής της διστακτικότητας εφαρμογής της αρχής αποτελεί η αλλαγή της πολιτικής απορρήτου της Google το 2012 (υπό το προϊσχύον καθεστώς της Οδηγίας). Η Google προχώρησε στη δημιουργία μιας ενιαίας πολιτικής απορρήτου για όλες της υπηρεσίες της (π.χ. Google Chrome, Google Search Engine), καθορίζοντας γενικότερους σκοπούς για τη συλλογή των δεδομένων που της επέτρεπαν να συνδυάζει τα δεδομένα που προέρχονταν από τις διάφορες υπηρεσίες της. Η ομάδα εργασίας του άρθρου 29 ανέθεσε στη Γαλλική αρχή για την προστασία των δεδομένων (την Commission nationale de l'informatique et des libertés – CNIL) τη διεξαγωγή έρευνας για τη συμβατότητα της πολιτικής απορρήτου της Google με τις διατάξεις για την προστασία των δεδομένων. Η CNIL έκρινε, μεταξύ άλλων, ότι οι σκοποί για τους οποίους η Google μπορεί να συνδυάζει τα δεδομένα των χρηστών της από όλες τις υπηρεσίες της δεν συμβαδίζουν με τους καθορισμένους και

[2]Ο λειτουργικός διαχωρισμός σημαίνει, ότι τα δεδομένα που χρησιμοποιούνται για στατιστικούς σκοπούς ή άλλους ερευνητικούς σκοπούς δεν θα πρέπει να είναι διαθέσιμα για να «υποστηρίξουν μέτρα ή αποφάσεις» που λαμβάνονται σε σχέση με τα υποκείμενα των δεδομένων (Art. 29 WP, 2013).

τους ρητούς σκοπούς που απαιτούσε η τότε ισχύουσα Οδηγία (άρθρο 6 παρ. 1 περ. β αυτής), ωστόσο δεν προχώρησε σε περαιτέρω έρευνα αλλά επικεντρώθηκε περισσότερο στις προϋποθέσεις ενημέρωσης των υποκειμένων σύμφωνα με τα άρθρα 10 και 11 της Οδηγίας (Rauhofer, 2015).

Επομένως, γίνεται κατανοητό ότι η αρχή του περιορισμού του σκοπού δεν συμβαδίζει με τα Big Data Analytics. Οι εγγυήσεις που προσφέρει η εν λόγω αρχή είναι πολύπλοκες, δύσκολο να εκτελεστούν, ενώ ενδέχεται να υπονομεύσουν τη χρηστικότητα της όλης διαδικασίας (Zarsky, 2016). Για να εξασφαλίσει τη συμμόρφωσή του με αυτήν, ο υπεύθυνος επεξεργασίας θα πρέπει να αναγνωρίσει όλους τους σκοπούς για την επίτευξη των οποίων απαιτείται η συλλογή των δεδομένων, καθώς και να αξιολογήσει εάν ο σκοπός της τυχόν περαιτέρω επεξεργασίας των δεδομένων είναι συμβατός με τον σκοπό της αρχικής συλλογής τους και σε περίπτωση μη συμβατής περαιτέρω επεξεργασίας, ο υπεύθυνος θα πρέπει αφενός να ενημερώσει σχετικά το υποκείμενο και αφετέρου να καταστήσει την εν λόγω επεξεργασία σύννομη, προσδιορίζοντας μια από τις διαθέσιμες νομικές βάσεις που προβλέπει ο ΓΚΠΔ (Πλατής, 2018). Το βάρος των υπεύθυνων επεξεργασίας προκειμένου να τηρήσουν τα οριζόμενα από την αρχή του περιορισμού του σκοπού είναι ιδιαίτερα μεγάλο, ενώ δεν λείπουν, όπως αναφέρθηκε ανωτέρω και ζητήματα σχετικά με την εφαρμογή και την επιβολή της στην πράξη.

5. 3. 2. Η αρχή της ελαχιστοποίησης των δεδομένων

Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, η οποία αποτελεί έκφανση της αρχής της αναλογικότητας (Ιγγλεζάκης, 2018), τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (άρθρο 5 παρ. 1 περ. γ του ΓΚΠΔ). Στην αιτιολογική σκέψη 39 αναφέρεται επιπροσθέτως, ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να υποβάλλονται σε επεξεργασία μόνο εάν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα. Θα πρέπει δηλαδή να συλλέγονται μόνο εκείνα τα δεδομένα που είναι κάθε φορά απαραίτητα για την επίτευξη του εκάστοτε επιδιωκόμενου σκοπού (Hoofnagle et al., 2019). Σκοπός της εν λόγω αρχής είναι ακριβώς η μείωση της συλλογής δεδομένων στον χαμηλότερο δυνατό βαθμό για την επίτευξη του σκοπού της επεξεργασίας (Voigt & Von dem Bussche, 2017).

Επιπλέον, εκτός από το στάδιο της συλλογής των προσωπικών δεδομένων, περιορισμοί τίθενται και στο στάδιο της αποθήκευσης και της διατήρησης αυτών.

Ειδικότερα, η αρχή του περιορισμού της περιόδου αποθήκευσης προβλέπεται στο άρθρο 5 παρ. 1 περ. ε του ΓΚΠΔ και ορίζει, ότι 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. Στο πλαίσιο αυτό και προκειμένου να διασφαλιστεί, ότι τα δεδομένα προσωπικού χαρακτήρα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο, ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτασή τους (Αιτιολογική Σκέψη 39 του Κανονισμού). Με βάση, δηλαδή, τις ανωτέρω αρχές, οι υπεύθυνοι επεξεργασίας υποχρεούνται να διασφαλίζουν, ότι τα δεδομένα που συλλέγουν και επεξεργάζονται είναι τα κατάλληλα κατ' είδος και έκταση για την επίτευξη του εκάστοτε σκοπού της επεξεργασίας και ότι κανένα άλλο διαθέσιμο μέσο δεν θα μπορούσε να επιτελέσει τον ίδιο σκοπό με λιγότερο αρνητικές συνέπειες για τα υποκείμενα (Πλατής, 2018), καθώς και να διαγράφουν τα δεδομένα που δεν χρησιμοποιούνται πλέον για τους σκοπούς για τους οποίους είχαν συλλεχθεί και να εφαρμόσουν περιοριστικές πολιτικές σε σχέση με τη διατήρηση των προσωπικών δεδομένων υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων (Tene & Polonetsky, 2012).

Εντούτοις, στο πλαίσιο των Big Data Analytics, η δυνατότητα αποθήκευσης τεράστιων ποσοτήτων δεδομένων με χαμηλό κόστος αφενός και η δυνατότητα επεξεργασίας αυτών αφετέρου, έχουν δημιουργήσει τέτοια κίνητρα στους φορείς που χρησιμοποιούν τέτοιου είδους μεθόδους, ώστε να συλλέγουν όσο το δυνατόν περισσότερα δεδομένα (και σε πολλές περιπτώσεις, όλα τα σημεία δεδομένων σε ένα συγκεκριμένο σύνολο, αντί για ένα δείγμα) για όσο το δυνατό μεγαλύτερα διαστήματα (ICO, 2017· Zarsky, 2016), επειδή ακριβώς η αξία των δεδομένων βρίσκεται πλέον στις πιθανές μελλοντικές χρήσεις τους (Datatilsynet, 2013), στις απρόσμενες δηλαδή δευτερεύουσες χρήσεις τους (Tene & Polonetsky, 2012). Με άλλα λόγια, η χρησιμότητα των δεδομένων σήμερα εξαρτάται από την ποσότητα των άλλων δεδομένων που έχουν συλλεχθεί και με τα οποία θα μπορούσαν να συγκεντρωθούν και να αποτελέσουν ένα σύνολο (Rouvroy, 2016). Φαίνεται, συνεπώς, ότι το επιχειρηματικό μοντέλο που στηρίζεται στα Big Data Analytics είναι αντίθετο, τόσο με την αρχή της ελαχιστοποίησης των δεδομένων, όσο και με την αρχή του περιορισμού της περιόδου αποθήκευσης (Bennett & Bayley, 2016· Datatilsynet, 2013· Tene & Polonetsky, 2012). Άλλωστε και στην πράξη διαπιστώνεται, ότι η εν λόγω αρχή δεν εφαρμόζεται όπως θα έπρεπε. Είναι χαρακτηριστικό, ότι το 90% περίπου των

ιστοτόπων δημιουργούν αναγνωριστικά cookies που διαρκούν πάνω από ένα έτος (Sanchez-Rola, et al., 2019).

Επιπροσθέτως, όσον αφορά την εφαρμογή της αρχής της ελαχιστοποίησης των δεδομένων στα Big Data Analytics, ζήτημα δημιουργείται όχι μόνο με την ποσότητα, αλλά και με την ποικιλία των δεδομένων που συλλέγονται. Πιο συγκεκριμένα, η αρχή της ελαχιστοποίησης των δεδομένων ορίζει μεταξύ άλλων, ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή με τον σκοπό της επεξεργασίας. Ωστόσο, τα Big Data Analytics στηρίζονται στην ανακάλυψη νέων, απρόσμενων συσχετισμών μεταξύ των δεδομένων, με αποτέλεσμα να χρησιμοποιούνται πολλές φορές, για την επίτευξη του εκάστοτε σκοπού και δεδομένα, τα οποία θα χαρακτηρίζονταν ως μη συναφή με αυτόν. Η συσχέτιση των δεδομένων που θα προκύψει τελικά από την ανάλυση αυτών, σε καμία περίπτωση δεν μπορεί να αιτιολογήσει αναδρομικά τη λήψη των δεδομένων, καθιστώντας τα αυτά συναφή με τον επιδιωκόμενο σκοπό (ICO, 2017). Χαρακτηριστικό παράδειγμα αποτελεί η χρήση δεδομένων σχετικά με τον τρόπο ζωής των ανθρώπων (π.χ. οι καταναλωτικές τους συνήθειες) για τον προσδιορισμό της πιστοληπτικής τους ικανότητας (ICO, 2017).

Γίνεται, επομένως, κατανοητό, ότι η αρχή της ελαχιστοποίησης των δεδομένων, σε συνδυασμό με την αρχή του περιορισμού της περιόδου αποθήκευσης φαίνεται ότι δεν συμβαδίζουν με τις σύγχρονες τεχνολογικές εξελίξεις και συγκεκριμένα με το περιβάλλον που έχουν δημιουργήσει σήμερα τα Big Data Analytics, καθώς υπονομεύουν την επιτυχία των πιθανών πρωτοβουλιών που στηρίζονται σε τέτοιου είδους τεχνολογίες (Zarsky, 2016). Οι φορείς που χρησιμοποιούν αυτές τις μεθόδους επωμίζονται το πολύ δύσκολο έργο, να καθορίσουν εκ των προτέρων τόσο τους σκοπούς της επεξεργασίας, όσο και τα δεδομένα τα οποία θα είναι αναγκαία και συναφή για την επίτευξη των σκοπών αυτών (ICO, 2017). Στο πλαίσιο αυτό, ο Rubinstein (2012) αναφέρει, ότι οι προϋποθέσεις τήρησης της αρχής της ελαχιστοποίησης των δεδομένων μπορούν να παραλύσουν τα Big Data Analytics και τα σχετικά με αυτά οικονομικά και κοινωνικά οφέλη, με αποτέλεσμα να είναι πολύ πιθανό να εμφανιστούν συχνά παραβιάσεις της εν λόγω αρχής. Πράγματι, όπως διαπιστώνεται στο άρθρο του Γραφείου του Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου (ICO, 2017), σε μία έρευνα που πραγματοποιήθηκε σε επιχειρήσεις του Ηνωμένου Βασιλείου, της Γαλλίας και της Γερμανίας, το 72% αυτών ανέφερε, ότι είχε συλλέξει δεδομένα τα οποία τελικά δεν είχε χρησιμοποιήσει, φανερώνοντας τη δυσκολία τήρησης της εν λόγω αρχής στην πράξη. Όπως αναφέρουν χαρακτηριστικά οι Tene & Polonetsky (2012), η ελαχιστοποίηση των δεδομένων απλά δεν αποτελεί πλέον τον κανόνα της αγοράς.

5. 3. 3. Η αρχή της ακρίβειας των δεδομένων

Η αρχή της ακρίβειας των δεδομένων προβλέπεται στη διάταξη του άρθρου 5 παρ. 1 περ. δ του ΓΚΠΔ και ορίζει τα εξής: «τα δεδομένα προσωπικού χαρακτήρα 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». Οι υπεύθυνοι επεξεργασίας πρέπει, δηλαδή, να διασφαλίζουν την απαραίτητη ακρίβεια των προσωπικών δεδομένων, λαμβάνοντας σε κάθε περίπτωση υπόψη και τους σκοπούς της επεξεργασίας (Hoofnagle et al., 2019), ενώ σε περίπτωση που διαπιστωθεί, ότι αυτά είναι ανακριβή, θα πρέπει να εφαρμόσουν τα κατάλληλα μέτρα είτε για τη διόρθωση είτε για τη διαγραφή τους (Πλατής, 2018). Η υποχρέωση διαγραφής ή διόρθωσης συνιστά καθήκον του υπεύθυνου επεξεργασίας, χωρίς να απαιτείται η υποβολή σχετικού αιτήματος του υποκειμένου των δεδομένων (Ιγγλεζάκης, 2018). Σε κάθε περίπτωση, στην παρούσα αρχή ενσωματώνεται και η υποχρέωση του υπευθύνου επεξεργασίας να ικανοποιήσει είτε το δικαίωμα διόρθωσης (άρθρο 16 του ΓΚΠΔ) είτε το δικαίωμα διαγραφής (άρθρο 17 του ΓΚΠΔ), εφόσον αυτά ασκηθούν από το υποκείμενο των δεδομένων (Πλατής, 2018).

Ωστόσο, στην περίπτωση των Big Data Analytics, επειδή ακριβώς οι ποσότητες των δεδομένων που υπόκεινται σε επεξεργασία και ανάλυση είναι τόσο μεγάλες, είναι ανεκτή μια ορισμένη ποσότητα "ακατάστατων" (δηλαδή ανακριβών) δεδομένων (Mayer-Schönberger & Cukier, 2013). Στο παρελθόν, όταν ο αριθμός των διαθέσιμων δεδομένων ήταν περιορισμένος, καθίστατο αναγκαίο να μειωθούν τα σφάλματα και να εξασφαλιστεί όσο το δυνατόν μεγαλύτερη ακρίβεια και υψηλή ποιότητα των δεδομένων (Mayer-Schönberger & Cukier, 2013). Στη σημερινή εποχή, οι Mayer-Schönberger & Cukier (2013) θεωρούν αυτήν την "ακαταστασία" που διέπει εν μέρει τα Big Data Analytics ως ένα θετικό χαρακτηριστικό, ως ένα αντάλλαγμα της δυνατότητας για απόκτηση πολύ μεγαλύτερων ποσοτήτων δεδομένων και προτείνουν την αποδοχή της.

Πράγματι, ένα ορισμένο επίπεδο "ακαταστασίας" / ανακρίβειας των δεδομένων (για παράδειγμα ένα λανθασμένο όνομα ή μια λανθασμένη διεύθυνση) δεν θα αποτελέσει πρόβλημα, όταν σκοπός της ανάλυσης είναι η ανίχνευση γενικών τάσεων (ICO, 2017). Εντούτοις, αυτή η "ακαταστασία" που διέπει τα Big Data Analytics ενδέχεται να είναι προβληματική, όταν σκοπός της επεξεργασίας είναι η κατάρτιση προφίλ του υποκειμένου των δεδομένων (ICO, 2017). Ειδικότερα, εάν τα δεδομένα που χρησιμοποιούνται σε μια αυτοματοποιημένη λήψη αποφάσεως ή στην κατάρτιση ενός

προφίλ είναι ανακριβή, οποιαδήποτε απόφαση ή προφίλ που θα προκύψει από την ανάλυση αυτών (που σε πολλές περιπτώσεις αφορά σημαντικά ζητήματα, όπως είναι η υγεία, η πιστοληπτική ικανότητα ή οι ασφαλιστικοί κίνδυνοι του υποκειμένου των δεδομένων) θα είναι και αυτή ελαττωματική (Art. 29 WP, 2017α).

Ωστόσο, ακόμα και αν τα δεδομένα που χρησιμοποιήθηκαν στην επεξεργασία ήταν ακριβή και επικαιροποιημένα, αυτό δεν συνεπάγεται απαραίτητα, ότι τα συμπεράσματα που θα αντληθούν από αυτά, θα είναι και αυτά ακριβή. Ακόμα, δηλαδή και αν τα δεδομένα εισόδου είναι ακριβή, μπορεί να υπάρχουν ζητήματα ως προς την αντιπροσωπευτικότητα των δεδομένων ή να εμφανίζονται λανθάνουσες προκαταλήψεις και μεροληψίες στα διάφορα στάδια της ανάλυσης (βλ. ανωτέρω κεφάλαιο 4.3), με αποτέλεσμα να μην εξαλείφεται εντελώς ο κίνδυνος λανθασμένων και επαχθών προβλέψεων και αποφάσεων σε σχέση με το υποκείμενο των δεδομένων (ICO, 2017· Art. 29 WP, 2017α).

Σε σχέση με τους παραπάνω κινδύνους που σχετίζονται με την ακρίβεια των δεδομένων στην περίπτωση της κατάρτισης προφίλ, στην αιτιολογική σκέψη 71 του ΓΚΠΔ αναφέρονται τα εξής: *«Προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία σε σχέση με το υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος*».

Αντίστοιχα και η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2017α) αναφέρει, ότι οι υπεύθυνοι επεξεργασίας πρέπει να λαμβάνουν υπόψη την ακρίβεια των δεδομένων σε όλα τα στάδια της διαδικασίας για την κατάρτιση ενός προφίλ και ιδιαίτερα κατά τη συλλογή, την ανάλυση, τη δημιουργία του προφίλ ενός ατόμου και την εφαρμογή του προφίλ για τη λήψη μιας απόφασης που το επηρεάζει. Επιπλέον,

καλεί τους υπεύθυνους επεξεργασίας να λάβουν αυστηρά μέτρα για τη διαρκή επαλήθευση και διασφάλιση της ακρίβειας των δεδομένων που επαναχρησιμοποιούνται ή αποκτώνται έμμεσα, ενώ τονίζει και τη μεγάλη σημασία που έχει η παροχή σαφών πληροφοριών σχετικά με τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία, έτσι ώστε το υποκείμενο των δεδομένων να μπορεί να διορθώσει τυχόν ανακρίβειες και να βελτιωθεί η ποιότητα των δεδομένων (Art. 29 WP, 2017α).

Συνεπώς, φαίνεται, ότι στην πράξη, τα Big Data Analytics δεν συμβαδίζουν με την αρχή της ακρίβειας των δεδομένων προσωπικού χαρακτήρα, καθώς περιλαμβάνουν την ανάλυση τεράστιων ποσοτήτων δεδομένων, στις οποίες αναπόφευκτα εμπεριέχονται λάθη και ανακρίβειες, οι οποίες όμως ενδέχεται να οδηγήσουν σε λανθασμένες ή/και μεροληπτικές αποφάσεις με σημαντικές επιπτώσεις για τα υποκείμενα των δεδομένων. Γενικότερα άλλωστε, τα δεδομένα -σε αντίθεση με την κρατούσα άποψη, ότι είναι εξ ορισμού αντικειμενικά- χειραγωγούνται εύκολα και ενδέχεται να είναι μονομερή, να επηρεάζονται από προτιμήσεις και προκαταλήψεις πολιτισμικού χαρακτήρα, ως προς το φύλο ή άλλου είδους, ή να είναι ακόμη και εσφαλμένα (Muller, 2017). Πρέπει, δηλαδή, σε κάθε περίπτωση να διασφαλίζεται, ότι τα δεδομένα που υπόκεινται σε επεξεργασία είναι πρωτίστως ορθά, αλλά παράλληλα και ποιοτικά, διαφοροποιημένα, επαρκώς εμπεριστατωμένα και αντικειμενικά (Muller, 2017), όπως επισημαίνεται τόσο στο κείμενο του ΓΚΠΔ όσο και από την ομάδα εργασίας του άρθρου 29. Εντούτοις, φαίνεται ότι στην πράξη δεν δίνεται η δέουσα προσοχή στη διασφάλιση της ποιότητας και της ακρίβειας των δεδομένων που υπόκεινται σε επεξεργασία, δεδομένου και του κόστους της εξασφάλισης μεγαλύτερης ακρίβειας, το οποίο σε πολλές περιπτώσεις υπερβαίνει κατά πολύ τα οφέλη που θα αποκομίσει αυτός που τα επεξεργάζεται (Barocas & Selbst, 2016), ενώ σε κάθε περίπτωση η ακρίβεια των δεδομένων δεν συνεπάγεται αυτομάτως ορθές, εμπεριστατωμένες και ενημερωμένες αποφάσεις και συμπεράσματα σχετικά με τα υποκείμενα των δεδομένων.

5. 3. 4. Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας

Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας προβλέπεται στο άρθρο 5 παρ. 1 περ. α του Κανονισμού, σύμφωνα με το οποίο: «Τα δεδομένα προσωπικού χαρακτήρα: α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων».

Την εποχή των Big Data Analytics δοκιμάζονται, όπως αναλύεται κατωτέρω και τα τρία στοιχεία της εν λόγω αρχής (νομιμότητα, αντικειμενικότητα, διαφάνεια).

Ειδικότερα δε, σε ότι έχει να κάνει με την αρχή της νομιμότητας της επεξεργασίας τα σημαντικότερα προβλήματα εμφανίζονται όταν η επεξεργασία βασίζεται στη συναίνεση του υποκειμένου.

5.3.4.1. Η αρχή της νομιμότητας της επεξεργασίας και ειδικότερα η συγκατάθεση του υποκειμένου

Η αρχή της νομιμότητας εξειδικεύεται στα άρθρα 6 επ. του ΓΚΠΔ και επιτάσσει τη συμμόρφωση των εμπλεκόμενων μερών με το σύνολο του εφαρμοστέου δικαίου, μεταξύ άλλων και με τις επιταγές του ίδιου του Κανονισμού (Πλατής, 2018). Στο πλαίσιο αυτό, η επεξεργασία των δεδομένων είναι σύννομη, μόνο εφόσον συντρέχει μία από τις νομικές βάσεις που προβλέπονται στην παρ. 1 του άρθρου 6 του ΓΚΠΔ και συγκεκριμένα: «α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης, γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί».

Ειδικότερα, ως συγκατάθεση του υποκειμένου των δεδομένων νοείται «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» (άρθρο 4 περ. 11 του ΓΚΠΔ). Ελεύθερη είναι κατ’ αρχάς η συγκατάθεση, όταν είναι προϊόν ελεύθερης επιλογής του υποκειμένου (Voigt & Von dem Bussche, 2017· Πλατής, 2018). Δεν θα πρέπει δηλαδή το υποκείμενο να νιώθει, ότι εξαναγκάζεται να συγκαταθέσει ή ότι θα υποστεί αρνητικές συνέπειες αν δεν

συγκαταθέσει (Ιγγλεζάκης, 2018). Έτσι, το υποκείμενο θα πρέπει ανά πάσα στιγμή να έχει τη δυνατότητα να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς δυσμενείς συνέπειες (Feiler, Forgó & Weigl, 2018· Ιγγλεζάκης, 2018· Πλατής, 2018). Επιπλέον, για να θεωρηθεί, ότι η συγκατάθεση είναι ελεύθερη, θα πρέπει να δίνεται αφενός για όλους τους σκοπούς της επεξεργασίας (όταν υπάρχουν περισσότεροι από ένας σκοποί) - θα πρέπει δηλαδή τα υποκείμενα των δεδομένων να μπορούν να επιλέγουν ελεύθερα τον σκοπό της επεξεργασίας που αποδέχονται και όχι να συγκατατίθενται γενικά σε ένα σύνολο σκοπών (Ιγγλεζάκης, 2018)- και αφετέρου χωριστά για όλες τις διαφορετικές πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα που ενδέχεται να πραγματοποιούνται (Αιτιολογική Σκέψη 32 και 43 του ΓΚΠΔ).

Ακόμη, κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης (άρθρο 7 παρ. 4 του ΓΚΠΔ και Αιτιολογική Σκέψη 43). Σκοπός της εν λόγω διάταξης είναι να διασφαλιστεί, ότι η επεξεργασία των προσωπικών δεδομένων για τα οποία παρέχεται η συγκατάθεση δεν θα λειτουργήσει ως αντιπαροχή του συμβολαίου ή της παρεχόμενης υπηρεσίας και κατ' επέκταση, ότι δεν θα αποκλείονται από τις εκάστοτε παρεχόμενες υπηρεσίες τα υποκείμενα που δεν επιθυμούν να συναινέσουν στην επεξεργασία των δεδομένων τους (European Data Protection Board [EDPB], 2020). Έτσι, με τη διάταξη αυτή επηρεάζεται σε μεγάλο βαθμό η παροχή online υπηρεσιών με αντάλλαγμα την πρόσβαση στα προσωπικά δεδομένα του χρήστη (Feiler, Forgó & Weigl, 2018· Voigt & Von dem Bussche, 2017). Για παράδειγμα, στην περίπτωση μιας εφαρμογής επεξεργασίας φωτογραφιών, η οποία ζητάει από τους χρήστες της, για να κάνουν χρήση της εφαρμογής, να ενεργοποιήσουν τον εντοπισμό της θέσης τους μέσω GPS, ενημερώνοντας τους παράλληλα, ότι θα χρησιμοποιήσουν τα εν λόγω δεδομένα για σκοπούς συμπεριφορικής διαφήμισης, η συγκατάθεση του υποκειμένου δεν μπορεί να θεωρηθεί, ότι είναι ελεύθερη, καθώς οι χρήστες δεν μπορούν να χρησιμοποιήσουν την εφαρμογή χωρίς να συναινέσουν στην ανωτέρω επεξεργασία των δεδομένων τους, ενώ ούτε τα δεδομένα τοποθεσίας αλλά ούτε και η συμπεριφορική διαφήμιση είναι απαραίτητα για τη λειτουργία της εφαρμογής (EDPB, 2020). Τέλος, δεν μπορεί να θεωρηθεί ελεύθερη η δοθείσα συγκατάθεση, όταν υπάρχει σαφής ανισότητα μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας (π.χ. στη σχέση μεταξύ εργαζομένου και εργοδότη) (Ιγγλεζάκης, 2018).

Προϋπόθεση της σύννομης συγκατάθεσης αποτελεί επίσης και το συγκεκριμένο αυτής. Πρέπει δηλαδή, η συγκατάθεση που δίνεται από το υποκείμενο των δεδομένων να αφορά συγκεκριμένο σκοπό επεξεργασίας και όταν υπάρχουν περισσότεροι σκοποί, να δίνεται ξεχωριστά για καθέναν από αυτούς (Πλατής, 2018). Ειδικότερα δε, για να εξασφαλιστεί, ότι η συναίνεση του υποκειμένου είναι συγκεκριμένη, ο υπεύθυνος επεξεργασίας πρέπει σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB, 2020) να εφαρμόσει τα εξής: α) προσδιορισμό του σκοπού ως εγγύηση κατά της υφέρπουσας διεύρυνσης λειτουργιών, β) λεπτομερή ανάλυση στα αιτήματα συγκατάθεσης και γ) σαφή διαχωρισμό των πληροφοριών που αφορούν την εξασφάλιση της συγκατάθεσης για δραστηριότητες επεξεργασίας δεδομένων από τις πληροφορίες σχετικά με άλλα θέματα. Συνεπώς, θα πρέπει η συγκατάθεση να δίνεται χωριστά για κάθε διαφορετικό σκοπό επεξεργασίας και για κάθε διαφορετική πράξη επεξεργασίας, προκειμένου να πληρείται τόσο η προϋπόθεση του ελεύθερου, όσο και η προϋπόθεση του συγκεκριμένου αυτής.

Επιπροσθέτως, η συγκατάθεση πρέπει να παρέχεται εν πλήρει επιγνώσει, πρέπει δηλαδή -στα πλαίσια και της αρχής της διαφάνειας- να είναι ενημερωμένη. Συγκεκριμένα, σύμφωνα με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB, 2020), πρέπει να παρέχονται στο υποκείμενο των δεδομένων τουλάχιστον οι εξής πληροφορίες: α) η ταυτότητα του υπεύθυνου επεξεργασίας, β) ο σκοπός καθεμίας από τις πράξεις επεξεργασίας για τις οποίες ζητείται η συγκατάθεση, γ) το είδος των δεδομένων που θα συλλεχθούν και θα χρησιμοποιηθούν, δ) η ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης, ε) πληροφορίες σχετικά με τη χρήση των δεδομένων για αυτοματοποιημένη λήψη αποφάσεων σύμφωνα με το άρθρο 22 παρ. 2 στοιχ. γ', όπου συντρέχει περίπτωση και στ) πληροφορίες σχετικά με τους ενδεχόμενους κινδύνους των διαβιβάσεων δεδομένων λόγω της απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων, όπως προβλέπεται στο άρθρο 46 του ΓΚΠΔ. Στο πλαίσιο αυτό, αν και δεν ορίζεται ρητά στον Κανονισμό ο τρόπος με τον οποίον πρέπει να παρέχονται οι πληροφορίες (οπότε και μπορούν να χρησιμοποιηθούν γραπτές δηλώσεις -ακόμα και με ηλεκτρονικά μέσα, προφορικές δηλώσεις, ακουστικά ή οπτικά μηνύματα κ.τ.λ.), εντούτοις θα πρέπει σε κάθε περίπτωση να χρησιμοποιείται απλή και σαφής διατύπωση και να αποφεύγονται οι μακροσκελείς και δυσνόητες πολιτικές απορρήτου, οι οποίες στο μεγαλύτερο μέρος τους περιλαμβάνουν περίπλοκη νομική ορολογία, ώστε να γίνεται αντιληπτό το περιεχόμενο αυτών από τον μέσο άνθρωπο και να διασφαλίζεται, ότι το υποκείμενο μπορεί εύκολα να αναγνωρίσει τον υπεύθυνο της επεξεργασίας και να κατανοήσει σε τι συναινεί (EDPB, 2020). Εάν δε η συγκατάθεση του υποκειμένου

των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα (άρθρο 7 παρ. 2 του ΓΚΠΔ).

Στο πλαίσιο αυτό, όταν το σύννομο της επεξεργασίας των δεδομένων βασίζεται στη συγκατάθεση του υποκειμένου, ο υπεύθυνος επεξεργασίας καλείται να συμμορφωθεί, εκτός από τις υποχρεώσεις ενημέρωσης των άρθρων 13 και 14 του ΓΚΠΔ και με την ανωτέρω υποχρέωση της εν πλήρει επιγνώσει συγκατάθεσης. Αν και οι εν λόγω υποχρεώσεις αλληλοκαλύπτονται σε μεγάλο βαθμό, για τη λήψη έγκυρης συγκατάθεσης του υποκειμένου, δεν χρειάζεται να αναφέρονται όλες οι πληροφορίες που προβλέπονται στα άρθρα 13 και 14 του ΓΚΠΔ (οι οποίες πρέπει φυσικά να περιλαμβάνονται σε κάποια άλλα σημεία) (EDPB, 2020· Feiler, Forgó & Weigl, 2018). Στην πράξη βέβαια, η συμμόρφωση με τις δύο αυτές υποχρεώσεις γίνεται συνήθως με ενιαίο τρόπο (EDPB, 2020).

Επιπροσθέτως, σύμφωνα με το άρθρο 7 παρ. 3 του ΓΚΠΔ: «Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της». Στο πλαίσιο της διάταξης αυτής και δεδομένης της προϋπόθεσης για ελεύθερη και ενημερωμένη συγκατάθεση, ο υπεύθυνος της επεξεργασίας οφείλει πριν την παροχή της συγκατάθεσης από το υποκείμενο των δεδομένων, να το ενημερώσει σχετικά με την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής του ανά πάσα στιγμή και χωρίς καμία δυσμενή συνέπεια, αλλά και τον τρόπο που μπορεί να ασκήσει το δικαίωμά του αυτό. Σε περίπτωση δε άσκησης του εν λόγω δικαιώματος, ο υπεύθυνος επεξεργασίας οφείλει να διαγράψει τα δεδομένα που έτυχαν επεξεργασίας λόγω της συγκατάθεσης του υποκειμένου, εφόσον δεν συντρέχει κάποιος άλλος από τους προβλεπόμενους στο άρθρο 6 παρ. 1 του Κανονισμού νόμιμους λόγους επεξεργασίας των δεδομένων που θα δικαιολογούσε τη διατήρησή τους (EDPB, 2020). Ειδικότερα δε, όταν η συναίνεση λαμβάνεται με ηλεκτρονικά μέσα (π.χ. μόνο με ένα κλικ του ποντικιού ή όταν το υποκείμενο καλείται να σύρει μια μπάρα), τα υποκείμενα των δεδομένων πρέπει, στην πράξη, να μπορούν να αποσύρουν τη συναίνεση τους εξίσου εύκολα (EDPB, 2020). Αντίστοιχα, όταν η συγκατάθεση λαμβάνεται μέσω της χρήσης της διεπαφής χρήστη για συγκεκριμένη υπηρεσία (π.χ. μέσω ενός ιστότοπου, μιας εφαρμογής, της διεπαφής μιας συσκευής που ανήκει στο Διαδίκτυο των Πραγμάτων ή μέσω e-mail), το υποκείμενο των δεδομένων πρέπει να

μπορεί να αποσύρει τη συγκατάθεσή του μέσω της ίδιας ηλεκτρονικής διεπαφής, καθώς η μετάβαση σε άλλη διεπαφή αποκλειστικά και μόνο για το λόγο της ανάκλησης της συγκατάθεσης θα απαιτούσε αδικαιολόγητη προσπάθεια (EDPB, 2020).

Τέλος, η συγκατάθεση πρέπει να είναι ρητή. Σχετικά, στην Αιτιολογική Σκέψη 32 του ΓΚΠΔ αναφέρεται ότι: «*Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς. Εάν η συγκατάθεση του υποκειμένου των δεδομένων πρόκειται να δοθεί κατόπιν αιτήματος με ηλεκτρονικά μέσα, το αίτημα πρέπει να είναι σαφές, περιεκτικό και να μην διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται*». Συνεπώς, τα προσυμπληρωμένα τετραγωνίδια, τα οποία απαιτούν θετική ενέργεια από το υποκείμενο για να απορριφθούν δεν είναι συμβατά με τις διατάξεις του ΓΚΠΔ για τη συγκατάθεση. Αντίστοιχα, μη συμβατά με τον Κανονισμό φαίνεται να είναι τόσο αιτήματα συγκατάθεσης τα οποία δίνουν μεγαλύτερη έμφαση στην επιλογή "αποδέχομαι" ή "επιτρέπεται" έναντι της επιλογής "απορρίπτω" ή "μπλοκάρω", καθώς στοχεύουν στο να επηρεάσουν το υποκείμενο να δεχθεί την επεξεργασία, όσο και τα αιτήματα συγκατάθεσης για τα cookies, τα οποία δεν διαθέτουν την επιλογή της απόρριψης, η οποία περιλαμβάνεται σε μία δεύτερη σελίδα που παρέχει περισσότερες πληροφορίες για την επεξεργασία και την οποία πρέπει να ανοίξει ξεχωριστά ο χρήστης (Nouwens, Liccardi, Veale, Karger & Kagal, 2020).

Γενικά, φαίνεται, ότι ο Κανονισμός θέτει πιο αυστηρές προϋποθέσεις σε σχέση με την προισχύουσα Οδηγία για την έγκυρη λήψη της συγκατάθεσης του υποκειμένου των δεδομένων. Οι προϋποθέσεις αυτές είναι ακόμα πιο αυστηρές, όταν πρόκειται για συγκατάθεση από ανήλικο ή για συγκατάθεση σε επεξεργασία ευαίσθητων προσωπικών

δεδομένων (Voigt & Von dem Bussche, 2017· Πλατής, 2018). Το βάρος δε για την απόδειξη όλων των ανωτέρω προϋποθέσεων βαρύνει τον υπεύθυνο επεξεργασίας, ο οποίος σύμφωνα με το άρθρο 7 παρ. 1 του ΓΚΠΔ πρέπει να είναι σε θέση να αποδείξει, ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των προσωπικών του δεδομένων. Σκοπός όλων των ανωτέρω διατάξεων και της αυστηρότητας αυτών είναι να ενισχυθεί η θέση των υποκειμένων και να διασφαλισθεί, ότι έχουν τον έλεγχο των προσωπικών τους δεδομένων (βλ. και Αιτιολογική Σκέψη 7 του ΓΚΠΔ).

Στην εποχή των Big Data Analytics, η συγκατάθεση του υποκειμένου ως νομική βάση για τη νομιμότητα της επεξεργασίας των δεδομένων του εμφανίζει τη μεγαλύτερη πρακτική σημασία (ιδιαίτερα στον ιδιωτικό και εμπορικό τομέα), ενώ δεν είναι απίθανο να στοιχειοθετηθεί και η περ. στ της παρ. 1 του άρθρου 6 του ΓΚΠΔ, η οποία μπορεί να λειτουργήσει ως εναλλακτική βάση για την επεξεργασία των δεδομένων (ICO, 2017). Εντούτοις, η λήψη της συγκατάθεσης εμφανίζεται στην πράξη ιδιαίτερα προβληματική. Κατ' αρχάς, η εξασφάλιση αυτής και η απόδειξή της από τους υπεύθυνους επεξεργασίας ενδέχεται να είναι ιδιαίτερα επαχθής, ειδικά σε περιπτώσεις επεξεργασίας δεδομένων πολλών υποκειμένων, πόσο δε μάλλον αν λάβει κανείς υπόψη τις αυξημένες προϋποθέσεις που θέτει ο Κανονισμός για την εγκυρότητα αυτής (Πλατής, 2018), με αποτέλεσμα σε πολλές περιπτώσεις -παρ' όλο που αποτελεί μονόδρομο για τους υπεύθυνους επεξεργασίας- να μην είναι εύκολα εφαρμόσιμη ως νομική βάση για την επεξεργασία των δεδομένων (Hoofnagle et al., 2019).

Παράλληλα, φαίνεται ότι ο Κανονισμός στηρίζεται σε ορισμένες υποθέσεις σχετικά με τον τρόπο λήψης αποφάσεων από τους ανθρώπους, οι οποίες δεν ανταποκρίνονται στην πραγματικότητα (van Ooijen & Vrabec, 2019). Ειδικότερα, το μοντέλο της αυτοδιαχείρισης των δεδομένων από το ίδιο το υποκείμενο στηρίζεται στην ιδέα ενός ενημερωμένου και ορθολογικού ανθρώπου που μπορεί να επεξεργαστεί έναν απεριόριστο αριθμό πληροφοριών και να λαμβάνει τις κατάλληλες αποφάσεις σχετικά με την παροχή συναίνεσης στην επεξεργασία των δεδομένων του, μεγιστοποιώντας κάθε φορά τη χρησιμότητά του (Hermstruwer, 2017· Solove, 2012). Εντούτοις, στην πράξη έχει παρατηρηθεί μια σημαντική διαφορά ανάμεσα στις προθέσεις των υποκειμένων σε σχέση με την παροχή πρόσβασης στα προσωπικά τους δεδομένα και την προστασία της ιδιωτικότητάς τους και στην εν τοις πράγμασι συμπεριφορά τους. Τα υποκείμενα των δεδομένων, παρά το γεγονός ότι εκφράζουν σοβαρές ανησυχίες σχετικά με τα προσωπικά τους δεδομένα και με το ποιος έχει πρόσβαση σε αυτά, δίνοντας μεγάλη αξία στην προστασία της ιδιωτικότητάς τους, εντούτοις επιδεικνύουν

μια εντελώς αντίθετη συμπεριφορά, συναινώντας με μεγάλη ευκολία στην επεξεργασία των δεδομένων τους, έναντι πολύ μικρού κάθε φορά οφέλους. Το φαινόμενο αυτό έχει ονομαστεί το παράδοξο της ιδιωτικότητας (*privacy paradox*) και πιθανότατα να οφείλεται στους διαφορετικούς παράγοντες που επηρεάζουν ανεξάρτητα τις προθέσεις των υποκειμένων και τις τελικές τους αποφάσεις (Norberg, Horne, D.R. & Horne, D.A., 2007) και συγκεκριμένα, η απόκλιση αυτή οφείλεται στα διάφορα εμπόδια που παρατηρούνται κατά τη διαδικασία λήψης ορθολογικών αποφάσεων από τους ανθρώπους (Solove, 2012).

Πιο συγκεκριμένα, σύμφωνα με τη θεωρία του φραγμένου ορθολογισμού (*bounded rationality*), όταν καλούνται να λάβουν αποφάσεις, τα άτομα περιορίζονται εξαιτίας της ανεπαρκούς πληροφόρησης, των εγγενών γνωστικών περιορισμών του ανθρώπινου εγκεφάλου και των χρονικών περιορισμών (Tsaoussi, 2014). Στο πλαίσιο αυτό, ο ορθολογικός άνθρωπος που αποσκοπεί στη μεγιστοποίηση της χρησιμότητάς του και ο οποίος καλείται να αντιμετωπίσει περίπλοκες καταστάσεις σε διάφορους τομείς της κοινωνικής και οικονομικής του δραστηριότητας, καταλήγει να λαμβάνει μη τέλειες αποφάσεις (απλώς ικανοποιητικές αντί για βέλτιστες) (Tsaoussi, 2014). Το ίδιο ακριβώς συμβαίνει και στην περίπτωση που τα υποκείμενα των δεδομένων καλούνται να αποφασίσουν εάν θα χορηγήσουν τη συγκατάθεση τους και κατ' επέκταση εάν θα παρέχουν πρόσβαση στα δεδομένα τους στον εκάστοτε υπεύθυνο επεξεργασίας, αποφάσεις οι οποίες συχνά συνδέονται με περίπλοκες συνέπειες που ενδέχεται να εμφανιστούν σε βάθος χρόνου.

Ειδικότερα, κατά τη διαδικασία χορήγησης της συναίνεσης από το υποκείμενο, εμφανίζονται κατ' αρχάς ζητήματα ανεπαρκούς πληροφόρησης. Οι υπεύθυνοι επεξεργασίας έχουν περισσότερες πληροφορίες από τα υποκείμενα σχετικά με τους σκοπούς της επεξεργασίας και τις προϋποθέσεις για τη μελλοντική χρήση των δεδομένων (Acquisti et al., 2017) και για αυτόν τον λόγο φέρουν και την υποχρέωση ενημέρωσης των υποκειμένων κατά τις διατάξεις του Κανονισμού. Ωστόσο, τα υποκείμενα των δεδομένων δεν διαβάζουν τις σχετικές πολιτικές απορρήτου προκειμένου να ενημερωθούν κατάλληλα προτού συγκαταθέσουν στην επεξεργασία των δεδομένων τους, ενώ ακόμα και αν μπορούσαν να τις διαβάσουν, δεν θα ήταν σε θέση να τις κατανοήσουν στο σύνολό τους. Στο πλαίσιο της προϋπόθεσης της εν πλήρει επιγνώσει συγκατάθεσης -όπως ακριβώς συμβαίνει και στο πλαίσιο της εφαρμογής της αρχής της διαφάνειας (βλ. κατωτέρω κεφάλαιο 5.3.4.3), ο όγκος των διαθέσιμων πληροφοριών, η πολυπλοκότητα των ούτως ή άλλως μακροσκελών πολιτικών απορρήτου και ο χρόνος που θα απαιτούνταν από το υποκείμενο για να τις διαβάσει και

να τις κατανοήσει, έχουν ως αποτέλεσμα την "εξάντληση" των υποκειμένων, τα οποία αδυνατούν να συμβαδίσουν με αυτούς τους ρυθμούς, με αποτέλεσμα να μην διαβάζουν τις πολιτικές απορρήτου και απλά να "κλικάρουν" την επιλογή της συγκατάθεσης αυτόματα και μηχανικά, χωρίς προηγουμένως να λαμβάνουν την απαραίτητη πληροφόρηση (EDPB, 2020· Froomkin, 2019· Susser, 2019· van Ooijen & Vrabec, 2019). Για τη λήψη μιας ουσιαστικής απόφασης σχετικά με την παροχή συγκατάθεσης απαιτείται ένα εξαιρετικά υψηλό επίπεδο επίγνωσης και κατανόησης, το οποίο όμως δεν παρέχεται στην πράξη από τις πολιτικές απορρήτου, με αποτέλεσμα το γεγονός, ότι τα υποκείμενα τις αποδέχονται και συναινούν στην επεξεργασία των δεδομένων τους, να μην αποτελεί ισχυρή απόδειξη, ότι αυτές οι αποφάσεις αντικατοπτρίζουν τις πραγματικές προτιμήσεις και τα ενδιαφέροντα τους (Susser, 2019).

Εντούτοις, ακόμη και αν υποτεθεί, ότι τα υποκείμενα διέθεταν τον απαραίτητο χρόνο και μπορούσαν να κατανοήσουν όλες τις πληροφορίες σχετικά με την επεξεργασία των δεδομένων τους και πάλι δεν θα ήταν σε θέση να λάβουν βέλτιστες αποφάσεις, εξαιτίας ακριβώς των γνωστικών περιορισμών και του εν γένει φραγμένου ορθολογισμού του ανθρώπινου εγκεφάλου, ο οποίος επιπίπτει συστηματικά σε λάθη (γνωστικά και συναισθηματικά) και καταφεύγει σε ευριστικούς κανόνες (συντομεύσεις) κατά τη λήψη μιας απόφασης (Acquisti et al., 2017· Tsaoussi, 2014). Αυτοί οι γνωστικοί περιορισμοί εμποδίζουν ακριβώς τα υποκείμενα των δεδομένων να λάβουν ορθολογικές αποφάσεις σχετικά με τα κόστη και τις ωφέλειες της συγκατάθεσης στη συλλογή, χρήση και αποκάλυψη των προσωπικών τους δεδομένων (Solove, 2012). Για παράδειγμα, η εκτίμηση των κινδύνων από τη συγκατάθεση στην επεξεργασία των δεδομένων ενδέχεται να στρεβλωθεί εξαιτίας του ευριστικού κανόνα της διαθεσιμότητας (*availability heuristic*), με βάση τον οποίο τα άτομα θεωρούν ως πιο επικίνδυνους και σημαντικούς εκείνους τους κινδύνους, για τους οποίους έχουν περισσότερα σχετικά σημεία σύγκρισης και κατ’ επέκταση είναι πιο εξοικειωμένα με αυτούς (Acquisti et al., 2017· Solove, 2012). Έτσι, ενδέχεται να προσπαθήσουν να εκτιμήσουν τους κινδύνους που μπορεί να προκύψουν από την παροχή πρόσβασης στα δεδομένα τους, λαμβάνοντας υπόψη το κατά πόσο άλλοι άνθρωποι, υπό παρόμοιες συνθήκες, συναίνεσαν στην επεξεργασία των δεδομένων τους (Acquisti et al., 2017). Αντίστοιχα, οι άνθρωποι έχουν την τάση να αποστρέφονται την απώλεια (*loss aversion*), με αποτέλεσμα να εκτιμούν περισσότερο τα προσωπικά τους δεδομένα, όταν αισθάνονται, ότι τα έχουν στην κατοχή τους και αντιθέτως τους δίνουν μικρότερη αξία, όταν νιώθουν, ότι έχουν χάσει τον έλεγχό τους (Acquisti et al., 2017). Στο πλαίσιο αυτό, οι άνθρωποι δεν είναι διατεθειμένοι να πληρώσουν για υπηρεσίες που θα

ενισχύσουν την προστασία της ιδιωτικότητάς τους, εντούτοις εκφράζουν σοβαρές ανησυχίες σχετικά με τη συλλογή των δεδομένων τους από διάφορες εταιρείες, ενώ είναι πρόθυμοι να λάβουν ένα υψηλότερο χρηματικό ποσό προκειμένου να παραχωρήσουν πρόσβαση στα δεδομένα τους σε σχέση με το ποσό που είναι διατεθειμένοι να πληρώσουν οι ίδιοι για να επανακτήσουν τον έλεγχο αυτών (Acquisti et al., 2017). Ιδιαίτερα σημαντικός είναι επίσης και ο τρόπος με τον οποίο παρουσιάζονται στο υποκείμενο οι διάφορες επιλογές που έχει, ο οποίος μπορεί να επηρεάσει σε σημαντικό βαθμό τις αποφάσεις του (το λεγόμενο σφάλμα διατύπωσης / *framing*) (Acquisti & Grossklags, 2007· Solove, 2012).

Στο πλαίσιο αυτό, οι υπεύθυνοι επεξεργασίας ενδέχεται να εκμεταλλευτούν αυτούς τους γνωστικούς περιορισμούς και τον εν γένει φραγμένο ορθολογισμό των υποκειμένων κατά τη λήψη αποφάσεων. Αποτελεί άλλωστε κοινή παραδοχή, ότι ο σχεδιασμός και ο τρόπος που παρουσιάζονται τα παράθυρα για την παροχή της συναίνεσης, μπορεί να κατευθύνει τα υποκείμενα σε συγκεκριμένες επιλογές / αποφάσεις (Machuletz & Böhme, 2020). Οι Utz, Degeling, Fahl, Schaub και Holz, (2019) διαπίστωσαν, ότι ο τρόπος με τον οποίο ζητείται η παροχή συγκατάθεσης από το υποκείμενο (π.χ. σε ποιο σημείο της σελίδας θα τοποθετηθεί το αίτημα, ο τρόπος που παρουσιάζονται οι διάφορες επιλογές κ.τ.λ.) επηρεάζει σε μεγάλο βαθμό τη συμπεριφορά των υποκειμένων. Για παράδειγμα, ένα από τα πιο γνωστά και ίσως ισχυρά εργαλεία για να καθοδηγηθούν τα υποκείμενα των δεδομένων σε συγκεκριμένες αποφάσεις είναι η χρήση των προεπιλεγμένων ρυθμίσεων, επειδή ακριβώς απευθύνεται σε αυτόματες και γνωστικές διαδικασίες του ανθρώπινου εγκεφάλου (van Ooijen & Vrabec, 2019). Ειδικότερα, έχει αποδειχθεί, ότι οι καταναλωτές, όταν τους παρουσιάζονται περισσότερες επιλογές, προτιμούν γενικά και επιλέγουν εκείνη την επιλογή που έχει επισημανθεί ως προεπιλογή (van Ooijen & Vrabec, 2019). Στην έρευνα των Johnson, Bellman και Lohse (2002) διαπιστώθηκε, ότι ο αριθμός των συμμετεχόντων που συναίνεσε στην επεξεργασία των δεδομένων τους για ερευνητικούς σκοπούς αυξήθηκε κατά 50%, όταν η αποδοχή της επεξεργασίας είχε οριστεί ως προεπιλογή. Αντίστοιχα, σε έρευνα τους οι Machuletz και Böhme (2020) διαπίστωσαν, ότι οι χρήστες αποδέχονται περισσότερους σκοπούς επεξεργασίας των δεδομένων τους, όταν στο εμφανιζόμενο παράθυρο για την παροχή της συγκατάθεσης υπάρχει ένα προεπιλεγμένο κουμπί, με το οποίο παρέχεται ταυτόχρονα συναίνεση για όλους τους σκοπούς. Οι περισσότεροι δε χρήστες που καταλήγουν να επιλέξουν την προεπιλεγμένη επιλογή δεν μπορούν να ανακαλέσουν στη μνήμη τους, τους σκοπούς στους οποίους συναίνεσαν, έχοντας παράλληλα την τάση να μετανιώνουν την απόφασή τους, αφού

πληροφορηθούν για αυτούς (Machuletz & Böhme, 2020). Επίσης, η χρήση κατάλληλων σημαδιών / υπαινιγμών, προκειμένου να αισθανθούν τα υποκείμενα των δεδομένων ότι έχουν τον έλεγχο των προσωπικών τους πληροφοριών, μπορεί να έχει ως αποτέλεσμα την αποκάλυψη περισσότερων προσωπικών δεδομένων από το υποκείμενο (van Ooijen & Vrabec, 2019). Για παράδειγμα, οι Hoofnagle και Urban (2014) σε έρευνα που πραγματοποίησαν, διαπίστωσαν, ότι το 62% των ερωτηθέντων πίστευε, ότι και μόνο η ύπαρξη μιας πολιτικής απορρήτου σε έναν ιστότοπο (ανεξάρτητα από το περιεχόμενο αυτής) σημαίνει, ότι ο συγκεκριμένος ιστότοπος δεν μπορεί να μοιραστεί τα δεδομένα που συλλέγει για τους χρήστες του με άλλες εταιρείες χωρίς την άδεια του χρήστη, δημιουργώντας αυτόματα ένα μεγαλύτερο αίσθημα ασφάλειας στους χρήστες.

Παράλληλα, προβλήματα στη διασφάλιση της ουσιώδους συγκατάθεσης των υποκειμένων των δεδομένων δημιουργούνται και από τον τρόπο που έχει διαμορφωθεί η σύγχρονη κοινωνικο – οικονομική πραγματικότητα, όπου το διαδίκτυο έχει κεντρικό ρόλο. Στο σύγχρονο ψηφιακό περιβάλλον, κάθε πολίτης επισκέπτεται καθημερινά δεκάδες ιστοσελίδες και πραγματοποιεί ποικίλες συναλλαγές, με αποτέλεσμα να έρχεται σε επαφή με έναν τεράστιο αριθμό αιτημάτων συγκατάθεσης. Στην πράξη δηλαδή, ο μέσος χρήστης καλείται να διαχειριστεί έναν τεράστιο αριθμό αιτημάτων, χωρίς να διαθέτει ούτε τον απαραίτητο χρόνο, ούτε και τους αναγκαίους πόρους (Schermer, Custers & van der Hof, 2014· Solove, 2012). Οι Jolls και Sunstein (2006) αναφέρουν σχετικά σε έρευνά τους, ότι οι καταναλωτές μαθαίνουν να σταματούν να δίνουν σημασία σε μηνύματα με τα οποία έρχονται συχνά σε επαφή, όπως εν προκειμένω με τα αιτήματα συγκατάθεσης. Κατ’ ουσία, τα αιτήματα συγκατάθεσης πλέον βρίσκονται παντού, με τα περισσότερα να παρέχουν είτε πολύ λίγες είτε πάρα πολλές επιλογές, με αποτέλεσμα να δημιουργείται στους χρήστες η εντύπωση, ότι οι επιλογές που διαθέτουν δεν έχουν νόημα και να τροφοδοτείται η συνήθεια να "κλικάρουν" οποιαδήποτε επιλογή θα εξαφανίσει το αίτημα από την οθόνη τους, αντί να ασχοληθούν και να λάβουν μια συνειδητή απόφαση σχετικά με τη χορήγηση της συγκατάθεσής τους (Utz et al., 2019).

Στο πλαίσιο αυτό, έχει ασκηθεί έντονη κριτική στο μοντέλο αυτό της παροχής ουσιώδους συγκατάθεσης εξαιτίας ακριβώς της ανισορροπίας δύναμης και ισχύος (*power imbalances*) που εμφανίζεται ανάμεσα στους χρήστες / υποκείμενα και στις διαδικτυακές πλατφόρμες / υπεύθυνους επεξεργασίας. Ειδικότερα, υποστηρίζεται, ότι το άτομο δεν έχει καθόλου ή έχει ελάχιστη μόνο διαπραγματευτική δύναμη, καθώς καλείται απλά να συναινέσει σε μια τυποποιημένη, take-it-or-leave-it πολιτική απορρήτου (Schermer et al., 2014). Επιπλέον, στις περισσότερες περιπτώσεις δεν

υπάρχουν ουσιαστικές εναλλακτικές για το υποκείμενο, καθώς πέρα από την κυριαρχία συγκεκριμένων φορέων στον χώρο του διαδικτύου (όπως είναι η Google και η Facebook), οι υπεύθυνοι επεξεργασίας στο μεγαλύτερο μέρος τους προσφέρουν τις ίδιες συνθήκες και προϋποθέσεις, όσον αφορά την επεξεργασία των δεδομένων των χρηστών τους (Koops, 2014).

Επιπροσθέτως, στα πλαίσια της προϋπόθεσης της ενημερωμένης συγκατάθεσης απαιτείται το υποκείμενο των δεδομένων να γνωρίζει σε τι συναινεί, ποιος είναι ο σκοπός της επεξεργασίας και ποιες πράξεις επεξεργασίας θα πραγματοποιηθούν. Ωστόσο, στην εποχή των Big Data Analytics και ιδιαίτερα στα πλαίσια της μηχανικής μάθησης, η μεγαλύτερη αξία των δεδομένων βρίσκεται ακριβώς στις δευτερεύουσες χρήσεις τους, στους απρόσμενους συνδυασμούς που θα προκύψουν μετά την ανάλυση αυτών και τον συνδυασμό τους με άλλα δεδομένα. Όπως αναφέρεται και ανωτέρω, το ζήτημα δημιουργείται ακριβώς επειδή κανένα μέρος (ούτε καν ο υπεύθυνος της επεξεργασίας, πόσο δε μάλλον το υποκείμενο των δεδομένων) δεν γνωρίζει ποιο θα είναι το αποτέλεσμα της ανάλυσης (Froomkin, 2019) ή πόσο αποκαλυπτικά μπορεί να είναι τα δεδομένα, για τα οποία παρέχεται η συγκατάθεση (Susser, 2019), καθιστώντας ουσιαστικά αδύνατο για κάποιον να μπορεί να κρίνει ποια είναι τα κόστη και τα οφέλη της αποκάλυψης ορισμένων δεδομένων του (Solove, 2012). Τα υποκείμενα των δεδομένων καλούνται να λάβουν σημαντικές αποφάσεις, χωρίς να είναι σε θέση να γνωρίζουν ποιες θα είναι οι συνέπειες της επεξεργασίας, τη στιγμή που παρέχουν τη συγκατάθεση τους (Froomkin, 2019· Susser, 2019), δεδομένου άλλωστε, ότι οι παραβιάσεις του δικαιώματος της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων μπορούν να εμφανιστούν σε βάθος χρόνου (π.χ. η συναίνεση για την επεξεργασία περισσότερων "ακίνδυνων" δεδομένων σε βάθος χρόνου, τα οποία εν τέλει σωρεύονται και οδηγούν στην αποκάλυψη ευαίσθητων πληροφοριών για το υποκείμενο) (Solove, 2012). Το πρόβλημα αυτό γίνεται εντονότερο, αν λάβει κανείς υπόψη πως, στα πλαίσια του φραγμένου ορθολογισμού, οι άνθρωποι πολλές φορές αδυνατούν να κάνουν επιλογές που αντικατοπτρίζουν τις αληθινές προτιμήσεις τους, όταν καλούνται να προβλέψουν μακροπρόθεσμα κόστη και κινδύνους (Hermstruwer, 2017). Για παράδειγμα, όσο μεγαλύτερη είναι η χρονική διαφορά ανάμεσα στην παροχή της συγκατάθεσης και στη χρήση των δεδομένων, τόσο μικρότερη είναι η πιθανότητα να υπολογίσει το υποκείμενο των δεδομένων τους πιθανούς κινδύνους τη στιγμή της παροχής της συγκατάθεσης, ενώ όσο μεγαλύτερα και πιο άμεσα είναι τα οφέλη από την παροχή της συγκατάθεσης τόσο μεγαλύτερη θα είναι και η υποτίμηση των μελλοντικών κινδύνων από το υποκείμενο (Hermstruwer, 2017).

Σε κάθε περίπτωση, ακόμα και αν ο χρήστης δεν συναινέσει στην επεξεργασία των δεδομένων του, αυτό δεν συνεπάγεται πάντα, ότι δεν θα χρησιμοποιηθούν αυτά. Στην έρευνα των Sanchez-Rola et al. (2019) διαπιστώθηκε, ότι περίπου το 90% των ιστοτόπων πραγματοποιούν κάποιου είδους παρακολούθηση (*tracking*) του χρήστη (π.χ. ορίζοντας τουλάχιστον ένα αναγνωριστικό cookie), πριν καν του παρουσιάσουν την πολιτική απορρήτου και ακόμα και αν ο χρήστης αποφασίσει να μην συναινέσει στην παρακολούθησή του. Αντίστοιχα, μετά την απόρριψη από τον χρήστη της παρακολούθησης μέσω cookies, σε πολλές περιπτώσεις, ο αριθμός των τελευταίων παραμένει ίδιος, ενώ δεν αποκλείεται και να αυξηθεί. Από την άλλη, στην έρευνα των Nouwens et al. (2020) διαπιστώθηκε, ότι μόνο το 11,8% των ιστοτόπων που ερευνήθηκαν, πληρούσαν τις βασικές προϋποθέσεις του Κανονισμού (δεν υπήρχαν προσυμπληρωμένα τετραγωνίδια, η μη αποδοχή της επεξεργασίας ήταν όσο εύκολη όσο και η αποδοχή και η παροχή της συγκατάθεσης ήταν ρητή), φανερώνοντας την πρακτική αδυναμία εφαρμογής του Κανονισμού και ειδικότερα των διατάξεων για τη συγκατάθεση του υποκειμένου σε πολλές περιπτώσεις.

Γίνεται, επομένως, κατανοητό, ότι στα πλαίσια του νέου Κανονισμού και των αυστηρότερων διατάξεων που αυτός προβλέπει για τη λήψη έγκυρης και νόμιμης συγκατάθεσης του υποκειμένου ως νομική βάση για την επεξεργασία των δεδομένων του, γίνεται προσπάθεια να αντιμετωπιστούν αρκετά ζητήματα που εμφανίζονταν υπό το προϊσχύον καθεστώς της Οδηγίας, εντούτοις η λήψη της συγκατάθεσης εξακολουθεί να εμφανίζεται ιδιαίτερα προβληματική. Συγκεκριμένα, υποστηρίζεται, ότι η συγκατάθεση των υποκειμένων σήμερα δεν είναι ούτε ενημερωμένη αλλά ούτε και ελεύθερη, γεγονός που οφείλεται σε ένα σύνολο διαφορετικών παραγόντων. Αφενός μεν το βάρος που εναποτίθεται στους υπεύθυνους επεξεργασίας για την εξασφάλιση και την απόδειξη όλων των προϋποθέσεων της έγκυρης συγκατάθεσης είναι ιδιαίτερα μεγάλο, αφετέρου δε δεν διασφαλίζεται, ότι τα υποκείμενα έχουν πράγματι τον έλεγχο των δεδομένων τους, είτε εξαιτίας της ανεπαρκούς πληροφόρησης και των εγγενών περιορισμών του ανθρώπινου εγκεφάλου που εμποδίζουν τη λήψη ορθολογικών αποφάσεων από τους ανθρώπους, είτε εξαιτίας του περιβάλλοντος που έχει διαμορφωθεί γύρω από τα δεδομένα, ιδιαίτερα στο πλαίσιο των Big Data Analytics και των δυνατοτήτων που προσφέρουν. Άλλωστε και η εφαρμογή των εν λόγω διατάξεων στην πράξη δεν έχει αποδειχθεί ιδιαίτερα αποτελεσματική, κατά την έννοια της κατά Pareto αποτελεσματικότητας. Χαρακτηριστικό παράδειγμα αποτελούν τα προσυμπληρωμένα τετραγωνίδια, τα οποία, όπως αναλύεται ανωτέρω, εξακολουθούν και χρησιμοποιούνται από ένα μεγάλο αριθμό ιστοτόπων και εφαρμογών, καθώς

φαίνεται να επηρεάζουν σε μεγάλο βαθμό τη συμπεριφορά των υποκειμένων σχετικά με την παροχή της συγκατάθεσής τους, παρά το γεγονός ότι ο Κανονισμός προβλέπει, ότι δεν θα πρέπει να εκλαμβάνονται ως σύννομη συγκατάθεση.

5.3.4.2. Η αρχή της αντικειμενικότητας της επεξεργασίας

Η αρχή της αντικειμενικότητας θα μπορούσε να συγκριθεί με τη γενική αρχή της καλής πίστης που υπάρχει σε διάφορα νομικά συστήματα (Hoofnagle et al., 2019). Στα πλαίσια της εν λόγω αρχής, πριν από την εκτέλεση της επεξεργασίας θα πρέπει να λαμβάνει χώρα αξιολόγησή της, ώστε να διασφαλίζεται, αφενός ότι δεν θα υπάρξουν αρνητικές επιπτώσεις στα δικαιώματα και στις ελευθερίες του υποκειμένου και αφετέρου ότι σε αντίθετη περίπτωση, αυτές θα είναι δικαιολογημένες (Πλατής, 2018). Για την αξιολόγηση της αντικειμενικότητας πρέπει, σε κάθε περίπτωση, να λαμβάνονται υπόψη τόσο οι επιπτώσεις της επεξεργασίας στα άτομα, όσο και οι προσδοκίες τους σχετικά με τον τρόπο χρησιμοποίησης των δεδομένων τους κατά την εφαρμογή των Big Data Analytics (ICO, 2017).

Εντούτοις, τα Big Data Analytics φαίνεται, ότι δεν συμβαδίζουν με την εν λόγω αρχή, δεδομένου ότι περιλαμβάνουν την επαναχρησιμοποίηση των δεδομένων για νέους, απροσδόκητους σκοπούς, μέσα από τη χρήση περίπλοκών αλγόριθμων και την εξαγωγή συμπερασμάτων για τα άτομα, που επιφέρουν σε πολλές περιπτώσεις απρόσμενα και ενδεχομένως ανεπιθύμητα αποτελέσματα (ICO, 2017). Στο πλαίσιο αυτό, ενδέχεται να προκύψουν, όπως αναλύεται ανωτέρω στο κεφάλαιο 4.3, μεροληπτικά και άδικα αποτελέσματα για το υποκείμενο των δεδομένων, τα οποία ενδέχεται να έχουν σημαντικές επιπτώσεις στη ζωή του (π.χ. εάν θα θεωρηθεί ένας κατηγορούμενος ως πιθανός υπότροπος ή όχι). Η ιδέα ενός αντικειμενικού και αλάνθαστου συστήματος τεχνητής νοημοσύνης μοιάζει σήμερα μάλλον ουτοπική. Ο κίνδυνος διακρίσεων που ελλοχεύον οι σύγχρονες αυτές τεχνολογίες επισημαίνεται και στον ίδιο τον Κανονισμό, όπου αναφορικά με το άρθρο 22 αυτού και τη λήψη αποφάσεων βάσει αυτοματοποιημένης επεξεργασίας, η Αιτιολογική Σκέψη 71 αναφέρει, ότι οι υπεύθυνοι επεξεργασίας οφείλουν μεταξύ άλλων να λαμβάνουν τέτοιου είδους μέτρα, έτσι ώστε να προλαμβάνονται τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος.

Στο πλαίσιο αυτό, το μεγαλύτερο ζήτημα που γεννάται από την καθιέρωση των Big Data Analytics σε σχέση με την αρχή της αντικειμενικότητας δεν εντοπίζεται τόσο στα ίδια τα μεροληπτικά ή άδικα αποτελέσματα της επεξεργασίας, αλλά στον τρόπο με τον οποίο το εκάστοτε σύστημα τεχνητής νοημοσύνης κατέληξε σε αυτά. Πράγματι, η απαγόρευση των διακρίσεων επικεντρώνεται παραδοσιακά σε εκείνα τα ανθρώπινα χαρακτηριστικά που είναι ζωτικής σημασίας για τις μεροληπτικές πρακτικές (π.χ. το φύλο, το χρώμα, η φυλή), εντούτοις σήμερα τα συστήματα τεχνητής νοημοσύνης βασίζονται σε πιο θολές και λιγότερο σαφείς κατηγορίες (Mantelero, 2018). Συγκεκριμένα, τα μεροληπτικά αποτελέσματα δεν οφείλονται πλέον στη συμμετοχή του υποκειμένου σε μια συγκεκριμένη κοινωνική ομάδα, αλλά στον εντοπισμό από το σύστημα τεχνητής νοημοσύνης κάποιων κοινών χαρακτηριστικών μεταξύ του υποκειμένου και μιας αλγοριθμικά διαμορφωμένης ομάδας ατόμων, στην οποία αποδίδονται ορισμένα χαρακτηριστικά και στην κατηγοριοποίηση του υποκειμένου στη συγκεκριμένη ομάδα (ICO, 2017). Για παράδειγμα, όπως αναφέρεται χαρακτηριστικά και ανωτέρω, για τον προσδιορισμό της πιστοληπτικής ικανότητας και εν γένει της οικονομικής κατάστασης των ανθρώπων χρησιμοποιούνται σήμερα οι καταναλωτικές τους συνήθειες (δηλαδή από ποια μαγαζιά ψωνίζουν και εάν άλλα άτομα που έχουν ψωνίσει από τα ίδια μαγαζιά βρέθηκαν ποτέ σε κατάσταση αδυναμίας πληρωμών), ενώ για την εύρεση της φυλετικής τους καταγωγής χρησιμοποιείται ο τόπος κατοικίας τους (π.χ. μέσω του ταχυδρομικού τους κώδικα ή της διεύθυνσης IP).

Γίνεται, επομένως, κατανοητό, ότι η αρχή της αντικειμενικότητας της επεξεργασίας δοκιμάζεται και αυτή σε μεγάλο βαθμό από τις σύγχρονες τεχνολογικές εξελίξεις. Οι περιπτώσεις, όπου η ανάλυση των δεδομένων οδηγεί σε διακρίσεις σε βάρος των υποκειμένων και σε μεροληπτικά αποτελέσματα είναι πολλές και διαφορετικές και, όπως περιγράφεται αναλυτικά στο κεφάλαιο 4.3 μπορεί να ανάγονται σε οποιοδήποτε στάδιο του σχεδιασμού και της λειτουργίας ενός συστήματος τεχνητής νοημοσύνης, ενώ μπορεί να είναι τόσο ακούσιες όσο και εκούσιες. Παράλληλα, οι δυνατότητες που προσφέρουν σήμερα η τεχνητή νοημοσύνη και δη η μηχανική μάθηση για την εύρεση νέων, απρόσμενων και προηγουμένως άγνωστων μοτίβων και συσχετίσεων μεταξύ των δεδομένων έχουν ως αποτέλεσμα να μην είναι πάντοτε ευδιάκριτο, πότε υφίσταται διάκριση σε βάρος κάποιου ατόμου. Η λήψη δηλαδή μιας απόφασης ενδέχεται να μην στηρίζεται άμεσα σε κάποιο από εκείνα τα χαρακτηριστικά που παραδοσιακά προστατεύονται από τη σχετική νομοθεσία για την απαγόρευση των διακρίσεων -τα οποία σε μεγάλο βαθμό επαναλαμβάνονται και στον Κανονισμό- αλλά σε άλλα, φαινομενικώς ακίνδυνα χαρακτηριστικά (π.χ. τόπος κατοικίας, καταναλωτικές

συνήθειες), τα οποία όμως λειτουργούν ως ενδείξεις των πρώτων και τα οποία μοιράζεται ένα σύνολο ανθρώπων που γίνεται αντιληπτό και ομαδοποιείται από το σύστημα τεχνητής νοημοσύνης. Οι ενδείξεις αυτές, καθώς και η κατηγοριοποίηση που πραγματοποιείται δεν είναι εύκολο να προβλεφθούν και να εντοπιστούν, με αποτέλεσμα να καθίσταται ιδιαίτερα δυσχερές για το υποκείμενο να μπορέσει να αντιληφθεί πότε μια απόφαση που το αφορά δεν πληροί την προϋπόθεση της αντικειμενικότητας και συνιστά διάκριση σε βάρος του.

5.3.4.3 Η αρχή της διαφάνειας της επεξεργασίας

Σύμφωνα με την αρχή της διαφάνειας της επεξεργασίας, η οποία περιλαμβάνει και το δικαίωμα ενημέρωσης του υποκειμένου και το δικαίωμα πρόσβασης στα δεδομένα του (Ιγγλεζάκης, 2018), η επεξεργασία των προσωπικών δεδομένων θα πρέπει να γίνεται με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Σκοπός της αρχής της διαφάνειας είναι η δημιουργία ενός κλίματος εμπιστοσύνης μεταξύ υποκειμένων και υπεύθυνων επεξεργασίας και ο σεβασμός των υποκειμένων και των δικαιωμάτων τους. Τα βασικά στοιχεία της διαφάνειας είναι η προσβασιμότητα και η δυνατότητα κατανόησης των πληροφοριών (Ishii, 2017). Πρέπει, δηλαδή, στο πλαίσιο της αρχής της διαφάνειας να παρέχονται στο υποκείμενο με απλό και κατανοητό τρόπο όλες οι κατάλληλες πληροφορίες σχετικά με την επεξεργασία που υφίστανται τα δεδομένα του και σχετικά με τον έλεγχο που μπορεί να ασκήσει επί αυτών, διαφορετικά θα λαμβάνονται αποφάσεις που το αφορούν, τις οποίες δεν θα μπορεί να κατανοήσει αλλά ούτε και να ελέγξει (European Data Protection Supervisor, 2016). Στο πλαίσιο αυτό, μέσω της αρχής της διαφάνειας το υποκείμενο των δεδομένων είναι σε θέση να ασκήσει και τα δικαιώματα που του παρέχονται από τον ΓΚΠΔ, καθώς ενημερώνεται τόσο για την ύπαρξη τους, όσο και για τον τρόπο με τον οποίο μπορεί να τα ασκήσει, ενώ παράλληλα ενισχύεται και η λογοδοσία (Zuiderveen Borgesius, 2015).

Το βασικό εργαλείο διαφάνειας που προβλέπει ο ΓΚΠΔ είναι το δικαίωμα της ενημέρωσης των υποκειμένων που περιλαμβάνεται στα άρθρα 12-14. Συγκεκριμένα, τα άρθρα 13 και 14 προβλέπουν το ελάχιστο περιεχόμενο των πληροφοριών που πρέπει να παρέχει ο υπεύθυνος επεξεργασίας, όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται από το υποκείμενο των δεδομένων ή όταν δεν συλλέγονται από αυτό αντίστοιχα. Και στις δύο περιπτώσεις, το περιεχόμενο των πληροφοριών είναι πανομοιότυπο και περιλαμβάνει – με κάποιες μικρές διαφοροποιήσεις λόγω των διαφορετικών πηγών προέλευσης των δεδομένων – τα βασικά σημεία της επεξεργασίας (π.χ. τα στοιχεία του υπεύθυνου επεξεργασίας, τους σκοπούς της επεξεργασίας, τα

δικαιώματα του υποκειμένου κ.τ.λ.), ενώ βασική διαφορά των δύο διατάξεων αποτελεί η χρονική στιγμή κατά την οποία παρέχονται οι πληροφορίες (Zuiderveen Borgesius, 2015). Ιδιαίτερα δε, όταν πρόκειται για περίπτωση αυτοματοποιημένης ατομικής λήψης αποφάσεων του άρθρου 22 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει πληροφορίες σχετικά με «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» (άρθρο 13 παρ. 2 περ. στ και άρθρο 14 παρ. 2 περ. ζ). Στο πλαίσιο αυτό, η ενημέρωση του υποκειμένου πρέπει να παρέχεται με σαφή και απλή διατύπωση, ώστε να γίνεται αντιληπτή από τον μέσο άνθρωπο, θα πρέπει δηλαδή να αποφεύγεται η χρήση σύνθετων προτάσεων, γλωσσικών δομών και περίπλοκης νομικής ορολογίας, καθώς και να είναι οι πληροφορίες συγκεκριμένες και οριστικές και να μην διατυπώνονται με αφηρημένους ή αμφιλεγόμενους όρους ή να αφήνουν περιθώριο για διαφορετικές ερμηνείες (Ιγγλεζάκης, 2018).

Πρακτικά, στον χώρο του διαδικτύου, η υποχρέωση ενημέρωσης υλοποιείται μέσω των πολιτικών απορρήτου (ή αλλιώς των δηλώσεων προστασίας προσωπικών δεδομένων) που εμφανίζονται στο παράθυρο των χρηστών κατά την επίσκεψη τους σε μια ιστοσελίδα ή κατά την είσοδο τους για πρώτη φορά σε μια εφαρμογή ή μια πλατφόρμα. Σκοπός των πολιτικών απορρήτου είναι ακριβώς η μείωση της ασύμμετρης πληροφόρησης που υπάρχει μεταξύ υπεύθυνων επεξεργασίας και υποκειμένων σχετικά με τις πρακτικές και τις μεθόδους επεξεργασίας των δεδομένων που χρησιμοποιούν οι πρώτοι.

Επιπλέον, σύμφωνα με το άρθρο 12 του ΓΚΠΔ, στο πλαίσιο της αρχής της διαφάνειας, ο υπεύθυνος επεξεργασίας θα πρέπει να λαμβάνει τα κατάλληλα μέτρα για να παρέχει δωρεάν (άρθρο 12 παρ. 5) στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14, κατά κανόνα γραπτώς ή ηλεκτρονικώς, σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση (άρθρο 12 παρ. 1), ενώ μπορεί να χρησιμοποιεί και τυποποιημένα εικονίδια προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιαστική επισκόπηση της σκοπούμενης επεξεργασίας (άρθρο 12 παρ. 7 και Αιτιολογική Σκέψη 60). Η πτυχή αυτή της αρχής της διαφάνειας είναι ιδιαίτερα σημαντική σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το

υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν, όπως στην περίπτωση επιγραμμικής διαφήμισης (Αιτιολογική Σκέψη 58).

Εντούτοις, όπως έχει διαπιστωθεί και στα προηγούμενα κεφάλαια, ένα βασικό χαρακτηριστικό, που αποτελεί παράλληλα και έναν από τους κινδύνους των Big Data Analytics είναι η αδιαφάνεια, με αποτέλεσμα οι σύγχρονες αυτές τεχνολογίες να βρίσκονται εξ' ορισμού σε αντίθεση με την αρχή της διαφάνειας. Η αδιαφάνεια των Big Data Analytics οφείλεται κυρίως στην εγγενή πολυπλοκότητα των συστημάτων τεχνητής νοημοσύνης, καθώς και στην ανάγκη προστασίας των εμπορικών δικαιωμάτων των επιχειρήσεων – υπεύθυνων επεξεργασίας (π.χ. δικαιώματα διανοητικής ιδιοκτησίας, επαγγελματικό απόρρητο).

Όσον αφορά ειδικότερα, τα δικαιώματα των υπεύθυνων επεξεργασίας, ο ίδιος ο ΓΚΠΔ τονίζει την ανάγκη εξισορρόπησης των αντικρουόμενων συμφερόντων, αναφέροντας χαρακτηριστικά στην Αιτιολογική Σκέψη 63: «*Το δικαίωμα αυτό [το δικαίωμα πρόσβασης και ενημέρωσης του υποκειμένου των δεδομένων] δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό*». Το δικαίωμα προστασίας των προσωπικών δεδομένων δεν είναι απόλυτο δικαίωμα και θα πρέπει, επομένως, σε κάθε περίπτωση να γίνεται μια στάθμιση των δικαιωμάτων με βάση την αρχή της αναλογικότητας.

Το μεγαλύτερο ζήτημα, ωστόσο δημιουργείται από την πολυπλοκότητα των συστημάτων τεχνητής νοημοσύνης. Όπως διαπιστώνεται χαρακτηριστικά σε άρθρο του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (European Data Protection Supervisor, 2016), τα μοντέλα που δημιουργούνται από τη μηχανική μάθηση δεν είναι στις περισσότερες περιπτώσεις κατανοητά από τον άνθρωπο, καθώς τα κριτήρια που ενδεχομένως θα βρει και θα χρησιμοποιήσει ένας αλγόριθμος μηχανικής μάθησης, όσο ορθά και αν είναι, δεν μπορούν να εξηγηθούν στους ανθρώπους, γεγονός που έχει μεγάλο αντίκτυπο στην αλγοριθμική διαφάνεια. Ιδιαίτερα στις περιπτώσεις της μη επιβλεπόμενης μηχανικής μάθησης και δη των νευρωνικών δικτύων και της βαθιάς μάθησης, όπου τα συστήματα μιμούνται τη λειτουργία του ανθρώπινου εγκεφάλου, η παροχή εξηγήσεων σχετικά με τον τρόπο λειτουργίας τους είναι πολύ δύσκολη ενδεχομένως και αδύνατη (Reed, 2018), ακριβώς επειδή τα συστήματα αυτά λειτουργούν με μεγάλη αυτονομία δημιουργώντας ένα σύνθετο δίκτυο συνδέσεων και αλληλεπιδράσεων μεταξύ των δεδομένων.

Στο πλαίσιο αυτό, έχει υποστηριχθεί ότι οι υποχρεώσεις ενημέρωσης με βάση την αρχής της διαφάνειας είναι ιδιαίτερα προβληματικές και εναποθέτουν ένα πολύ μεγάλο βάρος στους υπευθύνους επεξεργασίας, ακριβώς επειδή είναι πολύ δύσκολο να εξηγήσει κανείς στον μέσο άνθρωπο που δεν κατέχει εξειδικευμένες γνώσεις, τον τρόπο με τον οποίο λειτουργούν τα Big Data Analytics (ICO, 2017). Ιδιαίτερα στις περιπτώσεις της αυτοματοποιημένης λήψης αποφάσεων (άρθρο 22 του ΓΚΠΔ), για τις οποίες ο Κανονισμός προβλέπει μεταξύ άλλων την υποχρέωση παροχής σημαντικών πληροφοριών σχετικά με τη λογική που ακολουθείται, καθίσταται ιδιαίτερα δύσκολο για τον υπεύθυνο επεξεργασίας να εξηγήσει με απλά λόγια την πολύπλοκη αναλυτική διαδικασία και τους αλγορίθμους που κρύβονται πίσω από τα Big Data Analytics.

Τα προβλήματα που δημιουργεί η πολυπλοκότητα των Big Data Analytics είναι φανερά και στην πράξη. Οι πολιτικές απορρήτου – σε αντίθεση με τα όσα επιτάσσει η αρχή της διαφάνειας - αποτελούν συνήθως μακροσκελή, τεχνικά κείμενα με νομικούς όρους, τα οποία τελικά προορίζονται για την προστασία του οργανισμού που χρησιμοποιεί τα δεδομένα και όχι για την ενημέρωση των υποκειμένων (ICO, 2017). Οι Jensen και Potts (2004) ανέλυσαν 64 πολιτικές απορρήτου εταιρειών της Αμερικής (μεταξύ των οποίων και τις πολιτικές απορρήτου της Google και του e-Bay) και διαπίστωσαν, ότι μόνο το 6% αυτών είναι αναγνώσιμο από τους χρήστες του Διαδικτύου που είχαν ολοκληρώσει την πρωτοβάθμια ή τη δευτεροβάθμια εκπαίδευση, ενώ παράλληλα το 13% των πολιτικών απορρήτου μπορούσε να γίνει κατανοητό μόνο από άτομα με μεταπτυχιακή εκπαίδευση. Παράλληλα, τα υποκείμενα των δεδομένων έρχονται καθημερινά σε επαφή με έναν τεράστιο όγκο πληροφοριών σχετικά με τη διαχείριση των δεδομένων τους, με αποτέλεσμα, αντί να ενισχύεται ο έλεγχος που ασκούν σε αυτά, να εμποδίζεται η ικανότητα τους να επεξεργαστούν τις πληροφορίες αυτές, να ξεχωρίσουν τις σημαντικές και να λάβουν αποφάσεις που ανταποκρίνονται στις προτιμήσεις τους (van Ooijen & Vrabec, 2019). Οι McDonald και Cranor (2008) διαπίστωσαν σχετικά, ότι κάθε χρήστης του διαδικτύου θα χρειαζόταν για την ανάγνωση των πολιτικών απορρήτου 201 ώρες ετησίως, ενώ η αξία του χαμένου χρόνου σε όλη την Αμερική θα ανέρχονταν ετησίως σε 781 δισεκατομμύρια δολάρια. Στο πλαίσιο αυτό, ο χρόνος που απαιτείται για την ανάγνωση όλων των πολιτικών απορρήτου με τις οποίες έρχεται σε επαφή κάθε χρήστης και η δυσκολία κατανόησης των εννοιών που περιλαμβάνονται σε αυτές έχουν ως αποτέλεσμα να μην διαβάζουν τα υποκείμενα των δεδομένων τις πολιτικές απορρήτου, αλλά να συμφωνούν αυτόματα και μηχανικά σε αυτές, προκειμένου να κάνουν χρήση της εκάστοτε ιστοσελίδας ή εφαρμογής. Έτσι, αυτή η αβίαστη αποδοχή εκτενών και σε πολλές περιπτώσεις

ακατάληπτων γενικών όρων συναλλαγής δεσμεύει τα υποκείμενα σε μια ολιστική παρακολούθηση της συμπεριφοράς τους και εντέλει οδηγεί στον έλεγχο της μέσω φαινομενικά ελεύθερων, στην ουσία όμως προεπιλεγμένων κατευθύνσεων (Πλατής, 2018).

Τα τελευταία χρόνια βέβαια, έχουν γίνει αρκετές προσπάθειες ώστε να γίνουν οι πολιτικές απορρήτου πιο φιλικές προς τα υποκείμενα των δεδομένων. Για παράδειγμα η εφημερίδα Guardian χρησιμοποιεί καρτούν για να εξηγήσει την πολιτική απορρήτου της (ICO, 2017), ακολουθώντας τη σχετική σύσταση του Κανονισμού. Η απεικόνιση των πληροφοριών μπορεί να αποτελέσει μια αποτελεσματική λύση και να ενισχύσει σημαντικά τον έλεγχο των υποκειμένων στα δεδομένα τους, ωστόσο η χρήση τους θα πρέπει να γίνεται με προσοχή, καθώς η χρήση μιας τυποποιημένης γλώσσας που δημιουργεί ένα αίσθημα εμπιστοσύνης, μπορεί να έχει ως αποτέλεσμα τα υποκείμενα των δεδομένων να μην εστιάσουν την προσοχή τους στο γεγονός ότι λαμβάνουν μέρος μόνο των πληροφοριών, με αποτέλεσμα να μην μπορέσουν εν τέλει να αντιληφθούν τι ισχύει για τα δεδομένα τους (van Ooijen & Vrabec, 2019). Γενικότερα, η απλοποίηση των πληροφοριών που παρέχονται στα υποκείμενα ενδεχομένως να μην εξυπηρετεί την ανάγκη για συνολική πληροφόρηση των υποκειμένων σχετικά με τις περίπλοκες συνέπειες της επεξεργασίας των δεδομένων τους (Solove, 2012).

Σε κάθε περίπτωση, το πρόβλημα εξακολουθεί και υπάρχει. Στην ειδική έρευνα 487α του Ευρωβαρόμετρου (European Commission, Directorate-General for Justice and Consumers, co-ordinated by the Directorate-General for Communication, 2019) διαπιστώθηκε, ότι η πλειοψηφία των πολιτών (60%) διαβάζει τις πολιτικές απορρήτου στο διαδίκτυο, εντούτοις το 47% αυτών τις διαβάζει μόνο κατά ένα μέρος και μόνο το 13% τις διαβάζει πλήρως. Σημαντικό είναι και το ποσοστό των πολιτών που δεν διαβάζουν καθόλου τις πολιτικές απορρήτου, που ανέρχεται στο 37%. Το 66% των πολιτών που δήλωσαν ότι δεν διαβάζουν ή ότι διαβάζουν μερικώς μόνο τις πολιτικές απορρήτου εναπόθεσαν το γεγονός αυτό στο μέγεθος των κειμένων, ενώ το 31% απάντησε ότι τα κείμενα είναι ασαφή και δυσνόητα.

Κατόπιν των ανωτέρω, γίνεται κατανοητό, ότι η εφαρμογή της αρχής της διαφάνειας στην πράξη εμφανίζει αρκετά προβλήματα. Στην εποχή των Big Data Analytics, οι πολιτικές απορρήτου είναι μακροσκελείς και δυσνόητες, με αποτέλεσμα οι περισσότεροι χρήστες του διαδικτύου να τις προσπερνάνε αβίαστα και κατ' επέκταση να μην είναι σε θέση – λόγω ελλιπούς πληροφόρησης- να λάβουν τις βέλτιστες αποφάσεις σχετικά με τα δεδομένα τους, αυτές που πραγματικά ανταποκρίνονται στη

βούλησή τους. Το γεγονός αυτό, σε ένα μεγάλο μέρος των περιπτώσεων, οφείλεται στην αδυναμία των υπεύθυνων επεξεργασίας που χρησιμοποιούν τα Big Data Analytics να συμμορφωθούν προς τις υποχρεώσεις τους για ενημέρωση των υποκειμένων και να εξηγήσουν με απλό, κατανοητό τρόπο τη «λογική που ακολουθείται» πίσω από τα συστήματα τεχνητής νοημοσύνης, λόγω της πολυπλοκότητάς των τελευταίων και της αδυναμίας κατανόησής τους από τον άνθρωπο. Οι Kroll et al. (2016) υποστήριξαν μάλιστα την άποψη, ότι η αξιοποίηση μιας σειράς νέων τεχνολογικών εργαλείων, χωρίς τη συνδρομή της αλγοριθμικής διαφάνειας, θα οδηγήσει σε καλύτερα αποτελέσματα, εξασφαλίζοντας τη νομιμότητα των αυτοματοποιημένων αποφάσεων. Σε κάθε περίπτωση, η πραγματικότητα έχει δείξει, ότι θα πρέπει να υπάρξουν σημαντικές αλλαγές στον τομέα αυτό, προκειμένου να αντιμετωπιστεί αποτελεσματικότερα το φαινόμενο του "μαύρου κουτιού" και όλα τα ζητήματα που συνδέονται με αυτό.

5. 4. Το άρθρο 22 του ΓΚΠΔ

Οι σύγχρονες τεχνολογικές εξελίξεις και η καθιέρωση των Big Data Analytics και τεχνικών όπως η μηχανική μάθηση διευκολύνουν όλο και περισσότερο τη δυνατότητα κατάρτισης προφίλ των υποκειμένων και τη λήψη αποφάσεων επ’ αυτών με αυτοματοποιημένο τρόπο, εντούτοις ενέχουν παράλληλα σοβαρούς κινδύνους για τα δικαιώματα, τις ελευθερίες και τα έννομα συμφέροντα των υποκειμένων (Πλατής, 2018). Στο πλαίσιο αυτό, μεγάλη σημασία παρουσιάζει το άρθρο 22 του ΓΚΠΔ, το οποίο περιλαμβάνει το δικαίωμα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, το οποίο αποτελεί συνέχεια του άρθρου 15 της προισχύουσας Οδηγίας.

Ειδικότερα, σύμφωνα με την παρ. 1 του εν λόγω άρθρου: «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 έννοια της απόφασης αφορά γενικά μια συγκεκριμένη στάση ή μέτρο που λαμβάνεται σχετικά με κάποιο άτομο και έχει σε κάποιο βαθμό δεσμευτικό αποτέλεσμα (Mendoza & Bygrave, 2017). Έτσι, η αυτοματοποιημένη λήψη αποφάσεων περιλαμβάνει σήμερα ένα μεγάλο εύρος αποφάσεων, όπως είναι η εμφάνιση αποτελεσμάτων αναζήτησης, οι συναλλαγές υψηλής συχνότητας, αποφάσεις σχετικά με τη χορήγηση ενός δανείου, διοικητικές αποφάσεις (π.χ. ποια εταιρεία θα ελεγχθεί για φορολογικές παραβάσεις) και σε κάποιον βαθμό ακόμα και δικαστικές αποφάσεις (Brkan, 2019). Στο πλαίσιο αυτό, σύμφωνα με

την ανωτέρω διάταξη του Κανονισμού, το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, λαμβανόμενη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο, όπως συμβαίνει για παράδειγμα με την αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή τις πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση (Αιτιολογική Σκέψη 71 του ΓΚΠΔ).

Στην εν λόγω διάταξη περιλαμβάνεται, εκτός από τις αυτοματοποιημένες αποφάσεις και η κατάρτιση προφίλ, καθώς αυτού του είδους η επεξεργασία έχει αποκτήσει μεγάλη σημασία στην πράξη (Voigt & Von dem Bussche, 2017). Επισημαίνεται, ότι οι δύο αυτές έννοιες δεν ταυτίζονται, καθώς μπορεί να λαμβάνονται αυτοματοποιημένες αποφάσεις με ή χωρίς την κατάρτιση προφίλ, όπως αντίστοιχα και η κατάρτιση προφίλ μπορεί να λάβει χώρα χωρίς να ακολουθήσει η αυτοματοποιημένη διαδικασία λήψης μιας απόφασης (Πλατής, 2018). Στο άρθρο 4 παρ. 4 του Κανονισμού, η κατάρτιση προφίλ ορίζεται ως «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου».

Επιπροσθέτως, στην παρ. 2 του άρθρου 22 εισάγονται κάποιες εξαιρέσεις από την απαγόρευση της αυτοματοποιημένης λήψης αποφάσεων της παρ. 1 του ίδιου άρθρου και συγκεκριμένα η παρ. 1 δεν εφαρμόζεται όταν η απόφαση: α) είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας των δεδομένων. Η αναγκαιότητα της αυτοματοποιημένης απόφασης καθορίζεται με βάση τους συμβατικούς σκοπούς στους οποίους έχουν συμφωνήσει τα μέρη (Voigt & Von dem Bussche, 2017). Σε κάθε περίπτωση το κριτήριο της αναγκαιότητας δεν μπορεί να εφαρμοστεί τόσο αυστηρά, ώστε να φτάνει τα όρια της επιτακτικότητας, δεδομένου, ότι δύσκολα θα μπορούσε να συντρέξει μια τέτοια περίπτωση στην πράξη (Mendoza & Bygrave, 2017). Σκοπός της εν λόγω προϋπόθεσης είναι να αποτρέψει την καταστρατήγηση της διάταξης της παρ. 1 με τη σύναψη ενός τυποποιημένου συμβολαίου μεταξύ του υπεύθυνου επεξεργασίας και του υποκειμένου (Mendoza & Bygrave, 2017), 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. Η εξαίρεση αυτή θα μπορούσε για παράδειγμα να εφαρμοστεί για σκοπούς παρακολούθησης και πρόληψης της απάτης και της φοροδιαφυγής σύμφωνα με τους κανονισμούς, τα πρότυπα και τις συστάσεις των θεσμικών οργάνων της Ένωσης ή των εθνικών οργάνων εποπτείας (Αιτιολογική Σκέψη 71) και γ) βασίζεται στη ρητή συγκατάθεση του υποκειμένου των δεδομένων. Η συγκατάθεση πρέπει να πληροί και σε αυτήν την περίπτωση τις προϋποθέσεις των άρθρων 6-8 του ΓΚΠΔ και πρέπει να αναφέρεται ρητά στη λήψη αποφάσεων βάσει αποκλειστικά αυτοματοποιημένης επεξεργασίας (Voigt & Von dem Bussche, 2017). Στην πράξη, για τη σύννομη εφαρμογή τέτοιου είδους μεθόδων, ιδιαίτερα σημαντική είναι η λήψη της συγκατάθεσης του υποκειμένου (Feiler, Forgó & Weigl, 2018), η οποία φυσικά και εμφανίζει τα ίδια ζητήματα που αναφέρονται και ανωτέρω (βλ. κεφάλαιο 5.3.4.1).

Στη συνέχεια, στην παρ. 3 του άρθρου 22, ο Κανονισμός θέτει κάποιους περιορισμούς για τις εξαιρέσεις των περ. α και γ της παρ. 2, προβλέποντας, ότι στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας των δεδομένων πρέπει να εφαρμόζει κατάλληλα μέτρα για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων, τουλάχιστον του δικαιώματος εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης. Στην Αιτιολογική Σκέψη 71 εδ. δ' αναφέρεται, ότι στα ανωτέρω μέτρα περιλαμβάνονται επιπλέον η ειδική ενημέρωση του υποκειμένου των δεδομένων καθώς και το δικαίωμα να λάβει αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης. Ειδικότερα, η ειδική ενημέρωση του υποκειμένου υλοποιείται μέσα από την υποχρέωση ενημέρωσης των υποκειμένων, σύμφωνα με την οποία πρέπει να παρέχονται στα υποκείμενα μεταξύ άλλων και «πληροφορίες σχετικά με 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» (άρθρο 13 παρ. 2 περ. στ' και άρθρο 14 παρ. 2 περ. ζ' του ΓΚΠΔ) (Feiler, Forgó & Weigl, 2018). Επιπροσθέτως, στην Αιτιολογική Σκέψη 71 αναφέρονται επιπλέον μέτρα που μπορούν κατά περίπτωση να εφαρμοστούν και συγκεκριμένα αναφέρονται τα εξής: «*Προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία σε σχέση με το*

υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος».

Σκοπός της ανωτέρω διάταξης είναι, όπως αναφέρει και ο Πλατής (2018) να μην λαμβάνονται αποφάσεις από μηχανές για τα υποκείμενα, οι οποίες μπορεί να επιφέρουν σε αυτά (αρνητικές ή θετικές) νομικές συνέπειες ή θα μπορούσαν να επηρεάσουν σημαντικά τη ζωή τους κατ' ανάλογο τρόπο. Παράλληλα, ο Κανονισμός θέτει αυστηρότερες προϋποθέσεις, όταν η εν λόγω επεξεργασία αφορά ευαίσθητα προσωπικά δεδομένα (άρθρο 22 παρ. 4), καθώς και όταν το υποκείμενο των δεδομένων είναι παιδί (Αιτιολογική Σκέψη 71).

Ωστόσο, από τη διατύπωση του άρθρου 22 δεν προκύπτει ευθέως εάν το δικαίωμα που παρέχεται πρέπει να ασκηθεί από το υποκείμενο των δεδομένων ή εάν πρόκειται για μια θεσμοθετημένη απαγόρευση, την οποία οι υπεύθυνοι επεξεργασίας οφείλουν να λάβουν υπόψη χωρίς προηγούμενο σχετικό αίτημα από το υποκείμενο (Brkan, 2019· Voigt & Von dem Bussche, 2017). Συγκεκριμένα, σε αντίθεση με τα υπόλοιπα δικαιώματα των υποκειμένων που προβλέπονται στον Κανονισμό (π.χ. το δικαίωμα διαγραφής ή το δικαίωμα στη λήθη), τα οποία προϋποθέτουν την άσκησή τους από το υποκείμενο, στη συγκεκριμένη περίπτωση η αρνητική διατύπωση της διάταξης («το υποκείμενο των δεδομένων…να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ»), καθώς και η εξαίρεση της ρητής συγκατάθεσης του υποκειμένου που προβλέπεται στην παρ. 2 υποδεικνύουν, ότι πρόκειται ευθέως για απαγόρευση (Mendoza & Bygrave, 2017). Από την άλλη, η χρησιμοποίηση του όρου "δικαίωμα", αλλά και η διατύπωση της παρ. 4 του εν λόγω

άρθρου, στην οποία προβλέπεται ρητή απαγόρευση τέτοιων ειδών επεξεργασίας, όταν πρόκειται για ευαίσθητα προσωπικά δεδομένα («Οι αποφάσεις που αναφέρονται στην παράγραφο 2 δεν βασίζονται στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναφέρονται στο άρθρο 9 παράγραφος 1…») υποδεικνύουν ακριβώς το αντίθετο, ότι δηλαδή πρόκειται για ένα δικαίωμα του υποκειμένου, που πρέπει να ασκηθεί σε κάθε περίπτωση από αυτό (Mendoza & Bygrave, 2017).

Σε περίπτωση που γίνει δεκτή η πρώτη ερμηνεία, τότε ενδέχεται να προκύψουν επιζήμιες συνέπειες για τα υποκείμενα, δεδομένου, ότι σε περίπτωση μη άσκησης του εν λόγω δικαιώματος θα καθίσταντο σε κάθε περίπτωση νόμιμη η λήψη αυτοματοποιημένων αποφάσεων και η κατάρτιση προφίλ, ακόμα δηλαδή και αν δεν συνέτρεχαν οι προϋποθέσεις της παρ. 2 ή αν δεν είχαν τηρηθεί οι απαραίτητες εγγυήσεις που προβλέπονται στην παρ. 3 του άρθρου 22 (Brkan, 2019). Ορθότερη, συνεπώς, φαίνεται εκείνη η ερμηνεία του άρθρου 22 που εκλαμβάνει το δικαίωμα που προβλέπεται στο άρθρο αυτό ως γενική απαγόρευση της λήψης αυτοματοποιημένων αποφάσεων, με την οποία οφείλουν να συμμορφωθούν οι υπεύθυνοι επεξεργασίας σε κάθε περίπτωση, ή τουλάχιστον ως έναν περιορισμό αυτού του είδους της επεξεργασίας (Brkan, 2019· Mendoza & Bygrave, 2017· Voigt & Von dem Bussche, 2017). Αυτή είναι και η άποψη που υιοθετεί η ομάδα εργασία του άρθρου 29 (Art. 29 WP, 2017α), σύμφωνα με την οποία στο άρθρο 22 καθιερώνεται μια γενική απαγόρευση της λήψης αποφάσεων βάσει αυτοματοποιημένης επεξεργασίας, ανεξάρτητα από το εάν το υποκείμενο έχει προχωρήσει σε κάποια σχετική ενέργεια.

Παράλληλα, το άρθρο 22 του Κανονισμού αφορά μόνο αποφάσεις που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, δεν θα πρέπει δηλαδή να υπάρχει ανθρώπινη παρέμβαση και αξιολόγηση του περιεχομένου της απόφασης. Το ζήτημα που γεννάται εν προκειμένω είναι ο βαθμός της ανθρώπινης παρέμβασης που απαιτείται για να θεωρηθεί, ότι μία απόφαση δεν λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, οπότε και δεν υπόκειται στην ανωτέρω διάταξη. Θα μπορούσαν, δηλαδή, οι υπεύθυνοι επεξεργασίας ενσωματώνοντας μια μικρή ανθρώπινη συμμετοχή στη διαδικασία λήψης της απόφασης (π.χ. με την αυτόματη αποδοχή / έγκριση της απόφασης από έναν άνθρωπο, χωρίς αυτός να επαληθεύει την ορθότητά της) να αποφύγουν την εφαρμογή του άρθρου αυτού (Brkan, 2019· Voigt & Von dem Bussche, 2017). Ορθότερη βέβαια προκρίνεται η άποψη, ότι για να θεωρηθεί, ότι μια απόφαση δεν λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας θα πρέπει να παρέχεται στον άνθρωπο η εξουσία να αξιολογήσει την απόφαση στην ουσία της και να επηρεάσει το περιεχόμενο αυτής και

να μην αποτελεί η συμμετοχή του στην εν λόγω διαδικασία ακόμα ένα διαδικαστικό βήμα (Brkan, 2019· Voigt & Von dem Bussche, 2017). Αυτήν την άποψη προκρίνει και η Ομάδα Εργασίας του άρθρου 29 (Art. 29 WP, 2017α), σύμφωνα με την οποία θα πρέπει να υπάρχει ουσιαστική επίβλεψη της διαδικασίας λήψης της απόφασης από άτομο που διαθέτει τόσο την εξουσία όσο και την ικανότητα να αλλάξει την απόφαση, προκειμένου να θεωρηθεί ότι δεν συντρέχει η περίπτωση της παρ. 1 του άρθρου 22. Σε κάθε περίπτωση βέβαια, δεν είναι ακόμα ξεκάθαρο το μέγεθος της ανθρώπινης παρέμβαση που θα ήταν απαραίτητο για να μην τύχει εφαρμογής το άρθρο 22 του ΓΚΠΔ (Voigt & Von dem Bussche, 2017).

Επιπλέον, για να τύχει εφαρμογής η εν λόγω διάταξη θα πρέπει, οι αποφάσεις που λαμβάνονται να παράγουν έννομα αποτελέσματα που αφορούν το υποκείμενο ή το επηρεάζουν σημαντικά με παρόμοιο τρόπο. Σύμφωνα με την ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2017α), μια απόφαση παράγει έννομα αποτελέσματα όταν επηρεάζει τα δικαιώματα του υποκειμένου (όπως είναι η ψήφος στις εκλογές ή το δικαίωμα να συναναστρέφεται με άλλους) καθώς και όταν επηρεάζει το νομικό καθεστώς του υποκειμένου ή τα δικαιώματά του που πηγάζουν από μία σύμβαση (π.χ. ακύρωση συμβολαίου, άρνηση εισόδου σε χώρα ή άρνηση χορήγησης υπηκοότητας). Πιο προβληματική φαίνεται, ωστόσο, η δεύτερη περίπτωση, πότε δηλαδή μια απόφαση επηρεάζει το υποκείμενο σημαντικά με παρόμοιο τρόπο. Η περίπτωση αυτή συντρέχει, όταν η απόφαση δημιουργεί για το υποκείμενο σημαντικά προβλήματα που επιφέρουν αρνητικές προσωπικές και οικονομικές συνέπειες (Voigt & Von dem Bussche, 2017). Ειδικότερα, θα πρέπει η απόφαση να μπορεί να επηρεάσει σημαντικά τις καταστάσεις, τη συμπεριφορά ή τις επιλογές του υποκειμένου, να έχει μια παρατεταμένη ή μόνιμη επίδραση στο υποκείμενο και σε ακραίες περιπτώσεις να οδηγεί σε αποκλεισμό ή σε διακρίσεις σε βάρος του (Art. 29 WP, 2017α). Στο πλαίσιο αυτό, φαίνεται, ότι τα Big Data Analytics είναι πολύ πιθανό να πληρούν τις προϋποθέσεις της συγκεκριμένης διάταξης, δεδομένης της ικανότητας τους να καταρτίζουν το προφίλ των ατόμων και να λαμβάνουν αποφάσεις σχετικές με αυτά, μέσα από την εφαρμογή αλγορίθμων σε τεράστιες βάσεις δεδομένων (ICO, 2017). Αυτό άλλωστε προκύπτει έμμεσα και από τον ίδιο τον Κανονισμό, καθώς στην Αιτιολογική Σκέψη 71 στις περιπτώσεις που επηρεάζουν σημαντικά το υποκείμενο περιλαμβάνονται ενδεικτικά η άρνηση επιγραμμικής αίτησης πίστωσης και οι πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση. Εντούτοις, δεν φαίνεται να εμπίπτουν στη διάταξη αυτή οι προσωποποιημένες διαφημίσεις, καθώς δεν θεωρείται ότι παράγουν έννομα αποτελέσματα για το υποκείμενο ή ότι το επηρεάζουν σημαντικά με παρόμοιο τρόπο

(Feiler, Forgó & Weigl, 2018· Voigt & Von dem Bussche, 2017). Σε κάθε περίπτωση βέβαια, θα πρέπει να γίνεται στάθμιση ανάλογα με τις ειδικές συνθήκες της κάθε περίπτωσης (Voigt & Von dem Bussche, 2017).

Γίνεται επομένως κατανοητό, ότι για την εφαρμογή του συγκεκριμένου άρθρου και κατ' επέκταση για την προστασία των υποκειμένων των δεδομένων απαιτείται κάθε φορά, η συνδρομή ενός μεγάλου αριθμού αορίστων προϋποθέσεων. Ακριβώς λόγω αυτής της πολυπλοκότητας του, το συγκεκριμένο δικαίωμα εφαρμόζεται σπάνια, δεν γίνεται εύκολα κατανοητό, ενώ μπορεί πολύ εύκολα να παρακαμφθεί (Mendoza & Bygrave, 2017). Παρά το γεγονός, ότι η αυτοματοποιημένη λήψη αποφάσεων στην εποχή των Big Data Analytics έχει αποκτήσει ιδιαίτερη σημασία και εμφανίζεται όλο και πιο συχνά, το δικαίωμα του άρθρου 22 του Κανονισμού (και αντίστοιχα το δικαίωμα του άρθρου 15 της προισχύουσας Οδηγίας) δεν έχουν απασχολήσει σε μεγάλο βαθμό ούτε το ΔΕΕ αλλά ούτε και τα εθνικά δικαστήρια, ενώ δεν έχουν χρησιμοποιηθεί ούτε από τις εθνικές αρχές προστασίας των προσωπικών δεδομένων, με αποτέλεσμα να έχει περιορισμένη μόνο πρακτική σημασία (Mendoza & Bygrave, 2017).

5. 4. 1. Το δικαίωμα αιτιολόγησης της απόφασης

Το μεγαλύτερο ίσως ζήτημα που έχει δημιουργηθεί σε σχέση με το άρθρο 22 του Κανονισμού και έχει διχάσει τη νομική θεωρία είναι εάν από το άρθρο αυτό σε συνδυασμό και με τις λοιπές διατάξεις του Κανονισμού καθιερώνεται το δικαίωμα επεξήγησης των αποφάσεων που λαμβάνονται βάσει αυτοματοποιημένης επεξεργασίας. Ειδικότερα, η αλγοριθμική διαφάνεια και λογοδοσία, οι οποίες έχουν αποκτήσει ιδιαίτερη σημασία με την καθιέρωση των Big Data Analytics, πρέπει να συνεπάγονται την εφαρμογή τεχνικών και επιχειρησιακών μέτρων που διασφαλίζουν τη διαφάνεια και τη μη διακριτική μεταχείριση κατά την αυτοματοποιημένη λήψη αποφάσεων (Ευρωπαϊκό Κοινοβούλιο, 2018). Το υποκείμενο των δεδομένων θα πρέπει, δηλαδή, να είναι σε θέση να κατανοήσει τα συμπεράσματα που εξάγονται για αυτό και να διαπιστώσει εάν αυτά είναι ακριβή και δίκαια (European Data Protection Supervisor, 2015). Έτσι, το δικαίωμα της αιτιολόγησης των αποφάσεων θεωρείται ως ένας πολλά υποσχόμενος μηχανισμός (Wachter, Mittelstadt & Floridi, 2017), καθώς υπόσχεται ότι θα ανοίξει το "μαύρο κουτί", ότι θα προωθήσει την αμφισβήτηση και τη διόρθωση των αποφάσεων και θα ενισχύσει τη λογοδοσία (Edwards & Veale, 2017). Στο πλαίσιο αυτό, παρά το γεγονός, ότι στον Κανονισμό προβλέπεται γενικά η παροχή εγγυήσεων για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του υποκειμένου των δεδομένων (άρθρο 22 παρ. 3), στις οποίες περιλαμβάνεται και η

ενημέρωση του υποκειμένου σχετικά με τη λογική που ακολουθείται καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων (άρθρο 13 παρ. 2 περ. στ' και άρθρο 14 παρ. 2 περ. ζ' του ΓΚΠΔ), η οποία λαμβάνει χώρα κατά κανόνα πριν τη λήψη της αυτοματοποιημένης απόφασης, εντούτοις το δικαίωμα της ex post αιτιολόγησης της ληφθείσας απόφασης δεν συμπεριλήφθηκε στο κείμενο του Κανονισμού, παρά μόνο στην Αιτιολογική Σκέψη 71, η οποία αν και χρησιμοποιείται για την ερμηνεία των διατάξεων του Κανονισμού, δεν έχει από μόνη της νομικά δεσμευτική ισχύ. Γεννάται, συνεπώς, το ερώτημά, εάν θεσπίζεται εν τέλει το εν λόγω δικαίωμα η όχι, για το οποίο και έχουν εκφραστεί πολλές και διαφορετικές απόψεις.

Αφενός, μερίδα της θεωρίας υποστηρίζει, ότι οι διατάξεις του Κανονισμού θα πρέπει να ερμηνευθούν με τέτοιο τρόπο, ώστε να παρέχεται στο υποκείμενο των δεδομένων το δικαίωμα αιτιολόγησης της απόφασης που έχει ληφθεί για αυτό βάσει αυτοματοποιημένης επεξεργασίας. Πιο συγκεκριμένα, έχει υποστηριχθεί κατ' αρχάς η άποψη, ότι το δικαίωμα αυτό πρέπει να συναχθεί από τη διατύπωση και την ερμηνεία της υποχρέωσης ενημέρωσης των υποκειμένων που προβλέπεται στα άρθρα 13 και 14 του Κανονισμού (Goodman & Flaxman, 2017· Selbst & Powles, 2018), δεδομένου, ότι στην ενημέρωση αυτή πρέπει να περιλαμβάνονται και πληροφορίες σχετικά με τα στοιχεία που χρησιμοποιήθηκαν για την κατάρτιση στον τομέα ανάλυσης μαζικών δεδομένων, έτσι ώστε να επιτρέπεται στα άτομα να κατανοούν και να παρακολουθούν τις αποφάσεις που τους αφορούν (FRA, 2018· Ευρωπαϊκό Κοινοβούλιο, 2018). Πολλά επιχειρήματα από την άλλη στηρίζονται στην ίδια την Αιτιολογική Σκέψη 71, στην οποία, εκτός από τα μέτρα που προβλέπονται και στο άρθρο 22 παρ. 3 του Κανονισμού (δηλαδή το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης από την πλευρά του υπευθύνου επεξεργασίας, έκφρασης άποψης και αμφισβήτησης της απόφασης) περιλαμβάνεται ρητά και το δικαίωμα να λάβει το υποκείμενο αιτιολόγηση της απόφασης που ελήφθη στο πλαίσιο της εν λόγω εκτίμησης (FRA, 2018· ICO, 2017). Έτσι, αν και δεν είναι από μόνη της νομικά δεσμευτική, η εν λόγω Αιτιολογική Σκέψη λειτουργεί συμπληρωματικά του άρθρου 22 και έχει έναν σαφή επιβοηθητικό ρόλο στην ερμηνεία και στον καθορισμό του θετικού δικαίου (Selbst & Powles, 2018). Στο άρθρο της Brkan (2019) υποστηρίζεται επίσης η άποψη, ότι το εν λόγω δικαίωμα συνάγεται από μια μεθοδολογική ομαδοποίηση και μια συνδυαστική ερμηνεία των σχετικών διατάξεων του Κανονισμού (άρθρο 22, Αιτιολογική Σκέψη 71, άρθρο 13 παρ. 2 περ. στ', άρθρο 14 παρ. 2 περ. ζ' και άρθρο 15 παρ. 1 περ. η'), μέθοδος που έχει χρησιμοποιηθεί στο παρελθόν και από το ίδιο το ΔΕΕ για τη δημιουργία ενός

συγκεκριμένου δικαιώματος του υποκειμένου. Η ίδια άλλωστε υποστηρίζει, ότι η διατύπωση του άρθρου 22 παρ. 3, στο οποίο περιγράφονται κατ' ελάχιστο μόνο τα μέτρα που πρέπει να εφαρμόζονται, χωρίς να αποκλείεται η εφαρμογή και άλλων, καθώς και των άρθρων 13 και 14, σύμφωνα με τα οποία η ενημέρωση του υποκειμένου πρέπει να λαμβάνει χώρα τουλάχιστον στις περιπτώσεις του άρθρου 22 παρ. 1 και 4 - χωρίς να αποκλείεται η εφαρμογή τους και για τις περιπτώσεις του άρθρου 22 παρ. 3- αποτελούν ενδείξεις της βούλησης του νομοθέτη για τη θέσπιση ενός τέτοιου δικαιώματος. Σε διαφορετική, άλλωστε περίπτωση, καθίσταται ουσιαστικά αδύνατη και η δυνατότητα άσκησης του δικαιώματος αμφισβήτησης της απόφασης από το υποκείμενο των δεδομένων, καθώς δεν θα είναι σε θέση να κρίνει την ορθότητα της απόφασης και το αν μπορεί να κινηθεί νομικά κατά αυτής στη συγκεκριμένη περίπτωση (Brkan, 2019· Mendoza & Bygrave, 2017· Selbst & Powles, 2018).

Εντούτοις, υπάρχει και έντονος αντίλογος και έχε διατυπωθεί η άποψη, ότι από τις διατάξεις του Κανονισμού δεν προκύπτει η θέσπιση ενός τέτοιου δικαιώματος. Χαρακτηριστικά, οι Wachter, Mittelstadt και Floridi (2017) διατύπωσαν την άποψη, ότι από τις διατάξεις του ΓΚΠΔ προκύπτει μόνο ένα δικαίωμα ex ante επεξήγησης του τρόπου με τον οποίο λειτουργεί το σύστημα λήψης της απόφασης και όχι μιας ex post αιτιολόγησης των αιτίων που οδήγησαν στη συγκεκριμένη κάθε φορά απόφαση. Ειδικότερα, σύμφωνα με το ανωτέρω άρθρο, η ύπαρξη ενός τέτοιου δικαιώματος δεν προκύπτει κατ' αρχήν από τη διατύπωση του άρθρου 22 παρ. 3, ενώ η αναφορά του στην Αιτιολογική Σκέψη 71 έχει μικρή μόνο σημασία, δεδομένου ότι δεν μπορεί να παράξει νομικά δεσμευτικά αποτελέσματα, μπορεί απλώς να χρησιμοποιηθεί ως οδηγός για την ερμηνεία του σχετικού άρθρου.

Παράλληλα, υποστηρίζεται, ότι το εν λόγω δικαίωμα δεν προκύπτει ούτε από την υποχρέωση ενημέρωσης των άρθρων 13 και 14, η οποία εξ' ορισμού λαμβάνει χώρα πριν από τη λήψη της οποιασδήποτε απόφασης (η υποχρέωση ενημέρωσης πρέπει να πραγματοποιείται κατά τη λήψη των δεδομένων στην περίπτωση του άρθρου 13 και το αργότερο εντός μηνός από τη συλλογή των δεδομένων στην περίπτωση του άρθρου 14) και μπορεί κατ' επέκταση να περιλαμβάνει πληροφορίες μόνο για τη λειτουργικότητα του συστήματος λήψης της απόφασης. Τέλος, υποστηρίζεται, ότι ούτε και από το άρθρο 15, στο οποίο περιλαμβάνεται το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων συνάγεται η ύπαρξη ενός δικαιώματος αιτιολόγησης της απόφασης. Παρ' όλο που στο εν λόγω δικαίωμα δεν υπάρχουν οι χρονικοί περιορισμοί που εμφανίζονται στις περιπτώσεις των άρθρων 13 και 14, εντούτοις και στην προκειμένη περίπτωση η διατύπωση του άρθρου οδηγεί στο συμπέρασμα, ότι οι

πληροφορίες που οφείλει ο υπεύθυνος επεξεργασίας να παρέχει αφορούν μόνο τον τρόπο λειτουργίας του συστήματος και όχι το σκεπτικό και τις προϋποθέσεις της εκάστοτε απόφασης.

Σε κάθε περίπτωση, οι Wachter, Mittelstadt και Floridi (2017) αφήνουν ανοιχτό το ενδεχόμενο νομολογιακής θέσπισης ενός τέτοιου δικαιώματος, μέσω της ευρείας ερμηνείας των ανωτέρω διατάξεων, ενώ παράλληλα αναγνωρίζουν και το γεγονός, ότι η άσκηση των μέτρων που προβλέπονται στο άρθρο 22 παρ. 3 ενδέχεται να μην είναι ουσιαστική, σε περίπτωση που το υποκείμενο δεν μπορεί να κατανοήσει πως λήφθηκε η απόφαση που το αφορά.

Σε κάθε περίπτωση, η εφαρμογή του δικαιώματος αιτιολόγησης της απόφασης στην πράξη θα εμφάνιζε πολλές δυσκολίες. Πράγματι, σε πολλές περιπτώσεις, δεν είναι δυνατό να κατανοήσει κανείς, τον τρόπο με τον οποίο τα συστήματα τεχνητής νοημοσύνης καταλήγουν στις αποφάσεις τους (Reillon, 2018). Ιδιαίτερα σε περιπτώσεις μηχανικής μάθησης και δη βαθιάς μάθησης, οι μεταβλητές εισόδου ενδέχεται να στερούνται κάποιας βολικής ή σαφούς ανθρώπινης ερμηνείας (Edwards & Veale, 2017). Για παράδειγμα το LinkedIn ισχυρίζεται, ότι διατηρεί πάνω από 100.000 μεταβλητές για κάθε χρήστη, μερικές από τις οποίες είναι ξεκάθαρες (όπως π.χ. ηλικία), ενώ άλλες είναι πιο αφηρημένες (π.χ. ο τρόπος αλληλεπίδρασης με την ιστοσελίδα, όπως ο χρόνος που διαβάζει ένας χρήστης ή ο χρόνος που χρειάζεται ο χρήστης για να "κλικάρει" μια επιλογή) (Edwards & Veale, 2017). Ενδέχεται, λοιπόν, να είναι ιδιαίτερα δύσκολο να παρασχεθούν εξηγήσεις για τις εν λόγω μεταβλητές, έτσι ώστε να είναι επιδεκτικές ανθρώπινης ερμηνείας (Edwards & Veale, 2017). Φυσικά, έχουν υπάρξει στη βιβλιογραφία προτάσεις για την αντιμετώπιση των ανωτέρω ζητημάτων. Χαρακτηριστικά, οι Datta, Sen και Zick (2016) πρότειναν ένα σύνολο μέτρων, μέσω των οποίων μπορεί να γίνει αντιληπτός ο βαθμός κατά τον οποίο οι μεταβλητές εισόδου επηρεάζουν το τελικό αποτέλεσμα.

Στο πλαίσιο αυτό και δεδομένης της δυσκολίας εφαρμογής ενός τέτοιου δικαιώματος στην πράξη, η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2017α) σχετικά με την υποχρέωση ενημέρωσης του υποκειμένου σχετικά με τη λογική που ακολουθείται των άρθρων 13 και 14 του Κανονισμού υιοθέτησε μια σχετικά μετριοπαθή ερμηνεία, σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας πρέπει να βρουν απλούς τρόπους για να παρέχουν στα υποκείμενα όλες τις απαραίτητες πληροφορίες σχετικά με το σκεπτικό πίσω από την απόφαση ή τα κριτήρια στα οποία στηρίχθηκε αυτή, αλλά σε καμία περίπτωση δεν υποχρεούνται να παρέχουν μια σύνθετη επεξήγηση των αλγορίθμων που χρησιμοποιήθηκαν ή να αποκαλύψουν τον

αλγόριθμο στο σύνολό του. Επιπλέον, η ομάδα εργασίας του άρθρου 29 αναφέρει ότι σε κάθε περίπτωση θα πρέπει οι παρεχόμενες πληροφορίες να είναι αρκετές, προκειμένου το υποκείμενο των δεδομένων να κατανοήσει τις αιτίες των αποφάσεων που το αφορούν, φανερώνοντας ότι και αυτή τείνει προς την αποδοχή της ύπαρξης ενός δικαιώματος αιτιολόγησης της ληφθείσας απόφασης (Art. 29 WP, 2017α).

Συνεπώς, γίνεται κατανοητό, ότι η ύπαρξη του δικαιώματος της ex post αιτιολόγησης των αποφάσεων που αφορούν τα υποκείμενα των δεδομένων δεν προκύπτει ευθέως και ξεκάθαρα από τις διατάξεις του Κανονισμού. Πράγματι, η ενσωμάτωση ενός τέτοιου δικαιώματος στο κείμενο του Κανονισμού αποτέλεσε ένα αρκετά αμφιλεγόμενο θέμα, για αυτό και αποφασίστηκε εν τέλει η τοποθέτησή του μόνο στην Αιτιολογική Σκέψη 71 (Edwards & Veale, 2017), αφήνοντας την τελική κρίση στη δικαστική κρίση του ΔΕΕ (Brkan, 2019), το οποίο και καλείται να λάβει μια απόφαση για την ύπαρξη ή όχι του εν λόγω δικαιώματος. Σε κάθε περίπτωση, όμως, θα πρέπει να ληφθούν υπόψη και οι πρακτικές δυσκολίες εφαρμογής ενός τέτοιου δικαιώματος, οι οποίες πηγάζουν από τις δυνατότητες και την πολυπλοκότητα των σύγχρονων συστημάτων τεχνητής νοημοσύνης. Πρόκειται για ένα αρκετά περίπλοκο και αμφιλεγόμενο ζήτημα, το οποίο μόνο μέσα από την εφαρμογή του στην πράξη και τη σχετική ερμηνεία των εθνικών αλλά και του ευρωπαϊκού δικαστηρίου θα επιλυθεί και θα λάβει μια ξεκάθαρη μορφή.

5. 5. Καινοτόμες διατάξεις του Κανονισμού

Όπως έχει ήδη αναφερθεί, ο Κανονισμός ήρθε να αντικαταστήσει μια ανεπίκαιρη Οδηγία, η οποία, ούσα σε εφαρμογή από το 1995, αδυνατούσε πλέον να ανταποκριθεί στις σύγχρονες τεχνολογικές εξελίξεις, όπως τα Big Data Analytics, το Διαδίκτυο των Πραγμάτων, η υπολογιστική νέφους κ.ά. Στο πλαίσιο αυτό, παρά το γεγονός, ότι διατηρήθηκαν σε μεγάλο βαθμό η δομή και ο βασικός κορμός των διατάξεων της προϊσχύουσας Οδηγίας, εντούτοις με τον Κανονισμό εισήχθησαν και πολλές νέες, καινοτόμες διατάξεις, μερικές από τις οποίες – όπως αναλύεται κατωτέρω- έχουν ιδιαίτερη σημασία στο πλαίσιο των Big Data Analytics και αφορούν τόσο την επιβολή υποχρεώσεων για τους υπεύθυνους επεξεργασίας, όσο και τη θέσπιση δικαιωμάτων για τα υποκείμενα των δεδομένων.

5.5. 1. Η αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού

Σύμφωνα με την αρχή της λογοδοσίας, η οποία προβλέπεται στο άρθρο 5 παρ. 2 του Κανονισμού, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 του ίδιου άρθρου. Ουσιαστικά, με την αρχή της λογοδοσίας εισάγεται η γενική υποχρέωση του υπεύθυνου επεξεργασίας να επιδεικνύει συμμόρφωση με τις διατάξεις του Κανονισμού, πράγμα που σημαίνει, ότι πρέπει να λαμβάνει τα μέτρα εκείνα που κρίνονται απαραίτητα για τον σκοπό αυτό και να αποδεικνύει τη συμμόρφωσή του ενώπιον των αρμόδιων αρχών (Ιγγλεζάκης, 2018). Η αρχή της λογοδοσίας εξειδικεύεται περαιτέρω μέσω των διαφόρων υλικών και οργανωτικών υποχρεώσεων που θεσπίζει ο Κανονισμός για τους υπεύθυνους επεξεργασίας (Voigt & Von dem Bussche, 2017).

Στο πλαίσιο της εν λόγω αρχής, ιδιαίτερη σημασία παρουσιάζει και η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού που προβλέπεται στο άρθρο 25, η οποία αποτελεί έναν από τους πιο υποσχόμενους μηχανισμούς για την αποτελεσματική ρύθμιση των τεχνολογικών καινοτομιών. Σκοπός της συγκεκριμένης διάταξης είναι η ενσωμάτωση της προστασίας προσωπικών δεδομένων στον σχεδιασμό και στη λειτουργία των σύγχρονων τεχνολογιών επεξεργασίας των δεδομένων, όπως είναι τα Big Data Analytics και η μείωση των κινδύνων που είναι εγγενείς μέσα σε ένα σύστημα επεξεργασίας προσωπικών δεδομένων μέσω της προληπτικής διαμόρφωσης της τεχνολογίας και της εφαρμογής τεχνικών και οργανωτικών μέτρων προστασίας των δεδομένων (Ιγγλεζάκης, 2018).

Ειδικότερα, στην παρ. 1 του εν λόγω άρθρου εισάγεται η αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό (*privacy by design*), σύμφωνα με την οποία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας θα πρέπει σε κάθε περίπτωση να λαμβάνει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία. Άλλα

μέτρα, τα οποία θα μπορούσαν ενδεχομένως να εφαρμοστούν στο πλαίσιο της εν λόγω αρχής είναι, μεταξύ άλλων, η ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το συντομότερο δυνατόν, καθώς και η διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας (Αιτιολογική Σκέψη 78 του ΓΚΠΔ).

Παράλληλα, στην παρ. 2 του ίδιου άρθρου κατοχυρώνεται η αρχή της προστασίας εξ' ορισμού (*privacy by default*), σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει, ότι εξ ορισμού υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Επιπλέον, διευκρινίζεται, ότι η υποχρέωση αυτή ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους, ενώ παράλληλα πρέπει να διασφαλίζεται ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Η διάταξη αυτή, αποτελεί εξειδίκευση της αρχής της ελαχιστοποίησης των δεδομένων (άρθρο 5 παρ. 1 περ. γ του ΓΚΠΔ) (Ιγγλεζάκης, 2018) και αποσκοπεί στην προστασία των υποκειμένων από την ευρέως χρησιμοποιούμενη πρακτική των υπεύθυνων επεξεργασίας σήμερα, να συλλέγουν όσο το δυνατόν περισσότερα δεδομένα (Voigt & Von dem Bussche, 2017). Ειδικότερα, με την εφαρμογή της εν λόγω αρχής πρέπει κατά κανόνα να επιδιώκεται η θέσπιση φιλικών προς την ιδιωτικότητα προεπιλεγμένων ρυθμίσεων κατά τη λήψη της συγκατάθεσης του υποκειμένου, έτσι ώστε να προστατεύονται εκείνα τα άτομα που δεν διαθέτουν ούτε τις απαραίτητες τεχνικές γνώσεις αλλά ούτε και τον χρόνο για να διαμορφώσουν τις ρυθμίσεις ανάλογα με τις προτιμήσεις τους (Voigt & Von dem Bussche, 2017).

Οι αρχές αυτές, οι οποίες στην πράξη κατά κανόνα λειτουργούν συμπληρωματικά, έχουν έναν προληπτικό χαρακτήρα προκειμένου να περιοριστεί και αν είναι δυνατό να εξαλειφθεί ο κίνδυνος από την εφαρμογή συστημάτων επεξεργασίας δεδομένων, καθώς και το ενδεχόμενο κατάχρησης των προσωπικών δεδομένων (Ιγγλεζάκης, 2018). Στο πλαίσιο των εν λόγω αρχών, τεχνολογικά μέτρα θα επιτρέπουν ήδη από το προκαταρκτικό στάδιο της επεξεργασίας την ανωνυμοποίηση, ψευδωνυμοποίηση ή κρυπτογράφηση δεδομένων (Πλατής, 2018), ενώ προβλέπεται, ότι

και οι δημιουργοί / παραγωγοί καινοτόμων τεχνικών μέσων οφείλουν να αναπτύσσουν εφαρμογές, υπηρεσίες και προϊόντα υπό το πρίσμα των βασικών αρχών προστασίας των δεδομένων (Αιτιολογική Σκέψη 78 του ΓΚΠΔ). Τα μέτρα που απαριθμούνται τόσο στο άρθρο 25, όσο και στο προοίμιο του Κανονισμού είναι ενδεικτικά και θα πρέπει σε κάθε περίπτωση για την εφαρμογή τους να υιοθετείται μια κινδυνοκεντρική προσέγγιση, δηλαδή θα πρέπει να λαμβάνονται τα κατάλληλα κάθε φορά μέτρα, ανάλογα με τον βαθμό κινδύνου που διέπει τις συγκεκριμένες δραστηριότητες επεξεργασίας (Ιγγλεζάκης, 2018).

Επομένως, στο πλαίσιο της ανωτέρω διάταξης δημιουργείται ένα πλέγμα υποχρεώσεων για τους υπεύθυνους επεξεργασίας, οι οποίοι οφείλουν ήδη πριν από την πραγματοποίηση της εκάστοτε επεξεργασίας αλλά και καθ' όλη τη διάρκεια αυτής, να έχουν ως σημείο αναφοράς την προστασία των προσωπικών δεδομένων και εν γένει των δικαιωμάτων των υποκειμένων και να λαμβάνουν τα κατάλληλα κάθε φορά μέτρα για τη διασφάλισή τους. Σε κάθε περίπτωση όμως, στην περίπτωση των Big Data, λόγω του μεγέθους και της ποικιλομορφίας των δεδομένων που υποβάλλονται σε επεξεργασία, σε σχεδόν πραγματικό χρόνο, παρουσιάζονται πολλές προκλήσεις (D'Acquisto et al., 2015). Για παράδειγμα, εκτός από τα ζητήματα που δημιουργούνται κατά την εφαρμογή των Big Data Analytics σε σχέση με την αρχή της ελαχιστοποίησης των δεδομένων (ανωτέρω κεφάλαιο 5.3.2), τα οποία εμφανίζονται και κατά την εφαρμογή της αρχής της προστασίας εξ' ορισμού, θα πρέπει επίσης να δίνεται ιδιαίτερη προσοχή στην αποτελεσματικότητα των μέτρων που λαμβάνονται. Χαρακτηριστικό παράδειγμα αποτελούν οι τεχνικές της ψευδωνυμοποίησης και της ανωνυμοποίησης, οι οποίες αν και προτείνονται σε πολλές περιπτώσεις από τον Κανονισμό, εντούτοις, όπως αναφέρεται και σε άλλο σημείο της παρούσας εργασίας, αποδυναμώνονται σε μεγάλο βαθμό από τις σύγχρονες τεχνολογίες, όπως τα Big Data Analytics, καθώς χάρη στις δυνατότητες που προσφέρουν είναι πλέον δυνατή σε μεγάλο βαθμό η επαναταυτοποίηση των δεδομένων.

5. 5. 2. Εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων

Ένα άλλο, πολύ σημαντικό μέτρο ενίσχυσης της συμμόρφωσης με την αρχή της λογοδοσίας, το οποίο θα επηρεάσει σε μεγάλο βαθμό και την εφαρμογή των Big Data στην πράξη, αποτελεί η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, που προβλέπεται στο άρθρο 35 του Κανονισμού. Ειδικότερα, σύμφωνα με την παρ. 1 του εν λόγω άρθρου: «Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της

επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους». Η εκτίμηση αντικτύπου αποτελεί ουσιαστικά μια διαδικασία που έχει ως σκοπό να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά αυτής και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των προσωπικών τους δεδομένων με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους (Ιγγλεζάκης, 2018). Πρακτικά, συνιστά μια μέθοδο αντιμετώπισης ή με άλλα λόγια, διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (Ιγγλεζάκης, 2018).

Η πραγματοποίηση της εκτίμησης αντικτύπου είναι υποχρεωτική, όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Στην παρ. 3 του άρθρου 35 αναφέρονται ενδεικτικά τρείς τέτοιες περιπτώσεις, στις οποίες απαιτείται η εκτίμηση αντικτύπου και συγκεκριμένα: «α) σε περίπτωση συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο, β) σε περίπτωση μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή γ) σε περίπτωση συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα».

Επιπλέον, η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2017β) παραθέτει εννέα κριτήρια (πολλά από τα οποία περιλαμβάνονται και στο προοίμιο του Κανονισμού, στην Αιτιολογική Σκέψη 91), τα οποία πρέπει να λαμβάνονται υπόψη για την αξιολόγηση της αναγκαιότητας της εκτίμησης αντικτύπου και συγκεκριμένα: α) αξιολόγηση ή βαθμολόγηση πτυχών της προσωπικότητας, ιδίως όσων αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων, περιλαμβανομένης της κατάρτισης προφίλ και προβλέψεων, β) λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα

αποτελέσματα ή έχουν βαρύνουσες συνέπειες για τα φυσικά πρόσωπα (π.χ. αποκλεισμός, διακρίσεις), γ) συστηματική παρακολούθηση ή έλεγχος των υποκειμένων, συμπεριλαμβανομένης της παρακολούθησης ενός δημόσια προσβάσιμου χώρου, δ) επεξεργασία που περιλαμβάνει ειδικές κατηγορίες δεδομένων ή δεδομένων που σχετίζονται με ποινικές καταδίκες ή παραβάσεις, ε) επεξεργασία σε μεγάλη κλίμακα με κρίσιμους παράγοντες: i) τον αριθμό των εμπλεκόμενων υποκειμένων, ii) τον όγκο και το εύρος των δεδομένων, iii) τη διάρκεια της επεξεργασίας και iv) τη γεωγραφική έκταση της επεξεργασία, στ) συνδυασμός δεδομένων από διαφορετικές πηγές για διαφορετικούς σκοπούς επεξεργασίας ή από διαφορετικούς υπεύθυνους επεξεργασίας κατά τρόπο που υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου, ζ) δεδομένα που αφορούν ευάλωτα υποκείμενα (π.χ. παιδιά, εργαζόμενοι, ασθενείς), η) καινοτόμος χρήση ή εφαρμογή τεχνολογιών ή οργανωτικών λύσεων (π.χ. Διαδίκτυο των πραγμάτων, συνδυασμένη χρήση δακτυλικών αποτυπωμάτων) και θ) όταν η επεξεργασία εμποδίζει τα υποκείμενα να ασκήσουν δικαίωμά τους ή να κάνουν χρήση μιας υπηρεσίας ή μιας σύμβασης. Συγκεκριμένα, η εκτίμηση αντικτύπου είναι υποχρεωτική, όταν πληρούνται τουλάχιστον δύο από τα ανωτέρω κριτήρια, χωρίς βέβαια να αποκλείεται να συμβεί αυτό όταν συντρέχει ένα μόνο από τα ανωτέρω. Πρέπει δηλαδή, σε κάθε περίπτωση να πραγματοποιείται μια στάθμιση του κινδύνου με βάση τις εκάστοτε ισχύουσες συνθήκες.

Παράλληλα, σύμφωνα και με τα οριζόμενα στις παρ. 4 και 5 του άρθρου 35 έχουν εκδοθεί από τις εθνικές αρχές αντίστοιχοι κατάλογοι επεξεργασιών, για τις οποίες είναι απαραίτητη η εκτίμηση αντικτύπου. Στην Ελλάδα, συγκεκριμένα, η Αρχή Προσρασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΑΠΔΠΧ) προχώρησε στην έκδοση της υπ' αριθ. 65/2018 απόφασης της που δημοσιεύθηκε στο ΦΕΚ Β΄ 1622/10-5-2019. Στο πλαίσιο αυτό, γίνεται κατανοητό, ότι οι περισσότερες εφαρμογές των Big Data Analytics που περιλαμβάνουν την επεξεργασία προσωπικών δεδομένων θα εμπίπτουν σε αυτές τις περιπτώσεις, για τις οποίες είναι υποχρεωτική η εκτίμηση αντικτύπου (ICO, 2017). Σε κάθε περίπτωση βέβαια, ακόμα και εάν υπάρχουν αμφιβολίες συνίσταται να διενεργείται η εκτίμηση αντικτύπου ούτως ή άλλως, καθώς αποτελεί ένα χρήσιμο εργαλείο συμμόρφωσης για τους υπεύθυνους επεξεργασίας (Art. 29 WP, 2017β).

Η εκτίμηση αντικτύπου διενεργείται προληπτικά, πριν δηλαδή από την έναρξη της επεξεργασίας, όπως ακριβώς και η υποχρέωση προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ' ορισμού (Ιγγλεζάκης, 2018). Σε κάθε περίπτωση, δεν αποτελεί μια διαδικασία, η οποία πραγματοποιείται εφάπαξ, αλλά ο υπεύθυνος επεξεργασίας

υποχρεούται να προβεί σε επανεξέταση για να εκτιμήσει, εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας (άρθρο 35 παρ. 11 του ΓΚΠΔ).

Παράλληλα, το ελάχιστο περιεχόμενο της εκτίμησης αντικτύπου περιλαμβάνεται στην παρ. 7 του άρθρου 35 και αποτελείται από: «α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας, β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς, γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων». Εντούτοις, στον Κανονισμό δεν ορίζεται ο ακριβής τρόπος διενέργειας της εκτίμησης αντικτύπου και οι διαδικασίες που πρέπει να ακολουθηθούν. Η ομάδα εργασίας του άρθρου 29 περιλαμβάνει στο σχετικό της άρθρο (Art. 29 WP, 2017β) μια σειρά κριτηρίων, που μπορούν να χρησιμοποιηθούν, ενώ και οι εθνικές αρχές διαφόρων χωρών έχουν εκδώσει οδηγούς για τη μεθοδολογία που πρέπει να ακολουθείται (π.χ. η γαλλική αρχή - CNIL, η βρετανική αρχή – Information Commissioner’s Office) (Ιγγλεζάκης, 2018).

Στο πλαίσιο αυτό, σύμφωνα με το άρθρο 36 παρ. 1 του Κανονισμού, όταν η δυνάμει του άρθρου 35 εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει, ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας, ο τελευταίος οφείλει να ζητήσει τη γνώμη της εποπτικής αρχής πριν από την επεξεργασία. Πρακτικά, η διαβούλευση με την εποπτική αρχή προστασίας δεδομένων θα γίνεται υποχρεωτική, όταν δεν επαρκούν τα τεχνικά και οργανωτικά μέτρα που προβλέφθηκαν στην εκτίμηση αντικτύπου για τον μετριασμό των κινδύνων (Ιγγλεζάκης, 2018).

Ωστόσο, παρά την αδιαμφισβήτητη σημασία της για την αντιμετώπιση των κινδύνων που συνεπάγονται οι σύγχρονες τεχνολογικές εξελίξεις, η εκτίμηση αντικτύπου αποτελεί σε κάθε περίπτωση μια σύνθετη διαδικασία που απαιτεί έναν συνδυασμό τεχνικών, νομικών και κοινωνιολογικών γνώσεων (FRA, 2018) και

εναποθέτει ένα μεγάλο βάρος και κόστος στους υπεύθυνους επεξεργασίας. Επιπλέον, ο Manterelo (2018) διατύπωσε την άποψη, ότι στο πλαίσιο των Big Data Analytics, όπου η επεξεργασία των δεδομένων ελλοχεύει κινδύνους όχι μόνο σε ατομικό αλλά και σε συλλογικό επίπεδο, όπως είναι για παράδειγμα οι διακρίσεις, η εκτίμηση αντικτύπου θα έπρεπε να λαμβάνει υπόψη και να τονίζει επαρκώς και τα ηθικά και τα κοινωνικά ζητήματα που ανάγονται σε αυτές τις τεχνολογίες. Αντίστοιχα και ο Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (FRA, 2018) κάνει λόγο για την ανάγκη διεξαγωγής εκτιμήσεων αντικτύπου θεμελιωδών δικαιωμάτων, προκειμένου να εντοπίζονται πιθανές διακρίσεις, προκαταλήψεις και καταχρήσεις κατά την εφαρμογή των αλγορίθμων. Από την άλλη, στο άρθρο του Binns (2017) αναφέρεται, ότι μέσα από τη νομοθετική καθιέρωση υποχρεωτικών εκτιμήσεων αντικτύπου ενδέχεται να δημιουργηθεί μια τέτοια κατάσταση, όπου οι υπόχρεοι ακολουθούν τυφλά τους κανόνες χωρίς να κατανοούν την ύπαρξή τους ή ακολουθούν αυστηρά και τυπικά το γράμμα του νόμου, υποβαθμίζοντας τον γενικότερο σκοπό που επιδιώκεται με αυτόν, με αποτέλεσμα να επικεντρώνονται περισσότερο στην απόδειξη της συμμόρφωσής τους με συγκεκριμένες διαδικασίες και όχι στη διενέργεια μιας ευέλικτης, ουσιαστικής και ολιστικής εκτίμησης κινδύνου. Σε κάθε περίπτωση, στην πράξη θα φανούν τυχόν ελλείψεις και αδυναμίες της εν λόγω διάταξης καθώς και κατά πόσο είναι αποτελεσματική.

5. 5. 3. Το δικαίωμα στη λήθη

Το δικαίωμα διαγραφής ή δικαίωμα στη λήθη προβλέπεται στο άρθρο 17 του ΓΚΠΔ. Το εν λόγω δικαίωμα, αν και δεν προβλεπόταν ρητά από την προϊσχύουσα Οδηγία, εντούτοις η ύπαρξη του είχε αναγνωριστεί από το ΔΕΕ επί τη βάση του άρθρου 12 αυτής (υπόθεση C-131/12, βλ. υπό ανωτέρω κεφάλαιο 4.2). Μέσω του δικαιώματος διαγραφής, το οποίο αποτελεί ένα από τα πιο αμφιλεγόμενα ως προς την πρακτική εφαρμογή του (Πλατής, 2018), αποσκοπείται η ενίσχυση των δικαιωμάτων των χρηστών του Διαδικτύου και η εξισορρόπηση της έλλειψης ελέγχου επί των προσωπικών τους δεδομένων, στα πλαίσια ενός Διαδικτύου, το οποίο "δεν ξεχνά ποτέ" (Ιγγλεζάκης, 2017).

Ειδικότερα, σύμφωνα με την παρ. 1 του άρθρου 17: «το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους

λόγους: α) τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία, β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α) ή το άρθρο 9 παράγραφος 2 στοιχείο α) και δεν υπάρχει άλλη νομική βάση για την επεξεργασία, γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1 και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 2, δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα, ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών που αναφέρονται στο άρθρο 8 παράγραφος 1». Στο πλαίσιο, δηλαδή, της διάταξης αυτής, το υποκείμενο των δεδομένων, εφόσον επικαλείται και μπορεί να αποδείξει την ύπαρξη ενός από τους ανωτέρω λόγους, δικαιούται να ζητήσει τη διαγραφή των δεδομένων που το αφορούν (Πλατής, 2018).

Ζήτημα γεννάται, ως προς την εφαρμογή του συγκεκριμένου δικαιώματος στα δεδομένα που έχουν εξαχθεί ή συναχθεί με βάση προσωπικά δεδομένα που έχουν ανωνυμοποιηθεί ή γενικευθεί, ως αποτέλεσμα των τεχνικών ανάλυσης που χρησιμοποιούνται στα Big Data Analytics (Rubinstein, 2012). Σύμφωνα με την έρευνα που πραγματοποιήθηκε από το Πάνελ για το μέλλον της επιστήμης και της τεχνολογίας του Ευρωαϊκού Κοινοβουλίου (Sartor & Lagioia, 2020), η άσκηση του δικαιώματος στη διαγραφή πρέπει να έχει ως αποτέλεσμα και τη διαγραφή των προσωπικών δεδομένων που έχουν συναχθεί για το υποκείμενο, όχι όμως και τα δεδομένα που έχουν συναχθεί για μια ομάδα ατόμων (όπως ένα εκπαιδευμένο αλγοριθμικό μοντέλο). Από την άλλη, ο τρόπος διαγραφής δεν ορίζεται ρητά από τον Κανονισμό, εντούτοις θα πρέπει τα δεδομένα να καταστούν μη επεξεργάσιμα, εμποδίζοντας έτσι, την καθ’ οποιονδήποτε τρόπο χρήση τους από τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία ή οποιονδήποτε τρίτο (Πλατής, 2018).

Επιπλέον, στην παρ. 2 του άρθρου 17 περιλαμβάνεται η υποχρέωση του υπεύθυνου επεξεργασίας, όταν αυτός έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται σύμφωνα με την παράγραφο 1 να τα διαγράψει, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, να λάβει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους

υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα. Ακόμα όμως και αν δεν έχει υπάρξει δημοσιοποίηση των δεδομένων από τον υπεύθυνο επεξεργασίας, αυτός έχει την υποχρέωση να ανακοινώσει κάθε διαγραφή δεδομένων που διενεργείται σύμφωνα με το άρθρο 17 παράγραφος 1 σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια, καθώς και να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τους εν λόγω αποδέκτες, εφόσον αυτό ζητηθεί από το υποκείμενο των δεδομένων (άρθρο 19 του Κανονισμού).

Το δικαίωμα διαγραφής περιορίζεται και δεν εφαρμόζονται στον βαθμό που η επεξεργασία είναι απαραίτητη: «α) για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση, β) για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας, γ) για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχεία η) και θ), καθώς και το άρθρο 9 παράγραφος 3, δ) για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1, εφόσον το δικαίωμα που αναφέρεται στην παράγραφο 1 είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη σκοπών της εν λόγω επεξεργασίας, ή ε) για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων» (άρθρο 17 παρ. 3 του ΓΚΠΔ). Για τη στοιχειοθέτηση της εν λόγω διάταξης και τον αποκλεισμό της δυνατότητας άσκησης του δικαιώματος στη λήθη, απαιτείται σε κάθε περίπτωση μια στάθμιση των αντιτιθέμενων συμφερόντων (του υποκειμένου και του υπεύθυνου), την οποία θα πρέπει να πραγματοποιεί ο υπεύθυνος επεξεργασίας, ο οποίος φέρει και το βάρος να αποδείξει την ύπαρξη μιας εκ των ανωτέρω περιπτώσεων (Voigt & Von dem Bussche, 2017).

Στο πλαίσιο του δικαιώματος στη λήθη, η μετάβαση για τις επιχειρήσεις από την εποχή της χρονικά απεριόριστης και άσκοπης αποθήκευσης των δεδομένων σε αυτή της διαγραφής τους προϋποθέτει σημαντική προσπάθεια, προκειμένου να είναι σε θέση να ικανοποιήσουν αμελλητί το εν λόγω δικαίωμα (Πλατής, 2018), με αποτέλεσμα η

αποτελεσματική εφαρμογή του να καθίσταται ιδιαίτερα δύσκολη και σε πολλές περιπτώσεις ακόμα και ακατόρθωτη (Rubinstein, 2012). Παράλληλα η άσκηση του δικαιώματος στη διαγραφή ενδέχεται να δημιουργήσει σοβαρά ζητήματα στην ανάπτυξη της τεχνητής νοημοσύνης και ιδιαίτερα στην ακρίβεια και στην αξιοπιστία των συστημάτων, δεδομένου ότι διαγράφοντας δεδομένα από το αλγοριθμικό μοντέλο ενδεχομένως να αλλάξει και ο τρόπος "συμπεριφοράς" του (Humerick, 2017), ενώ παράλληλα μπορεί να καταστεί δύσκολη και η απόδειξη της ορθότητας του μοντέλου (Sartor & Lagioia, 2020). Επιπλέον, οι σοβαρές και ενδεχομένως ακόμα και ανεπίλυτες συγκρούσεις με το δικαίωμα ελευθερίας της έκφρασης, που ενδέχεται να δημιουργήσει το δικαίωμα διαγραφής στην πράξη (Rubinstein, 2012), αναγνωρίζονται και από τον ίδιο τον Κανονισμό (μέσα από τη θέσπιση της σχετικής εξαίρεσης στην παρ. 3 περ. α του άρθρου 17).

Εντούτοις, η σημαντικότερη κριτική που έχει ασκηθεί σχετικά με το δικαίωμα στη λήθη έχει να κάνει με τη εν τοις πράγμασι δυνατότητα διαγραφής των πληροφοριών στο Διαδίκτυο, όπου όλες οι πληροφορίες αντιγράφονται με μεγάλη ευκολία, με αποτέλεσμα να καθίσταται ιδιαίτερα δυσχερές να διασφαλιστεί η διαγραφή αυτών από παντού (Politou et al., 2018). Πράγματι, σε έρευνα των Novotny και Spiekermann (2014) διαπιστώθηκε, ότι οι τεχνολογίες ενίσχυσης της λήθης που χρησιμοποιούν οι διαδικτυακές υπηρεσίες δεν παρείχαν έξυπνες δυνατότητες διαγραφής ξεπερασμένων προσωπικών πληροφοριών, με αποτέλεσμα να μην μπορούν οι χρήστες των υπηρεσιών αυτών να αποκτήσουν μακροπρόθεσμο έλεγχο επί της αποθήκευσης των προσωπικών τους δεδομένων. Αντίστοιχα, από τον Μάιο του 2014 (όταν και αναγνωρίστηκε το δικαίωμα στη λήθη από το ΔΕΕ, δυνάμει της ανωτέρω αναφερόμενης απόφασης) έως και σήμερα η Google έχει δεχθεί 975.700 αιτήματα κατάργησης δεδομένων, τα οποία αφορούσαν 3.822.506 συνδέσμους URL, εκ των οποίων το 53,4% δεν καταργήθηκε (https://transparencyreport.google.com/eu-privacy/overview).

Σε κάθε περίπτωση, παρά τις δυσκολίες που εμφανίζονται κατά την εφαρμογή του δικαιώματος στη λήθη και την κριτική που έχει ασκηθεί σχετικά με την αποτελεσματικότητά του, φαίνεται ότι αποτελεί ένα σημαντικό εργαλείο συμμόρφωσης για τις εθνικές αρχές. Πράγματι, η ελληνική ΑΠΔΠΧ επί σχετικής προσφυγής χρήστη κατά της άρνησης του φορέα εκμετάλλευσης της μηχανής αναζήτησης Google να ικανοποιήσει αίτημα κατάργησης συνδέσμου (link) από τα αποτελέσματα αναζήτησης, με βάση το ονοματεπώνυμό του έκρινε, ότι η απάντηση της Google στο υπό κρίση αίτημα του προσφεύγοντος δεν είναι νόμιμα αιτιολογημένη για ορισμένες περιπτώσεις

συνδέσμων και έδωσε εντολή κατ' εφαρμογή της διάταξης του άρθρου 58 παρ. 2 γ' του ΓΚΠΔ στην εταιρεία Google LLC, ως υπεύθυνο επεξεργασίας, να προβεί άμεσα σε κατάργησή τους (απόφαση υπ' αριθ. 25/2019) ("Δικαίωμα στη λήθη: Νέα απόφαση της ΑΠΔΠΧ για την κατάργηση συνδέσμων από τη Google", 2019). Αντίστοιχα, η σουηδική αρχή προχώρησε στην επιβολή προστίμου ύψους περίπου 7 εκατομμυρίων ευρώ στη Google, καθώς, στο πλαίσιο λειτουργίας της μηχανής αναζήτησής της, δεν εκπλήρωσε τις υποχρεώσεις της όσον αφορά το δικαίωμα διαγραφής ("Δικαίωμα στη λήθη: Πρόστιμο 7 εκατομμυρίων ευρώ στη Google για παραβίαση του GDPR", 2020).

5. 5. 4. Το δικαίωμα στη φορητότητα των δεδομένων

Το δικαίωμα στη φορητότητα αποτελεί ένα νέο δικαίωμα που προσφέρει στο υποκείμενο των δεδομένων νέες δυνατότητες ανεξαρτησίας και αυτενέργειας στον ψηφιακό κόσμο (Πλατής, 2018). Συγκεκριμένα, στο άρθρο 20 παρ. 1 του Κανονισμού προβλέπεται, ότι: «το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα». Βασικός σκοπός της εν λόγω διάταξης είναι η διασφάλιση ενός κλίματος θεμιτού ανταγωνισμού μεταξύ των παρόχων υπηρεσιών (Voigt & Von dem Bussche, 2017), μειώνοντας το κόστος αλλαγής φορέων και κατ' επέκταση αποτρέποντας ένα αποτέλεσμα εγκλωβισμού για τα υποκείμενα (Feiler, Forgó & Weigl, 2018). Έτσι, το δικαίωμα στη φορητότητα δεν αποτελεί απλώς ένα δικαίωμα προστασίας των δεδομένων, αλλά ένα οικονομικό δικαίωμα, που επιτρέπει στους καταναλωτές να μοιραστούν τον πλούτο που δημιουργείται από τα Big Data και παρακινεί τους υπεύθυνους επεξεργασίας να προσφέρουν πρόσθετες δυνατότητες και εφαρμογές στους χρήστες τους (De Hert, Papakonstantinou, Malgieri, Beslay & Sanchez, 2018).

Το πεδίο εφαρμογής της εν λόγω διάταξης είναι αρκετά περιορισμένο, καθώς ισχύει μόνο εφόσον συντρέχουν σωρευτικά οι εξής προϋποθέσεις: α) η επεξεργασία βασίζεται σε συγκατάθεση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο α ή το άρθρο 9 παράγραφος 2 στοιχείο α ή σε σύμβαση σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο β και β) η επεξεργασία διενεργείται με αυτοματοποιημένα μέσα (άρθρο 20 παρ. 1 περ. α – β) (Ιγγλεζάκης, 2018). Παράλληλα, η άσκηση του εν λόγω δικαιώματος

γίνεται με την επιφύλαξη του άρθρου 17, ενώ δεν ισχύει για την επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας (άρθρο 20 παρ. 3 του Κανονισμού). Επιπλέον, όταν, σε συγκεκριμένο σύνολο δεδομένων προσωπικού χαρακτήρα, θίγονται περισσότερα του ενός υποκείμενα των δεδομένων, το δικαίωμα λήψης των δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να θίγει τα δικαιώματα και τις ελευθερίες άλλων υποκειμένων των δεδομένων (άρθρο 20 παρ. 4 και Αιτιολογική Σκέψη 68 του ΓΚΠΔ).

Επιπροσθέτως, σύμφωνα με την παρ. 2 του άρθρου 20: «Κατά την άσκηση του δικαιώματος στη φορητότητα των δεδομένων σύμφωνα με την παράγραφο 1, το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητά την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, σε περίπτωση που αυτό είναι τεχνικά εφικτό». Η διάταξη αυτή αφορά, κατά βάση, τους παρόχους υπηρεσιών κοινωνικής δικτύωσης (*social networking sites*) και υπηρεσιών νεφοϋπολογιστικής (*cloud computing*), καθώς και ένα πλήθος διαδικτυακών εφαρμογών, εφαρμογών ευφυών συσκευών και άλλες αυτοματοποιημένες εφαρμογές (Ιγγλεζάκης, 2018). Σκοπός της συγκεκριμένης διάταξης είναι η διευκόλυνση της περίπλοκης διαδικασίας αλλαγής παρόχων, έτσι ώστε να έχουν τα υποκείμενα τη δυνατότητα να μεταφέρουν τα διαδικτυακά τους προφίλ από τη μια πλατφόρμα στην άλλη μόνο με ένα "κλικ" (Voigt & Von dem Bussche, 2017). Στο πλαίσιο αυτό, οι υπεύθυνοι επεξεργασίας θα πρέπει να ενθαρρύνονται να αναπτύσσουν διαλειτουργικούς μορφότυπους που επιτρέπουν τη φορητότητα των δεδομένων (Αιτιολογική Σκέψη 68 του ΓΚΠΔ). Θα πρέπει, δηλαδή, να αναπτύσσονται διαλειτουργικά και όχι απλώς συμβατά συστήματα, έτσι ώστε να μην απαιτείται κάποια ιδιαίτερη προσπάθεια ή γνώση από την πλευρά του χρήστη (Ιγγλεζάκης, 2018). Σε καμία περίπτωση, όμως, δεν πρέπει να δημιουργείται στους υπεύθυνους επεξεργασίας η υποχρέωση να υιοθετούν ή να διατηρούν συστήματα επεξεργασίας που είναι συμβατά από τεχνική άποψη (Αιτιολογική Σκέψη 68 του ΓΚΠΔ). Η απευθείας διαβίβαση από έναν υπεύθυνο επεξεργασίας σε άλλον μπορεί, συνεπώς, να πραγματοποιείται όταν είναι δυνατή η επικοινωνία μεταξύ δύο συστημάτων, με ασφαλή τρόπο, και όταν το λαμβάνον σύστημα είναι τεχνικά εξοπλισμένο ώστε να λαμβάνει τα εισερχόμενα δεδομένα (Art. 29 WP, 2016).

Εντούτοις, η συμμόρφωση με το δικαίωμα στη φορητότητα και ιδιαίτερα με το δικαίωμα της απευθείας διαβίβασης των δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον, ενδέχεται να καταστεί ιδιαίτερα δύσκολη για τους

υπεύθυνους επεξεργασίας, θέτοντας σε κίνδυνο τα επιχειρηματικά μυστικά και τις πρακτικές που ακολουθούν (Voigt & Von dem Bussche, 2017). Οι κίνδυνοι αυτοί αναγνωρίζονται και από την ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2016), σύμφωνα με την οποία, η διάταξη του άρθρου 20 παρ. 4 πρέπει να θεωρηθεί, ότι περιλαμβάνει και δικαιώματα, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό. Εντούτοις, σε κάθε περίπτωση ο ενδεχόμενος επιχειρηματικός κίνδυνος δεν μπορεί να αποτελέσει από μόνος του βάση για άρνηση της απάντησης σε αίτημα φορητότητας, ενώ παράλληλα οι υπεύθυνοι επεξεργασίας μπορούν να διαβιβάζουν τα δεδομένα προσωπικού χαρακτήρα που παρέχονται από τα υποκείμενα των δεδομένων σε μορφή, η οποία δεν αποκαλύπτει πληροφορίες που εμπίπτουν στο πεδίο του επαγγελματικού απορρήτου ή των δικαιωμάτων διανοητικής ιδιοκτησίας (Art. 29 WP, 2016). Θα πρέπει δηλαδή, να γίνεται μια κατά περίπτωση στάθμιση των αντικρουόμενων συμφερόντων, προκειμένου να κριθεί ένα μπορεί να ασκηθεί από το υποκείμενο το δικαίωμα στη φορητότητα ή όχι.

Παράλληλα, η εφαρμογή του εν λόγω δικαιώματος στην πράξη, δεδομένου άλλωστε ότι πρόκειται για μια τεχνολογικά ουδέτερη διάταξη, η οποία όμως απαιτεί συγκεκριμένες τεχνολογίες για την εφαρμογή της (Wong & Henderson, 2019), δυσκολεύει σε μεγάλο βαθμό τους υπεύθυνους επεξεργασίας, καθιστώντας αντίστοιχα ιδιαίτερα δύσκολη και την άσκησή του από τα υποκείμενα. Συγκεκριμένα στην έρευνα των Wong και Henderson (2019) πραγματοποιήθηκαν 230 αιτήματα φορητότας σε ένα εύρος διαφορετικών υπεύθυνων επεξεργασίας, εκ των οποίων μόνο το 74,8% ολοκληρώθηκαν με επιτυχία. Ακόμα όμως και σε αυτές τις περιπτώσεις που τα αιτήματα φορητότητας ολοκληρώθηκαν με επιτυχία, η διαδικασία υποβολής των αιτήσεων ήταν πολλές φορές πολύπλοκη, ενώ τα πολλά και διαφορετικά μορφότυπα των αρχείων που παρέχονταν από τους υπεύθυνους επεξεργασίας σε πολλές περιπτώσεις δεν πληρούσαν τις προϋποθέσεις που θέτει ο Κανονισμός («δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο»), φανερώνοντας την αδυναμία του Κανονισμού να εξηγήσει επαρκώς τον τρόπο άσκησης και εφαρμογής του δικαιώματος στη φορητότητα.

Γίνεται, επομένως, κατανοητό, ότι το δικαίωμα στη φορητότητα κατέχει μια ιδιαίτερη δυναμική, καθώς βρίσκεται στο μεταίχμιο μεταξύ του δικαίου προστασίας των δεδομένων και άλλων κλάδων του δικαίου (δίκαιο ανταγωνισμού, δίκαιο προστασίας του καταναλωτή, δίκαιο πνευματικής ιδιοκτησίας κ.τ.λ.) (De Hert et al., 2018). Η ορθή εφαρμογή του εν λόγω δικαιώματος θα μπορούσε να ενισχύσει τόσο τη

θέση των υποκειμένων και τον έλεγχο τους επί των προσωπικών τους δεδομένων, όσο και τον ανταγωνισμό μεταξύ των διάφορων παρόχων υπηρεσιών. Ωστόσο, στην πράξη, φαίνεται να υπάρχει μια σύγχυση σχετικά με τον τρόπο εφαρμογής της νέας αυτής διάταξης και των διαφόρων δικαιωμάτων που παρέχονται στα υποκείμενα, με αποτέλεσμα να εμφανίζονται διαφορετικές ερμηνείες και πρακτικές μεταξύ των υπεύθυνων επεξεργασίας, πολλές από τις οποίες εν τέλει δεν είναι συμβατές με τις απαιτήσεις του Κανονισμού.

6. Συλλογική ιδιωτικότητα

Παραδοσιακά, η νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων αλλά και γενικότερα του δικαιώματος της ιδιωτικότητας βασίζεται κυρίως στο μοντέλο των ατομικών δικαιωμάτων, μέσω των οποίων ενισχύεται ο έλεγχος και η εξουσία του υποκειμένου στα δεδομένα που το αφορούν. Το μοντέλο αυτό ακολουθείται και στις δύο πλευρές του Ατλαντικού με πολλές φυσικά διαφοροποιήσεις (Mantelero, 2017). Εντούτοις, οι κίνδυνοι που ελλοχεύει σήμερα η χρήση των Big Data Analytics απευθύνονται, όχι μόνο σε ατομικό, αλλά και σε συλλογικό επίπεδο, δεδομένων των δυνατοτήτων που παρέχουν τόσο σε ιδιωτικούς όσο και σε δημόσιους φορείς να παρακολουθούν τις συνήθειες και τις κινήσεις ολόκληρων ομάδων ατόμων, να κατηγοριοποιούν τους ανθρώπους και να προσπαθούν έτσι να αναλύσουν και να προβλέψουν τη συμπεριφορά τους (Kammourieh et al., 2017). Το φαινόμενο αυτό έχει απασχολήσει ιδιαίτερα την ακαδημαϊκή κοινότητα και έχει θεσπιστεί για αυτό η έννοια της συλλογικής ιδιωτικότητας (*group privacy*).

Ειδικότερα, τα Big Data Analytics παρέχουν νέες προσεγγίσεις σχετικά με την ομαδοποίηση και την κατηγοριοποίηση των ατόμων. Η ομαδοποίηση των ατόμων είναι μια βασική και αναπόφευκτη αρχή της αλγοριθμικής ταξινόμησης, στα πλαίσια της οποίας, οι χρήστες γίνονται αντιληπτοί μέσα από μικρά μοτίβα και συσχετισμούς με άλλους χρήστες στο σύστημα, έτσι ώστε να σχηματιστούν ουσιαστικές ομάδες (δηλαδή κλάσεις), σύμφωνα με τη συμπεριφορά τους, τις προτιμήσεις τους και διάφορα άλλα χαρακτηριστικά (Mittelstadt, 2017). Τα Big Data Analytics βασίζονται ακριβώς στην εύρεση νέων και προηγουμένως απαρατήρητων μοτίβων και συσχετισμών εντός ενός συνόλου δεδομένων, με αποτέλεσμα να δημιουργούνται μέσα από αυτή τη διαδικασία νέα μέσα για την αναγνώριση και την ομαδοποίηση των ατόμων (Kammourieh et al., 2017). Έτσι, οι αλγοριθμικά διαμορφωμένες ομάδες τείνουν να είναι πιο ρευστές και πιο δυναμικές σε σχέση με τις παραδοσιακές, κοινωνικά καθορισμένες ομάδες που τείνουν να είναι πιο στατικές (Suh, Metzger, Reid & El Abbadi, 2018).

Στο πλαίσιο αυτό, τα άτομα προσδιορίζονται μέσω της συσχέτισής τους με ad hoc, εφήμερες αλλά εύστοχες ομάδες ατόμων, τα οποία φέρονται, ότι εμφανίζουν πολλές ομοιότητες μεταξύ τους, με αποτέλεσμα, να καθίσταται ιδιαίτερα σημαντική, όχι τόσο η ταυτοποίηση του ατόμου με την παραδοσιακή σημασία (π.χ. μέσω του ονόματος του), όσο η σωστή κατηγοριοποίησή του και ο συσχετισμός του με άλλα άτομα (Mittelstadt, 2017). Έτσι, οι αποφάσεις που λαμβάνονται σχετικά με το κάθε υποκείμενο των δεδομένων / χρήστη δεν βασίζονται απαραίτητα στην ανάλυση των προηγούμενων συμπεριφορών του, αλλά στη σύγκριση και την αντίθεση της

συμπεριφοράς του με αυτή των υπολοίπων ατόμων που έχουν κατηγοριοποιηθεί στην ίδια ομάδα με αυτό (Kammourieh et al., 2017). Τα χαρακτηριστικά και η σημασία που αποδίδονται σε μια συγκεκριμένη ομάδα, αποδίδονται αυτόματα και σε κάθε άτομο που έχει καταταχθεί σε αυτήν, χωρίς να αντικατοπτρίζουν απαραίτητα και τον τρόπο με τον οποίο το ίδιο το άτομο αυτοπροσδιορίζεται, βλέπει και αντιλαμβάνεται τον εαυτό του (Mantelero, 2017). Ακόμα, δηλαδή και αν ένα άτομο δεν φέρει στην πραγματικότητα όλα τα χαρακτηριστικά που συνδέονται με μια ομάδα, εντούτοις η κατηγοριοποίηση του σε αυτήν οδηγεί αυτόματα σε μια σειρά συμπερασμάτων σχετικά με το πρόσωπό του και κατ' επέκταση στη λήψη ποικίλων αυτοματοποιημένων αποφάσεων που το αφορούν (π.χ. σχετικά με το ύψος του ασφαλίστρου στην ασφάλιση υγείας, ή την πιθανότητα αδυναμίας πληρωμών στη χορήγηση ενός δανείου).

Παράλληλα, καθίσταται ιδιαίτερα δυσχερές, να γίνει αντιληπτός ο τρόπος με τον οποίο πραγματοποιείται η αλγοριθμική ταξινόμηση και διαμορφώνονται οι διάφορες ομάδες από τα υποκείμενα, δεδομένου άλλωστε, ότι σε πολλές περιπτώσεις δυσκολεύονται και οι ίδιοι οι αναλυτές των δεδομένων να τον κατανοήσουν. Έτσι, τα υποκείμενα των δεδομένων δεν μπορούν καν να αντιληφθούν, ότι κατηγοριοποιούνται σε μια συγκεκριμένη ομάδα, ούτε και γνωρίζουν τα λοιπά άτομα που υπάρχουν σε αυτήν, καθώς και τις συνέπειες που συνεπάγεται η συμμετοχή τους σε αυτήν, με αποτέλεσμα να είναι ευάλωτα στους κινδύνους που συνεπάγονται οι σύγχρονες τεχνολογίες (π.χ. διακρίσεις) (Kammourieh et al., 2017). Το πρόβλημα επιτείνεται, εάν λάβει κανείς υπόψη του την αδιαφάνεια που ούτως ή άλλως χαρακτηρίζει τα συστήματα τεχνητής νοημοσύνης εξαιτίας των σύνθετων και εξελιγμένων τεχνολογιών που χρησιμοποιούνται (Kammourieh et al., 2017). Φαίνεται, επομένως, ότι δημιουργείται πλέον ένα συλλογικό ενδιαφέρον των ατόμων που έχουν κατηγοριοποιηθεί σε μία ομάδα, να λάβουν γνώση του τρόπου με τον οποίο δημιουργούνται και χρησιμοποιούνται οι πληροφορίες που χαρακτηρίζουν την ομάδα τους (Mittelstadt, 2017).

Στο πλαίσιο αυτό, παρ' όλο που ο Κανονισμός δεν αναφέρεται ρητά στο συγκεκριμένο θέμα, προκρίνεται σε πολλές περιπτώσεις μια τέτοια ερμηνεία των διατάξεών του, που φαίνεται, ότι λαμβάνεται υπόψη η συλλογική διάσταση των επιπτώσεων των Big Data Analytics. Πράγματι, η ομάδα εργασίας του άρθρου 29 (Art. 29 WP, 2017α), στα πλαίσια της ερμηνείας του άρθρου 22 του ΓΚΠΔ, αναφέρει μεταξύ άλλων, ότι είναι πιθανό, μια αυτοματοποιημένη απόφαση που επηρεάζει σημαντικά το υποκείμενο να είναι αποτέλεσμα των ενεργειών άλλων ατόμων και όχι του ίδιου του υποκειμένου, με αποτέλεσμα το υποκείμενο να στερείται εν τέλει ευκαιριών, εξαιτίας

της συμπεριφοράς και των πράξεων τρίτων προσώπων. Χαρακτηριστικό παράδειγμα αποτελεί η μείωση του ορίου της πιστωτικής κάρτας ενός καταναλωτή όχι με βάση το ιστορικό αποπληρωμής του ίδιου, αλλά με βάση τη συμπεριφορά των λοιπών καταναλωτών που ζουν στην ίδια περιοχή και ψωνίζουν στα ίδια καταστήματα με αυτόν. Παράλληλα, στο άρθρο του Mittelstadt (2017) αναφέρεται, ότι μεγάλη σημασία για την αναγνώριση της συλλογικής ιδιωτικότητας, έχει ο τρόπος που θα ερμηνευτούν οι διατάξεις που αφορούν τα δικαιώματα των υποκειμένων να λάβουν πληροφορίες σχετικά με τη λογική που ακολουθείται στην αυτοματοποιημένη, αλγοριθμική λήψη αποφάσεων (άρθρα 13-15 του ΓΚΠΔ). Από την άλλη, έχει διατυπωθεί έντονα από σημαντική μερίδα της θεωρίας και η άποψη, ότι πρέπει πλέον να θεσπιστεί η προστασία της ιδιωτικότητας και των προσωπικών δεδομένων σε συλλογικό επίπεδο, να αναγνωριστούν δηλαδή οι ομάδες / κλάσεις των ατόμων ως φορείς των σχετικών δικαιωμάτων και να θεσμοθετηθεί η προστασία της συλλογικής ιδιωτικότητας ως τέτοιας (Mantelero, 2017· Mittelstadt, 2017).

Κατόπιν όλων των ανωτέρω, γίνεται κατανοητό, ότι παγιωμένα στοιχεία που συνέθεταν την έννοια της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων, τίθενται υπό αμφισβήτηση στην εποχή των Big Data Analytics. Σήμερα, τα άτομα κρίνονται και είναι αποδέκτες αποφάσεων όχι με βάση τα προσωπικά τους χαρακτηριστικά και τη δική τους συμπεριφορά, ούτε καν με βάση τη συμμετοχή τους σε κάποια κοινωνική ομάδα, αλλά με βάση κάποια χαρακτηριστικά που έχουν κοινά με τα υπόλοιπα μέλη μιας αλγοριθμικά διαμορφωμένης ομάδας και τα οποία εντοπίζονται κάθε φορά από τα συστήματα τεχνητής νοημοσύνης (ICO, 2017). Στο πλαίσιο αυτό, φαίνεται ότι τα συγκεκριμένα δικαιώματα έχουν αποκτήσει πλέον μια συλλογική διάσταση, δεδομένου ότι, οι ενέργειες και η συμπεριφορά ενός ανθρώπου ενδέχεται να επηρεάσουν σημαντικά τον τρόπο που θα αντιμετωπιστεί κάποιος άλλος, που έχει κατηγοριοποιηθεί στην ίδια ομάδα με τον πρώτο, με αποτέλεσμα να καθίσταται απαραίτητη για την αποτελεσματική προστασία τους -εκτός από τη σχετική ερμηνεία και την ενίσχυση της ήδη υπάρχουσας νομοθεσίας – και η θέσπιση νέων διατάξεων, οι οποίες απευθύνονται και προστατεύουν αποκλειστικά τις ομάδες των ανθρώπων, που δημιουργούνται από την αλγοριθμική επεξεργασία μεγάλων συνόλων δεδομένων.

7. Συμπεράσματα

Τα Big Data Analytics, όπως κάθε επιστημονική και τεχνολογική καινοτομία, αποτελούν ένα εργαλείο, το οποίο μπορεί να χρησιμοποιηθεί ποικιλοτρόπως. Αφενός, οι δυνατότητες που προσφέρουν για τις σύγχρονες κοινωνίες και οικονομίες είναι αμέτρητες και εκτείνονται σε ένα μεγάλο φάσμα τομέων, όπως είναι η ποιοτική βελτίωση της καθημερινότητας των πολιτών, η ενίσχυση της οικονομίας (από τον αγροτικό τομέα έως τον τομέα της διαφήμισης και του μάρκετινγκ), η ενίσχυση του τομέα της υγείας και της εκπαίδευσης, καθώς και η διαχείριση κρίσεων. Ταυτόχρονα, τα Big Data Analytics μπορούν να χρησιμοποιηθούν με αθέμιτο τρόπο, θέτοντας σε κίνδυνο τα ανθρώπινα δικαιώματα και τις ελευθερίες, λειτουργώντας με έναν αδιαφανή και δυσνόητο τρόπο, υποσκάπτοντας τον έλεγχο των υποκειμένων επί των δεδομένων τους, αναπαράγοντας προκαταλήψεις, διακρίσεις και μεροληπτικά αποτελέσματα, έχοντας φτάσει ακόμα και στο σημείο να στερούν από τα άτομα τη δυνατότητα της ελεύθερης και συνειδητής επιλογής.

Η δυναμική αυτή των Big Data Analytics, έγινε αντιληπτή και σε ενωσιακό επίπεδο, με την Ευρωπαϊκή Ένωση να στέφει έντονα το ενδιαφέρον της στη σωστή διαχείριση των δεδομένων και της τεχνητής νοημοσύνης, έτσι ώστε να αξιοποιηθούν στο μέγιστο οι δυνατότητες που προσφέρουν, χωρίς παράλληλα να θίγονται, αλλά αντιθέτως να ενισχύονται τα θεμελιώδη ανθρώπινα δικαιώματα και οι ευρωπαϊκές αξίες. Το όραμα της Ένωσης είναι ακριβώς να πρωταγωνιστήσει στην τεχνολογική αυτή επανάσταση μέσα από τη θέσπιση δεοντολογικής, ασφαλούς και προηγμένης τεχνητής νοημοσύνης με τη σφραγίδα της Ευρώπης (ΟΕΥΕ για την ΤΝ, 2019β). Η λεγόμενη αξιόπιστη τεχνητή νοημοσύνη θα πρέπει να είναι σύννομη, δεοντολογική και στιβαρή, με σκοπό τη δημιουργία ενός κλίματος αξιοπιστίας και εμπιστοσύνης μεταξύ όλων των παραγόντων και των διεργασιών που αποτελούν μέρος του κοινωνικοτεχνικού περιβάλλοντος του συστήματος καθ’ όλη τη διάρκεια του κύκλου ζωής του (ΟΕΥΕ για την ΤΝ, 2019β).

Στο πλαίσιο αυτό, το έργο του νομοθέτη συνίσταται ακριβώς στη σωστή ρύθμιση των σύγχρονων αυτών τεχνολογιών, έτσι ώστε να προάγεται η θεμιτή χρήση τους, με απώτερο σκοπό τη συνολική αύξηση της κοινωνικής ευημερίας και την πρόοδο του κοινωνικού συνόλου. Εντούτοις, η διαμόρφωση ενός κανονιστικού πλαισίου που διασφαλίζει την ασφάλεια των χρηστών και του κοινού καθίσταται σήμερα ιδιαίτερα δύσκολη δεδομένων των σύγχρονων συνθηκών, όπου η τεχνολογική καινοτομία και η παγκόσμια διάδοση αυτής είναι πάρα πολύ γρήγορη (Fenwick, Kaal & Vermeulen, 2016). Πράγματι, ο νόμος έπεται των τεχνολογικών εξελίξεων και σε πολλές

περιπτώσεις αδυνατεί να τις προφτάσει, γεγονός που έγινε έντονα αντιληπτό στην περίπτωση της νομοθεσίας για την προστασία των προσωπικών δεδομένων. Μια προ πολλού ξεπερασμένη Οδηγία, η οποία βρισκόταν σε ισχύ ήδη από το 1995 και αδυνατούσε να συμβαδίσει με τα τεχνολογικά άλματα που σημειώνονταν τον 21ο αιώνα αντικαταστάθηκε εν τέλει με τον ισχύοντα Κανονισμό 2016/679.

Ο Κανονισμός, ο οποίος σε αντίθεση με την Οδηγία έχει καθολική δεσμευτικότητα και άμεση ισχύ, επέκτεινε το πεδίο εφαρμογής του σε σημαντικό βαθμό, υπερβαίνοντας την έννοια της εδαφικότητας (Ιγγλεζάκης, 2018) ενώ παράλληλα διεύρυνε σε μεγάλο βαθμό τις δυνατότητες των εθνικών εποπτικών αρχών, στις οποίες περιλαμβάνονται και πάρα πολύ υψηλά διοικητικά πρόστιμα (άρθρο 83 του ΓΚΠΔ). Επιπλέον, αν και κατά κανόνα διατήρησε τη δομή και το μοντέλο της προϊσχύουσας Οδηγίας, προχώρησε περαιτέρω στην υιοθέτηση καινοτόμων διατάξεων, με σκοπό ακριβώς την αντιμετώπιση των σύγχρονων τεχνολογικών προκλήσεων. Εντούτοις, η αποτελεσματική εφαρμογή του Κανονισμού στην πράξη εμφανίζει πολλές δυσκολίες, με αποτέλεσμα, σε πολλές περιπτώσεις να καθίσταται αφενός ιδιαίτερα δύσκολη για τους υπεύθυνους επεξεργασίας η συμμόρφωση με αυτόν και αφετέρου να μην διασφαλίζεται ο έλεγχος των υποκειμένων επί των δεδομένων τους και εν γένει η προστασία των δικαιωμάτων τους. Ειδικότερα, τα Big Data Analytics φαίνεται να μη συμβαδίζουν με κάποιες από τις θεμελιώδεις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ενώ η γενική και σε πολλές περιπτώσεις μη τεχνική διατύπωση του Κανονισμού δημιουργεί ζητήματα ως προς την αποτελεσματική άσκηση των δικαιωμάτων των υποκειμένων και αντίστοιχα τη συμμόρφωση των υπεύθυνων επεξεργασίας με τις υποχρεώσεις τους. Σε κάθε περίπτωση, θα πρέπει να προκρίνεται μια ξεκάθαρη και σαφής ερμηνεία των διατάξεων του Κανονισμού, η οποία θα έχει ως γνώμονα την εξισορρόπηση των συμφερόντων των υπεύθυνων επεξεργασίας αφενός και των δικαιωμάτων των υποκειμένων αφετέρου, έτσι ώστε να καταστεί δυνατή η με σεβασμό στα ανθρώπινα δικαιώματα και ελευθερίες, εκμετάλλευση των δυνατοτήτων που προσφέρουν οι σύγχρονες τεχνολογικές εξελίξεις.

Στο πλαίσιο αυτό, για την αποτελεσματική ρύθμιση του φαινομένου των Big Data Analytics, το νομικό ενδιαφέρον τα τελευταία χρόνια έχει στραφεί στην αλληλεπίδραση του δικαίου προστασίας των δεδομένων με άλλους κλάδους του δικαίου και συγκεκριμένα με το δίκαιο προστασίας του καταναλωτή και το δίκαιο ανταγωνισμού. Ειδικότερα, τα προσωπικά δεδομένα, όπως αναφέρεται και σε άλλα σημεία της παρούσας εργασίας, αποτελούν αντικείμενο συναλλαγών στη σύγχρονη ψηφιακή οικονομία, με τις επιχειρήσεις να ανταγωνίζονται για την απόκτηση και την

επεξεργασία αυτών (Costa-Cabral & Lynskey, 2017). Στο πλαίσιο αυτής της οικονομίας που έχει διαμορφωθεί γύρω από τα δεδομένα, γίνονται ιδιαίτερα εμφανείς οι δεσμοί που συνδέουν τους τρεις αυτούς κλάδους του δικαίου. Πιο συγκεκριμένα, τα τρία αυτά νομικά καθεστώτα μοιράζονται τον πρωταρχικό σκοπό της προστασίας της ευημερίας των ατόμων στη σύγχρονη οικονομία της αγοράς, δεδομένης της ασυμμετρίας δύναμης και ισχύος μεταξύ των χρηστών και των επιχειρήσεων, εντούτοις έχουν διαφορετικές στοχοθεσίες, πεδία εφαρμογής και καθεστώτα επιβολής (Botta & Wiedemann, 2019). Έτσι, στις σύγχρονες ψηφιακές οικονομίες η συμμόρφωση με ένα εκ των τριών αυτών νομικών καθεστώτων δεν συνεπάγεται αυτόματα τη συμμόρφωση και με τα άλλα δύο, ενώ αντίστοιχα δεν αποκλείεται και η αλληλοεπικάλυψη τους.

Χαρακτηριστικό παράδειγμα αποτελεί η απόφαση της Ομοσπονδιακής Αρχής Ανταγωνισμού της Γερμανίας (*Bundeskartellamt*) σχετικά με τη Facebook, η οποία έκρινε, ότι το συγκεκριμένο μέσο κοινωνικής δικτύωσης κάνει κατάχρηση της δεσπόζουσας θέσης που κατέχει στην αγορά, θέση η οποία βασίζεται στην εκτεταμένη συλλογή, στην επεξεργασία και στον συνδυασμό όχι εκείνων των δεδομένων που παράγονται από τον χρήστη της Facebook, αλλά του τεράστιου όγκου δεδομένων που συλλέγεται από τρίτες πηγές (το λεγόμενο third party tracking). Με την απόφασή της αυτή, η Ομοσπονδιακή Αρχή Ανταγωνισμού της Γερμανίας έκανε δεκτό, ότι τα δεδομένα σήμερα αποτελούν έναν αποφασιστικό παράγοντα ανταγωνισμού και χρησιμοποίησε τις διατάξεις για την προστασία των δεδομένων και την παραβίαση αυτών, ως πρότυπο για την εξέταση της καταχρηστικής εκμετάλλευσης δεδομένων με βάση τις διατάξεις του δικαίου ανταγωνισμού ("Ανταγωνισμός και προσωπικά δεδομένα: Απόφαση σταθμός της Γερμανικής Αρχής Ανταγωνισμού για την επεξεργασία δεδομένων από τη Facebook", 2019). Αντίστοιχα, η Αρχή Ανταγωνισμού της Ιταλίας (Autorità Garante della Concorrenza e del Mercato) επέβαλε πρόστιμο στη Facebook λόγω παραβιάσεως του δικαίου προστασίας του καταναλωτή και συγκεκριμένα επειδή παραπλάνησε τους καταναλωτές, υποσχόμενη κατά την εγγραφή τους στην εφαρμογή μια δωρεάν υπηρεσία, για την οποία στην πραγματικότητα λειτουργούν ως αντίτιμο τα προσωπικά δεδομένα που μεταφέρουν οι χρήστες στη Facebook, καθώς και επειδή χρησιμοποίησαν επιθετικές εμπορικές πρακτικές με σκοπό την αποθάρρυνση των χρηστών να εμποδίζουν τη μεταφορά των προσωπικών τους δεδομένων σε ιστότοπους τρίτων μερών (Botta & Wiedemann, 2019). Φαίνεται, επομένως, ότι οι τρείς αυτοί κλάδοι του δικαίου αλληλοσυμπληρώνονται σε μεγάλο βαθμό και ο συνδυασμός τους μπορεί αποτελέσει ένα αποτελεσματικό εργαλείο στη

ρύθμιση των σύγχρονων ψηφιακών οικονομιών, εξαιτίας ακριβώς της ολιστικής αυτής προσέγγισης που επιτυγχάνεται.

Καταληκτικά, με την παρούσα εργασία επιδιώκεται να δοθεί μια σαφής εικόνα της σύγχρονης πραγματικότητας, όπως αυτή έχει διαμορφωθεί με την καθιέρωση των Big Data Analytics τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα, καθώς και με τη νομική αντιμετώπιση του φαινομένου αυτού. Ο ΓΚΠΔ, ο οποίος αποτελεί το βασικότερο εργαλείο για τη ρύθμιση τέτοιου είδους τεχνολογιών, έχει φέρει δραματικές αλλαγές σε ότι έχει να κάνει με την επεξεργασία προσωπικών δεδομένων στον ευρωπαϊκό χώρο, επηρεάζοντας από τους πιο μικρούς υπεύθυνους επεξεργασίας έως τους πιο μεγάλους κολοσσούς της ψηφιακής οικονομίας. Μέσω, λοιπόν, της παρούσας εργασίας επιχειρείται μια συστηματική ανάλυση των βασικότερων διατάξεων του Κανονισμού σε σχέση με τα Big Data Analytics, με σκοπό να εντοπιστούν τυχόν ζητήματα και δυσκολίες κατά την εφαρμογή αυτών στην πράξη. Μια τέτοιου είδους ρεαλιστική αποτύπωση του τρόπου εφαρμογής του Κανονισμού μπορεί να φανεί ιδιαίτερα χρήσιμη μελλοντικά, έτσι ώστε είτε μέσω της ανάλογης ερμηνείας των σχετικών διατάξεων είτε μέσω της νομοθετικής οδού, να αξιοποιηθούν οι δυνατότητες που προσφέρουν οι διατάξεις το ΓΚΠΔ στο μέγιστο και εν τέλει να επιτευχθεί μια καλύτερη και αποτελεσματικότερη εφαρμογή του στην πράξη που θα επιτρέψει τόσο την ανάπτυξη και την αξιοποίηση των συστημάτων τεχνητής νοημοσύνης που λειτουργούν με τα Big Data, όσο και την εξασφάλιση ενός υψηλού επιπέδου προστασίας των προσωπικών δεδομένων των υποκειμένων, αλλά και εν γένει των δικαιωμάτων και των ελευθεριών τους.

8. Βιβλιογραφικές Παραπομπές

Ξενόγλωσση Βιβλιογραφία

Acquisti, A. (2014). "The Economics and Behavioral Economics of Privacy". In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (pp. 76-95). Cambridge: Cambridge University Press. doi:10.1017/CBO9781107590205.005

Acquisti, A., & Grossklags, J. (2007). "What can behavioral economics teach us about privacy". In A. Acquisti, S. Gritzalis, C. Lambrinoudakis & S. di Vimercati (Eds.), *Digital privacy: theory, technologies, and practices* (pp. 363-377). CRC Press.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. S., Sadeh, N., Schaub, F., Sleeper, M. & Wang, Y. (2017). "Nudges for privacy and security: Understanding and assisting users' choices online", *ACM Computing Surveys (CSUR)*, *50*(3), 1-41.

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). "Applications of big data to smart cities", *Journal of Internet Services and Applications*, *6*(1), 25.

Andrejevic, M., & Gates, K. (2014). "Big data surveillance: Introduction", *Surveillance & Society*, *12*(2), 185-196.

Article 29 Data Protection Working Party. (2013). *Opinion 03/2013 on purpose limitation*. Ανακτήθηκε από: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party. (2014). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*. Ανακτήθηκε από: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

Article 29 Data Protection Working Party. (2016). *Guidelines on the right to data portability*. Ανακτήθηκε από: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

Article 29 Data Protection Working Party. (2017α). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Ανακτήθηκε από: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Article 29 Data Protection Working Party. (2017β). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.* Ανακτήθηκε από: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Barocas, S., & Selbst, A. D. (2016). "Big data's disparate impact", *Calif. L. Rev., 104*, 671 - 732.

Bennett, C. J., & Bayley, R. M. (2016). "Privacy protection in the era of 'big data': regulatory challenges and social assessments". In B. van der Sloot, D. Broeders & E. Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 205-227). Amsterdam University Press / WRR.

Big Data. (n.d.). Στο Gartner Information Technology Glossary. Ανακτήθηκε από: https://www.gartner.com/en/information-technology/glossary/big-data

Binns, R. (2017). "Data protection impact assessments: a meta-regulatory approach", *International Data Privacy Law*, *7*(1), 22-35.

Blanchette, J. F., & Johnson, D. G. (2002). "Data retention and the panoptic society: The social benefits of forgetfulness", *The Information Society*, *18*(1), 33-45.

Borgesius, F. Z. (2015). "Informed consent: We can do better to defend privacy", *IEEE Security & Privacy*, *13*(2), 103-107.

Botta, M., & Wiedemann, K. (2019). "The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey", *The Antitrust Bulletin*, *64*(3), 428-446.

Bourreau, M., & De Streel, A. (2018). The regulation of personalised pricing in the digital era. *Organisation for Economic Co-operation and Development, Directorate for Financial and Enterprise Affairs*. Ανακτήθηκε από: https://one.oecd.org/document/DAF/COMP/WD(2018)150/en/pdf

Brkan, M. (2019). "Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond", *International journal of law and information technology*, *27*(2), 91-121.

Brynjolfsson, E., Hitt, L. M., & Kim, H. H. (2011). "Strength in numbers: How does data-driven decisionmaking affect firm performance?". *Available at SSRN:* https://ssrn.com/abstract=1819486

Burrell, J. (2016). "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society*, *3*(1), 1-12.

Burri, M., & Schär, R. (2016). "The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy", *Journal of Information Policy, 6*(1), 479-511.

Calo, R. (2013). "Digital market manipulation", *Geo. Wash. L. Rev., 82*, 995-1051.

Costa-Cabral, F., & Lynskey, O. (2017). "Family ties: the intersection between data protection and competition in EU Law", *Common Market Law Review, 54*(1), 11-50.

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y. A., & Bourka, A. (2015). Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. *European Union Agency for Network and Information Security (ENISA)*. Ανακτήθηκε από: https://arxiv.org/ftp/arxiv/papers/1512/1512.06000.pdf

Datatilsynet (2013). *Big Data – privacy principles under pressure*. Ανακτήθηκε από: https://www.datatilsynet.no/globalassets/global/english/big-data-engelsk-web.pdf

Datta, A., Sen, S., & Zick, Y. (2016, May). "Algorithmic transparency via quantitative input influence: Theory and experiments with learning systems". In *2016 IEEE symposium on security and privacy (SP)* (pp. 598-617). IEEE.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). "The right to data portability in the GDPR: Towards user-centric interoperability of digital services", *Computer Law & Security Review 34*(2), 193-203.

Desjardins, J. (2019). How much data is generated each day. In *World Economic Forum*. Ανακτήθηκε από: https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

Diakopoulos, N. (2016). "Accountability in algorithmic decision making", *Communications of the ACM, 59*(2), 56-62.

Edwards, L., & Veale, M. (2017). "Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for", *Duke L. & Tech. Rev., 16 (1)*, 18-84.

European Commission (2019). *High – Expert Level Group on Artificial Intelligence*. Ανακτήθηκε από: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

European Commission (2020α). *Big data*. Ανακτήθηκε από: https://ec.europa.eu/digital-single-market/en/big-data

European Commission (2020β). *Factsheet: The European Data Strategy*. Ανακτήθηκε από: https://ec.europa.eu/commission/presscorner/detail/en/fs_20_283

European Commission (2020γ). *Shaping Europe's digital future*. Ανακτήθηκε από: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en

European Commission (2020δ). *Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence*. Ανακτήθηκε από: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273

European Commission, Directorate-General for Justice and Consumers, co-ordinated by the Directorate-General for Communication. (2019). *Special Eurobarometer 487a - The General Data Protection Regulation*. Ανακτήθηκε από: https://ec.europa.eu/commfrontoffice/publicopinionmobile/index.cfm/Survey/getSurveyDetail/surveyKy/2222

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1 Adopted on 4 May 2020*. Ανακτήθηκε από: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

European Data Protection Supervisor (2015). *Opinion 7/2015: Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*. Ανακτήθηκε από: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

European Data Protection Supervisor (2016) *Artificial intelligence, robotics, privacy and data protection: room document for the 38th data protection and privacy commissioners*. Ανακτήθηκε από: https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

European Union Agency for Fundamental Rights (2018). *#BigData: Discrimination in data-supported decision making.* Ανακτήθηκε από: https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

Federal Trade Commission (2015). *Internet of things: Privacy & security in a connected world.* Ανακτήθηκε από: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Feiler, L., Forgó, N., & Weigl, M. (2018). *The EU General Data Protection Regulation (GDPR): A Commentary*. Globe Law and Business

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2016). "Regulation tomorrow: what happens when technology is faster than the law", *Am. U. Bus. L. Rev., 6*, 561-594.

Froomkin, A. M. (2019). "Big Data: Destroyer of Informed Consent". *Yale Journal of Health Policy, Law, and Ethics, Forthcoming*.

Fuster, G. G., & Scherrer, A. (2015). Big Data and smart devices and their impact on privacy. *European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE), Directorate-General for Internal Policies.* Ανακτήθηκε από: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU%282015%29536455_EN.pdf

Gandomi, A., & Haider, M. (2015). "Beyond the hype: Big data concepts, methods, and analytics", *International journal of information management, 35*(2), 137-144.

Goodman, B., & Flaxman, S. (2017). "European Union regulations on algorithmic decision-making and a "right to explanation", *AI magazine, 38*(3), 50-57.

Granville, K. (2018). "Facebook and Cambridge Analytica: What you need to know as fallout widens", *The New York Times, 19*, 18.

Hermstruwer, Y. (2017). "Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data", *J. Intell. Prop. Info. Tech. & Elec. Com. L., 8*, 9-26.

Hirsch, D. D. (2019). "From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics", *79 Maryland Law Review 439-505 (2020).*

Hoofnagle, C. J., & Urban, J. M. (2014). "Alan Westin's privacy homo economicus", *Wake Forest L. Rev., 49*, 261-317.

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law, 28*(1), 65-98.

Humerick, M. (2017). "Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence", *Santa Clara High Tech. LJ, 34*, 393-418.

Hurley, M., & Adebayo, J. (2016). "Credit scoring in the era of big data", *Yale JL & Tech., 18*, 148-216.

Information Commissioner's Office (2017). *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. Ανακτήθηκε από: https://ico.org.uk/media/fororganisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

Ipsos, London Economics, Deloitte (2018). Consumer market study on online market segmentation through personalised pricing/offers in the European Union. *European Commission, Directorate-General for Justice and Consumers, Consumers, Health, Agriculture and Food Executive Agency (Chafea). Luxembourg: Publications Office of the European Union, 2018*. Ανακτήθηκε από: https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf

Ishii, K. (2017). "Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects", *AI & SOCIETY*, 34, 509–533.

Jagdev, G. (2019). "Exploring Influence of Big Data Analytics in Retail Sector", *International Journal of Research Studies in Computer Science and Engineering, 6*(1), 1-5.

Jensen, C., & Potts, C. (2004, April). "Privacy policies as decision-making tools: an evaluation of online privacy notices". In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 471-478).

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). "Defaults, framing and privacy: Why opting in-opting out", *Marketing Letters, 13*(1), 5-15.

Jolls, C., & Sunstein, C. R. (2006). "Debiasing through law", *The Journal of Legal Studies, 35*(1), 199-242.

Kalapesi, C. (2013). Unlocking the value of personal data: From collection to usage. In *World Economic Forum technical report*. Ανακτήθηκε από: http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

Kammourieh, L., Baar, T., Berens, J., Letouzé, E., Manske, J., Palmer, J., Sangokoya, D. & Vinck, P. (2017). "Group privacy in the age of big data". In L. Taylor, L. Floridi & B. Van der Sloot (Eds.), *Group privacy: New challenges of data technologies (Vol. 126)* (pp. 37-66). Springer.

Kilovaty, I. (2019). "Legally Cognizable Manipulation", *Berkeley Tech LJ, 34*, 449-502.

Kitchin, R. (2014). "Big Data, new epistemologies and paradigm shifts", *Big data & society, 1*(1), 1-12.

Kitchin, R., & McArdle, G. (2016). "What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets", *Big Data & Society, 3*(1), 1-10.

Klous, S. (2016). "Sustainable harvesting of the big data potential". In B. van der Sloot, D. Broeders & E. Schrijvers (Eds.), *Exploring the Boundaries of Big Data* (pp. 27-48). Amsterdam University Press / WRR.

Kokott, J., & Sobotta, C. (2013). "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law, 3*(4), 222-228.

Koops, B. J. (2014). "The trouble with European data protection law", *International data privacy law, 4*(4), 250-261.

Kroll, J. A., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2016). "Accountable algorithms", *U. Pa. L. Rev., 165*, 633-705.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). "Deep learning", *nature, 521*(7553), 436-444.

Lenz, R. (2019). "Big Data: Ethics and Law". *Available at SSRN:* https://ssrn.com/abstract=3459004

Machuletz, D., & Böhme, R. (2020). "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR", *Proceedings on Privacy Enhancing Technologies 2020*(2), 481-498.

Manheim, K. M., & Kaplan, L. (2018). "Artificial Intelligence: Risks to Privacy and Democracy", *21 Yale J.L. & Tech. 106 (2019),* 106-188.

Mantelero, A. (2017). "From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era". In L. Taylor, L. Floridi & B. Van der Sloot (Eds.), *Group privacy: New challenges of data technologies (Vol. 126)* (pp. 139-158). Springer.

Mantelero, A. (2018). "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", *Computer Law & Security Review, 34*(4), 754-772.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). "Big IoT data analytics: architecture, opportunities, and open research challenges", *IEEE Access, 5*, 5247-5261.

Mayer-Schönberger, V., & Padova, Y. (2016). “Regime Change? Enabling Big Data through Europe’s New Data Protection Regulation”. *Science and Technology Law Review, 17*(2), 315-335.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

McDonald, A. M., & Cranor, L. F. (2008). “The cost of reading privacy policies”, *Isjlp, 4*, 543-568.

Mehta, N., & Pandit, A. (2018). “Concurrence of big data analytics and healthcare: A systematic review”, *International journal of medical informatics, 114*, 57-65.

Mendoza, I., & Bygrave, L. A. (2017). “The right not to be subject to automated decisions based on profiling”. In T. E. Synodinou, P. Jougleux, C. Markou & T. Prastitou (Eds.), *EU internet law: Regulation and enforcement.* (pp. 77-98). Springer.

Mittelstadt, B. (2017). “From individual to group privacy in big data analytics”, *Philosophy & Technology, 30*(4), 475-494.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). “The ethics of algorithms: Mapping the debate”, *Big Data & Society, 3*(2), 1-21.

Moerel, E. M. L. (2014). *Big data protection: How to make the draft EU Regulation on Data Protection Future Proof*. Tilburg University. Ανακτήθηκε από: https://www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf

Muller, C. (2017). Artificial intelligence–The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society. *Opinion. European Economic and Social Committee*. Ανακτήθηκε από: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). “The privacy paradox: Personal information disclosure intentions versus behaviors”, *Journal of Consumer Affairs, 41*(1), 100-126.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). “Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence”. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).

Novotny, A., & Spiekermann, S. (2014). "Oblivion on the web: an inquiry of user needs and technologies". *In Proceedings of the European Conference on Information Systems (ECIS)*, Tel Aviv, Israel, June 9-11, 2014. Ανακτήθηκε από: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1175&context=ecis2014

Organisation for Economic Cooperation and Development, Directorate for Financial and Enterprise Affair, Competition Committee (2016). *Price discrimination. Background note by the Secretariat*. Ανακτήθηκε από: https://one.oecd.org/document/DAF/COMP(2016)15/en/pdf

Politou, E., Alepis, E., & Patsakis, C. (2018). "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions", *Journal of Cybersecurity*, *4*(1), 1-20.

Raghupathi, W., & Raghupathi, V. (2014). "Big data analytics in healthcare: promise and potential", *Health information science and systems*, *2*(1), 3.

Raguseo, E. (2018). "Big data technologies: An empirical investigation on their adoption, benefits and risks for companies", *International Journal of Information Management*, *38*(1), 187-195.

Rauhofer, J. (2015). "Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle", *Eur. Data Prot. L. Rev.*, *1*, 5-15.

Reding, V. (2012). "The European data protection framework for the twenty-first century", *International Data Privacy Law*, *2*(3), 119-129.

Reed, C. (2018). "How should we regulate artificial intelligence?", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), 1-12.

Reillon, V. (2018). Understanding artificial intelligence. *European Parliament. [Online]*. Ανακτήθηκε από: https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614654/EPRS_BRI%282018%29614654_EN.pdf

Robertson, V. H. (2020). "Excessive data collection: Privacy considerations and abuse of dominance in the era of big data ", *Common Market Law Review*, *57*(1), 161-190.

Rocher, L., Hendrickx, J. M., & De Montjoye, Y. A. (2019). "Estimating the success of re-identifications in incomplete datasets using generative models", *Nature communications*, *10*(1), 1-9.

Rouvroy, A. (2016). ‘Of data and men. ’Fundamental rights and freedoms in a world of big data. In *Report for the Council of Europe, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*. Ανακτήθηκε από: https://rm.coe.int/16806a6020

Rubinstein, I. (2012). “Big data: the end of privacy or a new beginning?”, *International Data Privacy Law (2013 Forthcoming)*, 12-56.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. (2019, July). “Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control ”. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (pp. 340-351).

Sartor, G. & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *A Study for the Panel for the Future of Science and Technology (STOA), managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.* Ανακτήθηκε από: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

Schermer, B. W., Custers, B., & van der Hof, S. (2014). “The crisis of consent: How stronger legal protection may lead to weaker consent in data protection”, *Ethics and Information Technology*, *16*(2), 171-182.

Schwab, K., Marcus, A., Oyola, J. O., Hoffman, W., &Luzi, M. (2011). Personal data: The emergence of a new asset class. In *An Initiative of the World Economic Forum*. Ανακτήθηκε από: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Selbst, A., & Powles, J. (2018, January). “Meaningful Information and the Right to Explanation”. In *Conference on Fairness, Accountability and Transparency* (pp. 48-48). PMLR.

Skiena, S. S. (2017). *The data science design manual*. Springer.

Solove, D. J. (2012). “Introduction: Privacy self-management and the consent dilemma”, *Harv. L. Rev.*, *126*, 1880-1903.

Suh, J. J., Metzger, M. J., Reid, S. A., & El Abbadi, A. (2018). “Distinguishing group privacy from personal privacy: The effect of group inference technologies on

privacy perceptions and behaviors". *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-22.

Susser, D. (2019). "Notice After Notice-and-Consent: Why Privacy Disclosures Are Valuable Even If Consent Frameworks Aren't", *Journal of Information Policy*, 9, 148-173.

Susser, D., Roessler, B., & Nissenbaum, H. (2018). "Online manipulation: Hidden influences in a digital world", *Georgetown Law Technology Review, 4(1),* 1-45.

Susser, D., Roessler, B., & Nissenbaum, H. (2019). "Technology, autonomy, and manipulation", *Internet Policy Review,* 8(2), 1-22.

Tene, O., & Polonetsky, J. (2012). "Big data for all: Privacy and user control in the age of analytics", *Nw. J. Tech. & Intell.Prop.*, *11*, 239-273.

Tsaoussi, A. (2014). *Bounded Rationality,* Encyclopedia of Law and Economics, edited by Prof. Jürgen Backhaus (Springer 2014).

Tsesis, A. (2014). "The right to erasure: Privacy, data brokers, and the indefinite retention of data", *Wake Forest L. Rev.*, *49*, 433-484.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). "(Un) informed Consent: Studying GDPR Consent Notices in the Field". In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 973-990).

van Ooijen, I., & Vrabec, H. U. (2019). "Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective", *Journal of consumer policy*, *42*(1), 91-107.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR). A Practical Guide* (1st Ed). Cham: Springer International Publishing.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). "Why a right to explanation of automated decision-making does not exist in the general data protection regulation", *International Data Privacy Law*, *7*(2), 76-99.

Wong, J., & Henderson, T. (2019). "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *International Data Privacy Law*, *9*(3), 173-191.

Woodcock, R. A. (2016). "Big data, price discrimination, and antitrust", *Hastings LJ*, *68*, 1371-1420.

Yilmazkuday, H. (2020). Stay-at-Home Works to Fight Against COVID-19: International Evidence from Google Mobility Data. *Available at SSRN*: https://ssrn.com/abstract=3571708

Zarsky, T. Z. (2016). "Incompatible: the GDPR in the age of big data", *Seton Hall L. Rev., 47,* 995-1020.

Zigurat Global Institute of Technology (2019). *SMART CITY SERIES: THE BARCELONA EXPERIENCE*. Ανακτήθηκε από: https://www.e-zigurat.com/blog/en/smart-city-barcelona-experience/

Zuiderveen Borgesius, F. (2015). Improving privacy protection in the area of behavioural targeting. *Available at SSRN*: https://ssrn.com/abstract=2654213

Ελληνόγλωσση Βιβλιογραφία

Ανταγωνισμός και προσωπικά δεδομένα: Απόφαση σταθμός της Γερμανικής Αρχής Ανταγωνισμού για την επεξεργασία δεδομένων από το Facebook (2019, Φεβρουάριος 7). Ανακτήθηκε από: https://www.lawspot.gr/nomika-nea/antagonismos-kai-prosopika-dedomena-apofasi-stathmos-tis-germanikis-arhis-antagonismoy

Βέργου, Ε. (2019, Μάρτιος 9). «Πώς γινόμαστε εμπόρευμα»: Ο άνθρωπος που ξεσκέπασε την Cambridge Analytica αποκαλύπτει. *CNN Greece.* Ανακτήθηκε από: https://www.cnn.gr/focus/story/168148/sk-pos-ginomaste-emporeyma-o-anthropos-poy-xeskepase-tin-cambridge-analytica-apokalyptei

Δικαίωμα στη λήθη: Νέα απόφαση της ΑΠΔΠΧ για την κατάργηση συνδέσμων από τη Google (2019, Αύγουστος 21). Ανακτήθηκε από: https://www.lawspot.gr/nomika-nea/dikaioma-sti-lithi-nea-apofasi-tis-apdph-gia-tin-katargisi-syndesmon-apo-ti-google

Δικαίωμα στη λήθη: Πρόστιμο 7 εκατομμυρίων ευρώ στη Google για παραβίαση του GDPR (2020, Μάρτιος 12). Ανακτήθηκε από: https://www.lawspot.gr/nomika-nea/dikaioma-sti-lithi-prostimo-7-ekatommyrion-eyro-sti-google-gia-paraviasi-toy-gdpr

Ευρωπαϊκή Επιτροπή (2014). COM(2014) 442 - ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ. *Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα.* Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52014DC0442&from=EL

Ευρωπαϊκή Επιτροπή (2017). COM(2017) 9- ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ

ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ. *«ΟΙΚΟΔΟΜΗΣΗ ΜΙΑΣ ΕΥΡΩΠΑΪΚΗΣ ΟΙΚΟΝΟΜΙΑΣ ΔΕΔΟΜΕΝΩΝ»*. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017DC0009&from=EL

Ευρωπαϊκή Επιτροπή (2018). COM(2018) 237 - ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΕΥΡΩΠΑΪΚΟ ΣΥΜΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ *Τεχνητή νοημοσύνη για την Ευρώπη*. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52018DC0237&from=EN

Ευρωπαϊκή Επιτροπή (2018). COM(2018) 795 - ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ - *Συντονισμένο σχέδιο για την τεχνητή νοημοσύνη*. Ανακτήθηκε από: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0023.02/DOC_1&format=PDF

Ευρωπαϊκή Επιτροπή (2020). COM(2020) 65 - *ΛΕΥΚΗ ΒΙΒΛΟΣ Τεχνητή νοημοσύνη - Η ευρωπαϊκή προσέγγιση της αριστείας και της εμπιστοσύνης*. Ανακτήθηκε από: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_el_1.pdf

Ευρωπαϊκή Επιτροπή (2020). COM(2020) 66 - ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ - *Ευρωπαϊκή στρατηγική για τα δεδομένα*. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52020DC0066&from=EL

Ευρωπαϊκό Κοινοβούλιο (2018). *(2018/C 263/10) - Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 14ης Μαρτίου 2017 σχετικά με τις επιπτώσεις των μαζικών δεδομένων στα θεμελιώδη δικαιώματα: ιδιωτική ζωή, προστασία δεδομένων, μη διακριτική μεταχείριση, ασφάλεια και επιβολή του νόμου (2016/2225(INI)).* Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, C 263, 61ο έτος, 82-90. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:C:2018:263:FULL&from=EL

Ιγγλεζάκης, Ι. (2018). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων* (2η έκδοση). Interactive Books

Ιγγλεζάκης, Ι. Δ. (2017, Ιανουάριος 18). Το δικαίωμα στη λήθη: Ένα νέο ψηφιακό δικαίωμα για τον Κυβερνοχώρο. Ανακτήθηκε από: https://www.lawspot.gr/nomika-blogs/ioannis_igglezakis/dikaioma-sti-lithi-ena-neo-psifiako-dikaioma-gia-ton-kyvernohoro#footnote7_x8i64zs

Ιγγλεζάκης, Ι. Δ. (2020). "Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων (Data Protection Impact Assessment). Δικαιοπολιτική θεώρηση ενός καινοτόμου εργαλείου προστασίας της ιδιωτικότητας στον 21ο αιώνα", *Επιθεώρηση Δικαίου Πληροφορικής*, *1*(1).

Μπούκης, Α. (2019). Τι είναι οι data brokers και πως εκμεταλλεύονται τα προσωπικά δεδομένα των καταναλωτών. Ανακτήθηκε από: https://www.capital.gr/me-apopsi/3377427/ti-einai-oi-data-brokers-kai-pos-ekmetalleuontai-ta-prosopika-dedomena-ton-katanaloton

Ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη. (2019α). *Ορισμός της τεχνητής νοημοσύνης: κύριες δυνατότητες και επιστημονικά πεδία*. Ανακτήθηκε από: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη. (2019β). *ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΓΙΑ ΑΞΙΟΠΙΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ.* Ανακτήθηκε από: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EL.pdf

Πλατής, Ε. (2018). *Προσωπικά Δεδομένα Προστασία GDPR* (1η έκδοση). Αθήνα: Εκδόσεις Παπαδόπουλος

Τσαούση, Α. (2018). *Θεσμοί, Δίκαιο και Κοινωνία: Κρίσιμες διατομές υπό το φως μιας βιωματικής θεώρησης* (1η έκδοση). Εκδόσεις Παπαζήση

ΠΑΡΑΡΤΗΜΑ - ΝΟΜΟΘΕΣΙΑ ΚΑΙ ΝΟΜΟΛΟΓΙΑ

Νομοθεσία και Ήπιο Δίκαιο

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. (1950, Νοέμβριος 4). Ανακτήθηκε από: https://www.echr.coe.int/Documents/Convention_ELL.pdf

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). (2016). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, L 119, 59ο έτος, 1-88. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EL

Νόμος 4624/2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις, Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ 137/Α/29-8-2019)

ΟΔΗΓΙΑ 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. (1995). Επίσημη Εφημερίδα τον Ευρωπαϊκών Κοινοτήτων, L 281, 31-50. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=DA

Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης. (1980). Κατευθυντήριες Γραμμές για την προστασία του απορρήτου και των διασυνοριακών ροών προσωπικών δεδομένων. Ανακτήθηκε από: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων. (1981, Ιανουάριος

28). Ανακτήθηκε από: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2016/C 202/02). Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, C 202, 59ο έτος, 389-405. Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=EL

Νομολογία και αποφάσεις εθνικών αρχών

European Court of Justice Case C - 131/12. *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González.* (2014). Digital reports (Court Reports - general). Ανακτήθηκε από: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Απόφαση 25/2019 - *Προσφυγή κατά της άρνησης του φορέα εκμετάλλευσης της μηχανής αναζήτησης Google να ικανοποιήσει αίτημα κατάργησης συνδέσμου (link) από τα αποτελέσματα αναζήτησης, με βάση το ονοματεπώνυμο του προσφεύγοντα.* (2019). Ανακτήθηκε από: https://www.dpa.gr/portal/page?_pageid=33%2C15453&_dad=portal&_schema=PORTAL&_piref33_15473_33_15453_15453.etos=2019&_piref33_15473_33_15453_15453.arithmosApofasis=&_piref33_15473_33_15453_15453.thematikiEnotita=-1&_piref33_15473_33_15453_15453.ananeosi=%CE%91%CE%BD%CE%B1%CE%BD%CE%AD%CF%89%CF%83%CE%B7

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Απόφαση 65/2018 - *Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντίκτυπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ*. (2019). Εφημερίς της Κυβερνήσεως της Ελληνικής Δημοκρατίας (ΦΕΚ Β΄ 1622/10-5-2019).