ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

THE GDPR INTERFERENCE WITH 5G / IOT NETWORKS, AI AND BIG DATA ANALYTICS

Διπλωματική Εργασία

της

Γεωργίας Καλαμαρά

Θεσσαλονίκη, Μάρτιος 2022

THE GDPR INTERFERENCE WITH 5G / IOT NETWORKS, AI AND BIG DATA ANALYTICS

Γεωργία Καλαμαρά

Πτυχίο Νομικής,ΑΠΘ,2017

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 03/03/2022

ΨΑΝΝΗΣ	ΜΥΛΩΣΗ	ΜΑΝΤΑΣ
ΚΩΝΣΤΑΝΤΙΝΟΣ	ΜΑΡΙΑ	ΜΙΧΑΗΛ
.....	.....	.....

Γεωργία Καλαμαρά

Περίληψη

Οι συνεχώς αναδυόμενες νέες τεχνολογίες όπως το 5G, η AI, το IoT και τα Big Data, που φαίνεται να αναπτύσσονται ταχύτερα από το νομικό πλαίσιο που τις περιβάλλει, έχουν φέρει στο επίκεντρο τη συζήτηση περί δεοντολογίας. Ως αποτέλεσμα, δημιουργήθηκε ένα νέο ηθικό πλαίσιο σε μια προσπάθεια ρύθμισης της προστασίας των ανθρωπίνων δικαιωμάτων, της ιδιωτικής ζωής και ατομικής αυτονομίας. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ (ΓΚΠΔ), ο οποίος τέθηκε σε ισχύ τον Μάιο του 2018, παρέχει ουσιαστική καθοδήγηση για την επίτευξη δίκαιης ισορροπίας μεταξύ των συμφερόντων των νέων αναδυόμενων τεχνολογιών και των χρηστών. Η συνύπαρξη συχνά προκαλεί ασυμμετρίες, καθιστώντας ζωτικής σημασίας την ανάδειξη των παρεμβάσεων του ευρωπαϊκού κανονισμού στις νέες τεχνολογίες, προκειμένου να βρεθεί η χρυσή τομή για την επίτευξη του απαιτούμενου πλαισίου προστασίας των προσωπικών δεδομένων. Η παρούσα έρευνα παρέχει μια παρουσίαση του περιεχομένου αυτών των τεχνολογιών και του ΓΚΠΔ, μέσω της ανασκόπησης ακαδημαϊκής βιβλιογραφίας, με στόχο την ανάδειξη της σημασίας αυτών, ξεχωριστά. Χαρτογραφεί έπειτα, τα σημεία σύγκρουσης μεταξύ της προστασίας των δεδομένων και της φύσης των νέων τεχνολογιών και εστιάζει στην αντίθεση των τελευταίων με ορισμένες βασικές αρχές του ΓΚΠΔ όπως (1) η συναίνεση, (2) η ελαχιστοποίηση δεδομένων και (3) η διαφάνεια. Η μελέτη καταλήγει στο συμπέρασμα ότι οι βασικές αρχές του ΓΚΠΔ, συμπεριλαμβανομένων των βελτιωμένων τεχνικών κρυπτογράφησης, ανωνυμοποίησης και ψευδωνυμοποίησης, καθώς και της προστασίας της ακεραιότητας των αποθηκευμένων προσωπικών δεδομένων, απαιτούνται επειγόντως ήδη από το στάδιο του σχεδιασμού.

Λέξεις Κλειδιά: GDPR, 5G, Internet of Things, Big Data Analytics, Artificial Intelligence

Abstract

The constantly emerging new technologies such as 5G, AI, IoT and Big Data analytics, which seem to be developing faster than the legal framework around them, have brought the ethics debate into focus. These challenges have created an ethical framework in an attempt to regulate the protection of human rights, as well as privacy and individual autonomy. The EU General Data Protection Regulation (GDPR), which came into force in May 2018, provides essential guidance for striking a fair balance between the interests of new emerging technologies and users. Coexistence often causes asymmetries, making it vital to highlight the interventions of the European regulation in new technologies in order to find the golden ratio to achieve the required data protection framework. This research provides a presentation of the content of these technologies and the GDPR, through a review of academic literature, with the aim of highlighting their importance individually. It then maps the points of conflict between data privacy and the nature of new technologies, and focuses on the latter's contrast with some key principles of the GDPR such as (1) consent, (2) data minimisation (3) and transparency. The study concludes that the key principles of GDPR, including improved encryption, anonymization and pseudonymization techniques, as well as protection of the integrity of stored personal data, are urgently required from the design stage.

Keywords: GDPR, 5G, Internet of Things, Big Data Analytics, Artificial Intelligence

Πίνακας περιεχομένων

Εισαγωγή

Για πρώτη φορά στην ιστορία η πλειοψηφία των ανθρώπων είναι συνδεδεμένη, με τους χρήστες του διαδικτύου να ξεπερνούν πλέον τα 4 δισεκατομμύρια. Όπως συμβαίνει με κάθε μεγάλη αλλαγή, έτσι και τώρα με τη χρήση του διαδικτύου, επέρχονται σημαντικές προκλήσεις και κίνδυνοι, μεταξύ των οποίων και θέματα που αφορούν την ιδιωτικότητα και την προστασία των προσωπικών δεδομένων των χρηστών. Παρόλα αυτά κάθε κίνδυνος μπορεί να δημιουργήσει και ευκαιρίες για βελτίωση συνθηκών. Έτσι, η ανάλυση δεδομένων μεγάλου όγκου γνωστή ως big data analytics, μπορεί να χρησιμοποιηθεί και για την πρόβλεψη φυσικών καταστροφών έχοντας ως συνέπεια τη διάσωση πολιτών ενώ, η εικονική πραγματικότητα (virtual reality) που γνωρίζει ταχύτατη ανάπτυξη λόγω της εξέλιξης της Τεχνητής Νοημοσύνης (AI), μπορεί να χρησιμοποιηθεί ακόμα και για την εκπαίδευση εργαζομένων, όπως για παράδειγμα προκειμένου να βοηθήσει χειρούργους να πραγματοποιούν επεμβάσεις με μηδενικό ρίσκο για τον ασθενή. Η προστασία δεδομένων δεν θα μπορούσε να μην βρίσκεται στο προσκήνιο της σχέσης ανάμεσα στη χρήση των τεχνολογιών αυτών και το νόμο, χάρη στο γεγονός ότι πολλές εφαρμογές τους περιλαμβάνουν την επεξεργασία πολύ μεγάλου όγκου προσωπικών δεδομένων[1]. Το 2018 η Ευρωπαϊκή Ένωση (EU) παρουσίασε τον Γενικό Κανονισμό για την Προστασία των Προσωπικών δεδομένων (EU) 2016/679 (GDPR), που έχει χαρακτηριστεί ως ο «πιο σκληρός νόμος για την ιδιωτικότητα και την ασφάλεια στον κόσμο».

Η ανάγκη για τη δημιουργία του Κανονισμού ήταν πλέον εμφανής καθώς τα υποκείμενα των δεδομένων μπορεί μεν να εξέφραζαν ανησυχίες σχετικά με τον αντίκτυπο που έχει στην ιδιωτική τους ζωή αλόγιστη χρήση των δεδομένων τους, αλλά στην πράξη συνέχιζαν να συνεισφέρουν τα δεδομένα τους ούτως ή άλλως, μέσω των συστημάτων και εφαρμογών που χρησιμοποιούσαν πλέον όλο και περισσότερο, παρέχοντας - και παραχωρώντας- τα προσωπικά τους δεδομένα, επειδή αυτό θεωρείται ως “τίμημα” της χρήσης υπηρεσιών διαδικτύου, με ορισμένες μελέτες να έχουν ήδη στο παρελθόν επισημάνει αυτό το "παράδοξο της ιδιωτικής ζωής". Στην πράξη ωστόσο, μήπως πράγματι οι χρήστες του διαδικτύου δεν έχουν άλλη επιλογή από το

[1]Kritikos,Mihalis, 2020. GDPR And AI: Making Sense Of A Complex Relationship.

να συνάψουν μια "ασυνείδητη σύμβαση" για να επιτρέψουν τη χρήση των δεδομένων τους;

Αυτό ήταν και το συμπέρασμα μελέτης που έγινε σε Αμερικανούς καταναλωτές από το Annenberg School for Communication. Η εν λόγω μελέτη, επέκρινε την άποψη ότι οι καταναλωτές συνεχίζουν να παρέχουν τα προσωπικά τους δεδομένα επειδή επιλέγουν συνειδητά τη συμμετοχή στην ανταλλαγή αυτών των δεδομένων με άλλα οφέλη, όπως εκπτώσεις και κατέληξε στο συμπέρασμα ότι οι περισσότεροι Αμερικανοί θεωρούν μάταιο να προσπαθούν να ελέγξουν τι ακριβώς είναι σε θέση να μάθουν οι εταιρείες για αυτούς. Οι καταναλωτές – υποκείμενα των δεδομένων δεν ήθελαν να χάσουν τον έλεγχο των προσωπικών τους δεδομένων και απλώς συμβιβάστηκαν με την κατάσταση αυτή, ενώ σε ορισμένες περιπτώσεις, το γεγονός ότι συνεχίζουν να χρησιμοποιούν υπηρεσίες που εξάγουν και αναλύουν τα προσωπικά τους δεδομένα, μπορεί επίσης να σημαίνει ότι επενδύουν ένα ορισμένο επίπεδο εμπιστοσύνης σε αυτούς τους οργανισμούς, ιδίως σε εκείνους που είναι μεγάλοι πάροχοι υπηρεσιών ή οικεία εμπορικά σήματα- με την πεποίθηση ότι οι εν λόγω οργανισμοί δε θα προβούν σε οποιαδήποτε ‘κακή’ χρήση των παρεχόμενων δεδομένων. Ο συμβιβασμός αυτός κρίνεται ρεαλιστικός, δεδομένης της πρακτικής δυσκολίας ανάγνωσης και κατανόησης των όρων και προϋποθέσεων ελέγχου της χρήσης των δεδομένων τους. Υποχρεώνει όμως ταυτόχρονα, τον εκάστοτε οργανισμό να ασκήσει ορθή διαχείριση των δεδομένων, ανταποκρινόμενος στην εμπιστοσύνη των υποκειμένων των δεδομένων;

Το 2015 η έκθεση Digital Trends της Microsoft, σημείωσε μια τάση που ονόμασε "Δικαίωμα στην ταυτότητά μου". Καταγράφοντας ότι πλέον, αντί να επιθυμούν απλώς να διαφυλάξουν την ιδιωτική τους ζωή μέσω της ανωνυμίας, ένα σημαντικό ποσοστό των παγκόσμιων καταναλωτών- υποκειμένων δεδομένων εξέφρασε την επιθυμία να μπορεί να ελέγχει πόσο καιρό θα παραμείνουν στο διαδίκτυο οι πληροφορίες που έχουν μοιραστεί και να επιδεικνύει ενδιαφέρον, για τις υπηρεσίες που παρέχουν βοήθεια στη διαχείριση της ψηφιακής ταυτότητας. Αυτό υποδηλώνει τις συνεχώς αυξανόμενες προσδοκίες σχετικά με τον τρόπο με τον οποίο οι οργανισμοί θα χρησιμοποιούν τα δεδομένα τους, ενώ το γεγονός ότι οι καταναλωτές- υποκείμενα δεδομένων συνεχίζουν να παρέχουν τα προσωπικά τους δεδομένα και να χρησιμοποιούν υπηρεσίες που τα συλλέγουν από αυτούς, δεν σημαίνει και απαραίτητα ότι είναι ευχαριστημένοι με τον τρόπο χρήσης των δεδομένων τους ή ότι απλώς

αδιαφορούν. Παρόλο που αρκετά υποκείμενα δεδομένων φαίνεται να έχουν συμβιβαστεί με μια κατάσταση επί της οποίας αισθάνονται ότι δεν έχουν πραγματικό έλεγχο, ήδη από το 2015 υπήρχαν στοιχεία για τις ανησυχίες που εκφράζουν σχετικά με τη χρήση των δεδομένων, αλλά και για την επιθυμία τους να έχουν μεγαλύτερο έλεγχο στον τρόπο χρήσης των δεδομένων τους.[2]

Άραγε ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) είναι σε θέση να δώσει λύση στις ανησυχίες των υποκειμένων των δεδομένων και να διαμορφώσει ένα ρυθμιστικό πλαίσιο, που θα παρέχει την απαιτούμενη προστασία από τις ραγδαίως εξελισσόμενες νέες τεχνολογίες και την τάση τους να "καταναλώνουν" όλο και περισσότερα δεδομένα;

Πρόσφατες μελέτες δείχνουν ότι οι άνθρωποι παράγουν 2,5 πεντάκις εκατομμύρια bytes δεδομένων κάθε μέρα, με το ποσό αυτό να αυξάνεται περισσότερο μελλοντικά. Ο τεράστιος όγκος πληροφοριών που μπορεί να αντληθεί από αυτά τα δεδομένα δικαιολογεί την προσπάθεια των περισσότερων επιχειρήσεων να φτάσουν αυτή τη συνεχώς αυξανόμενη καμπύλη εξέλιξης. Ενώ η ηθική παραδοσιακά εξελίσσεται σε μεγάλο χρονικό διάστημα, οι προκλήσεις που αντιμετωπίζει το ανθρώπινο είδος από την επιτάχυνση του αντικτύπου, του πεδίου εφαρμογής νεών τεχνολογιών και της ταχύτητας εξέλιξής τους, μας οδηγούν στο συμπέρασμα ότι στις σύγχρονες κοινωνίες συχνά δεν θα υπάρχει αυτή η πολυτέλεια. Στην Τέταρτη Βιομηχανική επανάσταση, τα ηθικά διλήμματα που σχετίζονται με την ιδιωτικότητα θα ανακύπτουν συχνότερα και το ερώτημα είναι, εάν ο Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών δεδομένων μπορεί να αποτελέσει ισχυρή ασπίδα προστασίας για τα δεδομένα των χρηστών.

1. Ορισμοί

1.1 Δεδομένα, Data

Με βάση το Πανεπιστήμιο του Cambridge ως δεδομένα ορίζονται πληροφορίες, ιδίως γεγονότα ή αριθμοί, που συλλέγονται για να εξεταστούν, να μελετηθούν και να

[2] Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2

χρησιμοποιηθούν για τη λήψη αποφάσεων, ή πληροφορίες σε ηλεκτρονική μορφή που μπορούν να αποθηκευτούν και να χρησιμοποιηθούν από υπολογιστή.[3]

1.2 Προσωπικά Δεδομένα, Personal Data

Δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή αναγνωρίσιμο ζωντανό άτομο. Διαφορετικές πληροφορίες, οι οποίες συγκεντρωμένες μαζί μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου προσώπου, συνιστούν δεδομένα προσωπικού χαρακτήρα.[4]

Για τον ΓΚΠΔ προστασίας χρήζουν τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία των εν λόγω δεδομένων. Ο ΓΚΠΔ παραμένει τεχνολογικά ουδέτερος και τίθεται σε ισχύ τόσο για την αυτοματοποιημένη όσο και για τη χειροκίνητη επεξεργασία δεδομένων, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται σύμφωνα με προκαθορισμένα κριτήρια (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία πώς αποθηκεύονται τα δεδομένα - σε ένα σύστημα ΤΠ, π.χ. μέσω βιντεοεπιτήρησης ή σε χαρτί, καθώς σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που ορίζονται στον ΓΚΠΔ.[5]

1.3 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, ΓΚΠΔ

Στις 25 Μαΐου 2018 τέθηκε σε ισχύ ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ). Το πρώτο στο είδος του νομοθέτημα ήταν πολλά υποσχόμενο κατά την ανάπτυξή του, έχοντας ως στόχο να εναρμονίσει τους νόμους περί ιδιωτικότητας και προστασίας δεδομένων σε ολόκληρη την Ευρώπη, βοηθώντας τους πολίτες της ΕΕ να κατανοήσουν καλύτερα τον τρόπο με τον οποίο χρησιμοποιούνται οι προσωπικές τους πληροφορίες, ενθαρρύνοντάς τους παράλληλα, να υποβάλουν καταγγελία σε περίπτωση παραβίασης των δικαιωμάτων τους. Ως νέο κανονιστικό πλαίσιο, ο ΓΚΠΔ ήταν μια αναγνώριση ότι η ψηφιακή οικονομία - που τροφοδοτείται από (προσωπικές) πληροφορίες - θα πρέπει να λειτουργεί με τη συγκατάθεση των χρηστών μετά από ενημέρωση και με σαφείς κανόνες, για τις εταιρείες που επιδιώκουν να

[3] Cambridge Dictionary

[4] European Commission, What is personal data?

[5] European Commission, What is personal data?

δραστηριοποιηθούν στην Ευρωπαϊκή Ένωση. Δεδομένου ότι ο ΓΚΠΔ έχει ως αφετηρία τον πολίτη, ο αντίκτυπος του κανονισμού στα άτομα -στην Ευρώπη και αλλού- αποτελεί σημαντικό σημείο αναφοράς για την κατανόηση των επιτυχιών και των αδυναμιών του.

1.4 Δίκτυα 5ης Γενιάς, 5G

Η ασύρματη τεχνολογία 5ης γενιάς (5G) είναι η τελευταία επανάληψη της κυψελοειδούς τεχνολογίας, η οποία έχει σχεδιαστεί για να αυξήσει σημαντικά την ταχύτητα και την απόκριση των ασύρματων δικτύων. Με το 5G, τα δεδομένα που μεταδίδονται μέσω ασύρματων ευρυζωνικών συνδέσεων μπορούν να ταξιδεύουν με ταχύτητες πολλών gigabit, με πιθανές μέγιστες ταχύτητες που φτάνουν τα 20 gigabit ανά δευτερόλεπτο (Gbps)[6] σύμφωνα με ορισμένες εκτιμήσεις. Αυτές οι ταχύτητες υπερβαίνουν τις ταχύτητες των ενσύρματων δικτύων και προσφέρουν καθυστέρηση 1 χιλιοστό του δευτερολέπτου (ms) ή χαμηλότερη, ιδιότητα χρήσιμη για εφαρμογές που απαιτούν ανατροφοδότηση σε πραγματικό χρόνο.[7] Το 5G θα επιτρέψει την απότομη αύξηση του όγκου των δεδομένων που μεταδίδονται μέσω ασύρματων συστημάτων λόγω του μεγαλύτερου διαθέσιμου εύρους ζώνης και της προηγμένης τεχνολογίας κεραιών.

1.5 IoT, Διαδίκτυο των Πραγμάτων

Συχνά αναφερόμενο ως «έξυπνες συσκευές» το Διαδίκτυο των Πραγμάτων (IoT) αποτελεί ένα σύστημα αλληλένδετων δεδομένων υπολογιστικών συσκευών, μηχανικών και ψηφιακών μηχανών, αντικειμένων ακόμα και ατόμων ή ζώων, στα οποία παρέχονται μοναδικές ταυτότητες και η δυνατότητα να μεταφέρουν και να ανταλλάσσουν δεδομένα σε ένα δίκτυο χωρίς να απαιτείται αλληλεπίδραση ανάμεσα στα άτομα ή ανάμεσα στα άτομα και τις συσκευές. Πρόκειται πιο συγκεκριμένα, για μια παγκόσμια διαδικτυακή υποδομή, που ενώνει φυσικά και εικονικά αντικείμενα με τη χρήση αισθητήρων, ώστε να επιτυγχάνεται η αποθήκευση και η μετάδοση δεδομένων σε κάθε στιγμή και κάθε μέρος.

1.6 Artificial Intelligence, AI

Τεχνητή Νοημοσύνη είναι ο τομέας της επιστήμης των υπολογιστών που ασχολείται με τη σχεδίαση και την υλοποίηση προγραμμάτων και υπολογιστικών συστημάτων, τα οποία λειτουργούν ως μια προσομοίωση της ανθρώπινης νοημοσύνης αναλύοντας το γύρω περιβάλλον και λαμβάνοντας δράση – με κάποιο βαθμό αυτονομίας-

[6] Tech Target, What is 5G?

[7] Tech Target, What is 5G?

ώστε να πετύχουν συγκεκριμένους σκοπούς. Η Τεχνητή νοημοσύνη αναφέρεται στην ικανότητα των μηχανών να μιμούνται στοιχεία της ανθρώπινης συμπεριφοράς τα οποία υπονοούν έστω και στοιχειώδη ευφυΐα, μέσω της συγκέντρωσης μεγάλων συνόλων δεδομένων (που αποκαλούνται bigdata), αλλά και προσωπικών δεδομένων, ανεξάρτητα, χωρίς δηλαδή να ακολουθούν πλέον μία γλώσσα προγραμματισμού. Αυτή η ευρεία χρήση της ΤΝ περιλαμβάνει: (i) τη μηχανική εκμάθηση (machine learning), η οποία εξάγει συμπεράσματα, πραγματοποιεί προβλέψεις και λαμβάνει αυτοματοποιημένες αποφάσεις για τα υποκείμενα και (ii) τους αλγόριθμους τεχνητής νοημοσύνης, οι οποίοι αποτελούν πλήρως αυτόνομα και συνδεδεμένα αντικείμενα.

1.7 Machine Learning, ML

Ο όρος μηχανική μάθηση χρησιμοποιείται για να ορίσει «οποιαδήποτε μεθοδολογία και σύνολο τεχνικών που βρίσκει νέα πρότυπα και γνώση στα δεδομένα, δημιουργώντας μοντέλα που μπορούν να χρησιμοποιηθούν για αποτελεσματικές προβλέψεις σχετικά με τα δεδομένα». Έχοντας την «ικανότητα μάθησης χωρίς ρητό προγραμματισμό», τα προγράμματα αυτά και οι τεχνικές μηχανικής εκμάθησης, βελτιώνονται αυτόματα βάσει της αποκτώμενης εμπειρίας. Αυτό περιλαμβάνει το σχεδιασμό, την ανάλυση, την ανάπτυξη αλλά και την εφαρμογή μεθόδων, που επιτρέπουν σε μια μηχανή να λειτουργεί μέσω μιας συστηματικής διαδικασίας και να φέρει εις πέρας δύσκολες εργασίες. Σημαντική ικανότητα του αλγορίθμου είναι η δυνατότητα να ορίζει ή να τροποποιεί κανόνες λήψης αποφάσεων προκειμένου να χειρίζεται νέες εισροές.

1.8 Big Data

Τα μεγάλα δεδομένα, είναι συλλογές δεδομένων που έχουν μεγάλο όγκο ή εξαιτίας της πολυπλοκότητάς τους δε μπορούν να γίνουν κατανοητά με τις παραδοσιακές μεθόδους. Περιλαμβάνουν τον όγκο των πληροφοριών, την ταχύτητα με την οποία αυτά δημιουργούνται και συλλέγονται, καθώς και την ποικιλία ή το εύρος των σημείων δεδομένων που καλύπτονται (γνωστά ως τα "τρία v" των μεγάλων δεδομένων: volume-velocity-variety). Τα μεγάλα δεδομένα προέρχονται συχνά από την εξόρυξη δεδομένων και φθάνουν σε πολλαπλές μορφές.

I. Ανάλυση Βασικών Εννοιών

1. Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, ΓΚΠΔ (GDPR)

Με τον Γενικό Κανονισμό Προστασίας Δεδομένων, ο νομοθέτης της ΕΕ προσπάθησε να δημιουργήσει ένα πλαίσιο προστασίας για τα προσωπικά δεδομένα των πολιτών της ΕΕ. Το ερώτημα που δημιουργήθηκε στη συνέχεια, αφορά το κατά πόσο ο GDPR καταφέρνει να μετριάσει τις ασυμμετρίες πληροφοριών σε μια αγορά διοικούμενη από βάσεις δεδομένων. Μπορεί ο Κανονισμός να διασφαλίσει στους πολίτες τη δυνατότητα να λαμβάνουν ενημερωμένες αποφάσεις σχετικά με τα διαδικτυακά τους δεδομένα;

Ο ΓΚΠΔ έδωσε μεγαλύτερη έμφαση σε ορισμένες πτυχές του τοπίου προστασίας δεδομένων στην Ευρωπαϊκή Ένωση (ΕΕ) και στον υπόλοιπο κόσμο, όπως η νομιμότητα, η δικαιοσύνη και η διαφάνεια της επεξεργασίας δεδομένων, η νομιμότητα του σκοπού, η επάρκεια, η συνάφεια και η ακρίβεια της επεξεργασίας. Επίσης στο κείμενο του Κανονισμού, δίνεται έμφαση στην επιβεβαίωση των κατάλληλων τεχνικών ή οργανωτικών μέτρων κατά της παράνομης ή μη εξουσιοδοτημένης επεξεργασίας και της τυχαίας απώλειας ή καταστροφής. Οι αλλαγές αυτές επηρεάζουν τελικά την επεξεργασία δεδομένων λόγω των προβλεπόμενων αρχών και κανόνων του κανονισμού.[8] Οι αρχές της επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες περιλαμβάνουν την αρχή της νομιμότητας, της αμεροληψίας και της διαφάνειας, την αρχή του περιορισμού του σκοπού, την αρχή της ελαχιστοποίησης των δεδομένων, την αρχή της ακρίβειας, την αρχή του περιορισμού της αποθήκευσης, την αρχή της ακεραιότητας και της εμπιστευτικότητας, και την αρχή της λογοδοσίας με τους αντίστοιχους κανόνες εφαρμογής, εφαρμόζονται σε κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, ενώ δεν μπορούν να εφαρμοστούν σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιο τρόπο ώστε να τρόπο ώστε το υποκείμενο των δεδομένων να μην είναι ή να μην είναι πλέον αναγνωρίσιμο.

Στο άρθρο 4 του ΓΚΠΔ δίνεται ο ορισμός της συγκατάθεσης ως "κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το

[8] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν". Η ύπαρξη ασυμμετριών στην πληροφόρηση, ωστόσο, εγείρει ερωτήματα σχετικά με τη συγκατάθεση, η οποία αποτελεί και ακρογωνιαίο λίθο της νομοθεσίας της ΕΕ για την προστασία των δεδομένων και κύριο νομικό λόγο για την επεξεργασία δεδομένων στην αγορά δεδομένων. Το πιο προφανές πρόβλημα με τη χρήση της συγκατάθεσης ως νομικού λόγου για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, είναι η ρητή προϋπόθεση αυτή να προέρχεται ύστερα από ενημέρωση.

Η ομάδα εργασίας του άρθρου 29 απαριθμεί ορισμένα βασικά στοιχεία της συγκατάθεσης προκειμένου αυτή να είναι νόμιμη και να υπηρετεί τα οριζόμενα στον Κανονισμό, όπως είναι η ταυτότητα του υπεύθυνου επεξεργασίας, ο σκοπός της επεξεργασίας, το είδος των δεδομένων που θα συλλεχθούν, το δικαίωμα ανάκλησης της συγκατάθεσης, η χρήση αυτοματοποιημένης λήψης αποφάσεων και η δυνατότητα διαβίβασης δεδομένων. Παράλληλα, θέτει ως προϋπόθεση ότι το υποκείμενο των δεδομένων πρέπει να γνωρίζει και να κατανοεί σε τι συμφωνεί. Η τελευταία προϋπόθεση έχει δημιουργήσει προβλήματα στην αγορά δεδομένων, καθώς δεν αρκεί, προκειμένου να πληρούνται τα νομικά πρότυπα της συγκατάθεσης μετά από ενημέρωση, η απλή προβολή της πολιτικής απορρήτου και το να ζητείται από τον χρήστη να κάνει κλικ στο "Συμφωνώ", δεδομένου ότι ο καταναλωτής δεν μπορεί να έχει επαρκείς γνώσεις σχετικά με τις δραστηριότητες επεξεργασίας από το στάδιο της συλλογής και ανάλυσης των δεδομένων, έως και τα βήματα που συνδέουν τη δραστηριότητά του με τις διαφημίσεις που του προβάλλονται, γεγονός που εξελίσσεται σε μια μακροχρόνια δυσκολία. Χαρακτηριστικό είναι το παράδειγμα της Google, η οποία το 2013 δέχτηκε επίπληξη από την ολλανδική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επειδή διέσπειρε βασικές πληροφορίες σε διάφορες ιστοσελίδες, χρησιμοποιώντας ασαφή ορολογία κατά την περιγραφή των δραστηριοτήτων επεξεργασίας της. Ως εκ τούτου, η Google δεν μπορούσε νομικά να χρησιμοποιήσει τη συγκατάθεση μετά από ενημέρωση ως λόγο επεξεργασίας, επειδή τα υποκείμενα των δεδομένων δεν μπορούσαν να "προσδιορίσουν τη φύση και το πεδίο εφαρμογής των δραστηριοτήτων επεξεργασίας".[9]

Στο αμέσως επόμενο άρθρο, άρθρο 5 του ΓΚΠΔ συναντάμε την αρχή της νομιμότητας. Η ιδέα της σύννομης και θεμιτής επεξεργασίας συνιστά μία εκτίμηση για το

[9] Van de Waerdt,Peter J., 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. In: Computer Law & Security Review, Volume 38.

αν η επεξεργασία θα έχει αρνητική ή αδικαιολόγητη επίδραση στα υποκείμενα που εμπλέκονται. Η Ευρωπαϊκή Επιτροπή Προστασίας Δεδομένων δίνει έναν ορισμό για τη νομιμότητα, στις δικές της κατευθυντήριες γραμμές για την προστασία των δεδομένων από τον σχεδιασμό τους (by design) ή εξ ορισμού (by default).

Στο κείμενο είναι σε αρκετά σημεία εμφανής η προσπάθεια του ΓΚΠΔ να δημιουργήσει εφαρμόσιμο πλαίσιο προστασίας, απέναντι στην επέλαση των νέων τεχνολογιών. Έτσι, στον ΓΚΠΔ μπορεί να διακρίνει κανείς δύο διαφορετικές πλευρές της νομιμότητας. Η πρώτη, την οποία μπορούμε να αποκαλέσουμε «νομιμότητα των πληροφοριών», είναι αυστηρά συνδεδεμένη με την ιδέα της διαφάνειας. Ορίζει ότι τα υποκείμενα των δεδομένων δεν πρέπει να εξαπατηθούν σχετικά με την επεξεργασία των δεδομένων τους, όπως εξηγείται στην Αιτιολογική Σκέψη (60). Η Αιτιολογική Σκέψη (71) εστιάζει σε μια διαφορετική διάσταση της νομιμότητας, που σχετίζεται με το νόμιμο του περιεχομένου ενός αυτοματοποιημένου συμπεράσματος ή απόφασης, με τη χρήση ενός συνδυασμού κριτηρίων, τα οποία μπορούν να συνοψιστούν κάνοντας αναφορά στις προηγούμενες αξίες της αποδοχής, της συνάφειας και της αξιοπιστίας (ουσιαστική νομιμότητα).

Η σύννομη επεξεργασία προϋποθέτει ότι, οι υπεύθυνοι επεξεργασίας μπορούν να αντιληφθούν μια πιθανώς αρνητική επίδραση, που θα έχει για παράδειγμα η χρήση της ΤΝ στους ανθρώπους και να την αξιολογούν εκ νέου. Σύμφωνα με την Ολλανδική Αρχή Προστασίας Δεδομένων «ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει δραστικά μέτρα και να αποδεικνύει πότε ένας αλγόριθμος λειτουργεί σύννομα και πότε η χρήση του συγκεκριμένου κάθε φορά αλγόριθμου δεν οδηγεί σε ακατάλληλα αποτελέσματα».

Όταν συλλέγονται δεδομένα, πρέπει να είναι σαφές γιατί συλλέγονται και πώς θα χρησιμοποιηθούν. Οι υπεύθυνοι επεξεργασίας πρέπει επίσης να είναι πρόθυμοι να παρέχουν λεπτομέρειες, σχετικά με την επεξεργασία των δεδομένων κατόπιν αίτησης του υποκειμένου των δεδομένων, διότι αυτό αποτελεί μέρος του δικαιώματος πληροφόρησης του. Όταν γίνεται σεβαστό αυτό το δικαίωμα, οι πολιτικές προστασίας της ιδιωτικής ζωής είναι πιο φιλικές προς τον χρήστη και με τον τρόπο αυτό προάγονται τα δικαιώματα των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας δεσμεύεται να παρέχει στο υποκείμενο των δεδομένων με συνοπτικό, διαφανή και κατανοητό τρόπο, με τη χρήση απλής γλώσσας, τις πληροφορίες σχετικά με τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Με την ενημέρωση του ατόμου επιτυγχάνεται η τήρηση της αρχής της διαφάνειας και αυτό πρέπει να γίνεται τόσο πριν από τη συλλογή των

δεδομένων, όσο και όταν γίνονται τυχόν μεταγενέστερες αλλαγές στον σκοπό ή τον τρόπο επεξεργασίας. Τα δεδομένα δεν συλλέγονται πάντοτε απευθείας από τα άτομα και μπορεί να προέρχονται από άλλα σύνολα δεδομένων, να συνάγονται με τη χρήση αλγορίθμων ή μέσω παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων. Η μη τήρηση της απαίτησης διαφάνειας εμποδίζει το υποκείμενο των δεδομένων να ασκεί τον έλεγχο των δεδομένων του και στερεί από το υποκείμενο των δεδομένων κάθε γνώση για τον τρόπο επεξεργασίας αυτών.[10]

Το κεφάλαιο ΙΙΙ, τμήμα 2 του ΓΚΠΔ αφιερώνεται εξ ολοκλήρου στις πληροφορίες που πρέπει να παρέχονται στα υποκείμενα των δεδομένων, αναφερόμενο σε δικαιώματα και υποχρεώσεις πληροφόρησης των υποκειμένων, όπως αυτά τους έχουν παραχωρηθεί για πρόσβαση στα προσωπικά τους δεδομένα, που υποβάλλονται σε επεξεργασία. Στο υποκείμενο των δεδομένων θα πρέπει να παρέχεται σημαντική ποσότητα συγκεκριμένων πληροφοριών κατά την επεξεργασία των προσωπικών τους δεδομένων. Στα άρθρα 13 και 14 του ΓΚΠΔ ορίζεται ότι πρέπει να παρέχονται πληροφορίες σχετικά με την ταυτότητα του επεξεργαστή δεδομένων, τους σκοπούς και τις νομικές βάσεις της επεξεργασίας, τυχόν τρίτους παραλήπτες των δεδομένων αυτών, τα δικαιώματα ΓΚΠΔ του υποκειμένου των δεδομένων και πολλά περισσότερα. Εάν οι δραστηριότητες επεξεργασίας δεδομένων περιλαμβάνουν αυτοματοποιημένη λήψη αποφάσεων ή δημιουργία προφίλ, η υποχρέωση ενημέρωσης του καταναλωτή εντείνεται περαιτέρω. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τη δημιουργία προφίλ και τη «λογική» πίσω από το προφίλ. Για να συμπληρώσει αυτήν την υποχρέωση ενημέρωσης, ο νομοθέτης της ΕΕ εισήγαγε επίσης το δικαίωμα λήψης ή πρόσβασης στα προσωπικά δεδομένα που σχετίζονται με το υποκείμενο των δεδομένων και με τον τρόπο αυτό, έχουν το δικαίωμα να ζητήσουν πληροφορίες σχετικά με τα δεδομένα τα οποία επεξεργάζονται από τον υπεύθυνο επεξεργασίας δεδομένων.

Στην πράξη, αυτές οι διατάξεις έχουν εφαρμοστεί με ποικίλους τρόπους: Το Facebook επιτρέπει στους χρήστες να κατεβάζουν ένα αρχείο στο οποίο εμπεριέχονται τα προσωπικά τους δεδομένα, ενώ η Google δίνει στους χρήστες τη δυνατότητα να δουν και να επεξεργαστούν το δικό τους προφίλ συμπεριφοράς, καθώς και μια πλήρη ροή της δραστηριότητάς τους με τις υπηρεσίες της Google. Ωστόσο, ακόμη και με όλα αυτά τα δικαιώματα πληροφόρησης, εξακολουθεί να είναι δύσκολο για το υποκείμενο των

[10]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

δεδομένων να αποκτήσει πλήρη γνώση των προσωπικών δεδομένων που υποβάλλονται σε επεξεργασία.[11]

Ο ΓΚΠΔ φαίνεται να ζητά μια δύσκολη, αν όχι αδύνατη, ισορροπία μεταξύ διαφάνειας και λεπτομέρειας. Από τη μία πλευρά, ένας υπεύθυνος επεξεργασίας είναι υποχρεωμένος να παρέχει στον καταναλωτή πληθώρα πληροφοριών, ειδικά εάν κάνει χρήση του δικαιώματός του να έχει πρόσβαση στα προσωπικά του δεδομένα. Από την άλλη πλευρά, ο υπεύθυνος επεξεργασίας δεδομένων υποχρεούται να παρέχει στο υποκείμενο των δεδομένων όλες αυτές τις πληροφορίες κατά τρόπο κατανοητό και ευανάγνωστο. Ωστόσο, η παροχή περισσότερων πληροφοριών και, ειδικότερα, πιο λεπτομερών πληροφοριών θα δυσχεράνει επίσης την κατανόηση των καταναλωτών. Ακόμα κι αν οι πληροφορίες πλαισιώνονται με ευανάγνωστο και απλό τρόπο, θα παραμείνει σχεδόν αδύνατο για έναν καταναλωτή να αντλήσει οποιοδήποτε πραγματικό νόημα, από την πρόσβαση για παράδειγμα σε όλα τα ερωτήματα αναζήτησης Google, ή τα βίντεο στο YouTube που είχε παρακολουθήσει στο παρελθόν, ή τις τοποθεσίες των Χαρτών Google και όλα τα άλλα σημεία δεδομένων που αυτή επεξεργάζεται. Στην πραγματικότητα, ένας ελεγκτής δεδομένων μπορεί να υπερφορτώσει έναν καταναλωτή με δεδομένα, αυξάνοντας μεν τις πληροφορίες, μειώνοντας όμως ουσιαστικά τη διαφάνεια . Ως αποτέλεσμα, λαμβάνοντας το παράδειγμα της στοχευμένης διαφήμισης, το υποκείμενο των δεδομένων εξακολουθεί να μην είναι σε θέση να προσδιορίσει ποιες ενέργειες ή ποια δεδομένα τον οδήγησαν να τοποθετηθεί σε αυτή τη συγκεκριμένη κατηγορία.[12]

2. Δίκτυα Τηλεπικοινωνιών 5ης Γενιάς, 5G

Το 5G είναι η πέμπτη γενιά τεχνολογίας δικτύου τηλεπικοινωνιών. Το επίσημο πρότυπο καθιερώθηκε τον Δεκέμβριο του 2017 από το έργο 3ης γενιάς εταιρικής σχέσης (3GPP), για να εξηγήσει τις προδιαγραφές του δικτύου 5G. Το 5G δίκτυο τηλεπικοινωνιών αξιοποιεί το μεγάλο φάσμα ζώνης (που αναφέρεται ως χιλιοστομετρικό κύμα), για πολύ υψηλή ταχύτητα και χαμηλή καθυστέρηση latency.[13]

[11] Van de Waerdt,Peter J., 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. In: Computer Law & Security Review, Volume 38.

[12] Van de Waerdt,Peter J., 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. In: Computer Law & Security Review, Volume 38.

[13] Le,L.B.,Wang,X.,Bogale,T.E, 2017. Chapter 9 - mmWave communication enabling techniques for 5G wireless systems: A link level perspective. In: mmWave Massive MIMO, A Paradigm for 5G, pp195-225.

Αν και ένα 4G δίκτυο προσφέρει υψηλή ταχύτητα και καλή συνδεσιμότητα, δεν είναι ικανό να συνδέσει όλες τις συσκευές σε απομακρυσμένες περιοχές με χαμηλό κόστος εγκατάστασης και συντήρησης. Το 5G λειτουργεί σε πολύ υψηλές συχνότητες και υποστηρίζει μεγάλο εύρος σύνδεσης (bandwidth), το οποίο επιτρέπει γρηγορότερη και μεγαλύτερη ανταλλαγή δεδομένων. Αυτό το δίκτυο τηλεπικοινωνιών μπορεί να συνδέσει ένα εκατομμύριο συσκευές ανά τετραγωνικό χιλιόμετρο και υποστηρίζεται επιπλέον όταν οι συσκευές αυτές κινούνται σε πολύ μεγάλες ταχύτητες (περίπου 500 kmph). Αυτή η ιδιότητα λείπει από το δίκτυο 4G. Ορισμένα από τα πλεονεκτήματα του δικτύου 5G είναι η υψηλή χωρητικότητα και παραγωγικότητα, η μειωμένη καθυστέρηση, η υψηλής πυκνότητας και ανεμπόδιστη σύνδεση, η ευρεία κάλυψη και η αυξημένη ενεργειακή απόδοση δικτύου. Τα δίκτυα 4G προσφέρουν τη μέγιστη ταχύτητα δεδομένων κορυφής (μέγιστο εφικτό ρυθμό δεδομένων για έναν χρήστη σε ιδανικές συνθήκες) 1Gbps και το μέγιστο ρυθμό δεδομένων με εμπειρία χρήστη (εφικτός ρυθμός δεδομένων για έναν χρήστη στο πραγματικό περιβάλλον δικτύου) περίπου 10 Mbps. Σε δίκτυα 5G, ο μέγιστος ρυθμός δεδομένων αναμένεται να αυξηθεί έως και 20 Gbps και ο ρυθμός δεδομένων με εμπειρία χρήστη θα βελτιωθεί 100 φορές σε δίκτυα 4G και θα φτάσει έως και 1 Gbps. Υψηλότερη αξιοπιστία, με ικανότητα εγγύησης του ποσοστού επιτυχίας της μετάδοσης δεδομένων υπό δηλωμένες συνθήκες, για μια συγκεκριμένη χρονική περίοδο (αναμενόμενο ποσοστό 5G έως 99,999%).[14] Χαμηλότερη καθυστέρηση, καθώς το σύστημα 5G αναμένεται να μειώσει τον λανθάνοντα χρόνο δέκα φορές στο επίπεδο χρήστη, σε σύγκριση με το σύστημα 4G.

Λόγω αυτών των τεχνικών χαρακτηριστικών, τα δίκτυα 5G αναμένεται να εξυπηρετήσουν ένα ευρύ φάσμα εφαρμογών και τομέων (όπως ενέργεια, μεταφορές, τραπεζικές συναλλαγές και υγεία, βιομηχανικά συστήματα ελέγχου, εκλογές) επιφέροντας αποτελέσματα σε έναν τεράστιο όγκο δεδομένων. Συνεπώς, οι πρωτοβουλίες των δικτύων 5G θα συμβάλουν στην ικανότητα των υποκειμένων των δεδομένων να δημιουργούν και να διαδίδουν ακόμα περισσότερα προσωπικά δεδομένα στον Ιστό. Μέσω των πρωτοβουλιών που λαμβάνουν κατά την απόδοσή τους, τα δίκτυα 5G ελλοχεύουν σημαντικότερους κινδύνους χάρη στην ευρύτερη εισβολή τους σε οικονομικές και κοινωνικές λειτουργίες και παρουσιάζουν για το λόγο αυτό σημαντικές διαφορές, σε σύγκριση με τις απειλές σε υπάρχοντα δίκτυα.

[14] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

Σε ένα περιβάλλον 5G οι διαφορετικές ασύρματες τεχνολογίες, οι πάροχοι υπηρεσιών και η εναλλαγή αυτών μέσω του διαμερισμού από ένα βασικό δίκτυο βασισμένο σε IP, θα βελτιώσουν μεν την ποιότητα των κινητών συσκευών, προκαλώντας δε τρωτά σημεία όσον αφορά τον έλεγχο πρόσβασης, την ασφάλεια επικοινωνίας, την εμπιστευτικότητα και τη διαθεσιμότητα των δεδομένων. Αυτοί οι παράγοντες περιπλέκουν και τα βασιζόμενα κυρίως στην κρυπτογραφία συστήματα διατήρησης ασφάλειας, καθώς η παραδοσιακή μέθοδος κρυπτογραφίας δεν είναι αρκετά αποτελεσματική, όταν πρόκειται να αναλυθούν μεγάλα δεδομένα σε πραγματικό χρόνο.[15]

Οι διευθύνσεις IP είναι προσωπικά δεδομένα, τα οποία κατηγοριοποιούνται ως δεδομένα θέσης. Οι υπηρεσίες διαδικτύου που βασίζονται στην τοποθεσία, αποτέλεσαν λόγο επέκτασης των υπηρεσιών γεωγραφικού εντοπισμού στο διαδίκτυο οι οποίες έχουν τη δυνατότητα να εκτιμούν την τοποθεσία του υποκειμένου των δεδομένων μιας διεύθυνσης IP. Παρόλο που η κατανομή της διεύθυνσης IP έχει αντιμετωπιστεί μέσω των προτύπων 5G, η διατήρηση των δεδομένων αυτών δεν μπορεί να συνεχίζεται πέραν της παύσεως του σκοπού για τον οποίο έχουν νόμιμα συλλεχθεί, ύστερα από τη σχετική συγκατάθεση του υποκειμένου σύμφωνα με την απαίτηση του Ευρωπαϊκού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Ο όρος αυτός συνδέεται στενά με την αρχή του περιορισμού του σκοπού, η οποία απαιτεί ότι οποιαδήποτε δεδομένα συλλέγονται μόνο για συγκεκριμένους σκοπούς και δεν υποβάλλονται σε επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς. Κάθε επιμέρους σκοπός πρέπει να ορίζεται εκ των προτέρων και η συγκατάθεση πρέπει να ζητείται σε βάση opt-in για κάθε ξεχωριστό σκοπό επεξεργασίας δεδομένων.

Η ελαχιστοποίηση των δεδομένων και ο περιορισμός της αποθήκευσης διευθύνσεων IP κρίνεται απαραίτητο να διασφαλιστούν, ιδιαίτερα με την έλευση του 5G και τον αυξημένο αριθμό νέων συσκευών και τη συνδεσιμότητα αυτών που θα οδηγήσουν σε αύξηση των δεδομένων. Η ανάγκη προστασίας του απορρήτου τοποθεσίας πηγάζει από το γεγονός ότι πέραν της σύνδεσης του με μια φυσική επίθεση, συνδέεται και με τη μη ζητηθείσα επικοινωνία ή τη στοχευμένη διαφήμιση καθώς και με τη δημιουργία προφίλ, επειδή περιλαμβάνει δεδομένα μιας πολύ ακριβούς τοπικής περιοχής, τα οποία μπορούν να συνδεθούν με άλλα και να αποκαλύψουν περαιτέρω προσωπικά δεδομένα. Για το λόγο αυτό θα πρέπει να επιβεβαιώνεται ότι κάθε φορά που απαιτείται επεξεργασία της

[15]Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

διεύθυνσης IP, τα δεδομένα θέσης δεν θα χρησιμοποιούνται για άλλο σκοπό και για περισσότερο χρόνο από τον απαραίτητο.[16]

3. Διαδίκτυο των Πραγμάτων, IoT

Το Διαδίκτυο των Πραγμάτων ή IoT είναι ένα ταχέως αναπτυσσόμενο δίκτυο διασυνδεδεμένων "πραγμάτων", με ενσωματωμένους αισθητήρες που συλλέγουν και ανταλλάσσουν δεδομένα μέσω του διαδικτύου, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Μέσω αποκλειστικών συστημάτων διευθυνσιοδότησης[17], τα "πράγματα" αυτά επικοινωνούν μεταξύ τους και συνεργάζονται με άλλα "πράγματα" κοντά τους, έχοντας ως σκοπό την επίτευξη κοινών στόχων. Στην πραγματικότητα μόνο το 1% από τις συσκευές που θα μπορούσαν να συνδεθούν, είναι συνδεδεμένες. Όσο περισσότερο ενισχύεται η ψηφιοποίηση και η συνδεσιμότητα, τόσο περισσότερα δεδομένα παράγονται, εμπόδιο αποτελεί η κατανόηση και η ορθή χρήση αυτών. Το Διαδίκτυο των πραγμάτων (IoT) μπορεί να οριστεί ως η διασύνδεση μοναδικά αναγνωρίσιμων ενσωματωμένων υπολογιστικών συσκευών εντός της υπάρχουσας υποδομής του Διαδικτύου. Τυπικά, το IoT αναμένεται να προσφέρει προηγμένη συνδεσιμότητα συσκευών, συστημάτων και υπηρεσιών που υπερβαίνει τις επικοινωνίες μεταξύ μηχανών (M2M) και καλύπτει μια ποικιλία πρωτοκόλλων, τομέων και εφαρμογών. Η διασύνδεση αυτών των ενσωματωμένων συσκευών (συμπεριλαμβανομένων των έξυπνων αντικειμένων) αναμένεται να εισαγάγει τον αυτοματισμό που καλύπτει όλους τους σημαντικούς τομείς της μηχανικής[18], ενώ παράλληλα θα επιτρέψει προηγμένες εφαρμογές όπως το έξυπνο δίκτυο και η έξυπνη επιτήρηση. Το IoT γίνεται περισσότερο εκλεπτυσμένο, αυξάνοντας διαρκώς τις δυνατότητες διασυνδεσιμότητας, με την παγκόσμια πρόβλεψη εξόδων για το IoT μέχρι το 2021 να φτάνει τα 1,1 τρισεκατομμύρια δολάρια, ενώ οι επενδύσεις στο IoT από Αμερικανικές start-ups έφτασαν τα 1,46 δισεκατομμύρια δολάρια το 2017. Η εκτίμηση για τα παγκόσμια έξοδα για την ασφάλεια του IoT άγγιζε τα 3,1 δισεκατομμύρια το 2021.

[16]Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

[17] Stergiou C. L., Psannis K. E., Gupta B. B., 2021. "IoT-based Big Data secure management in the Fog over a 6G Wireless Network". In: IEEE Internet of Things Journal, vol. 8, issue: 7, pp 5164 - 5171

[18] Kim Byung-Gyu, Psannis Konstantinos E., Bhaskar Harish, 2017. "Emerging Multimedia Technology for Smart Surveillance System with IoT Environment". In: The Journal of Supercomputing, Volume 73, Issue 3, pp 923–925.

Τα τελευταία χρόνια, σύμφωνα με έρευνες, η εμφάνιση των νέων τεχνολογιών και του Διαδικτύου των Πραγμάτων (IoT) έχει παρουσιάσει εκρηκτική αύξηση των δεδομένων. Ένας τεράστιος αριθμός δικτυωμένων συσκευών (αισθητήρες, ενεργοποιητές κ.λπ.) σε όλο τον κόσμο συλλέγει διαφορετικούς τύπους δεδομένων (περιβαλλοντικά, γεωγραφικά, λογιστικά κ.λπ.). Στη συνέχεια, οι συσκευές IoT μεταδίδουν τα δεδομένα που συλλέγονται, ώστε να μπορούν να αποθηκευτούν, να υποβληθούν σε επεξεργασία και να αναλυθούν. Με άλλα λόγια, οι άνθρωποι στην καθημερινή τους ζωή έρχονται σε επαφή με αμέτρητες συσκευές και άλλες τεχνολογικές εξελίξεις. Οι συσκευές αυτές συνδέονται μεταξύ τους και σχηματίζουν ένα δίκτυο, το οποίο μας οδηγεί στο IoT. Αυτή η νέα τεχνολογική τάση συνοδεύεται από αμέτρητες προσδοκίες ανάπτυξης και βελτίωσης σε όλους τους τομείς, αλλά και ανησυχίες σχετικά με την ασφάλεια και την παραβίαση της ιδιωτικής ζωής. Επίσης, μελέτες έχουν δείξει ότι μέχρι το 2030 θα είναι συνδεδεμένοι περίπου ένα τρισεκατομμύριο αισθητήρες[19], οι οποίοι θα συλλέγουν και θα μεταφέρουν μεγάλες ποσότητες δεδομένων.

Τα επόμενα χρόνια αναμένεται μια εκτόξευση του αριθμού των συνδεδεμένων συσκευών καθώς και των τοποθετημένων χώρων και των λειτουργιών που αυτές θα εκτελούν. Αυτή η σχετικά νέα και σε κάθε περίπτωση ταχέως αναπτυσσόμενη τεχνολογία που ονομάζεται Διαδίκτυο των Πραγμάτων (Internet of Things - IoT), εγείρεται στον τομέα των δικτύων και των τηλεπικοινωνιών με ιδιαίτερη έμφαση στον "σύγχρονο" τομέα των ασύρματων τηλεπικοινωνιακών συστημάτων. Το IoT ορίζεται από πολλούς ερευνητές ως "το δίκτυο συσκευών, οχημάτων, κτιρίων και άλλων αντικειμένων που είναι ενσωματωμένα με αισθητήρες και είναι συνδεδεμένα στο δίκτυο, επιτρέποντας στα αντικείμενα αυτά να συλλέγουν και να ανταλλάσσουν δεδομένα"[20]. Η ασφάλεια του IoT είναι ο τομέας που ασχολείται με την προστασία των συνδεδεμένων συσκευών και δικτύων στο IoT, το οποίο περιλαμβάνει την αυξανόμενη κυριαρχία αντικειμένων και οντοτήτων, που διαθέτουν μοναδικά αναγνωριστικά και τη δυνατότητα αυτόματης μετάδοσης δεδομένων μέσω δικτύου. Μεγάλο μέρος της αύξησης της επικοινωνίας του IoT προέρχεται από τις υπολογιστικές συσκευές και τα ενσωματωμένα συστήματα

[19] Plageras Andreas P and Psannis Konstantinos E., 2017. “Algorithms for Big Data Delivery over the Internet of Things”. In: 19th IEEE Conference on Business Informatics, Thessaloniki, Greece 24-26 July.

[20] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”. In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

αισθητήρων που χρησιμοποιούνται σε τομείς όπως η βιομηχανική επικοινωνία μηχανής-μηχανής (M2M), τα έξυπνα ενεργειακά δίκτυα, ο οικιακός και κτιριακός αυτοματισμός, η επικοινωνία μεταξύ οχημάτων και οι φορητές υπολογιστικές συσκευές.[21] Θα μπορούσε επίσης να οριστεί ως ένα είδος δικτύου φυσικών αντικειμένων ή πραγμάτων που είναι ενσωματωμένα με λογισμικό, ηλεκτρονικά, αισθητήρες και συνδεσιμότητα που τα ενεργοποιεί[22]. Εξαιτίας αυτού, το IoT επιτυγχάνει μεγαλύτερο ρυθμό και υπηρεσία με τη μετάδοση δεδομένων με φορείς εκμετάλλευσης και διάφορες διασυνδεδεμένες συσκευές. Εξαιτίας του όγκου των δεδομένων που χρησιμοποιούνται σε ένα ασύρματο δίκτυο, εγείρονται ζητήματα ασφάλειας και προστασίας της ιδιωτικής ζωής που πρέπει να αντιμετωπιστούν.

Παράλληλα, έχει υποστηριχθεί η άποψη ότι το πρόβλημα της ασφάλειας και του απορρήτου των δεδομένων στην καθημερινή ζωή θα μπορούσε να επιλυθεί ή να ελαχιστοποιηθεί με τη χρήση εργαλείων και υπηρεσιών ανάλυσης Big Data[23]. Ο όρος Big Data είναι ένας νέος δημοφιλής όρος, που χρησιμοποιείται για να περιγράψει την εκπληκτικά ραγδαία αύξηση του όγκου των δεδομένων σε δομημένη και μη δομημένη μορφή. Το Big Data χρησιμοποιεί συνήθως το Cloud Computing (CC) ως βασική τεχνολογία προκειμένου να λειτουργήσει. Παρόμοια με αυτό, μια άλλη τεχνολογία που θα μπορούσε να χρησιμοποιηθεί ως τεχνολογία βάσης είναι το Edge Computing (EC). Ως "βασική" τεχνολογία, το Cloud Computing ενοποιεί διάφορες τεχνολογίες και εφαρμογές για να επιτύχει τη μέγιστη χωρητικότητα και απόδοση της υπάρχουσας υποδομής. Ορισμένα από τα κύρια χαρακτηριστικά της τεχνολογίας Cloud Computing που σχετίζονται με τα χαρακτηριστικά του IoT είναι: α) αποθήκευση μέσω του Διαδικτύου, β) υπηρεσίες μέσω του Διαδικτύου, γ) εφαρμογές μέσω του Διαδικτύου, δ) ενεργειακή απόδοση και ε) υπολογιστική ικανότητα. Αρχικά, οι πρακτικά απεριόριστες δυνατότητες και πόροι του Cloud Computing προς αντιστάθμισμα των τεχνολογικών περιορισμών του,

[21] Stergiou C.L., Psannis K.E., Gupta B.B., Ishibashi Y., "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", 2018. In: Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184.

[22] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network". In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

[23] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network". In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

όπως η επεξεργασία, η αποθήκευση και η επικοινωνία, θα μπορούσαν να αποτελέσουν ένα ευεργετικό σενάριο για την τεχνολογία IoT. Όταν οι κρίσιμες εφαρμογές IoT μετακινούνται προς την τεχνολογία Cloud Computing, προκύπτουν ανησυχίες λόγω της έλλειψης εμπιστοσύνης στον πάροχο υπηρεσιών[24] ή της γνώσης σχετικά με τις συμφωνίες επιπέδου υπηρεσιών (SLA) και της γνώσης σχετικά με τη φυσική τοποθεσία των δεδομένων. Επιπλέον, το Mobile Cloud Computing (MCC) με την εμφάνισή του, ως σχετική εκδοχή του Cloud Computing, βελτιώθηκε από τις νέες εξελίξεις στον τομέα του "Cloud Computing". Το τελευταίο αποσκοπεί στην παροχή πρόσβασης σε δεδομένα και πληροφορίες από οπουδήποτε και οποτεδήποτε, εξαλείφοντας την ανάγκη για εξοπλισμό υλικού. Πιο συγκεκριμένα, το Mobile Cloud Computing ορίζεται ως ενσωμάτωση του υπολογιστικού νέφους και της κινητής πληροφορικής, καθιστώντας τις κινητές συσκευές πιο αποδοτικές, με την ικανότητα να χρησιμοποιηθεί ως βάση τόσο για το Διαδίκτυο των πραγμάτων όσο και για τις τεχνολογίες βιντεοεπιτήρησης, αλλά και να προσφέρει βελτιώσεις στη λειτουργία τους.

Μελλοντικά είναι πιθανό να υπάρχουν περισσότεροι αισθητήριες για κάθε είδους λειτουργία, όπως η μελέτη των συνθηκών του περιβάλλοντος, στατιστικές μετρήσεις υγείας, και κατασκευαστικοί αισθητήρες ικανοί να ελέγχουν την ποιότητα και τις συνθήκες παραγωγής. Επίσης είναι πιθανή η ανάπτυξη νέων ιατρικών αισθητήρων και ιατρικών συσκευών όπως πιεσόμετρων, εμφυτευμάτων ινσουλίνης κ.α. Οι δυνατότητες και οι καινοτομίες που μπορεί να φέρει η χρήση του IoT ελλοχεύουν και κινδύνους με κυριότερο αυτό της ασφάλειας της ιδιωτικότητας. Ένα από τα σημαντικότερα οφέλη της τεχνολογίας του Διαδικτύου των Πραγμάτων είναι η δημιουργία ενός άνευ προηγουμένου όγκου δεδομένων. Η αποθήκευση, η κατοχή και η ολοκλήρωση των δεδομένων καθίσταται κρίσιμη και ελλοχεύει κινδύνους για τα υποκείμενα των δεδομένων. Το διαδίκτυο καταναλώνει ήδη περισσότερο από το 5%[25] της συνολικής ενέργειας που παράγεται σήμερα και με αυτές τις απαιτήσεις, σίγουρα θα αυξηθεί ακόμη περισσότερο. Η δημιουργία ετερογενών δεδομένων από διαφορετικές φυσικές συσκευές απαιτεί γρήγορη ανάλυση σε πραγματικό χρόνο. Τα ελλιπή δεδομένα αποτελούν πρόβλημα για την

[24] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”. In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

[25] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”. In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

ανάλυση σε πραγματικό χρόνο[26], επομένως χρειαζόμαστε αλγορίθμους που προεπεξεργάζονται τα δεδομένα πριν από την ανάλυση. Η ανάλυση δεδομένων είναι η διαδικασία χρήσης αλγορίθμων που εκτελούνται σε ισχυρές πλατφόρμες για την ανακάλυψη κρυμμένων δυνατοτήτων σε μεγάλα δεδομένα, όπως κρυμμένα μοτίβα ή άγνωστες συσχετίσεις, για παράδειγμα, η εξαγωγή χρήσιμων γνώσεων και η εικόνα τους. Τη στιγμή που χιλιάδες συσκευές μπορούν να καταγράφουν τη δραστηριότητα και τη συμπεριφορά του ατόμου, με την ικανότητα να στέλνουν τα δεδομένα και τις μετρήσεις αυτές σε κάθε μέρος, ανά πάσα στιγμή, η απειλή για την ιδιωτικότητα και τα προσωπικά δεδομένα, ακόμα και για τα ευαίσθητα ιατρικά δεδομένα, είναι περισσότερο εμφανής από ποτέ. Καθώς οι εφαρμογές του IoT συνεχίζουν να αυξάνονται, εισάγονται σημαντικές ανησυχίες και εγείρονται συζητήσεις γύρω από την ασφάλεια, την ηθική, τις ιδιωτικές και νομικές προκλήσεις που έχουν σημαντικό αντίκτυπο στην καθημερινή ζωή. Εμφανίζεται πλέον η ανάγκη ύπαρξης παγκόσμιου νομοθετικού πλαισίου για τη ρύθμιση του IoT επειδή, ο κοινός χρήστης πρέπει να έχει τη δυνατότητα να ενημερωθεί για τις απειλές ασφάλειας, ηθικής και προστασίας της ιδιωτικής ζωής που επιβάλλονται από τις σύγχρονες συσκευές IoT.

Το IoT περιλαμβάνει δισεκατομμύρια ευφυή διασυνδεδεμένα "πράγματα", τα οποία έχουν τη δυνατότητα να συνδέονται οπουδήποτε και οποτεδήποτε, με εξαιρετική ακρίβεια μέσω οποιουδήποτε δικτύου. Ως "πράγματα" θεωρούνται, κάθε αντικείμενο που διαθέτει ενσωματωμένο σύστημα το οποίο μπορεί να εκπέμπει και να λαμβάνει πληροφορίες μέσω δικτύου και διαθέτει ένα μοναδικό αναγνωριστικό. Το IoT χρησιμοποιεί αισθητήρες και συσκευές για τη συλλογή δεδομένων από το περιβάλλον. Οι αλλαγές από το περιβάλλον γίνονται αντιληπτές από τον αισθητήρα και αποστέλλονται σε μια συσκευή. Οι αισθητήρες διατίθενται σε διάφορες μορφές, ανάλογα με τις ανάγκες του χρήστη και χωρίζονται σε παθητικούς, ενεργούς ή θερμικούς, μηχανικούς, ηλεκτρικούς αισθητήρες κ.λπ. Αυτοί οι αισθητήρες προωθούν τα δεδομένα τους στις συσκευές, με τη σειρά της η συσκευή καταναλώνει το υλικό και το στέλνει για επεξεργασία στο cloud, όπου συνήθως είναι συνδεδεμένες οι συσκευές αυτές, χρησιμοποιώντας μια πύλη για τη μετάδοση των δεδομένων στο δίκτυο εντός του cloud. Τα δεδομένα αυτά αποθηκεύονται στο cloud, το οποίο με τη σειρά του καθιστά προσβάσιμες τις υπηρεσίες και τις

[26] Stergiou C. L., Plageras A. P., Psannis K. E., Gupta B. B., 2019. “Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network”. In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.

λειτουργίες. Το IoT άρχισε να πολλαπλασιάζει την ανάπτυξή του, φτάνοντας από μισό δισεκατομμύριο διασυνδεδεμένων πραγμάτων το 2003 σε περίπου 25 δισεκατομμύρια το 2015. Μέχρι το τέλος του 2020, το IoT υπολλογιζόταν να αποκτήσει 50 δισεκατομμύρια και πλέον συσκευές συνδεδεμένες στο διαδίκτυο.[27]

Όμως, όσο κι αν οι εφαρμογές του IoT αυξάνονται συνεχώς με την πάροδο των ετών προκειμένου να κάνουν τη ζωή μας πιο άνετη και ομαλή, η ασφάλεια του χρήστη, των προσωπικών δεδομένων του και της ιδιωτικότητας του, εξακολουθούν να αποτελούν ένα από τα μεγαλύτερα ζητήματα για το IoT μέχρι σήμερα. Οι χάκερς μπορούν να παραβιάσουν τα συστήματα δεδομένων ή τις βάσεις δεδομένων εταιριών, αποκτώντας πρόσβαση στα δεδομένα του χρήστη. Ως εκ τούτου, υπάρχει επιτακτική ανάγκη να διασφαλισθεί η ασφάλεια των δεδομένων των χρηστών, ώστε να είναι αδύνατη η χρήση τους όταν πέσουν σε λάθος χέρια. Για το σκοπό αυτό, οι κυβερνήσεις διασφαλίζουν τη λογοδοσία για τη ροή δεδομένων στο πλαίσιο του IoT, διαδραματίζοντας κύριο ρόλο στο χειρισμό του και θεσπίζοντας κανονισμούς και νόμους για τις εταιρείες ώστε να ανταποκρίνονται στις απαιτήσεις των χρηστών.

Υπάρχουν ορισμένες προκλήσεις και ζητήματα στον ηθικό τομέα του IoT, τα οποία προκύπτουν από την κεντρική ηθική των ΤΠΕ και περιλαμβάνουν ζητήματα όπως η προσβασιμότητα, η ιδιωτικότητα, η ιδιοκτησία και η ακεραιότητα των πληροφοριών. Αρχικά, καθίσταται δύσκολη η ταυτοποίησή τους. Τα αντικείμενα πρέπει να ταυτοποιηθούν για να συνδεθούν με το IoT. Τα δεδομένα που συλλέγονται από αυτά τα αναρίθμητα αντικείμενα ωστόσο, καθιστούν δύσκολη την ακριβή ταυτοποίηση του ιδιοκτήτη του συγκεκριμένου αντικειμένου. Η συλλογή αυτών των δεδομένων χωρίς τη γνώση και τη συγκατάθεση του χρήστη αποτελεί ένα σημαντικό ζήτημα στα συστήματα IoT. Ο αυξανόμενος αριθμός των αντικειμένων του IoT καθιστά δύσκολο τον εντοπισμό και τον καθορισμό των ορίων του συστήματος. Η αντίθεση μεταξύ φυσικών, τεχνητών αντικειμένων και όντων μειώνεται, καθώς η μία κατηγορία μπορεί εύκολα να περάσει σε άλλη λόγω της προόδου της τεχνολογίας. Μια ακόμα πρόκληση του IoT είναι η ύπαρξη ζητημάτων μη προβλέψιμης συμπεριφοράς, μιας και οι άνθρωποι ενσωματώνονται στο περιβάλλον των συσκευών του IoT και αυτά τα "πράγματα" μπορεί, ενστικτωδώς, να παρεμβαίνουν πολλές φορές στα καθημερινά τους καθήκοντα, επηρεάζοντας συχνά τη ροή

[27] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

της καθημερινότητας. Γεννάται επομένως το ερώτημα εάν θα μπορούσαν, με την ίδια ευκολία, να επηρεάσουν και τις αποφάσεις των χρηστών.

Λόγω της απουσίας ξεκάθαρων ορίων, το σύστημα IoT μπορεί να αποτύχει να διακρίνει μεταξύ δημόσιων και ιδιωτικών δεδομένων, εφόσον και τα δύο συλλέγονται συλλογικά από τους αισθητήρες,[28] ενώ εξαιτίας του σταθερά αυξανόμενου αριθμού συσκευών, κόμβων, διακοπτών και δεδομένων, η κεντρική διακυβέρνηση και ο κεντρικός έλεγχος θα πάψουν να υφίστανται. Καθώς ο όγκος των πληροφοριών συνεχίζει να αυξάνεται, οι μεταφορές δεδομένων θα γίνουν πολύ ταχύτερες και οικονομικότερες ανάλογα με τη ζήτηση, γεγονός που θα έχει ως αποτέλεσμα την έλλειψη ελέγχου που οδηγεί σε περαιτέρω ευπάθειες.[29]

Μπορεί το IoT να αποτελέσει απειλή για τις καθημερινές συνήθειες και την διαβίωση των χρηστών; Μια παραβίαση στο δίκτυο IoT μπορεί να βλάψει άμεσα τη ζωή μας, επειδή πλέον μοιραζόμαστε ένα συλλογικό περιβάλλον με το σύστημα IoT. Για παράδειγμα, μια παραβίαση δεδομένων σε ένα έξυπνο σπίτι μπορεί να προκαλέσει διακυμάνσεις του θερμοστάτη,[30] θέτοντας τα άτομα σε κίνδυνο προς μη φυσιολογικές θερμοκρασίες, ομοίως, μια παραβίαση σε ένα έξυπνο αυτοκίνητο μπορεί να προκαλέσει παρερμηνείες και λάθη που αφορούν με ατυχήματα στους δρόμους.

Η ανάπτυξη του IoT εδραιώνεται στις περισσότερες χρήσεις της ζωής μας, όπως τα τηλέφωνα, οι οικιακές συσκευές, οι αισθητήρες, τα αυτοκίνητα, έξυπνα ρολόγια, συσκευές ιατρικής παρακολούθησης και πλαίσια θεμελίωσης μεγάλης κλίμακας. Η διατήρηση της ιδιωτικής ζωής εξελίσσεται σε δύσκολη υπόθεση, λόγω αυτού του κολοσσιαίου όγκου πληροφοριών. Καθώς αυτά τα πλαίσια συνεχίζουν να αναπτύσσονται και οι μεθοδολογίες ελέγχου και παρακολούθησης αυτών των συσκευών ψηφιοποιούνται και συνδέονται με το Διαδίκτυο, εγείρουν ζητήματα προστασίας της ιδιωτικής ζωής. Οι χάκερ μπορούν να διεισδύσουν σε κρίσιμες πληροφορίες αβίαστα, επειδή αυτές είναι προσβάσιμες μέσω του διαδικτύου. Ως εκ τούτου, το ζήτημα της εγγύησης της κατάλληλης ασφάλισης της ιδιωτικής ζωής του χρήστη είναι ουσιώδες.

Η ύπαρξη ενός νομικού πλαισίου μπορεί να μειώσει τους πιθανούς κινδύνους για τους χρήστες και να διασφαλίσει τη σωστή λειτουργία των δικτύων IoT. Για να

[28] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.
[29] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.
[30] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

εξασφαλιστεί η ασφάλεια και η προστασία των δεδομένων του χρήστη, αυτά θα πρέπει να διατηρούνται ιδιωτικά, με την παράλληλη θέσπιση ενός ισχυρού νομικού πλαισίου. Το πλαίσιο αυτό, θα μπορούσε να προέλθει και από την ενοποίηση υφιστάμενων νόμων, σε παγκόσμιο επίπεδο, όπως ο Electronic Communication Privacy Act και άλλοι όπως οι GDPR, HIPPA, FIPPS[31] αλλά και τη θέσπιση νέων νόμων που στοχεύουν άμεσα στο IoT και μπορούν να ελαχιστοποιήσουν τους κινδύνους και τις ανεπιθύμητες, συχνά εχθρικές δραστηριότητες.

4. Τεχνητή Νοημοσύνη, ΤΝ (Artificial Intelligence, AI)

Η ευρεία χρήση και η ταχεία εξέλιξη της τεχνητής νοημοσύνης μπορεί να είναι ένα από τα χαρακτηριστικά της τέταρτης βιομηχανικής επανάστασης. Ενώ αναπτύσσεται από τη δεκαετία του 1950, είναι πλέον παρούσα ως μια βιώσιμη και κυρίαρχη οντότητα, αν και παραμένει εξίσου μια από τις πιο παρεξηγημένες και υποτιμημένες τεχνολογίες τις εποχής μας. Αποτελεί επιπλέον έναν όρο ομπρέλα για διάφορους τύπους τεχνολογίας.

Η ιδέα ότι οι ανθρώπινες δραστηριότητες μπορούν να προσομοιωθούν από μια μηχανή βρίσκεται στον πυρήνα της έρευνας και της ανάπτυξης της ΤΝ, που ορίζεται ως «η ικανότητα μας μηχανής να μιμείται την ευφυή ανθρώπινη συμπεριφορά». Αυτό δεν συνεπάγεται αυτόματα την επίτευξη ενσυναίσθησης η συνείδησης ως αναγκαίο στόχο της ΤΝ. Η ΤΝ είναι σε μεγάλο βαθμό, το προϊόν ενός συνόλου οδηγιών, που ονομάζεται αλγόριθμος, ο οποίος περιγράφει μια διαδικασία που πρέπει να εκτελεστεί υπό ορισμένες συνθήκες. Βασικό στοιχείο για τη λειτουργία των συστημάτων τεχνητής νοημοσύνης είναι ότι δεν θα πρέπει να υπάρχει καθορισμένη κάθε πιθανή περίσταση. Είναι πολυτιμότερο να μπορεί ο υπολογιστής να διακρίνει μοτίβα και κατά συνέπεια, τα επαναλαμβανόμενα ή ελαφρώς μεταβαλλόμενα αποτελέσματα. Όσο περισσότερα είναι τα δεδομένα τόσο καλύτερα θα επιτευχθεί η μηχανική μάθηση και όσο καλύτερη είναι η ποιότητα των δεδομένων τόσο καλύτερη θα είναι και η Τεχνητή Νοημοσύνη.

Η πρόβλεψη για την παγκόσμια επένδυση σε συστήματα τεχνητής νοημοσύνης ανέρχεται σε 77,6 δισεκατομμύρια δολάρια μέχρι το 2022, ενώ η χρήση των συστημάτων αυτών θα μπορούσε να προσθέσει στην παγκόσμια οικονομία από 3,5 έως 5,8

[31] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

τρισεκατομμύρια δολάρια. Ο αντίκτυπος της χρήσης της Τεχνητής νοημοσύνης έχει γίνει ήδη αισθητός στην κοινωνία, ενώ θα συνεχίσουν να υπάρχουν αλλαγές στην αγορά εργασίας με την τεχνητή νοημοσύνη να παίρνει τη θέση της χειρωνακτικής, επαναλαμβανόμενης εργασίας. Οι εργαζόμενοι θα πρέπει να επανεκπαιδευτούν και όχι να αντικατασταθούν, καθώς οι επιχειρήσεις θα χρειάζονται την σωστή υποστήριξη για να δημιουργήσουν τα προγράμματα Τεχνητής Νοημοσύνης. Επιπλέον, ζητήματα ασφαλείας μπορεί να ανακύψουν όσο οι μηχανές αποκτούν δυνατότητες αναγνώρισης προσώπων, έχουν πρόσβαση σε προσωπικές πληροφορίες και εισχωρούν βαθύτερα στην καθημερινή μας ζωή. Έρευνες δείχνουν ότι το 37% ανθρώπων αισθάνεται ότι η κατάσταση θα είναι χειρότερη εξαιτίας της τεχνολογίας μέχρι το 2030.

Ο GDPR περιλαμβάνει διατάξεις που αφορούν τη ρύθμιση ζητημάτων σχετικών με την Τεχνητή Νοημοσύνη και ειδικά με τη δημιουργία προφίλ, το οποίο ορίζεται στο άρθρο 4 ως: "Κάθε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που αποτελείται από τη χρήση αυτών των δεδομένων για την αξιολόγηση ορισμένων προσωπικών πτυχών που σχετίζονται με ένα φυσικό πρόσωπο, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν ότι η απόδοση του φυσικού ατόμου στην εργασία, οικονομική κατάσταση, υγεία, προσωπικές προτιμήσεις, ενδιαφέροντα, αξιοπιστία, συμπεριφορά, τοποθεσία ή κινήσεις." Η αιτιολογική σκέψη 71 του GDPR αναφέρεται επίσης σε παραδείγματα αυτοματοποιημένης λήψης αποφάσεων «όπως η αυτόματη απόρριψη μιας διαδικτυακής πιστωτικής αίτησης ή πρακτικές ηλεκτρονικής πρόσληψης χωρίς καμία ανθρώπινη παρέμβαση». Η διατύπωση εδώ αντικατοπτρίζει την δυνητικά παρεμβατική φύση των τύπων αυτοματοποιημένου προφίλ που διευκολύνονται από τα μεγάλα αναλυτικά δεδομένα. Ο GDPR δεν εμποδίζει την αυτοματοποιημένη λήψη αποφάσεων ή τη δημιουργία προφίλ, αλλά δίνει στους ιδιώτες δικαίωμα να μην υπόκεινται σε καθαρά αυτοματοποιημένη λήψη αποφάσεων. Τονίζει ακόμα στο κείμενό του ότι, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να χρησιμοποιεί «κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για τη δημιουργία προφίλ».

Σχετικό παράδειγμα αποτελεί η πρακτική του credit scoring στην οποία προχώρησαν τα τραπεζικά ιδρύματα προκειμένου να αντιμετωπίσουν τις συνεχείς μεταβολές της αγοράς καταναλωτικής πίστης. Συγκεκριμένα η ανάπτυξη αυτοματοποιημένων διαδικασιών λήψης αποφάσεων, γνωστών ως credit scoring, που χρησιμοποιείται για την πρόβλεψη της πιθανότητας ένας υποψήφιος ή υφιστάμενος

δανειολήπτης να μη μπορέσει να εξυπηρετήσει το χρέος του.[32] Η αξιολόγηση της πιστοληπτικής ικανότητας του αιτούνται στηρίζεται στη σύγκριση μεταξύ των χαρακτηριστικών ενός πελάτη με πελάτες προηγούμενων χρονικών περιόδων, των οποίων τα δάνεια έχουν ήδη αποπληρωθεί. Εφόσον το αποτέλεσμα της μεθοδολογίας κριθεί από τον υπάλληλο ως μη ορθό, υπάρχει η δυνατότητα επέμβασης και επιπλέον αξιολόγησης της αίτησης, βασιζόμενη στην ανθρώπινη εμπειρία και κρίση του υπαλλήλου. Καθίσταται επομένως σαφές ότι, η πρακτική του credit scoring αξιοποιεί μεν τη χρήση τεχνητής νοημοσύνης, όλα όμως τα συλλεγόμενα δεδομένα καλύπτονται από το GDPR και ο δικαιούχος έχει δικαίωμα να μάθει τα κριτήρια με τα οποία απορρίφθηκε. Αυτός είναι και ο λόγος για τον οποίο χρησιμοποιούνται αλγόριθμοι μηχανικής μάθησης που μπορούν να εξηγηθούν (whitebox) έναντι αλγορίθμων όπως τα νευρωνικά δίκτυα που δεν μπορούν.

Τα προγράμματα AI δεν αναλύουν γραμμικά δεδομένα με τον τρόπο που είχαν αρχικά προγραμματιστεί. Αντ' αυτού μαθαίνουν από τα δεδομένα προκειμένου να ανταποκρίνονται έξυπνα σε νέα δεδομένα και να προσαρμόζουν ανάλογα τα αποτελέσματά τους, «… δίνοντας στους υπολογιστές συμπεριφορές που θα μπορούσαν να θεωρηθούν έξυπνες στους ανθρώπους». Η έννοια της τεχνητής νοημοσύνης υπάρχει εδώ και αρκετό καιρό, αλλά η ταχέως αυξανόμενη υπολογιστική ισχύς (ένα φαινόμενο γνωστό ως νόμος του Μουρ) οδήγησε την τεχνητή νοημοσύνη σε μια πρακτική πραγματικότητα. Μία από τις ταχέως αναπτυσσόμενες προσεγγίσεις με τις οποίες επιτυγχάνεται η ΤΝ είναι η Μηχανική Μάθηση (ML), με την οποία επιτυγχάνονται αποτελέσματα όπως η παραγωγή λόγου, εικόνας και αναγνώρισης προσώπων.

Σε γενικές γραμμές, η μηχανική μάθηση μπορεί να χωριστεί σε δύο τύπους μάθησης: εποπτευόμενη και χωρίς επίβλεψη. Στην εποπτευόμενη μάθηση, οι αλγόριθμοι αναπτύσσονται με βάση ετικέτες δεδομένων. Υπό αυτήν την έννοια, οι αλγόριθμοι έχουν εκπαιδευτεί να χαρτογραφούν από την είσοδο στην έξοδο με την παροχή δεδομένων με «σωστές» τιμές που έχουν ήδη εκχωρηθεί σε αυτούς. Αυτή η αρχική φάση «προπόνησης» δημιουργεί μοντέλα, στα οποία μπορούν να γίνουν προβλέψεις στη δεύτερη φάση. Αντίθετα, στη μη επιτηρούμενη μάθηση οι αλγόριθμοι δεν εκπαιδεύονται και αντ' αυτού, αφήνονται χωρίς οδηγίες σχετικά με το τι πρέπει να αναζητήσουν. Και στις δύο περιπτώσεις, η ισχύς της μηχανικής μάθησης έγκειται στην ικανότητα των αλγορίθμων να

[32] Tsolka, Evaggelia, 2019. Οι νέες τεχνολογίες υπό το πρίσμα του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Η διαδικασία του credit scoring και profiling στην περίπτωση Ελληνικού Τραπεζικού Ιδρύματος, Διπλωματική Εργασία, Χαροκόπειο Πανεπιστήμιο.

αλλάζουν την παραγωγή τους με βάση γνώσεις που έχουν αποκτήσει καθ' όλη την λειτουργία τους. Συνοπτικά, τα δεδομένα μεγάλης κλίμακας, μπορούν να θεωρηθούν ως ένα στοιχείο που είναι δύσκολο να αξιοποιηθεί. Το AI όμως μπορεί να θεωρηθεί ως το κλειδί για το ξεκλείδωμα της αξίας αυτών, ενώ η μηχανική μάθηση ως ένας από τους τεχνικούς μηχανισμούς που υποστηρίζουν και διευκολύνουν την τεχνητή νοημοσύνη. Ο συνδυασμός και των τριών εννοιών μπορεί να ονομαστεί «ανάλυση δεδομένων μεγάλης κλίμακας».[33]

5. Big Data Analytics - Ανάλυση Δεδομένων Μεγάλης Κλίμακας

Τα μεγάλα δεδομένα Big Data, είναι συλλογές δεδομένων μεγάλες σε όγκο ή αρκετά περίπλοκες για να γίνουν αντιληπτές με τις παραδοσιακές μεθόδους. Σε μία απόπειρα να κατανοήσουμε την σημασία τους, θα μπορούσαμε να φανταστούμε τα (μικρά) δεδομένα σαν το ιστορικό των αγορών που πραγματοποιούμε διαδικτυακά και τα μεγάλα δεδομένα, σαν το ιστορικό αγορών όλων των καταναλωτών της χώρας. Η ανάλυσή τους απαιτεί μια διαφορετική προσέγγιση για να καταφέρουμε να αποκτήσουμε οποιαδήποτε ουσιαστική γνώση και πληροφορία. Συνήθως, δεν αφορούν τις αναγκαίες πληροφορίες που μια επιχείρηση χρειάζεται για την καθημερινή της λειτουργία, διαθέτουν ωστόσο πληροφορίες των «παρασκηνιακών» ενεργειών οι οποίες κατόπιν συλλογής μπορούν να αποτελέσουν πηγή πληροφοριών και γνώσεων που διαφορετικά δεν θα μπορούσαν να εντοπιστούν. Τα μεγάλα δεδομένα περιέχουν επίσης αδόμητα δεδομένα από πηγές όπως είναι τα μέσα κοινωνικής δικτύωσης, τα μειλ ή τα σχόλια. Σύμφωνα με το περιοδικό Forbes, ήδη από το 2017 το 53% των εταιριών είχε υιοθετήσει την ανάλυση δεδομένων μεγάλου όγκου (Big Data Analytics). Προκειμένου να δοθεί μια ολοκληρωμένη εικόνα των δυνατοτήτων των μεγάλων δεδομένων, δε θα μπορούσε να μη γίνει αναφορά στα βασικά χαρακτηριστικά των Big Data, στα λεγόμενα 3 Vs : a. Volume (όγκος), b. Velocity (ταχύτητα), c. Variety (ποικιλία).

A.5.1 Volume

Τα μεγάλα δεδομένα αφορούν τον όγκο. Όγκος δεδομένων που μπορεί να φτάσει σε πρωτοφανή ύψη. Υπολογίζεται ότι κάθε μέρα δημιουργούνται 2,5 quintillion bytes

[33] Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2

δεδομένων, με αποτέλεσμα μέχρι το 2020 να έχουν δημιουργηθεί 40 zettabytes δεδομένων.[34] Ως αποτέλεσμα, δεν είναι πλέον ασυνήθιστο για τις μεγάλες εταιρείες να έχουν Terabytes - και ακόμη και Petabytes - δεδομένων σε συσκευές αποθήκευσης και σε διακομιστές. Τα δεδομένα αυτά βοηθούν στη διαμόρφωση του μέλλοντος μιας εταιρείας και των δράσεών της, ενώ παράλληλα παρακολουθούν την πρόοδο. Η έννοια των μεγάλων δεδομένων ασχολείται με την υψηλή ποσότητα και ποιότητα των δεδομένων που αποτελούνται από Terabytes και Petabytes δεδομένων.[35] Ο όγκος είναι το αντικείμενο των μεγάλων δεδομένων, επειδή κάθε μορφή ανάλυσης μεγάλων δεδομένων πρέπει να ενεργεί σε ένα μεγάλο σύνολο δεδομένων. Ένα από τα οφέλη της ανάλυσης μεγάλων δεδομένων είναι η ικανότητά της να προβλέπει και να δίνει πληροφορίες.

A.5.2 Velocity

Η αύξηση των δεδομένων και η συνακόλουθη σημασία τους έχει αλλάξει τον τρόπο με τον οποίο βλέπουμε τα δεδομένα. Υπήρχε κάποτε μια εποχή που δεν βλέπαμε τη σημασία των δεδομένων στον εταιρικό κόσμο, αλλά με την αλλαγή του τρόπου συλλογής τους, έχουμε καταλήξει να βασιζόμαστε σε αυτά καθημερινά. Η ταχύτητα ουσιαστικά μετράει πόσο γρήγορα έρχονται τα δεδομένα. Κάποια δεδομένα θα έρχονται σε πραγματικό χρόνο, ενώ άλλα θα έρχονται σε στιγμές και θα μας αποστέλλονται σε παρτίδες. Τα μεγάλα δεδομένα εξετάζουν πέρα από το μέγεθος και την ταχύτητα, την ποικιλία και ίσως την αξία και την αληθοφάνεια. Ο ορισμός των μεγάλων δεδομένων δεν πρέπει να εστιάζει μόνο στο μέγεθος των δεδομένων στην αποθήκευση, αλλά πρέπει να λαμβάνεται υπόψη η ποικιλία και η ταχύτητα των δεδομένων.

A.5.3 Variety

Ένα άλλο στοιχείο των μεγάλων δεδομένων είναι η ποικιλία των διαφόρων ασύμβατων μορφών δεδομένων, η μη ευθυγραμμισμένη δομή και τα ασυνεπή δεδομένα.[36] Αυτό είναι το χαρακτηριστικό που κάνει τα δεδομένα να είναι μεγάλα σε όγκο, επειδή περιλαμβάνουν τόσο δομημένα, ημιδομημένα όσο και αδόμητα δεδομένα. Παλαιότερα τα

[34] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[35] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[36] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

δεδομένα έπαιρναν τη μορφή αρχείων βάσεων δεδομένων - όπως excel, csv και access - πλέον οι ποικίλες πηγές προέρχονται, για παράδειγμα, από τα δεδομένα των μέσων κοινωνικής δικτύωσης, τα οποία περιλαμβάνουν κοινωνικά δίκτυα όπως το Facebook, το Instagram, το Snapchat, το Twitter και από ιστολόγια, Weblogs και Clickstreams, αλλά και νέες πηγές δεδομένων, όπως οι τεχνολογίες πραγματικού χρόνου, οι οποίες περιλαμβάνουν δεδομένα που παράγονται από μηχανές, π.χ. αισθητήρες, τσιπ, ρομπότ, διάφορες συσκευές και αναγνωριστικά ραδιοσυχνοτήτων (RFID), χωρικά δεδομένα π.χ. το Παγκόσμιο Σύστημα Εντοπισμού Θέσης (GPS) και δεδομένα συμβάντων.[37]

Τα μεγάλα δεδομένα είναι επομένως κάτι πολύ περισσότερο από απλώς μεγάλο αριθμό δεδομένων. Αποτελούν ένα τρόπο παροχής ευκαιριών για την αξιοποίηση νέων και υφιστάμενων δεδομένων, καθώς και την ανακάλυψη νέων τρόπων συλλογής μελλοντικών δεδομένων, που θα κάνουν πραγματικά τη διαφορά για τους λειτουργούς των επιχειρήσεων και θα τις καταστήσουν πιο ευέλικτες. Το πρόβλημα ασφάλειας και ιδιωτικότητας θα μπορούσε να λυθεί ή να ελαχιστοποιηθεί με τη χρήση εργαλείων και υπηρεσιών ανάλυσης μεγάλων δεδομένων. Τα μεγάλα δεδομένα είναι ένας δημοφιλής όρος, που χρησιμοποιείται για να περιγράψει την εκπληκτικά ταχεία αύξηση του όγκου των δεδομένων σε δομημένη και μη δομημένη μορφή. Η ακρίβεια των μεγάλων δεδομένων μπορεί να οδηγήσει σε μία πιο συνεπή λήψη αποφάσεων και οι καλύτερες αποφάσεις μπορούν να οδηγήσουν σε μεγαλύτερη επιχειρησιακή αποτελεσματικότητα, μείωση του κόστους και μείωση του κινδύνου. Τα μεγάλα δεδομένα συνήθως χρησιμοποιούν το Cloud Computing ως βασική τεχνολογία για να λειτουργήσουν[38]. Παραδοσιακά, η ανάλυση ενός συνόλου δεδομένων περιλαμβάνει, σε γενικές γραμμές, προσδιορισμό των σχετικών καταχωρήσεων προκειμένου να ληφθεί πληροφορία από τα δεδομένα. Η ανάλυση δεδομένων μεγάλης κλίμακας, από την άλλη πλευρά, συνήθως δεν εκκινείται με ένα προκαθορισμένο ερώτημα για τη δοκιμή μιας συγκεκριμένης υπόθεσης. Περιλαμβάνει συχνά μια «φάση ανακάλυψης» της εκτέλεσης μεγάλου αριθμού αλγορίθμων έναντι των δεδομένων για την εύρεση συσχετίσεων μεταξύ αυτών.

[37]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[38] Stergiou C.L., Psannis K.E., Gupta B.B., Ishibashi Y., "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", 2018. In: Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184.

Η τρέχουσα κατάσταση στη μηχανική μάθηση είναι γνωστή ως βαθιά μάθηση (deep learning), η οποία περιλαμβάνει την τροφοδοσία τεράστιων ποσοτήτων δεδομένων μέσω μη γραμμικών νευρωνικών δικτύων, τα οποία ταξινομούν τα δεδομένα με βάση τις εξόδους από κάθε διαδοχικό στρώμα. Η πολυπλοκότητα της επεξεργασίας δεδομένων μέσω τόσο μεγάλων δικτύων δημιουργεί ένα φαινόμενο «μαύρου κουτιού». Αυτό προκαλεί μια αναπόφευκτη αδιαφάνεια, που καθιστά δύσκολο να κατανοήσουμε τους λόγους για τις αποφάσεις που λαμβάνονται ως αποτέλεσμα της βαθιάς μάθησης. Αυτή η αδυναμία της ανθρώπινης νόησης να κατανοήσει τη λογική λήψης αποφάσεων, είναι μια από τις έντονες διαφορές μεταξύ της ανάλυσης δεδομένων μεγάλης κλίμακας και των πιο παραδοσιακών μεθόδων ανάλυσης δεδομένων. Για την ανάλυση δεδομένων για έρευνα, είναι συχνά απαραίτητο να βρεθεί ένα στατιστικά αντιπροσωπευτικό δείγμα ή μία τυχαία δειγματοληψία. Ωστόσο, μια μεγάλη προσέγγιση δεδομένων αφορά τη συλλογή και ανάλυση όλων των διαθέσιμων δεδομένων.

Ένα άλλο χαρακτηριστικό της ανάλυσης δεδομένων μεγάλης κλίμακας είναι η χρήση δεδομένων για διαφορετικό σκοπό από αυτόν για τον οποίο αρχικά συλλέχθηκαν τα δεδομένα, τα οποία μάλιστα ενδέχεται να έχουν παρασχεθεί ακόμη και από διαφορετικό οργανισμό. Αυτό συμβαίνει επειδή εξαιτίας της ανάλυσης δεδομένων μεγάλης κλίμακας, υπάρχει η δυνατότητα εξόρυξης δεδομένων για νέες πληροφορίες και ο εντοπισμός συσχετισμών, μεταξύ φαινομενικά διαφορετικών συνόλων δεδομένων. Οι εξελίξεις στην τεχνολογία όπως το IoT, καθώς και η εξελισσόμενη δύναμη της ανάλυσης δεδομένων μεγάλης κλίμακας, οδηγούν στην αντικατάσταση του παραδοσιακού τρόπου συνειδητής παροχής προσωπικών δεδομένων από τα υποκείμενα, π.χ. κατά τη συμπλήρωση μιας ηλεκτρονικής φόρμας, από διαφορετικούς και ποικίλους τρόπους συλλογής προσωπικών δεδομένων.

Σε πολλές περιπτώσεις τα δεδομένα που χρησιμοποιούνται έχουν δημιουργηθεί αυτόματα, για παράδειγμα παρακολουθώντας τη διαδικτυακή δραστηριότητα, αντί να παρέχονται συνειδητά από άτομα. Τα παρατηρούμενα δεδομένα καταγράφονται αυτόματα, π.χ. μέσω διαδικτυακών cookies ή αισθητήρων που συνδέονται με την αναγνώριση προσώπου,[39] ενώ τα παράγωγα δεδομένα παράγονται από άλλα δεδομένα με σχετικά απλό και απλό τρόπο, π.χ. τον υπολογισμό της κερδοφορίας των πελατών από τον αριθμό των επισκέψεων σε ένα κατάστημα και τα αντικείμενα που αγοράστηκαν. Με τον

[39] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

τρόπο αυτό, εταιρείες όπως η DataSift λαμβάνουν δεδομένα από το Twitter (με τη χρήση της υπηρεσίας GNIP), το Facebook και άλλα κοινωνικά μέσα και τα καθιστούν διαθέσιμα για ανάλυση, μάρκετινγκ και άλλους σκοπούς.[40] Το Γραφείο Εθνικών Στατιστικών (Office of National Statistics -ONS) πειραματίστηκε με τη χρήση γεωγραφικών δεδομένων από το Twitter, προκειμένου να εξάγει συμπεράσματα για τα πρότυπα διαμονής και κινητικότητας των ανθρώπων και να συμπληρώσει τις επίσημες εκτιμήσεις πληθυσμού. Οι φωτογραφίες με γεωγραφικές ετικέτες στο Flickr, μαζί με τα προφίλ των συντελεστών, έχουν χρησιμοποιηθεί ως αξιόπιστος τρόπος μέτρησης, για τον υπολογισμό του αριθμού των επισκεπτών σε τουριστικούς χώρους και την χώρα ή τον τόπο προέλευσης αυτών. Τα δεδομένα σχετικά με την προέλευση των αγοραστών, μπορούν να χρησιμοποιηθούν για το σχεδιασμό διαφημιστικών καμπανιών, ενώ τα δεδομένα σχετικά με τα μοτίβα κίνησης σε ένα αεροδρόμιο, μπορούν να χρησιμοποιηθούν ακόμα και για τον καθορισμό του ύψους των ενοικίων των καταστημάτων και των εστιατορίων.[41]

Ο ΓΚΠΔ διατηρεί στο κείμενό του έντονη τη σημασία της δικαιοσύνης. Στο άρθρο 5 παράγραφος 1 στοιχείο α) αναφέρει ότι τα προσωπικά δεδομένα πρέπει να «υποβάλλονται σε επεξεργασία με δίκαιο, νόμιμο και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων». Συχνά η ανάλυση μεγάλου όγκου δεδομένων, χαρακτηρίζεται ως απειλητική για τα προσωπικά δεδομένα και αυτό συμβαίνει επειδή, περιλαμβάνει την επαναχρησιμοποίηση δεδομένων με απρόσμενους τρόπους, τη χρήση σύνθετων αλγορίθμων και την εξαγωγή συμπερασμάτων σχετικά με άτομα, έχοντας συχνά απρόσμενα και μερικές φορές ανεπιθύμητα αποτελέσματα. Επομένως, ένα βασικό ερώτημα για οργανισμούς που χρησιμοποιούν προσωπικά δεδομένα για την ανάλυση δεδομένων μεγάλης κλίμακας είναι, εάν η επεξεργασία είναι δίκαιη, λαμβάνοντας βεβαίως υπόψη ότι ορισμένοι τύποι δεδομένων μεγάλης κλίμακας, όπως η δημιουργία προφίλ, μπορεί να έχουν διεισδυτικές επιπτώσεις για τα άτομα. Οι οργανισμοί πρέπει επομένως να εξετάσουν εάν η χρήση των προσωπικών δεδομένων σε εφαρμογές μεγάλων δεδομένων, ανταποκρίνεται στις εύλογες προσδοκίες των ανθρώπων, συχνά όμως η πολυπλοκότητα των μεθόδων ανάλυσης μεγάλων δεδομένων, όπως η μηχανική μάθηση, μπορεί να καταστήσει δύσκολη την τήρηση της, απαιτούμενης από τους οργανισμούς, διαφάνειας

[40] Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2

[41] Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2

σχετικά με την επεξεργασία των προσωπικών δεδομένων. Για τον λόγο αυτό η αξιολόγηση του κατά πόσο η επεξεργασία είναι δίκαιη, πρέπει να περιλαμβάνει την εξέταση των επιπτώσεων της επεξεργασίας στα άτομα μαζί με τις προσδοκίες τους σχετικά με τον τρόπο χρήσης των δεδομένων τους, αλλά και με την απαραίτητη διαφάνεια σχετικά με το ποιες πληροφορίες χρησιμοποιούνται για την επεξεργασία.

Τα μεγάλα δεδομένα είναι τεράστια σε όγκο, υψηλή ταχύτητα, διαφορετική ποικιλία, εξαντλητική έκταση, λεπτομερή ανάλυση, σχεσιακή και ευέλικτη φύση. Έχει γίνει επίσης και μια διάκριση με βάση την πηγή των δεδομένων όπως αυτά κατευθύνθηκαν, αυτοματοποιημένα και εθελοντικά δεδομένα. Τα κατευθυνόμενα δεδομένα προέρχονται από το άμεσο βλέμμα της τεχνολογίας παρακολούθησης σε ένα μέρος ή άτομο. Τα αυτοματοποιημένα δεδομένα προέρχονται από τις ανθρώπινες δραστηριότητες σε ψηφιακές συσκευές, για παράδειγμα, παγκόσμιο σύστημα εντοπισμού θέσης (GPS) σε snapchat ή Χάρτες Google, cookie πλοήγησης σε ιστότοπους κ.λπ.[42]

Παρόλο που τα μεγάλα δεδομένα, η τεχνητή νοημοσύνη και η μηχανική μάθηση διαδίδονται ευρέως στον δημόσιο και τον ιδιωτικό τομέα και μπορεί να θεωρούνται όλο και περισσότερο ως "συνήθης επιχειρηματική δραστηριότητα", τα βασικά χαρακτηριστικά της ανάλυσης μεγάλων δεδομένων εξακολουθούν να αντιπροσωπεύουν μια βαθμιαία αλλαγή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η ανάλυση μεγάλων δεδομένων με τη χρήση τεχνικών που έχουν καταστεί δυνατές μέσω της ΤΝ δημιουργεί επιπτώσεις στην προστασία των δεδομένων και καθιστά δυσκολότερη την εφαρμογή των αρχών προστασίας δεδομένων, λόγω της χρήσης τους σε ένα πλαίσιο μεγάλων δεδομένων. Οι επιπτώσεις αυτές προκύπτουν όχι μόνο από τον όγκο των δεδομένων, αλλά και από τους τρόπους με τους οποίους αυτά παράγονται, την τάση εύρεσης νέων χρήσεων για αυτά, την πολυπλοκότητα της επεξεργασίας και την πιθανότητα απροσδόκητων συνεπειών για τα άτομα.[43]

[42]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[43]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

ΙΙ. Οι παρεμβολές του Γενικού Κανονισμού Προστασίας Δεδομένων

1. ΓΚΠΔ και Τεχνητή Νοημοσύνη, GDPR and AI

Η Τεχνητή Νοημοσύνη αποτελεί πρωταρχικό παράγοντα της λεγόμενης Τέταρτης Βιομηχανικής Επανάστασης όχι μόνο για τις τεχνολογικές δυνατότητες αλλά και για το γεγονός ότι αγγίζει τον μέσο χρήστη μέσω της προσβασιμότητας σε φθηνή υπολογιστική ισχύ και σύνδεση. Τα προσωπικά δεδομένα και η Τεχνητή Νοημοσύνη αναπτύσσουν μία «σχέση» διπλής κατεύθυνσης, εφόσον η πρώτη επιτρέπει τη συλλογή και την αξιοποίηση μεγάλου όγκου δεδομένων αλλάζοντας συχνά τον σκοπό και τη χρήση τους. Μπορούν ωστόσο ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679, οι αρχές και τα ρυθμιστικά εργαλεία που εισάγει, να αντιμετωπίσουν τις νομικές προκλήσεις της τεχνητής νοημοσύνης και να εγγυηθούν την προστασία των δικαιωμάτων των προσώπων;

Η τεχνητή νοημοσύνη ενισχύεται από: α) τη διαθεσιμότητα και την προσβασιμότητα τεράστιας -και συχνά φθηνής- υπολογιστικής ισχύος και υποδομής, β) τη συνεχώς αυξανόμενη διαθεσιμότητα μεγάλων συνόλων δεδομένων από διάφορους τομείς, γ) την εξέλιξη στατιστικών και πιθανολογικών μεθόδων, δ) την τάση να μετατρέπονται όλο και περισσότεροι χώροι σε περιβάλλοντα με γνώμονα την τεχνολογία ή φιλικά προς την πληροφορική. Η τεχνητή νοημοσύνη τροφοδοτείται από ένα ευρύ φάσμα τεχνολογικών οδηγών: συνδεσιμότητα κινητής τηλεφωνίας, υποδομή cloud, πολλαπλασιασμός αισθητήρων, πρόοδος στην επεξεργαστική ισχύ, λογισμικό μηχανικής μάθησης και αποθήκευση[44]. Η μηχανική εκμάθηση εκμεταλλεύεται την επεκτάσιμη επεξεργασία τεράστιων συνόλων δεδομένων που παρέχεται από την ευρεία και χαμηλού κόστους διαθεσιμότητα του cloud και των ουσιαστικά απεριόριστων πόρων του. Τα τελευταία χρόνια, οι πάροχοι Cloud άρχισαν να προσφέρουν υπηρεσίες και εργαλεία μηχανικής εκμάθησης που υποστηρίζονται από το cloud, με σημαντική εστίαση στην προγνωστική ανάλυση. Ωστόσο, η τεχνητή νοημοσύνη συνεχίζει να αναπτύσσεται ειδικά μέσω του Big Data και του γενικού Internet of Things.

Η πανταχού παρούσα τεχνητή νοημοσύνη παρά την χρησιμότητά της, εγείρει πολλά ηθικά ζητήματα. Στον τομέα της υγειονομικής περίθαλψης, για παράδειγμα, τα

[44] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

ρομπότ μεταξύ άλλων μαθαίνουν να παρακολουθήσουν την ευημερία των ασθενών, αλλά και να συνταγογραφήσουν φάρμακα εάν αυτό είναι απαραίτητο. Τι συμβαίνει όμως στην περίπτωση που ένα σύστημα AI για παράδειγμα συνιστά λάθος φάρμακο για έναν ασθενή ή δεν παρατηρεί όγκο σε ακτινολογική σάρωση; Η εκτεταμένη χρήση της τεχνητής νοημοσύνης εφαρμόζεται επί του παρόντος, ή σχεδιάζεται να βρίσκεται και σε πολλά εθνικά δικαστικά συστήματα, εγείροντας τις ίδιες αμφιβολίες και προβληματισμούς.

Τα έξυπνα συστήματα μεταφοράς (ITS) και οι ευρέως διαδεδομένοι αισθητήρες που είναι εγκατεστημένοι σε μια έξυπνη πόλη μπορούν, μεταξύ άλλων, να αποτρέψουν υψηλά ποσοστά ατυχημάτων, κυκλοφοριακή συμφόρηση και ατμοσφαιρική ρύπανση από την κυκλοφορία και τις εκπομπές άνθρακα, ωστόσο, η παράλληλη χρήση καμερών αναγνώρισης, δεδομένων κινητής τηλεφωνίας και άλλων τεχνολογιών που χρησιμοποιούνται για την παρακολούθηση ατόμων είτε στους δρόμους είτε στις δημόσιες συγκοινωνίες, εγείρουν ανησυχίες σχετικά με το απόρρητο. Η χρήση αυτόνομων αυτοκινήτων, για παράδειγμα, μπορεί μεν να μειώσει τα αυτοκινητιστικά ατυχήματα, αλλά είναι εξαιρετικά δύσκολο να απαντηθεί το ηθικό ερώτημα σχετικά με τον τρόπο με τον οποίο πρέπει να προγραμματίζονται τα αυτοκινούμενα ώστε να «συμπεριφέρονται» ορθά. Ως επιπλέον παράδειγμα, ένα εργαλείο AI που βοηθά ή εκτελεί αποκλειστικά διαδικασίες πρόσληψης, μπορεί να είναι μια εκπληκτική τεχνολογική καινοτομία για μια γρήγορη και ακριβή επιλογή υποψηφίου, αλλά η εξόρυξη των προσωπικών δεδομένων λόγω της μηχανικής μάθησης μπορεί να οδηγήσει σε διακρίσεις. Τα bots που χρησιμοποιούνται για την απόσυρση των δημοσιεύσεων στα μέσα κοινωνικής δικτύωσης, τη γλωσσική ανάλυση των δειγμάτων γραφής των υποψηφίων, τις συναισθηματικές καταστάσεις, τις μη λεκτικές συμπεριφορές αποτελούν μεθόδους που μπορούν πλέον να χρησιμοποιηθούν για την πρόσληψη ενός υποψηφίου. Παρόλα αυτά, δεν παύουν να αποτελούν μεθόδους για τις οποίες ο υποψήφιος δεν έχει ενημερωθεί νόμιμα, δίκαια και με διαφάνεια ή δεν είχε απαραίτητα προηγουμένως δώσει τη συγκατάθεσή του, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (εφεξής GDPR).

Οι κατευθυντήριες γραμμές δεοντολογίας για την αξιόπιστη τεχνητή νοημοσύνη σύμφωνα με την ομάδα εμπειρογνωμόνων υψηλού επιπέδου για την τεχνητή νοημοσύνη της Ευρωπαϊκής Επιτροπής, είναι ανθρωποκεντρικές, με κύριο άξονά τους την αξιοπιστία. Όπως προκύπτει και από τα κείμενα των Συνθηκών της ΕΕ, του Χάρτη των Θεμελιωδών Δικαιωμάτων, τη Σύμβαση του Οβιέδο και του Γενικού Κανονισμού προστασίας προσωπικών δεδομένων, ο σεβασμός της ανθρώπινης αξιοπρέπειας είναι ύψιστης

προτεραιότητας. Η αξία του ανθρώπου παραμένει αδιαπραγμάτευτη, ώστε να μπορούμε να μιλάμε για την αρχή της αυτονομίας, πράγμα που σημαίνει ότι τα άτομα είναι ελεύθερα να κάνουν τις δικές τους επιλογές για τη δική τους ζωή και αυτό μπορεί να συμβαίνει επειδή, έχοντας προηγουμένως ενημερωθεί, έχουν δώσει τη συγκατάθεσή τους από την οποία μπορούν να αποσυρθούν ή όχι.

Είναι γεγονός ότι η φύση των συστημάτων τεχνητής νοημοσύνης είναι δια μέτρου αντίθετη με ορισμένες από τις πιο βασικές αρχές του ΓΚΠΔ, καθιστώντας δύσκολη την προσπάθεια περιορισμού αυτών υπό το πλαίσιο του νέου κανονισμού προστασίας για τα προσωπικά δεδομένα. Στο πλαίσια της συγκεκριμένης εργασίας αξίζει να γίνει συνοπτική μνεία αυτών των υφιστάμενων αντιθέσεων και στη συνέχεια, αναλυτική αναφορά σε αυτές. Τα συστήματα τεχνητής νοημοσύνης είναι κατά πρώτον, φύσει ασυμβίβαστα με την αρχή του περιορισμού του σκοπού, καθώς ανιχνεύουν μόνα τους μοτίβα και συσχετισμούς μεταξύ των δεδομένων, με σκοπό την ανάλυση αυτών. Είναι επίσης ασυμβίβαστα με την αρχή της ελαχιστοποίησης δεδομένων, επειδή η λειτουργία τους υποστηρίζεται από τη χρήση όλων των διαθέσιμων δεδομένων, πέρα από τα απλώς απαραίτητα και σχετικά με τον σκοπό της επεξεργασίας. Η εξάρτησή τους από τα Big Data, έρχεται σε σύγκρουση με την αρχή της ακρίβειας και απαιτεί την αντικατάσταση αυτών με δεδομένα καλύτερης ποιότητας, προερχόμενα από διάφορες ομάδες ή τον δημόσιο τομέα. Ωστόσο και στις περιπτώσεις που χρησιμοποιούνται ακριβή δεδομένα, αυτά τείνουν να μένουν αποθηκευμένα για απεριόριστες περιόδους, αντίθετα με την αρχή του χρονικού περιορισμού αποθήκευσης. Η αδυναμία τους να παράσχουν ενημέρωση για συγκατάθεση σε συνδυασμό με την απαγόρευση της αποκλειστικά αυτοματοποιημένης λήψης αποφάσεων και την επεξεργασία δεδομένων ειδικής κατηγορίας περιορίζουν τις νομικές βάσεις επεξεργασίας(κατά την αρχή της νομιμότητας). Η αρχή της διαφάνειας, κρίνεται μεν χρήσιμη για την αξιολόγηση της διαδικασίας που ακολουθείται από την τεχνητή νοημοσύνη, αλλά είναι δύσκολο να ευθυγραμμιστεί με τους κινδύνους χειραγώγησης, τις απειλές ασφάλειας και τις γνωστοποιήσεις πνευματικής ιδιοκτησίας.[45] Κάτω από αυτό το πρίσμα θα προχωρήσουμε σε σύντομη ανάλυση βασικών αρχών του ΓΚΠΔ και πώς αυτές τυγχάνουν εφαρμογής στο πεδίο της Τεχνητής Νοημοσύνης, σε μια προσπάθεια να τονιστεί η αντίθεση των αρχών αυτών με τις λειτουργίες της ΤΝ.

[45] Siapka, Anastasia, 2018. The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI, Διπλωματική Εργασία, Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών.

1.1 Η Αρχή της Διαφάνειας στο πεδίο της Τεχνητής Νοημοσύνης (αρ.5 παρ.1 στοιχ. α΄ ΓΚΠΔ)

Η πολυπλοκότητα της επεξεργασίας που γίνεται με τη χρήση ΤΝ και το γεγονός ότι τέτοια επεξεργασία δεν μπορεί να είναι πλήρως κατανοητή, ειδικά όταν βασίζεται σε μηχανική εκμάθηση, καθιστά ιδιαίτερα δύσκολη τη διασφάλιση της διαφάνειας. Το ζήτημα της διαφάνειας μπορεί να προκύψει σε δύο χρονικά σημεία, όταν οι πληροφορίες για τα δεδομένα του υποκειμένου τοποθετούνται σε ένα πληροφοριακό σύστημα που περιλαμβάνει αλγόριθμους ΤΝ (εκ των προτέρων διαφάνεια) ή αφότου το αλγοριθμικό μοντέλο του συστήματος χρησιμοποίησε τα δεδομένα του υποκειμένου, για να εξάγει συγκεκριμένα αποτελέσματα (εκ των υστέρων διαφάνεια). Σε ότι αφορά όμως τα συστήματα Τεχνητής Νοημοσύνης κρίνεται πολύ δυσχερής η εφαρμογή της καθώς σύμφωνα με τον Burrell (2016) διακρίνονται από τρεις μορφές αδιαφάνειας : α) Τεχνικός αναλφαβητισμός, κάτι το οποίο καθιστά το άρθρο 13 για πρόσβαση στην λογική που χρησιμοποιείται από τον αλγόριθμο άχρηστο για τον μέσο άνθρωπο, β) Επιθυμητή αδιαφάνεια εκ μέρους των εταιρειών, με πρόφαση ότι ο αλγόριθμος αποτελεί περιουσιακό στοιχείο και θα είναι εις βάρος τους να αποκαλυφθεί η λογική τους, γ) Αναντιστοιχία μεταξύ της ανθρώπινης σημασιολογικής ερμηνείας και κρίσης και της λήψης αποφάσεων μέσω αλγορίθμων υψηλής βελτιστοποίησης και πολυπλοκότητας. Καταλήγοντας, η αδιαφάνεια που περιβάλλει με έναν πέπλο τους αλγορίθμους τεχνητής νοημοσύνης δε βοηθάει τον μέσο άνθρωπο να καταλάβει ουσιαστικά εάν επηρεάστηκε αρνητικά ή όχι από την απόφαση που πάρθηκε για εκείνον, ώστε να αποφασίσει να αμφισβητήσει την απόφαση σύμφωνα με το άρθρο 22 παρ.3 του ΓΚΠΔ.[46]

1.2 Η Αρχή Περιορισμού του Σκοπού στο πεδίο της Τεχνητής Νοημοσύνης (αρ.5 παρ.1 στοιχ. β΄ ΓΚΠΔ)

Η αρχή του περιορισμού του σκοπού αποτελεί μία από τις θεμελιώδεις αρχές του κανονισμού για την προστασία των προσωπικών δεδομένων. Η αρχή αυτή φαίνεται να βρίσκεται σε δυσαρμονία με τις δυνατότητες της ΤΝ για επεξεργασία. Αυτό συμβαίνει διότι, η χρήση αλγορίθμων και η δυνατότητα αξιοποίησης της μηχανικής εκμάθησης βασίζεται και τροφοδοτείται από την τάση να συγκεντρώνονται όσο το δυνατόν

[46] Tsolka, Evaggelia, 2019. Οι νέες τεχνολογίες υπό το πρίσμα του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Η διαδικασία του credit scoring και profiling στην περίπτωση Ελληνικού Τραπεζικού Ιδρύματος, Διπλωματική Εργασία, Χαροκόπειο Πανεπιστήμιο.

περισσότερα δεδομένα και από την παραγωγή νέων δεδομένων και νέων τύπων δεδομένων. Ο επαναπροσδιορισμός του σκοπού της χρήσης των δεδομένων είναι ένα κύριο χαρακτηριστικό των εφαρμογών ΤΝ, στο συνδυασμό τους με τα Μεγάλα Δεδομένα.

Για να εξακριβωθεί πότε ο επαναπροσδιορισμός του σκοπού είναι νόμιμος, πρέπει πρώτα να διευκρινιστεί αν ο καινούριος σκοπός είναι συμβατός ή όχι με τον σκοπό για τον οποίο εξαρχής συλλέχθηκαν τα δεδομένα. Σύμφωνα με τη γνώμη της Ομάδας Εργασίας του Άρθρου 29, τα σχετικά κριτήρια είναι τα εξής: α) η απόσταση ανάμεσα στο νέο σκοπό και τον πρώτο σκοπό, β) η αντιστοίχιση του νέου σκοπού με τις προσδοκίες του υποκειμένου των δεδομένων, με τη φύση των δεδομένων και με την επίδρασή του στα ενδιαφέροντα του υποκειμένου των δεδομένων και γ) τα μέτρα προστασίας που λαμβάνει ο υπεύθυνος επεξεργασίας, ώστε να διασφαλίσει το νόμιμο της επεξεργασίας και να εμποδίσει τυχόν αδικαιολόγητες επιπτώσεις. Αντιθέτως, η αρχή του περιορισμού του σκοπού της επεξεργασίας των δεδομένων, δεν απαγορεύει την επαναχρησιμοποίηση για επιστημονικούς ή/και στατιστικούς σκοπούς. Η έννοια της επιστημονικής έρευνας θα πρέπει να ερμηνεύεται διασταλτικά (Αιτιολογική σκέψη 159).

1.3 Η Αρχή της Συγκατάθεσης στο πεδίο της Τεχνητής Νοημοσύνης (αρ.6 παρ.1 στοιχ. α΄ ΓΚΠΔ)

Η συγκατάθεση πρέπει να πληροί τις απαιτήσεις που ορίζει ο κανονισμός στο άρθρο 4 παράγραφος 11 και να περιέχει τις εξής προϋποθέσεις: «ελεύθερη, συγκεκριμένη, ενημερωμένη και ξεκάθαρη ένδειξη των επιθυμιών του υποκειμένου των δεδομένων με την οποία, με δήλωση ή με σαφή καταφατική ενέργεια, υποδηλώνει συμφωνία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν». Στο άρθρο 7 ορίζονται οι υποχρεώσεις του υπευθύνου επεξεργασίας όταν η συγκατάθεση αποτελεί νόμιμη βάση επεξεργασίας, ενώ στον GDPR δίνεται έμφαση και στον τρόπο υποβολής του αιτήματος συναίνεσης που απαιτεί κατανοητή και εύκολα προσβάσιμη μορφή, με χρήση σαφούς και απλής γλώσσας (άρθρο 7 παρ. 2). Σε περίπτωση αιτήματος με ηλεκτρονικά μέσα, αυτό πρέπει να είναι σαφές, περιεκτικό και να μην διαταράσσει άσκοπα τη χρήση της υπηρεσίας για την οποία παρέχεται (αιτιολογική σκέψη 32).

Η νόμιμη επεξεργασία δεν μπορεί να βασίζεται σε σιωπηρή συγκατάθεση, όπως είναι η εγκατάσταση της εφαρμογής ή τα προεπιλεγμένα πλαίσια εντός αυτής. Η συναίνεση οφείλει να αναφέρεται σε συγκεκριμένους σκοπούς και χρήσεις προσωπικών πληροφοριών. Στην ευρωπαϊκή προσέγγιση το γεγονός ότι τα άτομα δημοσιεύουν

πληροφορίες για αυτά στα μέσα κοινωνικής δικτύωσης δεν υποδηλώνει ότι νομιμοποιούν –μέσω σιωπηρής συγκατάθεσης– οποιαδήποτε δευτερεύουσα, περαιτέρω χρήση.[47]

Επιπλέον, η συναίνεση, και ιδιαίτερα η «ψηφιακή», έχει επικριθεί επανειλημμένα και εντατικά, επειδή είναι πιθανό να μετατραπεί σε μια κενή, τελετουργική διαδικασία, με αποτέλεσμα να οδηγήσει το υποκείμενο σε «πλάνη». Διαδικτυακά, η συναίνεση παρέχεται συνήθως κάνοντας κλικ σε έναν σύνδεσμο περί «πολιτικής απορρήτου», συχνά τοποθετούμενου στο κάτω μέρος κάθε σελίδας ή στις ρυθμίσεις της εφαρμογής. Η συναίνεση μερικές φορές δηλώνεται κάνοντας κλικ σε ένα πλαίσιο «OK» σε ένα cookie banner ή σε κάποιο αναδυόμενο παράθυρο ρυθμίσεων (έκφραση ενέργειας) ή συνηθέστερα παραμένοντας στον ιστότοπο χωρίς έξοδο ή αλλαγή ρυθμίσεων (παράλειψη).

Το μοντέλο συναίνεσης έχει επίσης επικριθεί λόγω του δυαδικού χαρακτήρα του, καθώς προσφέρεται περιορισμένη, κυρίως δυαδική επιλογή, σε ένα «χρήστη» που βρίσκεται σε ένα ελεγχόμενο διαδικτυακό περιβάλλον και αναμένει κέρδη από μια ανταποδοτική διαδικτυακή δραστηριότητα και για το λόγο αυτό, είναι πρόθυμος και ενθαρρύνεται να παράσχει συγκατάθεση. Νέες προσεγγίσεις συναίνεσης έχουν προταθεί για να ξεπεραστούν τα μειονεκτήματα αυτού του δυαδικού μοντέλου: ο Επίτροπος Πληροφοριών[48] πρότεινε «μια διαδικασία βαθμιαίας συναίνεσης, στην οποία οι άνθρωποι μπορούν να συναινέσουν ή όχι, σε διαφορετικές χρήσεις των δεδομένων τους σε όλη τη σχέση τους με έναν πάροχο υπηρεσιών, αντί να υπάρχει μια απλή δυαδική επιλογή στην αρχή», η οποία θα μπορούσε ή θα έπρεπε να σχετίζεται με «ακριβώς έγκαιρες ειδοποιήσεις». Οι V. Mayer-Schönberger και Y. Padova[49] προτείνουν τη μετάβαση από μηχανισμό που βασίζεται στη συλλογή σε μηχανισμό που βασίζεται στη χρήση. Ωστόσο, παραμένει αμφίβολο εάν το λεγόμενο μοντέλο «ειδοποίησης και συναίνεσης» είναι κατάλληλο ή πρακτικό σε ένα «πλαίσιο μεγάλων δεδομένων-AI».

---

[47] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[48] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[49] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

Δεδομένης της ηθικά μετασχηματιστικής φύσης της, η (έγκυρη) συναίνεση απαιτεί ένα σαφώς καθορισμένο πεδίο δράσης, δηλαδή το άτομο που συναινεί πρέπει να έχει τις σχετικές πληροφορίες ώστε να γνωρίζει σε τι συναινεί. Στις περιπτώσεις αυτές η χρήση του «opt-in» αντί του «opt-out» συμβαδίζει με τη διαφάνεια[50]. Προκειμένου να είναι έγκυρη η συγκατάθεσή του, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει, τουλάχιστον, την ταυτότητα του υπευθύνου επεξεργασίας, τις κατηγορίες δεδομένων προς επεξεργασία και τους σκοπούς της επεξεργασίας για τους οποίους προορίζονται τα δεδομένα προσωπικού χαρακτήρα. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους.

Παραμένει αμφισβητήσιμο εάν αυτή η νομοθετική σειρά θα διασφαλίσει ότι «οι χρήστες θα εξετάζουν, θα αξιολογούν ορθολογικά και θα ανταποκρίνονται σε αυτές τις πληροφορίες κατά την άσκηση των δικαιωμάτων συγκατάθεσής τους», καθώς οι χρήστες διστάζουν να διαβάσουν τις ειδοποιήσεις απορρήτου[51]. Ακόμη και αν οι πολιτικές και οι ειδοποιήσεις ικανοποιούν τις νομικές υποχρεώσεις, είναι πολύ αμφίβολο εάν η συναίνεση μπορεί να θεωρηθεί έτσι επαρκής ως νομική βάση.

Μια περαιτέρω πρόκληση αναφέρεται στον αντίκτυπο της ανάκλησης της συγκατάθεσης. Το δικαίωμα ανάκλησης της συγκατάθεσης αντικατοπτρίζει και εγγυάται το δικαίωμα του ατόμου για ενημερωτική αυτοδιάθεση, ωστόσο, η ανάκληση της συγκατάθεσης και, αντίστοιχα, η απόσυρση/διαγραφή δεδομένων μπορεί να αποτελέσει απειλή για την ανάπτυξη της τεχνητής νοημοσύνης. Η ανάκληση αυτή θα μπορούσε να περιορίσει τον όγκο των διαθέσιμων δεδομένων για μάθηση. Το σύστημα AI δε θα μπορεί πλέον να χρησιμοποιεί αυτές τις συγκεκριμένες αναφορές δεδομένων για την ανάπτυξη των αλγορίθμων του. Ως εκ τούτου, πρέπει να διασφαλίσει ότι το σύνολο δεδομένων δεν έχει παραμορφωθεί ή υπονομευθεί λόγω της απόσυρσης ορισμένων δεδομένων, η οποία αποτελεί σημαντικό πρόβλημα για οργανισμούς με μικρότερα σύνολα δεδομένων (π.χ.

[50] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) “ARTIFICIAL INTELLIGENCE-PROOF” ?

[51] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) “ARTIFICIAL INTELLIGENCE-PROOF” ?

υπηρεσίες εκκίνησης)[52]. Παρόλα αυτά, η τεχνητή νοημοσύνη συνεχίζει να μαθαίνει από προηγούμενα δεδομένα και τίθεται το ερώτημα πώς μπορεί να σταματήσει ταυτόχρονα η μάθηση της τεχνητής νοημοσύνης από αυτά τα δεδομένα, χωρίς να επηρεαστεί η προηγούμενη ανάπτυξή της; Οι λύσεις που προτείνονται είναι τεχνικής φύσης με τη μορφή απομόνωσης ή διαγραφής του σκέλους μάθησης, το οποίο ενσωμάτωσε τα πλέον μη συναινετικά δεδομένα ή επανεκπαίδευση των υπαρχόντων μοντέλων τεχνητής νοημοσύνης χρησιμοποιώντας τα τροποποιημένα σύνολα δεδομένων.[53]

1.4 Η Αρχή Αναλογικότητας και Αρχή ελαχιστοποίησης των δεδομένων στο πεδίο της Τεχνητής Νοημοσύνης (αρ.5 παρ.1 στοιχ. γ΄ ΓΚΠΔ)

Η Οδηγία 95/46/ΕΚ και του Συμβουλίου της 24ης Οκτωβρίου 1995 ενσωμάτωσε την αρχή της αναλογικότητας, ως μία από τις βασικές αρχές που σχετίζονται με την σύννομη χρήση των προσωπικών δεδομένων και ως ένα εξισορροπητικό στοιχείο, ανάμεσα στα δικαιώματα και τα ενδιαφέροντα του υπεύθυνου επεξεργασίας και του υποκειμένου των δεδομένων. Ένα παράδειγμα καινοτομίας που συνεπάγεται η υιοθέτηση του ΓΚΠΔ είναι, η μεγαλύτερη έμφαση που δόθηκε στην έννοια της αναλογικότητας, μέσα από την αποκαλούμενη ως «αρχή ελαχιστοποίησης των δεδομένων» (Άρθρο 5§1 στοιχ. γ').

Το Άρθρο 25§2 αναφέρεται επίσης, στην ελαχιστοποίηση των δεδομένων. Σχετίζεται με την ΤΝ και τα Μεγάλα Δεδομένα, καθώς διατάσσει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων για να διασφαλίσει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Η αρχή της ελαχιστοποίησης των δεδομένων έρχεται –σχεδόν από τον ορισμό της- σε αντίθεση με την ανάλυση Μεγάλων Δεδομένων και με τα συστήματα μηχανικής εκμάθησης τα οποία βασίζονται, αν δεν εξαρτώνται εξ' ολοκλήρου, στην υπερβολικά μεγάλη συλλογή δεδομένων και στην πιθανότητα αυτά να συνδυαστούν ή να χρησιμοποιηθούν εκ νέου. Πιο συγκεκριμένα ορίζει ότι τα προσωπικά δεδομένα πρέπει να «είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για

[52] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[53] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία». Το ποια προσωπικά δεδομένα θεωρούνται «αναγκαία» διαφέρει και εξαρτάται από τα συστήματα ΤΝ και τον σκοπό για τον οποίο χρησιμοποιούνται.

Η Νορβηγική Αρχή Προστασίας Δεδομένων προτείνει σαν πρακτική ότι οι υπεύθυνοι επεξεργασίας πρέπει να θέσουν όρια, τα οποία είναι επαρκή για να επιτευχθεί ο σκοπός της επεξεργασίας, παρά να χρησιμοποιούν όλα τα διαθέσιμα δεδομένα. Ένα παράδειγμα όπου ένα σύστημα ΤΝ δημιουργήθηκε, λαμβάνοντας υπόψη τα παραπάνω, είναι ένα εργαλείο που σχεδιάστηκε από τη Νορβηγική φορολογική διοίκηση με σκοπό να ελέγχει τις επιστροφές φόρου για τυχόν λάθη. Ελέγχθηκαν πεντακόσιες μεταβλητές αλλά μόνο οι τριάντα συμπεριλήφθηκαν στο τελικό μοντέλο ΤΝ, αφού αυτές κρίθηκαν οι σχετικές και κοντινές με την αποστολή. Όπως επισημάνθηκε από τον M. Butterworth[54], «αν η επεξεργασία των δεδομένων είναι σύμφωνη με την αρχή του περιορισμού του σκοπού, τότε είναι σύμφωνη και με την αρχή της ελαχιστοποίησης των δεδομένων». Η ελαχιστοποίηση δεν αποκλείει την ένταξη επιπρόσθετων προσωπικών δεδομένων σε μια επεξεργασία, όσο η πλεονάζουσα αυτή ένταξη είναι ωφέλιμη, σχετικά με τους σκοπούς της επεξεργασίας, οι οποίοι υπερτερούν των πρόσθετων κινδύνων για το υποκείμενο των δεδομένων.

1.5 Η Αρχή της ακρίβειας των δεδομένων στο πεδίο της Τεχνητής Νοημοσύνης (αρ.5 παρ.1 στοιχ. δ΄ ΓΚΠΔ)

Η έμφαση που δίνεται στην αρχή της ακρίβειας των δεδομένων υπογραμμίζεται από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB), στο προσχέδιο για τις κατευθυντήριες γραμμές του σχετικά με το απόρρητο εκ σχεδιασμού και το απόρρητο εξ ορισμού. Η ποιότητα των δεδομένων κρίνεται ιδιαιτέρως σημαντική, στην εποχή των Μεγάλων Δεδομένων, καθώς αυτά συχνά συλλέγονται και αναπαράγονται χωρίς κανέναν έλεγχο ποιότητας. Σύμφωνα με το άρθρο 5 § 1 στοιχ. δ' τα δεδομένα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται. Η υποχρέωση διασφάλισης της ακρίβειας των δεδομένων πρέπει να ερμηνευθεί σχετικά με τον σκοπό και την φύση ή την κατηγορία των δεδομένων που τίθενται σε επεξεργασία. Η αρχή της ακρίβειας προϋποθέτει ότι οι υπεύθυνοι επεξεργασίας δεδομένων, οι οποίοι εκτελούν διεργασίες

[54] Butterworth, M., 2018. The ICO and artificial intelligence: The role of fairness in the GDPR framework. In: Computer Law & Security Review, Volume 34, Issue 2, pp 257-268.

μηχανικής εκμάθησης, μπορούν να διασφαλίσουν ότι τα δεδομένα εκπαίδευσης αντιπροσωπεύουν ένα περιβάλλον, στο οποίο ο εκπαιδευόμενος αλγόριθμος θα αναπτυχθεί χωρίς να περιέχει στερεοτυπικές διακρίσεις, που εντοπίζονται στον πραγματικό κόσμο.

1.6 Η Αρχή λογοδοσίας στο πεδίο της Τεχνητής Νοημοσύνης (αρ.5 παρ.2 ΓΚΠΔ)

Με την ευρεία έννοια, η αρχή της λογοδοσίας ρίχνει στους υπεύθυνους επεξεργασίας το βάρος της εφαρμογής ειδικών μέτρων μέσα στους οργανισμούς τους, με σκοπό να διασφαλίσουν ότι πληρούνται οι προϋποθέσεις για την προστασία των δεδομένων. Στο πεδίο της ΤΝ, η πλήρωση των σχετικών με την λογοδοσία, απαραίτητων προϋποθέσεων, δεν φαίνεται να είναι ένα εύκολο έργο, δεδομένης της αδιαφάνειας της επεξεργασίας και της χρήσης αλγορίθμων, οι οποίοι βασίζονται στην ανάλυση μεγάλου όγκου δεδομένων για να εξακριβώσουν τυχόν συσχετίσεις. Μία από τις πλευρές της λογοδοσίας που θα έχει περισσότερες επιπτώσεις στην ανάπτυξη και την εφαρμογή ΤΝ είναι η καινούρια υποχρέωση που επιβάλλεται στους υπεύθυνους επεξεργασίας στο Άρθρο 35 του Κανονισμού: η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (data protection impact assessment -DPIA). Η τελευταία, αποτελεί κομμάτι μιας πιο γενικής προσέγγισης της προστασίας των δεδομένων, "βάσει κινδύνων"[55], σκοπεύοντας στο να στρέψει τον έλεγχο της προστασίας των δεδομένων προς περισσότερες πρακτικές διαχείρισης κινδύνων.[56]

Η τεχνητή νοημοσύνη μπορεί να αντιμετωπίσει την ανάλυση μεγάλων δεδομένων σε διάφορα σχήματα, μεγέθη και μορφές. Η γαλλική DPA, CNIL σημειώνει ότι η τεχνητή νοημοσύνη και τα μεγάλα δεδομένα είναι αδιάσπαστα[57], ενώ αποφασιστικό παράγοντα αποτελεί και η εκθετική αύξηση και διαθεσιμότητα δεδομένων, συμπεριλαμβανομένων αυτών που συλλέγονται και παράγονται από το Διαδίκτυο των Πραγμάτων. Στην

[55] Η Αιτιολογική Σκέψη (76). Για να χαρακτηριστεί ένας κίνδυνος ως «υψηλός», πρέπει να αξιολογηθεί «βάσει αντικειμενικής εκτίμησης». Το Άρθρο 35 § 3 ορίζει τις περιπτώσεις εκείνες, οι οποίες αδιαμφισβήτητα υπάγονται στην κατηγορία «υψηλός κίνδυνος».

[56]Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[57]Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

πραγματικότητα, η σχέση μεταξύ της τεχνητής νοημοσύνης και των μεγάλων δεδομένων είναι αμφίδρομη: η τεχνητή νοημοσύνη, μέσω της μηχανικής μάθησης, χρειάζεται τεράστιο όγκο δεδομένων για την εκμάθηση δεδομένων στον τομέα των μεγάλων δεδομένων. Ταυτόχρονα, τα μεγάλα δεδομένα χρησιμοποιούν τεχνικές τεχνητής νοημοσύνης για την εξαγωγή αξίας από μεγάλα σύνολα δεδομένων. Η τεχνητή νοημοσύνη μπορεί να ξεκλειδώσει την αξία των αναλυτικών στοιχείων μεγάλων δεδομένων. Με τον συνδυασμό τους, το AI και το Big Data αποτελούν «μέρος της επιχείρησης» για πολλούς οργανισμούς τόσο στο δημόσιο όσο και τον ιδιωτικό τομέα».

2. ΓΚΠΔ και Μεγάλα Δεδομένα, GDPR and Big Data Analytics

Κατά την εξέταση των μεγάλων δεδομένων ως μορφή ανάλυσης, η ομάδα εργασίας του άρθρου 29 όρισε τα μεγάλα δεδομένα ως εξής: "Τα μεγάλα δεδομένα αναφέρονται στην εκθετική αύξηση τόσο της διαθεσιμότητας όσο και της αυτοματοποιημένης χρήσης των πληροφοριών: πρόκειται για γιγαντιαία ψηφιακά σύνολα δεδομένων που κατέχουν εταιρείες, κυβερνήσεις και άλλοι μεγάλοι οργανισμοί, τα οποία στη συνέχεια αναλύονται εκτενώς με τη χρήση αλγορίθμων υπολογιστών. Τα μεγάλα δεδομένα μπορούν να χρησιμοποιηθούν για τον εντοπισμό γενικότερων τάσεων και συσχετίσεων, αλλά μπορούν επίσης να υποστούν επεξεργασία προκειμένου να επηρεάσουν άμεσα τα άτομα". Ο ορισμός της ομάδας του άρθρου 29 εστιάζει στην ποσοτική, αναλυτική και προγνωστική ιδιότητα των μεγάλων δεδομένων και στη δυνητική χρήση τους για την επίτευξη συγκεκριμένων αποτελεσμάτων. Ποσοτικά, τα μεγάλα δεδομένα επεξεργάζονται μεγάλο όγκο δεδομένων για να καταλήξουν σε ένα αποτέλεσμα, ενώ η αναλυτική τους ιδιότητα δίνει έμφαση στην επεξεργασία μεγάλων συνόλων δεδομένων, με τη χρήση προδιαγεγραμμένων μηχανισμών για την επίτευξη ενός στόχου. Τα μεγάλα δεδομένα χρησιμοποιούνται για την παροχή στοχευμένων διαφημίσεων μέσω της ανάλυσης της διαδικτυακής συμπεριφοράς και ενεργούν σε μια ποικιλία δεδομένων που συγκεντρώνονται με διάφορα τεχνολογικά μέσα, με ή χωρίς τη γνώση των εμπλεκόμενων ατόμων, για την εξαγωγή συμπερασμάτων από άγνωστες προηγουμένως πληροφορίες από την εν λόγω βάση δεδομένων.[58]

[58]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

Αυτό σημαίνει ότι αν οι οργανισμοί που επεξεργάζονται μεγάλα δεδομένα, χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα, τότε πρέπει όχι μόνο να γνωρίζουν αλλά και να λαμβάνουν υπόψη τις επιπτώσεις της επεξεργασίας τους στα άτομα, τις κοινότητες και τις κοινωνικές ομάδες που αυτά αφορούν. Αυτό μπορεί να είναι λιγότερο απλό από ό,τι σε πιο συμβατικά σενάρια επεξεργασίας δεδομένων, εξαιτίας των ενίοτε νέων και απροσδόκητων τρόπων με τους οποίους χρησιμοποιούνται τα δεδομένα στις αναλύσεις. Ένας οργανισμός που συλλέγει δεδομένα προσωπικού χαρακτήρα υποχρεούται γενικά να παρέχει μια ειδοποίηση προστασίας της ιδιωτικής ζωής, που να εξηγεί τους σκοπούς για τους οποίους χρειάζεται τα δεδομένα, συχνά όμως αυτή μπορεί να μην εξηγεί απαραίτητα τις λεπτομέρειες του τρόπου με τον οποίο θα χρησιμοποιηθούν τα δεδομένα.[59] Η υπερβολική συλλογή δεδομένων αποτελεί ζήτημα προστασίας των δεδομένων, αλλά μπορεί επίσης να δυσχεράνει τον εντοπισμό και την επεξεργασία των δεδομένων που πραγματικά χρειάζονται από τις επιχειρήσεις. Οι αναλύσεις μεγάλων δεδομένων μπορεί να ανακαλύψουν απροσδόκητους συσχετισμούς, για παράδειγμα μεταξύ δεδομένων σχετικών με τον τρόπο ζωής των ανθρώπων και την πιστοληπτική τους ικανότητα, χωρίς αυτό να σημαίνει ότι οποιαδήποτε πληροφορία μπορεί να αποκτηθεί σχετικά με αυτούς, είναι απαραίτητα σχετική με τον σκοπό της αξιολόγησης του πιστωτικού κινδύνου. Η εύρεση όποιας συσχέτισης, δεν μπορεί να δικαιολογήσει εκ των υστέρων την αρχική λήψη αυτών των δεδομένων. Η απαίτηση της αρχής σύμφωνα με την οποία τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να διατηρούνται περισσότερο από όσο είναι απαραίτητο για τον σκοπό για τον οποίο υποβάλλονται σε επεξεργασία, υποστηρίζει την προστασία της ιδιωτικής ζωής των ατόμων και αντικατοπτρίζει την ορθή πρακτική στη διαχείριση τηρούμενων αρχείων.

Ωστόσο, στον κόσμο των μεγάλων δεδομένων αυτό μπορεί να είναι προβληματικό για δύο λόγους. Πρώτον, με τη χρήση των μεγάλων δεδομένων η ικανότητα αποθήκευσης δεδομένων αυξάνεται διαρκώς και το κόστος αποθήκευσης μειώνεται. Δεύτερον, η ικανότητα επεξεργασίας τεράστιων όγκων δεδομένων, μπορεί να ενθαρρύνει τους υπεύθυνους επεξεργασίας δεδομένων να διατηρούν ιστορικά δεδομένα για μεγάλο χρονικό διάστημα, πέραν της περιόδου που απαιτείται για τους συνήθεις επιχειρηματικούς σκοπούς. Ο ΓΚΠΔ εισάγει το "δικαίωμα στη λήθη", δίνοντας στα υποκείμενα των δεδομένων το δικαίωμα διαγραφής τους σε διάφορες περιπτώσεις, όταν για παράδειγμα τα

[59] Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2

δεδομένα δεν είναι πλέον απαραίτητα για τον σκοπό για τον οποίο συλλέχθηκαν, ή όταν η επεξεργασία τους γίνεται βάσει συγκατάθεσης και το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση αυτή. Αυτό είναι ιδιαίτερα σημαντικό για τις επιχειρήσεις και όχι για τον δημόσιο τομέα, δεδομένου ότι το δικαίωμα στη λήθη δεν ισχύει εάν η επεξεργασία είναι απαραίτητη για νομική υποχρέωση ή για την άσκηση δημόσιας εξουσίας. Μπορεί να είναι πρακτικά δύσκολο για μια επιχείρηση να βρει και να διαγράψει τα δεδομένα κάποιου, εάν αυτά είναι αποθηκευμένα σε πολλά διαφορετικά συστήματα. Συνεπώς, οι οργανισμοί πρέπει να είναι σε θέση να καθιστούν εξαρχής σαφείς τους λόγους για τους οποίους πρέπει να συλλέγουν και να επεξεργάζονται συγκεκριμένα σύνολα δεδομένων. Πρέπει να υπάρχει σαφήνεια σχετικά με την επεξεργασία των εν λόγω δεδομένων, προκειμένου τα συλλεγόμενα δεδομένα να είναι συναφή και όχι υπερβολικά, σε σχέση με τον εν λόγω στόχο. Πρόκληση αποτελεί ο καθορισμός των σκοπών επεξεργασίας και των σχετικών δεδομένων ανά περίπτωση.

Συχνά, η ανάλυση μεγάλων δεδομένων δεν απαιτεί τη χρήση δεδομένων που ταυτοποιούν τα άτομα, καθιστώντας έτσι την ανωνυμοποίηση ένα επιτυχημένο εργαλείο, με δυνατότητα να απομακρύνει την επεξεργασία από τη σφαίρα της προστασίας δεδομένων και να μετριάσει τον κίνδυνο απώλειας προσωπικών δεδομένων. Οι οργανισμοί που χρησιμοποιούν τεχνικές ανωνυμοποίησης πρέπει να προβαίνουν σε στιβαρές εκτιμήσεις του κινδύνου επαναπροσδιορισμού. Εάν τα δεδομένα προσωπικού χαρακτήρα μπορούν να ανωνυμοποιηθούν πλήρως, δεν είναι πλέον δεδομένα προσωπικού χαρακτήρα. Στο πλαίσιο αυτό, "ανωνυμοποιημένο" σημαίνει ότι ελλείπει πλέον η δυνατότητα αναγνώρισης ενός ατόμου από τα ίδια τα δεδομένα ή από των συνδυασμό αυτών με άλλα δεδομένα, λαμβανομένων υπόψη όλων των μέσων που είναι εύλογα πιθανό να χρησιμοποιηθούν για την αναγνώρισή του. Εάν τα δεδομένα δεν είναι πλέον δεδομένα προσωπικού χαρακτήρα, δεν καλύπτονται από τη νομοθεσία περί προστασίας δεδομένων, όπως ο ίδιος ο Κανονισμός καθιστά σαφές: "Οι αρχές της προστασίας των δεδομένων δεν θα πρέπει επομένως να εφαρμόζονται σε ανώνυμες πληροφορίες, δηλαδή σε πληροφορίες που δεν αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ή σε δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα κατά τρόπο ώστε το υποκείμενο των δεδομένων να μην είναι ή να μην είναι πλέον ταυτοποιήσιμο".[60] Ως εκ τούτου, ένα βασικό ερώτημα για τους οργανισμούς μεγάλων δεδομένων είναι αν χρειάζεται να

[60]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

χρησιμοποιούν δεδομένα που ταυτοποιούν φυσικά πρόσωπα, τη στιγμή που υπάρχουν πολλά παραδείγματα χρήσης ανωνυμοποιημένων δεδομένων στην ανάλυση μεγάλων δεδομένων. Οι οργανισμοί που χρησιμοποιούν ανωνυμοποιημένα δεδομένα πρέπει να είναι σε θέση να αποδείξουν ότι έχουν εκτιμήσει εμπεριστατωμένα τον κίνδυνο μιας εκ νέου ταυτοποίησης και έχουν υιοθετήσει λύσεις ανάλογες με τον κίνδυνο αυτό, όπως μια σειρά από τεχνικά μέτρα, συγκάλυψη δεδομένων, ψευδωνυμοποίηση και συγκέντρωση, καθώς και νομικές και οργανωτικές διασφαλίσεις.

Το κατά πόσον παραμένουν προσωπικά δεδομένα εξαρτάται από το κατά πόσον ο οργανισμός διατηρεί τα "κλειδιά"[61] ανωνυμοποίησης και άλλα σχετικά δεδομένα που επιτρέπουν την ταυτοποίηση των υποκειμένων των δεδομένων. Ακόμη και αν τα δεδομένα παραμένουν δεδομένα προσωπικού χαρακτήρα, αυτό εξακολουθεί να αποτελεί σχετική εγγύηση που πρέπει να εξεταστεί, ώστε η επεξεργασία να μπορεί να συμμορφώνεται με τις αρχές προστασίας δεδομένων.

Σε ένα πλαίσιο μεγάλων δεδομένων οι απαιτήσεις αυτές μπορεί να είναι προβληματικές, και έχει προταθεί ότι οι ανακοινώσεις για την προστασία της ιδιωτικής ζωής δεν είναι εφικτές όσον αφορά την ανάλυση μεγάλων δεδομένων. Αυτό υποστηρίζεται για διάφορους λόγους. Αφενός γιατί οι άνθρωποι δεν είναι πρόθυμοι να διαβάσουν μακροσκελείς ειδοποιήσεις απορρήτου και αφετέρου γιατί το πλαίσιο στο οποίο συλλέγονται τα δεδομένα (π.χ. από εφαρμογές smartphone ή συσκευές IoT) μπορεί να καταστήσει πρακτικά δύσκολη την παροχή τους. Οι αναλύσεις που χρησιμοποιούνται στα μεγάλα δεδομένα είναι πολύ δύσκολο να εξηγηθούν με όρους που μπορούν να κατανοήσουν οι άνθρωποι. Δεδομένου ότι οι αναλύσεις μεγάλων δεδομένων συχνά περιλαμβάνουν επαναχρησιμοποίηση δεδομένων, ο υπεύθυνος επεξεργασίας δεδομένων δεν μπορεί να προβλέψει εξαρχής όλες τις χρήσεις που μπορεί να γίνουν με τα δεδομένα.

Στα μεγάλα δεδομένα συναντάται το λεγόμενο "παράδοξο της διαφάνειας ", καθώς τα μεγάλα δεδομένα υπόσχονται διορατικότητα σε ένα θέμα και ταυτόχρονα οι μηχανισμοί ανάλυσης μεγάλων δεδομένων είναι κρυπτικοί.[62] Απαιτείται κάποιο επίπεδο διαφάνειας ώστε το υποκείμενο των δεδομένων να είναι σε θέση να πληροφορείται για θέματα που αφορούν την επεξεργασία των προσωπικών του δεδομένων, άλλωστε αυτό αποτελεί μέρος

[61] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[62]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

του δικαιώματος του υποκειμένου των δεδομένων, παρά την ύπαρξη λόγων που δικαιολογούν την ύπαρξη κρυπτογραφημένων μηχανισμών, όπως για την προστασία του εμπορικού απορρήτου ή της εθνικής ασφάλειας.

Πώς οι νέοι κανόνες που τέθηκαν σε εφαρμογή με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, επηρεάζουν όμως τη συλλογή δεδομένων; Χωρίς αμφιβολία, ο μεγαλύτερος τρόπος με τον οποίο η νομοθεσία του GDPR θα επηρεάσει τη συλλογή δεδομένων είναι ότι θα οδηγήσει σε αυξημένη εξάρτηση από τα αναλυτικά στοιχεία σε πραγματικό χρόνο. Η ανάλυση σε πραγματικό χρόνο λαμβάνει δεδομένα που μόλις συλλέχθηκαν και τα θέτει σε άμεση χρήση και ανάλυση. Με τη συλλογή δεδομένων που συλλέγονται άμεσα, δεν απαιτείται πλέον η διατήρηση των εν λόγω δεδομένων για μεγάλο χρονικό διάστημα, κάτι που είναι ένα από τα ζητήματα που επιδιώκει να αντιμετωπίσει το GDPR. Υπό αυτό το πρίσμα όσες επιχειρήσεις επιθυμούν να συνεργαστούν με πελάτες εντός της ΕΕ, οφείλουν να είναι ακριβείς σχετικά με το τι ζητούν, με τη χρονική διάρκεια διατήρησης των δεδομένων και με τη χρήση και τον σκοπό συλλογής αυτών. Με τον τρόπο αυτό θα επηρεαστούν επίσης τα μέσα κοινωνικής δικτύωσης, μια λεωφόρος που χρησιμοποιούν πολλές επιχειρήσεις για την αύξηση του πελατολογίου αλλά και της αφοσίωσης των πελατών σε αυτές. Αυτό δεν προκαλεί έκπληξη, λαμβάνοντας υπόψη πόσες προσωπικές πληροφορίες καταλήγουν σε λογαριασμούς κοινωνικών μέσων, αρκεί να παρακολουθήσει κανείς τις πρόσφατες ειδήσεις του Facebook για την κυκλοφορία νέων εργαλείων απορρήτου και γίνεται προφανές ότι οι κανόνες εμπλοκής διαρκώς αλλάζουν. Οι επιχειρήσεις όλων των μεγεθών θα πρέπει να συμφωνήσουν με την ιδέα ότι οι πελάτες θα αποκτήσουν πλέον, μεγαλύτερο έλεγχο στα προσωπικά τους δεδομένα. Επιπλέον, όλα αυτά τα Big Data που συλλέγονται θα πρέπει όχι μόνο να αποθηκεύονται με ασφάλεια, αλλά και να είναι διαθέσιμα προς πελάτες που επιθυμούν να αποκτήσουν πρόσβαση σε αυτά προκειμένου να μεταβούν σε συνέχεια σε κάποιο άλλο προμηθευτή. Τα μεγάλα δεδομένα, η τεχνητή νοημοσύνη και η μηχανική μάθηση διαδίδονται ευρέως στον δημόσιο και τον ιδιωτικό τομέα. Μπορεί να θεωρούνται όλο και περισσότερο ως "συνήθης επιχειρηματική δραστηριότητα", όμως τα βασικά χαρακτηριστικά της ανάλυσης μεγάλων δεδομένων εξακολουθούν να αποτελούν μια βαθμιαία αλλαγή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η ανάλυση μεγάλων δεδομένων μέσω της χρήσης τεχνικών που κατέστησε δυνατή η ΤΝ, δημιουργεί επιπτώσεις στην προστασία των δεδομένων και καθιστά δυσκολότερη την εφαρμογή αρχών προστασίας δεδομένων, όταν αυτά χρησιμοποιούνται σε ένα πλαίσιο μεγάλων δεδομένων. Οι επιπτώσεις αυτές

προκύπτουν όχι μόνο από τον όγκο των δεδομένων, αλλά και από τους τρόπους με τους οποίους αυτά παράγονται, την τάση εύρεσης νέων χρήσεων για αυτά και από την πολυπλοκότητα της επεξεργασίας και την πιθανότητα απροσδόκητων συνεπειών για τα άτομα. Η διαφάνεια εξακολουθεί να διαδραματίζει σημαντικό ρόλο και μπορεί να επιτευχθεί, ακόμη και σε έναν πολύπλοκο κόσμο τεχνητής νοημοσύνης και μηχανικής μάθησης.

Με την επιλογή ορισμένων αρχών και διατάξεων του ΓΚΠΔ, η συμβατότητα των μεγάλων δεδομένων με τον ΓΚΠΔ τίθεται σε δοκιμασία και είναι εμφανές ότι υπάρχουν περισσότερα σημεία τριβής παρά επαφής. Οι αναλύσεις μεγάλων δεδομένων διαθέτουν στοιχεία που έρχονται σε αντίθεση με τις αρχές του περιορισμού του σκοπού, την ελαχιστοποίηση των δεδομένων, την αυτοματοποιημένη λήψη αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ) και τις ειδικές κατηγορίες δεδομένων, όπως αναφέρεται στον κανονισμό. Η ατελείωτη επιθυμία για συνέχιση της καινοτομίας έχει επιφέρει, αφενός, το λαμπρό μέλλον και τις προσδοκίες των μεγάλων δεδομένων και, αφετέρου, την ανάγκη η καινοτομία αυτή να βρίσκεται εντός των ορίων του νόμου. Αυτές οι τριβές είναι θεμελιώδεις για το όραμα της τεχνολογικής καινοτομίας της ΕΕ και μάλιστα σε ολόκληρο τον κόσμο. Αν και υπάρχουν εγγενείς τεχνολογικές λύσεις που μπορούν να ενσωματωθούν στη δυναμική των μεγάλων δεδομένων, όπως η προστασία της ιδιωτικής ζωής μέσω σχεδιασμού, εξακολουθούν να υπάρχουν αμφιβολίες για το πώς μπορεί να αμβλυνθεί πλήρως αυτή η αντίφαση.

2.1 Η Αρχή Περιορισμού του Σκοπού στο πλαίσιο των Big Data Analytics (αρ.5 παρ.1 στοιχ. β΄ ΓΚΠΔ)

Η αρχή αυτή ενσωματώνεται στο άρθρο 5 παράγραφος 1 στοιχείο β) του ΓΚΠΔ, το οποίο ορίζει 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 περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 («περιορισμός του σκοπού»), ". Η αρχή αυτή ορίζει ρητά τον περιορισμό της συλλογής και της περαιτέρω επεξεργασίας των δεδομένων, καθώς η εν λόγω συλλογή πρέπει να έχει καθορισμένο σκοπό. Ο σκοπός αυτός πρέπει να είναι σαφής από τον υπεύθυνο επεξεργασίας πριν από την έναρξη της επεξεργασίας των δεδομένων. Η αρχή αυτή έχει δύο συνιστώσες, δηλαδή ένα στοιχείο

καθορισμού του σκοπού και ένα στοιχείο συμβατότητας. Το στοιχείο της εξειδίκευσης του σκοπού φαίνεται στη φράση "καθορισμένους, ρητούς και νόμιμους σκοπούς" , ενώ το στοιχείο της συμβατότητας φαίνεται στη φράση "δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς". Ο σκοπός της επεξεργασίας των δεδομένων πρέπει πρώτα να καθορίζεται κατά τη στιγμή της συλλογής ή/και πριν από την επεξεργασία των δεδομένων αυτών, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για τον σκοπό αυτό, ώστε να μπορεί να κάνει συνειδητή επιλογή είτε να δώσει τη συγκατάθεσή του είτε όχι, ή να ασκήσει με άλλο τρόπο τα δικαιώματά του ελέγχου.

Η χρήση και η διατήρηση μεγάλου όγκου δεδομένων χωρίς προκαθορισμένο σκοπό είναι ένα σημαντικό χαρακτηριστικό των μεγάλων δεδομένων, το οποίο αποτελεί παρέκκλιση από την αρχή του περιορισμού του σκοπού. Προκειμένου να επεξεργαστεί ένας υπεύθυνος επεξεργασίας δεδομένων προσωπικού χαρακτήρα δεδομένα σε μια εφαρμογή μεγάλων δεδομένων, πρέπει να προσδιορίσει τον σκοπό της συλλογής, καθώς και κάθε περαιτέρω χρήση, πριν ή κατά τη στιγμή της συλλογής. Για να χρησιμοποιήσει περαιτέρω ο υπεύθυνος επεξεργασίας τα δεδομένα του υποκειμένου των δεδομένων, για μια ανάλυση μεγάλων δεδομένων, προκειμένου να καταλήξει σε μια απόφαση σχετικά με το εν λόγω υποκείμενο των δεδομένων, θα πρέπει να συμμορφωθεί με την αρχή του περιορισμού του σκοπού, η οποία προφανώς θα είναι πολύ δύσκολο να επιτευχθεί. Για παράδειγμα, υπάρχει νόμιμη επεξεργασία δεδομένων προσωπικού χαρακτήρα εάν η επεξεργασία γίνεται για το έννομο συμφέρον του υπευθύνου επεξεργασίας, εκτός εάν το υποκείμενο των δεδομένων έχει υπέρτερο συμφέρον ή θεμελιώδες δικαίωμα.[63]

Τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τον αρχικό σκοπό για τον οποίο συλλέχθηκαν, ωστόσο, υπάρχουν περιπτώσεις στις οποίες ένας υπεύθυνος επεξεργασίας επιθυμεί να επαναχρησιμοποιήσει δεδομένα προσωπικού χαρακτήρα για ασύμβατο σκοπό. Για παράδειγμα, οι εταιρείες που χρησιμοποιούν την ανάλυση μεγάλων δεδομένων συνήθως επαναχρησιμοποιούν τα δεδομένα για άλλο σκοπό, που είναι διαφορετικός από τον αρχικό σκοπό για τον οποίο ελήφθησαν. Στην περίπτωση αυτή, η εταιρεία που "επαναχρησιμοποιεί" θα πρέπει να λάβει τη συγκατάθεση των υποκειμένων των δεδομένων των οποίων τα προσωπικά δεδομένα επαναχρησιμοποιούνται, η λήψη της

[63]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

συγκατάθεσης ενός υποκειμένου των δεδομένων για ένα ευρύ φάσμα σκοπών, θα καταστεί δύσκολη για μια οντότητα ανάλυσης μεγάλων δεδομένων, επειδή ο ΓΚΠΔ έχει ορίσει συγκεκριμένες προϋποθέσεις για μια έγκυρη συγκατάθεση.

Το υποκείμενο των δεδομένων έχει επίσης το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή και πρέπει να ενημερωθεί για το δικαίωμα αυτό πριν δώσει τη συγκατάθεσή του. Επιπλέον, όταν ένα υποκείμενο δεδομένων έχει δώσει τη συγκατάθεσή του για την επαναχρησιμοποίηση των προσωπικών του δεδομένων για άλλο σκοπό, τότε ο υπεύθυνος επεξεργασίας μπορεί να επεξεργαστεί περαιτέρω τα δεδομένα για ασύμβατο σκοπό. Αυτός είναι ο λόγος για τον οποίο η Ομάδα του άρθρου 29, ανέφερε ότι απαιτείται η συγκατάθεση "opt in" των υποκειμένων των δεδομένων να είναι "ελεύθερη, συγκεκριμένη, ενημερωμένη και σαφής, διαφορετικά η περαιτέρω χρήση των δεδομένων δεν μπορεί να θεωρηθεί συμβατή" ιδίως για περιπτώσεις όπως η "συμπεριφορική διαφήμιση, διαφήμιση βάσει θέσης, ψηφιακή έρευνα αγοράς βάσει εντοπισμού, παρακολούθηση και κατάρτιση προφίλ για σκοπούς άμεσης εμπορικής προώθησης ή μεσιτείας δεδομένων".[64] Λαμβάνοντας υπόψη αυτά τα σημεία, θα είναι δύσκολο για μια οντότητα συλλογής μεγάλων δεδομένων να αποκτήσει ευρεία συγκατάθεση από ένα υποκείμενο των δεδομένων για την επαναχρησιμοποίηση των δεδομένων που συλλέχθηκαν αρχικά και δεν μπορεί να περιορίσει ένα υποκείμενο των δεδομένων από το να αποσύρει τη συγκατάθεσή του όταν διαπιστωθεί η επαναχρησιμοποίηση των προσωπικών του δεδομένων.

Εξετάζοντας αυτή την αρχή του περιορισμού του σκοπού, οι εταιρείες των οποίων οι δραστηριότητες εξαρτώνται από την ανάλυση μεγάλων δεδομένων ενδέχεται να αντιμετωπίσουν κάποιο επίπεδο περιορισμών όσον αφορά τη συμμόρφωση με την εν λόγω αρχή. Αυτό ισχύει ιδιαίτερα όταν εξετάζεται η σημασία της ειδοποίησης και της συγκατάθεσης για την αποτελεσματικότητα αυτής της αρχής. Τις περισσότερες φορές, κατά τη στιγμή της συλλογής και ανάλυσης μεγάλων δεδομένων, οι μέθοδοι και τα πρότυπα που εμπλέκονται είναι τέτοια που ούτε η οντότητα συλλογής ούτε το υποκείμενο των δεδομένων είχαν λάβει υπόψη τους κατά τη στιγμή της συλλογής, με αυτό να δημιουργεί πίεση στην εφαρμογή του προκαθορισμένου σκοπού για τη συλλογή. Επομένως, αυτό σημαίνει ότι για να τεθεί σε εφαρμογή η αρχή του περιορισμού του σκοπού, μια οντότητα συλλογής που εμπλέκεται στην ανάλυση μεγάλων δεδομένων, θα

[64]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

πρέπει να ενημερώσει το υποκείμενο των δεδομένων για κάθε μελλοντική επεξεργασία στην οποία θα προβεί και επίσης, να διασφαλίσει ότι οι εν λόγω σκοποί δεν υπερβαίνονται. Αυτό πιθανότατα θα ισοδυναμεί με ένα πολύ δαπανηρό, δύσκολο ή αδύνατο εγχείρημα για την οντότητα συλλογής δεδομένων. Ούτε η παροχή ενός ευρείας έκτασης σκοπού θα σώσει την επεξεργασία, αλλά μάλλον θα την καταστήσει παράνομη και απαράδεκτη ως αντίθετη με τη διάταξη που απαιτεί ο σκοπός να είναι "συγκεκριμένος και ρητός".[65]

Υπάρχουν εξαιρέσεις από την αρχή του περιορισμού του σκοπού, η οποία επιτρέπει την περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα, εφόσον η περαιτέρω επεξεργασία γίνεται για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς. Για παράδειγμα, όταν γίνεται ανάλυση μεγάλων δεδομένων, ανακαλύπτονται απρόβλεπτοι συσχετισμοί δεδομένων, οι οποίοι στη συνέχεια χρησιμοποιούνται για νέο σκοπό. Αυτό έρχεται σε ευθεία αντίθεση με την αρχή του περιορισμού του σκοπού που απαγορεύει τη χρήση δεδομένων για σκοπό ασύμβατο με τον αρχικό σκοπό. Επιβάλλεται στις εταιρείες αυτές να ενημερώνουν το υποκείμενο των δεδομένων και να ζητούν τη συγκατάθεσή του για τη χρήση των δεδομένων του για νέο σκοπό που ανακαλύπτεται ως αποτέλεσμα της ανάλυσης μεγάλων δεδομένων. Συμπερασματικά, η αρχή της εξειδίκευσης του σκοπού έρχεται σε σύγκρουση με την έννοια της ανάλυσης μεγάλων δεδομένων, παρόλο που υπάρχουν εξαιρέσεις που επιτρέπουν την ανάλυση μεγάλων δεδομένων, οι εξαιρέσεις αυτές δεν επαρκούν για τη μεγιστοποίηση των δυνατοτήτων της ανάλυσης μεγάλων δεδομένων.[66]

2.2 Η Αρχή ελαχιστοποίησης των δεδομένων στο πλαίσιο των Big Data Analytics (αρ.5 παρ.1 στοιχ. γ΄ ΓΚΠΔ)

Η ελαχιστοποίηση των δεδομένων είναι θεμελιώδης αρχή του δικαίου περί προστασίας της ιδιωτικής ζωής και των δεδομένων. Η αρχή αυτή περιορίζει τον υπεύθυνο επεξεργασίας να συλλέγει δεδομένα προσωπικού χαρακτήρα στο ελάχιστο επίπεδο για την επίτευξη του νόμιμου σκοπού του. Αυτό προβλέπεται στο άρθρο 5 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ, το οποίο ορίζει ότι "Τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα,

[65]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[66]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»)". Στην ουσία, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να συλλέγονται και να αποθηκεύονται μόνο στο βαθμό που είναι απαραίτητο και θα πρέπει να διαγράφονται όταν εξαντλείται ο σκοπός για τον οποίο συλλέχθηκαν. Αυτό θεωρείται ως αντίφαση στα μεγάλα δεδομένα διότι, τα μεγάλα δεδομένα αφορούν τη συλλογή και επεξεργασία μεγάλου όγκου δεδομένων, τα οποία θα είναι δύσκολο να συμμορφωθούν με την αρχή της ελαχιστοποίησης. Η αρχή αυτή επιτρέπει τα δεδομένα προσωπικού χαρακτήρα να περιορίζονται στον σκοπό για τον οποίο συλλέχθηκαν και δεν θα πρέπει να αποθηκεύονται περισσότερο από όσο είναι απαραίτητο για τον σκοπό αυτό.

Ο ΓΚΠΔ θέτει περαιτέρω την ευθύνη στον εκτελούντα την επεξεργασία ή τον υπεύθυνο επεξεργασίας να θέτει σε εφαρμογή τεχνικά και οργανωτικά μέτρα για να διασφαλίσει την ελαχιστοποίηση των δεδομένων. Ο υπεύθυνος επεξεργασίας δεδομένων αναμένεται να διαγράφει τα δεδομένα που δεν είναι πλέον συναφή με τον σκοπό για τον οποίο συλλέχθηκαν και πρέπει να εφαρμόζονται περιοριστικά μέτρα για τη διατήρηση των δεδομένων προσωπικού χαρακτήρα. Με τη χρήση τεχνολογιών που ενισχύουν την προστασία της ιδιωτικής ζωής και καθιστούν δυνατή την αποφυγή της χρήσης δεδομένων προσωπικού χαρακτήρα, επιτυγχάνεται μια πιο φιλική προσέγγιση προς την προστασία της ιδιωτικής ζωής. Η επεξεργασία δεδομένων θα πρέπει να χρησιμοποιεί μόνο όσα δεδομένα απαιτούνται για την επιτυχή εκτέλεση μιας δεδομένης εργασίας. Επιπλέον, τα δεδομένα που συλλέγονται για έναν σκοπό δεν μπορούν να επαναχρησιμοποιηθούν χωρίς περαιτέρω συγκατάθεση. Η επεξεργασία θα πρέπει να είναι συμβατή με τον αρχικό σκοπό τους και η παρουσία ενός άλλου λόγου επεξεργασίας δεν δίνει αυτόματα τη δυνατότητα για περαιτέρω επεξεργασία των δεδομένων αυτών.[67] Με άλλα λόγια, το γεγονός και μόνο ότι υπάρχει έννομο συμφέρον για περαιτέρω επεξεργασία, δεν δικαιολογεί από μόνο του την επεξεργασία αυτή. Η αρχή αυτή επιβάλλει στους οργανισμούς την υποχρέωση να περιορίσουν την επεξεργασία των δεδομένων, στην επεξεργασία αυτή που είναι αναγκαία για τους σχετικούς σκοπούς.

Η αρχή αυτή σχετίζεται με το είδος των δεδομένων και το πεδίο εφαρμογής των δεδομένων που πρέπει να συλλέγονται. Σχετίζεται επίσης με τη διάρκεια για την οποία μπορούν να διατηρηθούν τα δεδομένα, και τα δεδομένα αυτά δεν πρέπει να διατηρούνται

[67]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

περισσότερο από όσο είναι απαραίτητο. Η αρχή αυτή έρχεται σε σύγκρουση με τα χαρακτηριστικά των μεγάλων δεδομένων, όπου τα δεδομένα έχουν αξία και μειώνουν την πιθανή μελλοντική τους χρήση. Τα μεγάλα δεδομένα δίνουν τη δυνατότητα διατήρησης δεδομένων για μια απρόβλεπτη μελλοντική χρήση, γεγονός που έρχεται σε ευθεία αντίθεση με την αρχή της ελαχιστοποίησης των δεδομένων, η οποία απαιτεί τα δεδομένα να μη διατηρούνται περισσότερο από όσο είναι απαραίτητο για τον αρχικό σκοπό της συλλογής τους. Τα μεγάλα δεδομένα επιτρέπουν μεγάλη συλλογή και διατήρηση δεδομένων, ενώ η ελαχιστοποίηση των δεδομένων επιτρέπει τη συλλογή και διατήρηση δεδομένων σε μικρότερο βαθμό από τον αναγκαίο, γεγονός που καθιστά περαιτέρω ασύμβατες τις δύο έννοιες. Η ασυμβατότητα αυτή επιτείνεται περαιτέρω από το δικαίωμα του υποκειμένου των δεδομένων να ζητήσει τη διαγραφή των δεδομένων του όταν δεν είναι πλέον απαραίτητο να τηρούνται, το οποίο είναι ευρέως γνωστό ως δικαίωμα στη λήθη. Αυτό περιπλέκει περαιτέρω τις προσδοκίες των χρηστών των μεγάλων δεδομένων, όταν τα δεδομένα δεν μπορούν να συλλεχθούν και να διατηρηθούν για περαιτέρω χρήση.[68]

Για να γνωρίζουμε αν τα δεδομένα προσωπικού χαρακτήρα τηρούνται στη σωστή ποσότητα, πρέπει να είναι σαφής ο σκοπός της τήρησης των δεδομένων αυτών. Ωστόσο, ο ίδιος ο πυρήνας των μεγάλων δεδομένων αντιτίθεται σε αυτή την αρχή, καθώς τα μεγάλα δεδομένα δίνουν κίνητρα για τη συλλογή μεγάλου όγκου δεδομένων για μεγάλο χρονικό διάστημα για απρογραμμάτιστες χρήσεις. Αυτά τα δύο στοιχεία θέτουν έναν περιορισμό στην ανάλυση μεγάλων δεδομένων, επειδή τα μεγάλα δεδομένα, τις περισσότερες φορές, συνεπάγονται τη συλλογή μεγάλου όγκου δεδομένων χωρίς καθορισμένο σκοπό, αυτό θα αποτελέσει πρόκληση για την εφαρμοσιμότητά τους στο πλαίσιο του ΓΚΠΔ λόγω αυτής της διάταξης. Βάση της αρχής αποτελεί η πεποίθηση ότι, όταν ένας υπεύθυνος επεξεργασίας έχει πρόσβαση σε λιγότερα δεδομένα, είναι λιγότερο πιθανό να παραβιάσει την ιδιωτική ζωή του υποκειμένου των δεδομένων. Πιστεύεται επίσης ότι όταν ένας υπεύθυνος επεξεργασίας διατηρεί μεγάλο όγκο δεδομένων για μεγαλύτερο χρονικό διάστημα, τα δεδομένα αυτά είναι πιθανό να αποτελέσουν αντικείμενο απειλών στον κυβερνοχώρο και διαρροής δεδομένων, γι' αυτό και η ελαχιστοποίηση των δεδομένων μειώνει αυτόν τον κίνδυνο, ο οποίος όμως με τη σειρά του εμποδίζει τις δυνατότητες των μεγάλων δεδομένων.

[68]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

Η ελαχιστοποίηση των δεδομένων σκοπεύει επίσης στην αύξηση της αυτονομίας του υποκειμένου των δεδομένων επί των δικών του δεδομένων και τον περιορισμό του υπεύθυνου επεξεργασίας από την υπερβολική και απαράδεκτη χρήση των δεδομένων, που αποτελούν τις πιθανές ανησυχίες των μεγάλων δεδομένων. Ως αιτιολόγηση των μεγάλων δεδομένων, η καινοτόμος ανάπτυξη της επιστήμης των δεδομένων και άλλων τομέων που σχετίζονται με αυτά, δίνει την πεποίθηση ότι υπάρχει μελλοντική χρήση των δεδομένων που αναλύονται σήμερα και, επομένως, τα δεδομένα αυτά δεν πρέπει να διατεθούν μέχρι να εξαντληθούν οι δυνατότητές τους. Αυτό συμβαίνει διότι με τα μεγάλα δεδομένα έρχεται μεγάλη γνώση που οδηγεί σε κοινωνική ανάπτυξη, ωστόσο, η ελαχιστοποίηση των δεδομένων θα εμποδίσει αυτή τη φευγαλέα αισιοδοξία.[69]

2.3 Η Αρχή της διαφάνειας στο πλαίσιο των Big Data Analytics (άρθρα 12-14 ΓΚΠΔ)

Ο κύριος στόχος της αρχής της διαφάνειας, είναι να διασφαλιστεί ότι τα υποκείμενα των δεδομένων ενημερώνονται για τον τρόπο και τον λόγο με τον οποίο και για τον οποίο υφίστανται διακρίσεις από τους αλγορίθμους.[70] Για παράδειγμα, όταν μια αίτηση δανείου δεν γίνεται δεκτή, ο λόγος για την απόφαση αυτή πρέπει να παρέχεται στο υποκείμενο των δεδομένων μαζί με τη γνωστοποίηση πληροφοριών για τα δεδομένα που χρησιμοποιήθηκαν για την επίτευξη της εν λόγω απόφασης, δεδομένου ότι η απόφαση ήταν αυτοματοποιημένη και δεν υπόκειται σε ανθρώπινη παρέμβαση. Η έλλειψη διαφάνειας της επεξεργασίας των δεδομένων στην ανάλυση μεγάλων δεδομένων περιπλέκει περαιτέρω το ερώτημα κατά πόσον τα άρθρα 12 παράγραφος 1 έως 15 ΓΚΠΔ μπορούν να τηρηθούν κατά την αυτοματοποιημένη λήψη αποφάσεων. Αυτό μπορεί να γίνει αντιληπτό με δύο έννοιες, πρώτον, η αδυναμία παροχής της λογικής πίσω από μια απόφαση αποτελεί παραβίαση του δικαιώματος επεξήγησης και, δεύτερον, η αδυναμία του υποκειμένου των δεδομένων να γνωρίζει ποια δεδομένα εισήχθησαν στον αλγόριθμο, γεγονός που αντιβαίνει στο δικαίωμα πρόσβασης. Για παράδειγμα, η βαθιά μάθηση, η οποία είναι μια από τις πιο σύγχρονες τεχνικές μηχανικής μάθησης, τοποθετεί τις εξόδους σε επίπεδα χρησιμοποιώντας τα επίπεδα για την είσοδο.

[69] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[70] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

Αυτή η πολύπλοκη διαδικασία διαστρωμάτωσης δημιουργεί αυτό που αποκαλείται "μαύρο κουτί", το οποίο χαρακτηρίζει περαιτέρω τη μη διαφάνεια της διαδικασίας και το υποκείμενο των δεδομένων, πιθανότατα, δεν θα κατανοήσει τον λόγο πίσω από αυτή την απόφαση. Είναι σημαντικό να σημειωθεί ότι ορισμένοι έχουν υποστηρίξει ότι το δικαίωμα επεξήγησης διακυβεύεται από την προσθήκη της λέξης "αποκλειστικά" στο άρθρο 22, δηλώνοντας ότι θα είναι εύκολο να τηρηθεί με την απλή εισαγωγή ενός ανθρώπινου στοιχείου στην επεξεργασία, η ανθρώπινη παρέμβαση ωστόσο, θα απαιτεί συνεχές ανθρώπινο στοιχείο που θα εκτελεί επαναλαμβανόμενες εργασίες, γεγονός που αντίκειται εξαρχής στο όλο νόημα της αυτοματοποίησης. Το ζήτημα της διαφάνειας στην αυτοματοποιημένη λήψη αποφάσεων καθίσταται συνεχώς επίκαιρο, διότι οι εταιρείες χάνουν τους καταναλωτές λόγω του ζητήματος της εμπιστοσύνης και των ανησυχιών για την προστασία της ιδιωτικής ζωής.

2.4 Η Αυτοματοποιημένη λήψη αποφάσεων στο πλαίσιο των Big Data Analytics

Οι συντάκτες του ΓΚΠΔ περιέγραψαν την κατάρτιση προφίλ ως κάθε μορφή αυτοματοποιημένης επεξεργασίας που αναλύει και προβλέπει τη ζωή κάποιου, η οποία έχει σημαντικές επιπτώσεις σε αυτόν. Για παράδειγμα, η κατάρτιση προφίλ μπορεί να χρησιμοποιεί δεδομένα για την πρόβλεψη ή την εξαγωγή συμπερασμάτων για ευαίσθητα δεδομένα που οδηγούν σε ένα ακριβές προφίλ για ένα πρόσωπο ή με άλλο τρόπο. Αυτό το προφίλ μπορεί, για παράδειγμα, να επηρεάσει την απόφαση σχετικά με την αίτηση πίστωσης και την πρόσληψη προσωπικού, την αστυνόμευση και την εθνική ασφάλεια. Το δικαίωμα αυτό ασκείται με την παροχή επαρκούς ενημέρωσης για την κατάρτιση προφίλ στο υποκείμενο των δεδομένων. Επιπλέον, πρέπει να παρέχεται στο υποκείμενο των δεδομένων η "εμπλεκόμενη λογική, η σημασία και οι προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας". Ωστόσο, υπάρχουν εξαιρέσεις στην αυτοματοποιημένη λήψη αποφάσεων, αυτό περιλαμβάνει όταν ζητείται η ρητή συγκατάθεση του υποκειμένου των δεδομένων. Επίσης, όταν, η αυτοματοποιημένη απόφαση είναι απαραίτητη για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας. Η εξαίρεση αυτή θα είναι επιτρεπτή κυρίως στην πρόληψη δόλιων δραστηριοτήτων. Παρά τις εξαιρέσεις αυτές, το υποκείμενο των δεδομένων διατηρεί ακόμα το δικαίωμα να χρησιμοποιήσει ανθρώπινη παρέμβαση και μπορεί να αμφισβητήσει την αυτοματοποιημένη απόφαση.

Ο ΓΚΠΔ προστατεύει περαιτέρω το υποκείμενο των δεδομένων, δίνοντάς του το δικαίωμα να ζητήσει "πληροφορίες σχετικά με τη λογική που εμπλέκεται" στην αυτοματοποιημένη λήψη αποφάσεων και τις συνέπειες της απόφασης αυτής. Η δημιουργία προφίλ είναι ένα από τα αποτελέσματα της ανάλυσης μεγάλων δεδομένων και αυτό σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να ενημερώνεται πριν από τη διενέργεια αυτής της κατάρτισης προφίλ. Για παράδειγμα, η Google συνδυάζει διάφορα δεδομένα για να δημιουργήσει ένα προφίλ χρήστη, η κατάρτιση προφίλ διευκολύνεται από τα μεγάλα δεδομένα πολύ περισσότερο από ό,τι τα cookies λόγω των διαφορετικών χαρακτηριστικών τους.[71] Κατά την εύρεση κρυμμένων ομοιοτήτων, δημιουργούνται προφίλ από μεγάλα σύνολα δεδομένων και γίνονται προβλέψεις, οι οποίες διαμορφώνουν το προφίλ ενός ατόμου. Η ομάδα εργασίας του άρθρου 29 έχει επίσης δηλώσει στη γνώμη της σχετικά με την κατάρτιση προφίλ ότι «η κατάρτιση προφίλ δεν μπορεί να υπερτονιστεί λόγω της εμφάνισης των μεγάλων δεδομένων και ότι οι κίνδυνοι της θα πρέπει να μετριαστούν».

Πρέπει να σημειωθεί ότι για τη διασφάλιση της διαφάνειας στις αυτοματοποιημένες αποφάσεις που αφορούν δεδομένα προσωπικού χαρακτήρα, είναι σημαντικό ο υπεύθυνος επεξεργασίας να παρέχει στο υποκείμενο των δεδομένων πληροφορίες για το νόημα και τη λογική πίσω από την αυτοματοποιημένη λήψη αποφάσεων, είτε τα δεδομένα συλλέγονται από το υποκείμενο των δεδομένων είτε όχι. Αυτό είναι ιδιαίτερα σημαντικό, διότι συμβαδίζει με το πνεύμα του ΓΚΠΔ, το οποίο απαιτεί υψηλό επίπεδο διαφάνειας στην επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη συλλογή και τη χρήση τους. Επιπλέον, ο συνδυασμός της ανάλυσης μεγάλων δεδομένων με τη μηχανική μάθηση θα έχει κάποιες συνέπειες στις αποφάσεις που λαμβάνονται μέσω αυτής της διαδικασίας, οι οποίες θα επηρεάσουν το άτομο που εμπλέκεται, διότι οι υπολογιστές δεν έχουν ενσυναίσθηση. Λόγω του γεγονότος ότι η ανάλυση μεγάλων δεδομένων περιλαμβάνει τη "σκέψη και δράση με δεδομένα", διαφοροποιείται από την παραδοσιακή ανάλυση που χρησιμοποιεί ερωτήματα με τον εντοπισμό των σημαντικών καταχωρίσεων. Η "σκέψη με δεδομένα" περιλαμβάνει την εύρεση συσχετίσεων μέσω της εκτέλεσης αλγορίθμων έναντι δεδομένων.[72] Κατά

[71]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

[72]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

συνέπεια, η "δράση με δεδομένα" περιλαμβάνει την εφαρμογή αυτών των συσχετίσεων σε συγκεκριμένες περιπτώσεις μέσω της χρήσης νέων αλγορίθμων.

Η αυτοματοποιημένη λήψη αποφάσεων, η οποία περιλαμβάνει τη χρήση συστημάτων μάθησης για τη λήψη αποφάσεων, μπορεί να δημιουργήσει ορισμένες δυσκολίες στην ελευθερία και τα δικαιώματα των ατόμων, ιδίως κατά των διακρίσεων σε σχέση με τη φυλή, το φύλο ή τη θρησκεία. Η αιτιολογική σκέψη 71 αναφέρει ότι οι ευαίσθητες πληροφορίες δεν υποβάλλονται σε επεξεργασία, είτε είναι απαραίτητες για την εκτέλεση σύμβασης είτε όχι, με συγκατάθεση ή με εξουσιοδότηση του νόμου, εκτός εάν είναι απαραίτητες για λόγους δημοσίου συμφέροντος. Ωστόσο, αυτή η εξαίρεση θα απαιτήσει από τον υπεύθυνο επεξεργασίας να εφαρμόσει τεχνικά μέτρα για την αποτροπή των διακρίσεων. Ο αλγόριθμος μηχανικής μάθησης προγραμματίζεται από ανθρώπους μέσω της χρήσης αριθμών και δεδομένων που συλλέγονται από την κοινωνία. Η κοινωνία από την οποία συλλέγονται αυτά τα δεδομένα είναι γεμάτη με διακρίσεις και ανισότητες, είναι αναπόφευκτο ότι τα δεδομένα θα είναι το ίδιο μεροληπτικά. Υπάρχει επίσης κάποια προκατάληψη προς τα μεγάλα δεδομένα, επειδή ορισμένες ομάδες μπορεί να υποεκπροσωπούνται στα δεδομένα, πράγμα που σημαίνει αναπόφευκτα ότι οι αλγόριθμοι θα ευνοούν κάποια ομάδα ανθρώπων περισσότερο από τις άλλες. Η στήριξη αποκλειστικά στην εξόρυξη δεδομένων ως έκφραση των μεγάλων δεδομένων θα καταστήσει τους υπεύθυνους επεξεργασίας δεδομένων μη συμμορφούμενους με τον ΓΚΠΔ. Υπάρχουν, ωστόσο, περιπτώσεις όπου οι αλγόριθμοι μηχανικής μάθησης μπορούν να εντοπίσουν μοτίβα ανισορροπίας ή διακρίσεων σε ένα σύνολο δεδομένων, σε μια τέτοια περίπτωση, ο αλγόριθμος μπορεί να προγραμματιστεί ώστε να αποφεύγει εντελώς αυτά τα σύνολα δεδομένων που εισάγουν διακρίσεις.[73]

3. ΓΚΠΔ και Διαδίκτυο των Πραγμάτων, GDPR and Internet of Things (IoT)

Από τις 25 Μαΐου 2018 όλες οι χώρες της ΕΕ άρχισαν να εφαρμόζουν τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ). Η εν λόγω νομοθεσία έχει ως στόχο την προστασία και τη ρύθμιση του απορρήτου των δεδομένων και εφαρμόζεται σε κάθε οργανισμό που κατέχει ή επεξεργάζεται δεδομένα πολιτών της ΕΕ, ανεξαρτήτως του

[73]Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

τόπου όπου έχει την έδρα του. Οι κυρώσεις για μη συμμόρφωση μπορεί να φτάσουν το 4% των παγκόσμιων εσόδων των εταιρειών.

Με τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ, ο οποίος τέθηκε σε ισχύ στις 25 Μαΐου 2018, ο κλάδος του IoT, ιδίως μεταξύ των διαφόρων κλάδων, αναμένεται να επηρεαστεί σε μεγάλο βαθμό, δεδομένου ότι χρησιμοποιεί ποικίλες και τεράστιες ποσότητες προσωπικών πληροφοριών. Αυτός ο κανονισμός ενισχύει τα δικαιώματα προστασίας της ιδιωτικής ζωής των οντοτήτων πληροφοριών και διασφαλίζει την ελεύθερη μεταφορά προσωπικών πληροφοριών μεταξύ κρατών μελών της ΕΕ. Χάρη στον Κανονισμό οι ευρωπαίοι πολίτες είναι σε θέση να ελέγχουν τις προσωπικές τους πληροφορίες, δημιουργώντας έτσι ένα υψηλό επίπεδο προστασίας της ιδιωτικής ζωής προστασίας, εντός των πλαισίων της Ευρωπαϊκής Ένωσης. Με την εισαγωγή του Κανονισμού, οι εταιρείες που ασχολούνται με προσωπικές πληροφορίες αναμένεται να επηρεαστούν σε μεγάλο βαθμό. Ως εκ τούτου, η συμμόρφωση με τον ΓΚΠΔ είναι απαραίτητη για τις εταιρείες που διαχειρίζονται δεδομένα χρηστών.[74]

Το σήμα κατατεθέν για τη συλλογή δεδομένων στις μέρες μας είναι οι συσκευές Internet of Things. Με τους αισθητήρες που καταγράφουν κάθε πληροφορία από το περιβάλλον, οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και τις παραβιάσεις δεδομένων δεν ήταν ποτέ άλλοτε τόσο ζωτικής σημασίας. Οι συσκευές IoT, όπως τα smartphones και οι κάμερες IP, συλλέγουν, αναλύουν και αποθηκεύουν τεράστιο όγκο δεδομένων και έτσι οι εταιρείες που χρησιμοποιούν αυτές τις τεχνολογίες θα πρέπει να αξιολογούν τον χειρισμό και την αποθήκευση των δεδομένων και να εφαρμόσουν τυχόν αναγκαίες αλλαγές προκειμένου να συμμορφωθούν με τον ΓΚΠΔ. Φορητές συσκευές τεχνολογίας για την υγεία και τη φυσική κατάσταση, οι ιατρικές συσκευές IoT, ακόμη και τα συνδεδεμένα αυτοκίνητα, όλα έχουν τη δυνατότητα πρόσβασης σε δεδομένα που καθιστούν ένα άτομο αναγνωρίσιμο και, επομένως, οι παραγωγοί τέτοιων τεχνολογιών θα πρέπει να ακολουθήσουν ένα πλαίσιο προστασίας της ιδιωτικής ζωής κατά το σχεδιασμό, όπου η προστασία της ιδιωτικής ζωής λαμβάνεται υπόψη σε κάθε στάδιο της διαδικασίας σχεδιασμού.[75] Ο ΓΚΠΔ θέτει αυτό το πλαίσιο με επίκεντρο την προστασία της ιδιωτικής ζωής στο προσκήνιο και απαιτεί από τους φορείς επεξεργασίας δεδομένων να υιοθετήσουν νέα μέτρα για να αποδείξουν τη συμμόρφωσή τους με τους νέους κανονισμούς. Επομένως,

[74] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.
[75] Lanner, 2017. Internet of Things Privacy: What GDPR Means For IoT Data.

πώς επηρεάζει ο Γενικός Κανονισμός για την Προστασία Δεδομένων τη συλλογή δεδομένων IoT; Ο κλάδος του IoT χρησιμοποιείται σε διάφορους τομείς, όπως η αυτοκινητοβιομηχανία, η ασφάλεια και η επιτήρηση, η ιατρική, το έξυπνο σπίτι, αλλά και τα ασύρματα δίκτυα T2T. Σύμφωνα με την Gartner, μέχρι το 2018 η "δύναμη" του IoT έφτανε τα 11,2 δισεκατομμύρια "πράγματα" του Διαδικτύου, που σημαίνει ότι κάθε ένα από τα "πράγματα" αποθηκεύει, επανεπεξεργάζεται και διανέμει περισσότερες από 50 δισεκατομμύρια προσωπικές πληροφορίες.

Το Διαδίκτυο είναι επίσης μεγαλύτερο από ποτέ. Ο αριθμός των ανθρώπων που ήταν συνδεδεμένοι στο διαδίκτυο το 2017 ήταν 3,58 δισεκατομμύρια, από 2,42 δισεκατομμύρια πριν από 5 χρόνια και 1,36 δισεκατομμύρια πριν από 10 χρόνια, γεγονός που αντιπροσωπεύει σημαντική αύξηση της παγκόσμιας συνδεσιμότητας. Εισάγεται το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT), ένα νέο παράδειγμα του Machine to Machine (M2M) που βασίζεται σε συνδέσεις IP. Το 2018 ο αριθμός των συνδεδεμένων συσκευών στο IoT μόνο, αναμένεται να ξεπεράσει τον παγκόσμιο πληθυσμό.[76] Το Διαδίκτυο των πραγμάτων υπόσχεται πολύπλοκα συστήματα που αντιλαμβάνονται το εξωτερικό περιβάλλον και λαμβάνουν αποφάσεις χωρίς την ανάγκη ανθρώπινης παρέμβασης. Αυτό σημαίνει ότι πολύ περισσότερες πληροφορίες σχετικά με την ανθρώπινη ζωή πρόκειται να συλλέγονται και να επεξεργάζονται από αυτά τα συστήματα, με ορισμένα περιβάλλοντα, όπως τα έξυπνα σπίτια, να είναι ικανά να ανιχνεύουν και να διαχειρίζονται πολύ ευαίσθητα και προσωπικά δεδομένα. Αυτό καθιστά την προστασία των δεδομένων απαραίτητο χαρακτηριστικό στα συστήματα IoT.

Όταν συμβεί μια παραβίαση δεδομένων μπορεί να έχει σημαντικό αντίκτυπο στη ζωή των ανθρώπων, ανάλογα με την ευαισθησία των δεδομένων. Η οντότητα που υπέστη την παραβίαση αντιμετωπίζει επίσης άμεσο οικονομικό κόστος. Προκειμένου να ανακάμψει από το περιστατικό απαιτείται έρευνα, στην οποία ενδεχομένως να συμμετέχουν πολλοί άνθρωποι και οικονομικοί πόροι. Η απώλεια της εμπιστοσύνης των χρηστών και των ενδιαφερομένων μερών βλάπτει και την εικόνα της αγοράς στο σύνολο. Το Διαδίκτυο των Πραγμάτων (IoT) βασίζεται σε μεγάλο βαθμό στο συνδυασμό αισθητήρων του πραγματικού κόσμου με τη δύναμη του Διαδικτύου. Οι αισθητήρες συλλέγουν πληροφορίες από το εξωτερικό περιβάλλον και στη συνέχεια τα δεδομένα συνδυάζονται με πληροφορίες που φιλοξενούνται στο cloud και αναλύονται στο σύνολό τους, προκειμένου να παράγουν δράσεις ή να παρέχουν συμβουλές σε συνάρτηση με το

[76] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

περιβάλλον. Ως αποτέλεσμα, όσο περισσότερα δεδομένα είναι διαθέσιμα τόσο περισσότερο το σύστημα είναι ικανό να παράγει το σωστό/καλύτερο αποτέλεσμα. Σε αντίθεση με τα συστήματα που βασίζονται στον άνθρωπο, το IoT είναι σε θέση να λειτουργεί 24 ώρες την ημέρα, 365 ημέρες το χρόνο και να αποθηκεύει όλα όσα συλλέγει για εύκολη πρόσβαση, ώστε να μην ξεχνάει τίποτα.[77]

Σήμερα υπάρχουν αισθητήρες για τη συλλογή σχεδόν κάθε πληροφορίας από το περιβάλλον. Μερικά παραδείγματα αισθητήρων είναι: εικόνα, βίντεο, ήχος, τοποθεσία, εγγύτητα, θερμοκρασία, υγρασία, επιτάχυνση, πίεση, αέρια και καρδιακός παλμός. Σε έναν κόσμο όπου τα δεδομένα έχουν γίνει ένα επικερδές περιουσιακό στοιχείο, ο κόσμος του IoT με τους αισθητήρες αποτελεί μια πιθανή απειλή. Η ανεξέλεγκτη συλλογή πληροφοριών σε ευαίσθητα περιβάλλοντα, όπως το έξυπνο σπίτι απαιτούν ισχυρή προστασία δεδομένων και ελέγχους απορρήτου.

Πολλές από τις δραστηριότητες επεξεργασίας δεδομένων που σχετίζονται με τη λειτουργία του IoT θα εμπίπτουν στο ουσιαστικό πεδίο εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων (ΓΚΠΔ), δεδομένου ότι οι IoT συσκευές τείνουν να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Κατά συνέπεια, η προστασία των δεδομένων θα πρέπει να ενσωματωθεί σε κάθε μορφή λύσης IoT από την αρχή και καθ' όλη τη διάρκεια του κύκλου ζωής, ως μέρος της αρχής της "προστασίας της ιδιωτικής ζωής μέσω του σχεδιασμού".[78] Η εκτίμηση αντικτύπου προστασίας δεδομένων μπορεί κατά πάσα πιθανότητα, να είναι απαραίτητη. Έννοιες της διαφάνειας, της δικαιοσύνης, του περιορισμού του σκοπού, της ελαχιστοποίησης των δεδομένων, της ακρίβειας των δεδομένων και ης δυνατότητας υλοποίησης των υποκειμένων των δεδομένων, θα πρέπει να ενσωματωθούν στο σχεδιασμό του προϊόντος IoT. Όλα αυτά θα πρέπει να τεκμηριώνονται και να αποδεικνύονται ως μέρος της αρχής της λογοδοσίας του ΓΚΠΔ.

Η Βιομηχανία του IoT, η οποία μεταφέρει σημαντικά τον έλεγχο της χρήσης των πληροφοριών στα άτομα, αναμένεται να επηρεαστεί από τον ΓΚΠΔ σε μεγάλο βαθμό και είναι σημαντικό να αυξηθεί η ευαισθητοποίηση σχετικά με την κατάσταση του οικονομικού αντίκτυπου στον συγκεκριμένο κλάδο. Οι παραβιάσεις του ΓΚΠΔ, οι οποίες θεωρούνται ως περιπτώσεις παραβίασης μικρής κλίμακας, θα μπορούσαν να οδηγήσουν

[77] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[78] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

σε πρόστιμο είτε 10 εκατομμυρίων είτε 2% του παγκόσμιου κύκλου εργασιών μιας επιχείρησης (όποιο από τα δύο είναι μεγαλύτερο). Ενώ, πιο σοβαρές παραβιάσεις μπορεί να οδηγήσουν σε πρόστιμο είτε 20 εκατ. ευρώ ή 4% του παγκόσμιου κύκλου εργασιών μιας επιχείρησης (όποιο από τα δύο είναι μεγαλύτερο), αυτό είναι και το μέγιστο πρόστιμο που μπορεί να επιβληθεί για την πιο σοβαρή παράβαση, όπως για παράδειγμα εάν η συναίνεση για την επεξεργασία των δεδομένων του πελάτη είναι ανεπαρκής ή εάν ο σχεδιασμός της επιχείρησης παραβιάζει τον πυρήνα των προσωπικών πληροφοριών.[79] Εάν απαιτείται συγκατάθεση, θα πρέπει να παρέχονται σαφής και συγκεκριμένες πληροφορίες στα υποκείμενα των δεδομένων, με τη χρήση απλής και εύκολης γλώσσας, ενώ το υποκείμενο έχει επίσης το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή.

Καθίσταται πλέον δυνατή η συλλογή μεγάλου όγκου προσωπικών δεδομένων με πολλούς διαφορετικούς τρόπους, χωρίς ο χρήστης να το γνωρίζει σαφώς. Κατά συνέπεια, η ανάπτυξη του IoT εγείρει ανησυχίες όσον αφορά την ασφάλεια και την προστασία της ιδιωτικής ζωής, ιδίως όσον αφορά τις πληροφορίες και τη συγκατάθεση των χρηστών. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) δίνει έμφαση στην ευαισθητοποίηση των ψηφιακών πολιτών, απαιτώντας συνείδηση κατά την επεξεργασία και τη χρήση. Ωστόσο, η εφαρμογή του ΓΚΠΔ μαζί με τις σχετικές συστάσεις εξακολουθεί να αποτελεί ένα ανοικτό ζήτημα στο περιβάλλον του IoT. Ο χρήστης καλείται να υπογράψει συγκατάθεση μετά από ενημέρωση, δηλαδή ο χρήστης ενημερώνεται μέσω των υποχρεώσεων που του αποστέλλει ο πάροχος υπηρεσιών για τους σκοπούς για τους οποίους συλλέγονται τα προσωπικά του δεδομένα. Αυτή η υπογραφή σχετίζεται με το ψευδώνυμο που ο χρήστης εκδίδει στον ίδιο τον πάροχο υπηρεσιών, περιορίζοντας έτσι κάποια πιθανή διασταυρούμενη ανταλλαγή δεδομένων του χρήστη μεταξύ παρόχων.[80] Η υπογεγραμμένη συγκατάθεση μπορεί αργότερα να αποδείξει τη γνησιότητα της συγκατάθεσης, γεγονός που είναι χρήσιμο για να αποδειχθεί ότι ο χειρισμός των δεδομένων είναι σύμφωνος με τη συγκατάθεση του χρήστη σε περίπτωση ελέγχου ενός παρόχου.

Η πλειονότητα των συνδεδεμένων συσκευών αποτυγχάνει να εξηγήσει επαρκώς στα υποκείμενα των δεδομένων πώς η λαμβάνει χώρα η επεξεργασία των προσωπικών

[79] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[80] Laurent, Maryline, et al. 2019. Authenticated and Privacy-Preserving Consent Management in the Internet of Things. In: Procedia Computer Science, Volume 151, pp 256-263.

δεδομένων τους. Η αποτυχία αυτή δεν αποτελεί ίσως έκπληξη, δεδομένης της έκτασης στην οποία οι υπηρεσίες IoT περιλαμβάνουν σημαντικά περισσότερα μέρη από τις παραδοσιακές υπηρεσίες (για παράδειγμα, κατασκευαστές αισθητήρων, κατασκευαστές υλικού, λειτουργικά συστήματα IoT, πωλητές λογισμικού IoT, φορείς εκμετάλλευσης κινητής τηλεφωνίας, κατασκευαστές συσκευών, τρίτες εφαρμογές, προγραμματιστές εφαρμογών).[81] Μια βασική δυσκολία, στο πλαίσιο του IoT, είναι να προσδιοριστεί εάν ένας ενδιαφερόμενος φορέας ενεργεί ως υπεύθυνος επεξεργασίας δεδομένων ή εκτελών την επεξεργασία δεδομένων, σε μια συγκεκριμένη δραστηριότητα επεξεργασίας. Σύμφωνα με τη γνώμη της ομάδας εργασίας του άρθρου 29 για το IoT, οι κατασκευαστές συσκευών θεωρούνται Υπεύθυνοι Επεξεργασίας για τα προσωπικά δεδομένα που παράγονται από τις συσκευές αυτές, καθώς σχεδιάζουν το λειτουργικό σύστημα ή καθορίζουν τη συνολική λειτουργικότητα του εγκατεστημένου λογισμικού. Οι προγραμματιστές εφαρμογών που οργανώνουν διεπαφές για να επιτρέπουν στα άτομα να έχουν πρόσβαση τα δεδομένα τους, που είναι αποθηκευμένα από τον κατασκευαστή της συσκευής, θα θεωρηθούν επίσης υπεύθυνοι επεξεργασίας. Άλλα τρίτα μέρη είναι Υπεύθυνοι Ελέγχου όταν χρησιμοποιούν συσκευές IoT για τη συλλογή και επεξεργασία πληροφοριών σχετικών με άτομα. Αυτά τα τρίτα μέρη χρησιμοποιούν συνήθως τα δεδομένα που συλλέγονται μέσω της συσκευής για άλλους σκοπούς, που είναι διαφορετικοί από την κατασκευαστή της συσκευής (π.χ., μια ασφαλιστική εταιρεία προσφέρει χαμηλότερες αμοιβές με την επεξεργασία δεδομένων που συλλέγονται από έναν μετρητή βημάτων).[82] Άλλα ενδιαφερόμενα μέρη, όπως οι πλατφόρμες δεδομένων IoT και οι κοινωνικές πλατφόρμες, μπορεί εξίσου να θεωρηθούν ως υπεύθυνοι επεξεργασίας για τις δραστηριότητες επεξεργασίας, για τις οποίες καθορίζουν σκοπούς και τα μέσα. Αντιθέτως, μπορούν να θεωρηθούν ως εκτελούντες την επεξεργασία όταν επεξεργάζονται δεδομένα για λογαριασμό άλλου ενδιαφερόμενου φορέα IoT που ενεργεί ως υπεύθυνος επεξεργασίας.

Το IoT έχει εξελιχθεί σε έναν από τους πιο ελκυστικούς στόχους για τους παγκόσμιους χάκερ. Πρόσφατες μελέτες έχουν κατηγοριοποιήσει και αναλύσει διάφορα ζητήματα ασφάλειας που προκύπτουν σε IoT περιβάλλοντα τα οποία έχουν ετερογένεια και μεγάλη κλίμακα αντικειμένων. Αυτά τα ζητήματα τεχνικής ασφάλειας αποτελούν

[81] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

[82] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

απειλή για τις συσκευές IoT που περιέχουν ιδιωτικές πληροφορίες.[83] Παρά την εμφάνιση διάφορων ευπαθειών, το πιο σημαντικό είναι το πρόβλημα των ενημερώσεων ασφαλείας. Σύμφωνα με την HP News, μια IoT συσκευή έχει κατά μέσο όρο 25 τρωτά σημεία, ενώ υπάρχουν επίσης πολλές μελέτες που έχουν επιβεβαιώσει ότι οι συσκευές IoT έχουν τρωτά σημεία, τα οποία βρίσκονται εκτεθειμένα στους επιτιθέμενους. Όπως αναφέρθηκε προηγουμένως, με τον αριθμό των συσκευών IoT πάνω από το ένα δισεκατομμύριο και ο αριθμός των ευπαθειών θα αγγίζει φυσικά ένα τεράστιο ποσό. Δεδομένου ότι υπάρχουν ενημερώσεις ασφαλείας στις διάφορες συσκευές, οι χρήστες αναπόφευκτα κατακλύζονται από τις ενημερώσεις. Ακόμη και αν μια εταιρεία παρέχει αυτοματοποιημένες ενημερώσεις, συχνά αυτές σταματούν όταν επικεντρώνονται στην κατασκευή της επόμενης συσκευής, αφήνοντας τους χρήστες με ελαφρώς ξεπερασμένο υλικό που μπορεί να αποτελέσει κίνδυνο για την ασφάλεια και να οδηγήσει σε διάφορα περιστατικά παραβίασης. Υπό αυτές τις συνθήκες, διάφορες μελέτες βρίσκονται σε εξέλιξη για την επίλυση του ζητήματος της ασφάλειας στο IoT περιβάλλον.[84]

Στην περίπτωση της χρήσης του Διαδικτύου, οι πληροφορίες σχετικά με τη συμπεριφορά των χρηστών συλλέγονται κατά την πλοήγησή τους στο Διαδίκτυο. Το IoT θα αναλύσει όχι μόνο το ιστορικό αναζήτησης αλλά και διάφορα μοτίβα ζωής και συμπεριφοράς του χρήστη, μπορούν να συλλεχθούν πιο ποικίλες και ευαίσθητες πληροφορίες. Υπάρχουν επίσης πολιτικές για τη συλλογή δεδομένων για κάθε συσκευή IoT, συμπεριλαμβανομένων πολιτικών ελέγχου πρόσβασης κάθε "πράγματος" και τύπου δεδομένων, που μπορεί να έρχονται σε σύγκρουση με τα άρθρα του ΓΚΠΔ για την καθιέρωση πολιτικών ελέγχου.[85] Μία από τις διαδικασίες επεξεργασίας προσωπικών πληροφοριών είναι ότι σήμερα παρέχεται στους ανθρώπους το δικαίωμα στη λήθη. Εάν το υποκείμενο των δεδομένων ζητά να διαγραφούν πληροφορίες, είναι δύσκολο, τεχνικά, αυτές να διαγραφούν εντελώς, επειδή υπάρχουν τόσες πολλές διαφορετικές και τεράστιες ποσότητες προσωπικών πληροφοριών που διακινούνται μέσω του IoT, για αυτό και είναι απαραίτητο να αναθεωρηθούν οι πληροφορίες που κατέχει μια εταιρεία. Κάθε τελικό σημείο στο περιβάλλον IoT, τα λεγόμενα "πράγματα", μεταδίδουν αυτόματα δεδομένα,

[83] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[84] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[85] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

επικοινωνούν με άλλα τελικά σημεία και αλληλεπιδρούν μεταξύ τους. Στο IoT, τα "πράγματα" ενίοτε συναλλάσσονται και λειτουργούν για λογαριασμό του χρήστη. Για παράδειγμα, εάν ένα έξυπνο ψυγείο αντιλαμβάνεται ότι τα τρόφιμα λιγοστεύουν, συνδέεται με το Διαδίκτυο και αγοράζει τα απαραίτητα είδη για τον χρήστη. Σε αυτήν την περίπτωση, η αξιοποίηση των πληροφοριών είναι αυτοματοποιημένη και οι πληροφορίες του χρήστη ανταλλάσσονται με διάφορα αντικείμενα. Ο ΓΚΠΔ, που διαχειρίζεται τη χρήση των προσωπικών πληροφοριών, μπορεί να έχει ως αποτέλεσμα τη μείωση αυτών των πλεονεκτημάτων του IoT.[86] Οι κατασκευαστές IoT συλλέγουν τεράστιες ποσότητες πληροφοριών που παράγονται σε περιβάλλοντα IoT και ερευνούν μεθόδους ανάλυσης αυτού του τεράστιου όγκου δεδομένων, για την καλύτερη δυνατή κατανόηση του συστήματος και της συμπεριφοράς των χρηστών. Για να προσφέρουν περισσότερη αξία και έσοδα, οι κατασκευαστές IoT αναλύουν τα δεδομένα που φαίνονται άσχετα μεταξύ τους και προσδιορίζουν τη σχέση μεταξύ της συμπεριφοράς και των προτύπων χρήσης ενός καταναλωτή. Με άλλα λόγια, τα δεδομένα που παραδίδονται από ένα τελικό σημείο είναι λιγότερο πιθανό να προκαλέσουν ζήτημα προστασίας της ιδιωτικής ζωής, αλλά τα δεδομένα που συλλέγονται και συγκεντρώνονται σε διάφορα τελικά σημεία μπορούν να προκαλέσουν ζητήματα προστασίας της ιδιωτικής ζωής. Επομένως, οι συγκεντρωτικές πληροφορίες έχουν τη δυνατότητα να συμπεριληφθούν στο διευρυμένο ορισμό των προσωπικών πληροφοριών, στις οποίες ο ΓΚΠΔ εφαρμόζεται και οι οποίες αντιστοιχούν στον τομέα ελέγχου των προσωπικών πληροφοριών.[87]

Οι εφαρμογές στο IoT μπορεί, σκόπιμα ή ακούσια, άμεσα ή έμμεσα, να επεξεργάζονται "ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα". Για παράδειγμα, τα έξυπνα wearables μπορεί να συλλέγουν έμμεσα πληροφορίες που, κατά τη διάρκεια μιας χρονικής περιόδου, μπορούν να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων σχετικά με την υγεία ή την ευημερία του ατόμου. Στην περίπτωση αυτή, ενδέχεται να χρειαστεί να γίνουν περαιτέρω εκτιμήσεις και μπορεί να απαιτείται ρητή συγκατάθεση σύμφωνα με το άρθρο 9 παράγραφος 2 του ΓΚΠΔ για τη συλλογή δεδομένων.[88] Αξίζει να σημειωθεί ότι ειδικές κατηγορίες δεδομένων προσωπικού

[86] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[87] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[88] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

χαρακτήρα μπορούν επίσης να σχετίζονται με ευάλωτα υποκείμενα δεδομένων. Για παράδειγμα, οι προγραμματιστές συνδεδεμένων κατοικιών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα που σχετίζονται με την υγεία, μπορεί να έχουν σχεδιαστεί ειδικά για να επεξεργάζονται τα δεδομένα των ηλικιωμένων. Σε τέτοιες περιπτώσεις, οι ενδιαφερόμενοι φορείς του IoT πρέπει να φρονίζουν για την παροχή σαφών και ολοκληρωμένων πληροφοριών με φιλικό προς τον χρήστη τρόπο. Είναι σημαντικό για τους ενδιαφερόμενους φορείς του IoT να διεξάγουν αξιολόγηση σχετικά με τις δραστηριότητες επεξεργασίας, για να προσδιορίσουν τους αντίστοιχους ρόλους προστασίας δεδομένων (π.χ. υπεύθυνος επεξεργασίας, από κοινού υπεύθυνοι επεξεργασίας ή εκτελών την επεξεργασία) και να κατανέμουν σωστά τις ευθύνες (ιδίως σε σχέση με υποχρεώσεις διαφάνειας και παραβίασης δεδομένων, καθώς και τα δικαιώματα των υποκειμένων των δεδομένων).[89]

Η συμμόρφωση με τις νομικές απαιτήσεις σχετικά με την προστασία της ιδιωτικής ζωής των δεδομένων είναι, φυσικά, πρωταρχικής σημασίας για κάθε υπεύθυνο παίκτη στο οικοσύστημα IoT. Οργανισμοί σε αυτόν τον χώρο πρέπει να είναι σε θέση να αποδείξουν ότι έχουν ενσωματώσει πλήρως τα ζητήματα προστασίας της ιδιωτικής ζωής των δεδομένων στην τεχνολογία τους. Ωστόσο, εκτός από την εξέταση των απαιτήσεων νομικής συμμόρφωσης, είναι σημαντικό να μπορεί το IoT να προσφέρει πολύτιμα οφέλη για την κοινωνία, τη βιομηχανία και τα άτομα. Δημιουργεί επίσης κινδύνους για την προστασία της ιδιωτικής ζωής, ιδίως σε σχέση με την ατομική αξιοπρέπεια και αυτονομία. Το θέμα είναι ότι όλα όσα είναι νομικά συμβατά και τεχνικά εφικτά, δεν είναι και ηθικά βιώσιμα, όπως υποστήριξε ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων, Giovanni Buttarelli, στη Διεθνή Διάσκεψη των Επιτρόπων Προστασίας Δεδομένων και Ιδιωτικότητας 2018.[90] Καθίσταται επομένως ζήτημα ηθικής των δεδομένων και αυτό απαιτεί από τους οργανισμούς να έχουν μια πιο θεμελιώδη συζήτηση, σχετικά με το ποιος είναι ο βασικός σκοπός/στόχος που ελπίζουμε να επιτύχουμε με το IoT και πώς αυτό εξισορροπείται με τους κινδύνους για τα άτομα; Ποια είναι η σωστή προσέγγιση που πρέπει να ακολουθήσουμε; Πρόκειται για μια ευρεία, σαρωτική συζήτηση υψηλού επιπέδου που δεν πρέπει να διεξάγεται αποκλειστικά μεταξύ των υπευθύνων προστασίας δεδομένων ή των δικηγόρων προστασίας δεδομένων, αλλά μάλλον με τεχνολόγους, επιστήμονες δεδομένων, ομάδες προϊόντων και κινδύνων. Πρόκειται για την

[89] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

[90] Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?

αναπροσαρμογή της συζήτησης από την καθαρή νομοθετική συμμόρφωση, σε ένα βασικό ερώτημα σχετικά με την ηθική χρήση των δεδομένων.

3.1 Η Συγκατάθεση στα πλαίσια του Internet of Things (IoT) (αρ.6 παρ.1 στοιχ. α΄ ΓΚΠΔ).

Ο κλάδος του IoT επηρεάζεται έντονα από το GDPR. Οι προσωπικές πληροφορίες που απαιτούνται στο IoT περιβάλλον δεν είναι μόνο ευαίσθητες πληροφορίες, αλλά έχουν και τεράστιο όγκο. Παρόλο που δεν υπάρχει νόμος για την προστασία της ιδιωτικής ζωής ειδικά για τον τομέα του IoT, η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC)[91] διεξάγει συζητήσεις σχετικά με την πολιτική ασφάλειας και την προστασία της ιδιωτικής ζωής στο περιβάλλον του IoT. Η FTC υπέβαλε σχόλια σχετικά με τις ανησυχίες για τις παραβιάσεις της ιδιωτικής ζωής των συσκευών IoT και την κατεύθυνση της προστασίας των πληροφοριών δραστηριοτήτων που σχετίζονται με το IoT μέσω της έκθεσης "Benefits, Challenges, and Potential Roles for the Government in Fostering the Advantage of the Internet of Things".[92] Στην εν λόγω δήλωση, η FTC τόνισε ότι οι συσκευές IoT που μπορούν να συλλέγουν, να μεταδίδουν και να μοιράζονται ευαίσθητες πληροφορίες των καταναλωτών σχετικά με τις φυσικές τους συνήθειες και τον τρόπο ζωής τους, είναι επικίνδυνες όταν συνδυάζονται με πληροφορίες που συλλέγονται από άλλες συσκευές.[93]

Λόγω των χαρακτηριστικών της συλλογής και της κοινής χρήσης προσωπικών πληροφοριών του IoT, υπάρχει η πιθανότητα να υπάρξουν περισσότερες δυσκολίες στη διαδικασία συναίνεσης. Σύμφωνα με το ΓΚΠΔ, υπάρχουν προϋποθέσεις υπό τις οποίες είναι απαραίτητο τα υποκείμενα να ενημερώνονται για τον σκοπό της συλλογής προσωπικών πληροφοριών, με εύληπτους όρους και να απλοποιείται η διαδικασία παροχής συγκατάθεσης. Παρεμβαίνοντας στη διαδικασία συγκατάθεσης, οι καταναλωτές θα είναι πιο διστακτικοί στη συλλογή ευαίσθητων και ποικίλων προσωπικών πληροφοριών και οι κανονισμοί αυτοί θα έχουν σημαντικό οικονομικό αντίκτυπο.

Οι νέοι κανονισμοί αναφέρουν επίσης ότι τα παιδιά ηλικίας κάτω των 13 ετών δεν μπορούν να δώσουν συγκατάθεση εκ μέρους τους για την επεξεργασία των προσωπικών

[91] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[92] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[93] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

τους δεδομένων, ενώ η συγκατάθεση για τα παιδιά ηλικίας μεταξύ 13 και 15 ετών υπόκειται στους επιμέρους νόμους του κάθε κράτους μέλους. κάθε κράτους μέλους, αν και η προεπιλεγμένη θέση θα είναι συνήθως ότι δεν μπορούν να συναινέσουν.[94]

Η συμμόρφωση με τον GDPR σε περιβάλλοντα IoT συνοδεύεται από πολλές προκλήσεις, με πρώτη τη συγκατάθεση. Μπορούμε να ελέγξουμε ποια δεδομένα συλλέγονται για ποιον, ή ποια δεδομένα συλλέγονται καθόλου; Μπορεί ένας φιλοξενούμενος –σε ένα έξυπνο σπίτι- να απαγορεύσει τη συλλογή των δεδομένων του ενώ βρίσκεται στο σπίτι; Τα σημερινά συστήματα IoT δυσκολεύονται να παρέχουν αυτό το είδος ελέγχου και οι επικοινωνίες M2M βασίζονται στο ίδιο το γεγονός ότι η ανθρώπινη συμβολή δεν είναι απαραίτητη για τη λειτουργία του συστήματος.[95] Οι διαδικτυακές υπηρεσίες έχουν συνήθως μια πολιτική απορρήτου όπου αναφέρουν ποια είδη δεδομένων συλλέγουν και για ποιους σκοπούς - η αποδοχή αυτού του εγγράφου πριν από τη χρήση της υπηρεσίας είναι υποχρεωτική και θεωρείται συναίνεση, αλλά αυτό είναι ένα στατικό έγγραφο που δεν ταιριάζει με τη δυναμική φύση του IoT. Συχνά είναι γραμμένο με τρόπο που είναι δύσκολο να κατανοηθεί από τον μέσο άνθρωπο, είναι επίσης μια απόφαση μιας χρήσης που αφαιρεί από τον χρήστη τη δυνατότητα να είναι σε θέση να τροποποιεί/προσαρμόζει τι θα συλλέγεται. Ένα άλλο ζήτημα είναι ότι σε περιβάλλοντα IoT ένα άτομο δεν είναι πάντα ενεργός χρήστης της υπηρεσίας που συλλέγει τα δεδομένα του, οπότε το άτομο αυτό δεν έδωσε κανενός είδους συγκατάθεση και μπορεί να αγνοεί εντελώς ότι τα δεδομένα του συλλέγονται.[96] Ως μόνη λύση φαίνεται συχνά η απενεργοποίηση του/των αισθητήρα/ων, γεγονός που ουσιαστικά διακόπτει ή καταστρέφει εντελώς το σύστημα. Ο ΓΚΠΔ αναφέρει ότι η συγκατάθεση πρέπει να δίνεται με δήλωση ή σαφή θετική ενέργεια, και για τα δημόσια περιβάλλοντα IoT, όπου η ιδιωτικότητα μπορεί να αποτελέσει ζήτημα, υπάρχει ακόμα πολύς δρόμος για να επιτευχθεί ένας ολοκληρωμένος και επαληθεύσιμος τρόπος για τον πλήρη χειρισμό της συγκατάθεσης.

[94] Lanner, 2017. Internet of Things Privacy: What GDPR Means For IoT Data.

[95] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[96] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

3.2 Η Αρχή ελαχιστοποίησης των δεδομένων στα πλαίσια του Internet of Things (IoT) (αρ.5 παρ.1 στοιχ. γ΄ ΓΚΠΔ).

Η δεύτερη πρόκληση είναι η "ελαχιστοποίηση των δεδομένων" και η αρχή του "περιορισμού του σκοπού". Στο περιβάλλον ενός έξυπνου σπιτιού οι αισθητήρες που αναπτύσσονται μπορούν να συλλέγουν ιδιαίτερα προσωπικές πληροφορίες. Ο περιορισμός της συλλογής δεδομένων σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους τα δεδομένα αυτά υποβάλλονται σε επεξεργασία, είναι ίσως ανέφικτο σε αυτό το περιβάλλον. Για παράδειγμα, ο ήχος και το βίντεο συλλαμβάνονται σε ακατέργαστη μορφή, οπότε ο μόνος τρόπος να περιοριστεί η συλλογή δεδομένων είναι να τα λογοκρίνει αμέσως μετά τη λήψη τους, γεγονός που μας οδηγεί στην επόμενη πρόκληση.[97]

Έστω ότι ο χρήστης έχει αποδεχτεί μια πολιτική απορρήτου και γνωρίζει ακριβώς τι συλλέγεται. Επιτρέπει η τρέχουσα υπηρεσία στον χρήστη να δει πώς γίνεται η επεξεργασία αυτών των δεδομένων; π.χ. πώς πόσες φορές συλλέχθηκαν συγκεκριμένες πληροφορίες σε μια ημέρα, πού αποστέλλονται και ποια διαδρομή ακολούθησε για να φτάσει εκεί[98]; Μοιράστηκαν με τρίτους, και αν ναι με ποιους; Αυτό το είναι πολύ σχετικό με τον ΓΚΠΔ, δεδομένου ότι τα δεδομένα που αφορούν Ευρωπαίους πολίτες πρέπει να αποθηκεύονται εντός της Ευρωπαϊκής Ένωσης και να τηρούν τους νόμους της ΕΕ. Το αίτημα πρόσβασης των υποκειμένων των δεδομένων (DSAR[99]) είναι ένα εργαλείο του ΓΚΠΔ που επιτρέπει στα άτομα να ζητούν πρόσβαση σε δεδομένα που μια εταιρεία κατέχει γι' αυτούς.

Το "δικαίωμα στη λήθη" είναι ένα αποκλειστικό ευρωπαϊκό δικαίωμα, όπου μια εταιρεία οφείλει να διαγράψει όλα τα δεδομένα που κατέχει για ένα άτομο όταν της ζητηθεί. Στο IoT, τόσο η διαφανής επεξεργασία όσο και το δικαίωμα στη λήθη γίνονται πιο σύνθετα να αντιμετωπιστούν, ξεκινώντας από το γεγονός ότι τα δεδομένα ενδεχομένως θα μεταπηδούν από συσκευή σε συσκευή πολύ περισσότερες φορές από το συνηθισμένο πριν φτάσουν στον τελικό προορισμό όπου θα αποθηκευτούν μόνιμα. Ως εκ τούτου, για τις εταιρείες θα είναι πιο δύσκολο να παρακολουθούν πού βρίσκεται κάθε κομμάτι δεδομένων, όχι μόνο για λόγους απεικόνισης και διαφάνειας αλλά και για τους σκοπούς της διαγραφής.

[97] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[98] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[99] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

3.3 Η Αναφορά Παραβίασης Δεδομένων στα πλαίσια του Internet of Things (IoT)

Οι παραβιάσεις δεδομένων το 2017 προκάλεσαν χάος, με μεγάλες εταιρείες όπως η Equifax να αποτυγχάνουν να διασφαλίσουν τα δεδομένα των πελατών. Ενώ δεν υπάρχει έλλειψη εργαλείων για την προστασία των δεδομένων, οι παραβιάσεις τείνουν να συμβαίνουν λόγω κακών πρακτικών ασφαλείας ή τυχαίων λαθών.[100] Ο ΓΚΠΔ ορίζει μια προθεσμία 72 ωρών για τις εταιρείες να αναφέρουν παραβιάσεις δεδομένων στις Αρχές Προστασίας Δεδομένων (ΑΠΔ) αφότου τις αντιληφθούν. Αυτό είναι πιθανό να αποδειχθεί εξαιρετικά δύσκολο για όλους, δεδομένου ότι η εκτίμηση της έκτασης και των συνεπειών μιας παραβίασης δεδομένων είναι δύσκολη. Σε περιβάλλοντα IoT, η εύρεση και αξιολόγηση μιας παραβίασης δεδομένων μεταξύ εκατοντάδων ή χιλιάδων συσκευών που έχουν αναπτυχθεί, θα αποδειχθεί σίγουρα ότι δεν είναι εύκολη υπόθεση.

3.4 Η ιδιωτικότητα μέσω σχεδιασμού και η ασφάλεια δεδομένων στα πλαίσια του Internet of Things (IoT)

Ο ΓΚΠΔ απαιτεί ρητά από τους υπευθύνους επεξεργασίας δεδομένων να εφαρμόζουν αποτελεσματικά και αποδεδειγμένα μέτρα για να εγγυώνται την ιδιωτικότητα και την εμπιστευτικότητα ενός χρήστη. Λαμβάνοντας υπόψη το πλαίσιο του IoT, αυτό αντιπροσωπεύει ένα ακόμη πιο δύσκολο σημείο που πρέπει να ληφθεί υπόψη, λόγω της φύσης αυτών των συσκευών που τείνει να έχει περιορισμένο υλικό και απλές διαμορφώσεις συστήματος, καθιστώντας δύσκολη την ανάπτυξη προηγμένων και αποτελεσματικών μηχανισμών ασφαλείας. Έλεγχος ταυτότητας σε βάθος και προηγμένες τεχνικές, όπως η πλήρης ομομορφική κρυπτογράφηση (FHE)[101] είναι πιθανόν να αποκλείονται. Μια πρόσφατη έρευνα σχετικά με τα πρωτόκολλα IoT και τους κινδύνους ασφαλείας δείχνει επίσης ότι υπάρχει ακόμη πολύς δρόμος για την προστασία των συστημάτων IoT.

3.5 Το Δικαίωμα Αποζημίωσης στα πλαίσια του Internet of Things (IoT)

Το δικαίωμα αποζημίωσης αποτελεί ένα άρθρο που σχετίζεται άμεσα με όλες τις εταιρείες και με τις IoT επιχειρήσεις, ωστόσο ο λόγος για τον οποίο η βιομηχανία IoT έχει μεγάλη επιρροή είναι ότι, ένας φορέας επίθεσης μπορεί να οδηγήσει σε διάφορους τύπους

[100] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[101] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

διαρροής προσωπικών πληροφοριών. Από επιχειρηματική άποψη, εάν η επιχείρηση συμμορφώνεται με τις διατάξεις του ΓΚΠΔ, μπορεί να αποκτήσει δικαιώματα στο δικαίωμα μη αποζημίωσης.[102] Ωστόσο, οι IoT εταιρείες δυσκολεύονται να αποκτήσουν αυτά τα δικαιώματα, καθώς υπάρχει μία μεγάλη πιθανότητα να μην είναι σε θέση να συμβαδίσουν με τις ενημερώσεις ασφαλείας ενός τεράστιου αριθμού συσκευών, και οι προϋποθέσεις για την προστασία των προσωπικών πληροφοριών που κάθε συσκευή συλλέγει είναι πολύ πιο αυστηρές από ό,τι για άλλες βιομηχανικές δραστηριότητες.

3.6 Οι Απειλές Προστασίας της Ιδιωτικής ζωής στα πλαίσια του Internet of Things (IoT)

Οι απειλές που παραβιάζουν την ιδιωτική ζωή του χρήστη οδηγούν σε δυνητικά δυσμενείς επιπτώσεις. Η επικρατέστερη απειλή συνδέει ένα αναγνωριστικό, για παράδειγμα, όνομα, διεύθυνση, προσωπικά δεδομένα με τον χρήστη. Αυτή η διαδικασία που ονομάζεται ταυτοποίηση μπορεί να ενδυναμώσει και να προκαλέσει άλλες απειλές, όπως η σκιαγράφηση προφίλ και η παρακολούθηση.[103] Ο χρήστης μπορεί να ταυτοποιηθεί κυρίως μέσω της παρακολούθησης με κάμερες, των δακτυλικών αποτυπωμάτων και των μηχανισμών αναγνώρισης ομιλίας. Αυτή η νεοαποκτηθείσα ταυτότητα μπορεί να συσχετιστεί με μια συγκεκριμένη ρύθμιση που παραβιάζει την ιδιωτικότητα και αποτελεί δυνητική απειλή για τη ζωή του χρήστη.

3.7 Η Αποθήκευση Δεδομένων στα πλαίσια του Internet of Things (IoT)

Οι εταιρείες που αποθηκεύουν δεδομένα για οποιοδήποτε χρονικό διάστημα θα πρέπει να προσαρμόσουν ή να εφαρμόσουν συστήματα αποθήκευσης ώστε να λαμβάνουν υπόψη το πλαίσιο προστασίας της ιδιωτικής ζωής από τον σχεδιασμό. Οι εταιρείες που αποθηκεύουν δεδομένα, είτε στο cloud ή σε εσωτερικό hardware, θα πρέπει να διασφαλίσουν ότι συμμορφώνονται με τους κανονισμούς πρόσβασης και τις αρχές ελαχιστοποίησης των δεδομένων, καθώς και να παρέχουν επαρκή ασφάλεια και προστασία στον κυβερνοχώρο με μέτρα, όπως η κρυπτογράφηση των δεδομένων σε κάθε δυνατή ευκαιρία.[104] Η αντιστοίχιση εφαρμογών σε αποθηκευτικούς χώρους θα διασφαλίσει επίσης ότι κάθε εφαρμογή μπορεί να αντιστοιχιστεί με τον φυσικό

[102] Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.

[103] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[104] Lanner, 2017. Internet of Things Privacy: What GDPR Means For IoT Data.

αποθηκευτικό χώρο που καταλαμβάνει, με τα δεδομένα να είναι αναγνωρίζονται ότι περιέχουν προσωπικές πληροφορίες.

3.8 Η Εξατομίκευση βάσει κοινωνικού περιβάλλοντος στα πλαίσια του Internet of Things (IoT)

Η εκθετική ανάπτυξη των εταιρειών μέσων κοινωνικής δικτύωσης τα τελευταία χρόνια έχει δημιουργήσει ένα τεράστιο διαδικτυακό θησαυροφυλάκιο πραγματικών ταυτοτήτων. Αποθηκεύουν ποικιλία όγκου και μορφών δεδομένων για τους χρήστες τους, συμπεριλαμβανομένων ονομάτων, ηλεκτρονικών μηνυμάτων, λίστες φίλων, κοινωνικοοικονομικών στοιχείων, ατομικών φωτογραφιών, τοποθεσιών και ούτω καθεξής. Χρησιμοποιούν αυτά τα δεδομένα για προσαρμογές, αναζήτηση και προβολή στο διαδίκτυο. Λόγω του αντίκτυπου αυτών των δικτύων στην τρέχουσα ζωή μας, τα άτομα είναι συχνά έτοιμα να να αποκαλύψουν περισσότερα προσωπικά δεδομένα από το κανονικό. Αυτό οδηγεί σε ανεπιθύμητες καταστάσεις. Το 2008, το 8% των αμερικανικών οργανισμών που απασχολούσαν 1000+ εργαζόμενους είχαν απολύσει έναν εργαζόμενο λόγω της απελευθέρωσης ανεπιθύμητων πληροφοριών στα μέσα κοινωνικής δικτύωσης.[105] Οι μεγάλες εταιρείες επιτρέπουν σε εφαρμογές τρίτων να αποκτήσουν πρόσβαση στα προφίλ των χρηστών τους μέσω ενός Application Programming προγραμματισμού. Οι χάκερ μπορούν να έχουν πρόσβαση στις κοινωνικές πληροφορίες του θύματος μέσω του API εύκολα, γεγονός που θέτει σε κίνδυνο την ιδιωτική τους ζωή.

Η κατάρτιση προφίλ συμπεριφοράς είναι η πράξη της συλλογής μακροπρόθεσμων πληροφοριών σχετικά με τις δραστηριότητες του χρήστη και εξατομίκευση της διεπαφής χρήστη από τα δεδομένα αυτά. Η πράξη αυτή έχει γίνει δημοφιλής τα τελευταία χρόνια στην αναζήτηση μέσω διαδικτύου, διαδικτυακές διαφημίσεις και στις εταιρείες ηλεκτρονικού εμπορίου. Η κατάρτιση προφίλ συμπεριφοράς παρακολουθεί ένα ευρύ φάσμα ενεργειών του χρήστη για μεγάλο χρονικό διάστημα χρησιμοποιώντας cookies του προγράμματος περιήγησης με πρακτικά μηδενική συγκατάθεση του χρήστη. Αυτό προκαλεί μη ζητηθέντα μάρκετινγκ.[106] Εξάλλου, για την προώθηση προϊόντων με τη χρήση διαφημίσεων, εταιρείες όπως η Google συνδέουν συμπεριφορικό προφίλ με τους

[105] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

[106] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

λογαριασμούς των διακομιστών τους για να προβάλλονται οι διαφημίσεις σε όλους τους υπολογιστές και τις κινητές συσκευές, με αποτέλεσμα την πιθανότητα άλλα άτομα να αποκτήσουν πρόσβαση στο εξατομικευμένο και ιδιωτικό περιεχόμενο του χρήστη.[107]

Η αλληλεπίδραση και παρουσίαση που παραβιάζει την ιδιωτικότητα βασίζεται στη διαβίβαση ιδιωτικών δεδομένων μέσω ενός δημόσιου μέσου και στην πράξη την αποκάλυψή τους σε ένα ανεπιθύμητο πλήθος. Πολλές υπηρεσίες IoT βασίζονται σε ουσιαστική αλληλεπίδραση με τον χρήστη. Αυτό το σύστημα αλληλεπίδρασης και παρουσίασης μπορεί να παρατηρηθεί από τους ανθρώπους στην περιοχή, καθώς είναι δημόσιο. Οι προσωπικές πληροφορίες και τα ιδιωτικά δεδομένα μπορούν να ανταλλάσσονται από αυτό το σύστημα και τον εγγενή χρήστη που μπορεί να θέσει τα ιδιωτικά δεδομένα του χρήστη σε κίνδυνο. Σε μια έξυπνη πόλη, για παράδειγμα, όταν ο χρήστης μπορεί να ζητήσει οδηγίες για ένα συγκεκριμένο εστιατόριο ή ιατρική κλινική, εάν οι πληροφορίες αυτές εμφανίζονται σε μια κοντινή δημόσια οθόνη παρουσίασης, ορατή στους παρευρισκόμενους, οι πιθανοί παραβάτες μπορεί να λάβουν γνώση ευκολότερα και να χρησιμοποιήσουν αυτές τις πληροφορίες για τα κεκτημένα τους.[108]

Εξαιτίας της συνεχούς εξέλιξης της τεχνολογικής βιομηχανίας, οι υπηρεσίες ασύρματης πιστότητας και GPS γίνονται όλο και πιο ακριβείς. Αυτό έχει οδηγήσει στην ανάπτυξη εφαρμογών για κινητά τηλέφωνα που μπορούν να εντοπίσουν την ακριβή τοποθεσία του χρήστη χρησιμοποιώντας αποτελεσματικές διεπαφές προγραμματισμού εφαρμογών και πλαίσια για να προσφέρουν προσφορές βάσει τοποθεσίας στη συγκεκριμένη τοποθεσία.

Το IoT συνεχίζει να ευημερεί όπως βλέπουμε στον 21ο αιώνα. Καθώς η εστίασή μας μετατοπίζεται στην ενσωμάτωση περισσότερων «έξυπνων» συσκευών στη ζωή μας για να την κάνουμε πιο ομαλή, τα μεγαλύτερα μειονεκτήματα αυτών των συσκευών τείνουν συνήθως να περνούν κάτω από το ραντάρ μας. Με την ανάλυση των προκλήσεων στον τομέα της ασφάλειας, της ιδιωτικής ζωής, της ηθικής και της νομικής φύσης του IoT, γίνεται φανερό πώς οι προκλήσεις αυτές έχουν σημαντικό αντίκτυπο στην καθημερινή μας ζωή και ότι η έρευνα που επικεντρώνεται σε αυτές τις αρνητικές πτυχές είναι αρκετά περιορισμένη, δεδομένης της σημαντικής ανάπτυξης του IoT τις τελευταίες δύο δεκαετίες.

[107] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

[108] Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.

Οι περιπτώσεις χρήσης παρέχουν μια εικόνα για πώς τα ζητήματα της ασφάλειας, της ηθικής, της ιδιωτικής ζωής, της εμπιστοσύνης και των νόμων έχουν αντίκτυπο στην κοινωνία και την καθημερινή μας ζωή. Ένας τρόπος για την καταπολέμηση αυτών των ζητήματα είναι η θέσπιση ειδικών νόμων για το IoT.

Ο GDPR αποτελεί σημαντική πρόκληση για τους προγραμματιστές, τους κατασκευαστές και τους παρόχους υπηρεσιών IoT, δεδομένης της έλλειψης μιας καθιερωμένης στρατηγικής για την εξασφάλιση, τη διαχείριση και την ενημέρωση των συσκευών IoT. Για τους χρήστες, αντιπροσωπεύει το πιο ολοκληρωμένο νομικό μέσο για να βοηθήσει την προστασία των δικαιωμάτων τους στην ψηφιακή εποχή, σε μια περίοδο όπου η ιδιωτική τους ζωή βρίσκεται όλο και περισσότερο υπό απειλή.[109] Οι νέοι κανονισμοί του ΓΚΠΔ θα έχουν μετασχηματιστική επίδραση στον τρόπο με τον οποίο οι συσκευές IoT καταγράφουν και αποθηκεύουν προσωπικά δεδομένα και, με περαιτέρω κανονισμούς σχετικά με τη ρομποτική, την τεχνητή νοημοσύνη και την αυτοματοποίηση, θα μπορούσε να διαμορφώσει το μέλλον των προϊόντων, συσκευών και συσκευών του Διαδικτύου των πραγμάτων και των εφαρμογών. Οι κανονισμοί συναίνεσης σχετικά με τα προσωπικά δεδομένα παιδιών ηλικίας κάτω των 13 ετών, για παράδειγμα, θα μπορούσαν να αναγκάσουν τους λιανοπωλητές και τους κατασκευαστές να προσαρμόσουν τα προϊόντα τους ώστε να περιλαμβάνουν γονικούς ελέγχους ή περιορισμένες διαδικτυακές υπηρεσίες όταν οι συσκευές και τα προϊόντα χρησιμοποιούνται από παιδιά ηλικίας 13 ετών και κάτω.[110] Θα μπορούσαν επίσης να αλλάξουν τον τρόπο με τον οποίο οι επιχειρήσεις και οι οργανισμοί αποκτούν τη συγκατάθεση των υποκειμένων, με σενάρια όπως η συγκατάθεση που αποτελεί προϋπόθεση για την πώληση ή τη χρήση υπηρεσιών δεν θα θεωρείται ελεύθερα δοσμένη συγκατάθεση. Με μεγάλα πρόστιμα για όσους δεν συμμορφώνονται, ωστόσο, μένει να δούμε, το πόσο καλά οι προγραμματιστές IoT, οι έμποροι λιανικής πώλησης και οι κατασκευαστές ανταποκρίνονται στους νέους κανονισμούς.

[109] Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.

[110] Lanner, 2017. Internet of Things Privacy: What GDPR Means For IoT Data.

4. ΓΚΠΔ και Δίκτυα τηλεπικοινωνιών 5ης γενιάς, GDPR and 5G

Το 5G αναπτύσσεται σε όλο τον κόσμο και υπόσχεται απρόσκοπτη συνδεσιμότητα και υποστήριξη ποικίλων καινοτομιών, όπως έξυπνα σπίτια, αυτοκίνητα χωρίς οδηγό, βιομηχανικό αυτοματισμό, τρισδιάστατες ταινίες και επαυξημένη πραγματικότητα. Το 5G πρόκειται να επιτρέψει την ανάπτυξη δισεκατομμυρίων συσκευών του Διαδικτύου των Πραγμάτων (IoT) και τη δημιουργία ενός τεράστιου αριθμού νέων εφαρμογών. Αυτές οι καινοτομίες έχουν τη δυνατότητα να βελτιώσουν τη ζωή των ανθρώπων, διευκολύνοντας, για παράδειγμα, την εξ αποστάσεως χειρουργική επέμβαση και άλλες καινοτομίες προς όφελος της ανθρώπινης ζωής. Το 5G δεν είναι απλά ένα ταχύτερο δίκτυο κινητής τηλεφωνίας και δεν είναι μόνο θέμα των τηλεπικοινωνιακών παρόχων.[111] Καθώς η συνδεσιμότητα γίνεται όλο και πιο ρευστή και ευέλικτη, το 5G θα αλλάξει τους τύπους υπηρεσιών και τα πιθανά επιχειρηματικά μοντέλα με απρόβλεπτους τρόπους- με τον ίδιο τρόπο που η οικονομία διαμοιρασμού και οι εφαρμογές έχουν αλλάξει τον τρόπο με τον οποίο αλληλεπιδρούμε με οργανισμούς, κυβερνήσεις και μεταξύ μας. Ο όγκος και η λεπτομέρεια των δεδομένων κίνησης και θέσης που παράγονται κατά τη διάρκεια των επικοινωνιών 5G θα αυξηθούν, οι οργανισμοί θα μπορούν να προσαρμόζουν τις απαιτήσεις του εικονικού τους δικτύου για συγκεκριμένες περιπτώσεις χρήσης ενώ μια αλματώδης αύξηση των νέων εφαρμογών που βασίζονται στα δεδομένα και αξιοποιούν το 5G θα μπορούσε να οδηγήσει σε αύξηση του όγκου και της ποικιλίας χρήσης προσωπικών δεδομένων.

Ενώ το 5G αντιπροσωπεύει μια σημαντική αλλαγή στη χρήση των δικτύων κινητής τηλεφωνίας, τα υφιστάμενα καθεστώτα προστασίας του απορρήτου των δεδομένων που είναι τεχνολογικά ουδέτερα και αντιμετωπίζουν ήδη ένα ευρύ φάσμα χρήσεων δεδομένων που συλλέγονται μέσω εφαρμογών, λειτουργικών συστημάτων κινητών συσκευών, μέσων κοινωνικής δικτύωσης, ιστότοπων και φορέων εκμετάλλευσης δικτύων, είναι πιθανό να επαρκούν για την αντιμετώπιση της χρήσης των νέων δυνατοτήτων 5G στο διαδικτυακό οικοσύστημα.[112]

[111] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[112] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

Α.4.1 Το περιεχόμενο των δικτύων 5G

Ένα δίκτυο κινητής τηλεφωνίας αποτελείται από τρία εννοιολογικά μέρη: δίκτυο ραδιοπρόσβασης που επιτρέπει στις συσκευές που βρίσκονται σε μια ορισμένη περιοχή (κυψέλη) να συνδεθούν σε μια κεραία στον πύργο κυψέλης, δίκτυο πυρήνα και δίκτυο μεταφοράς μεταξύ των στοιχείων ραδιοπρόσβασης και πυρήνα. Για να επιτευχθούν υψηλότερες ταχύτητες, τα δίκτυα 5G πρόκειται να χρησιμοποιούν υψηλότερες ραδιοσυχνότητες. Ωστόσο, τα σήματα που μεταδίδονται σε υψηλότερες συχνότητες εξασθενούν ταχύτερα και, ως εκ τούτου, διανύουν μικρότερη απόσταση.[113] Τα σήματα είναι επίσης λιγότερο ικανά να ταξιδέψουν μέσα από κτίρια ή δέντρα, απαιτώντας έτσι μικρότερες κυψέλες, πολλές από τις οποίες θα βρίσκονται στο επίπεδο του εδάφους ή μέσα σε κτίρια (όπως το WiFi σήμερα). Το μικρότερο μέγεθος κυψέλης στο 5G συνεπάγεται ότι θα παράγονται και πιο ακριβή δεδομένα γεωγραφικού εντοπισμού στα δίκτυα. Ωστόσο, τα δορυφορικά συστήματα εντοπισμού θέσης, όπως το GPS, τα οποία κινούν πολλές καταναλωτικές υπηρεσίες που βασίζονται στην τοποθεσία, όπως την πλοήγηση ή την παρακολούθηση της φυσικής κατάστασης, θα συνεχίσουν να παρέχουν υψηλότερο επίπεδο ακρίβειας.[114] Αν μη τι άλλο, αυτό υπογραμμίζει εκ νέου την ανάγκη για οριζόντιους κανόνες που θα διασφαλίζουν την συνεχή προστασία για τους καταναλωτές, ανεξάρτητα από την τεχνολογία ή τον επιχειρηματικό τομέα.

Α.4.2 Ο Σχεδιασμός των δικτύων 5G

Είναι πολύ σημαντικό, ιδίως για την τυποποίηση και τους προμηθευτές του 5G, να λαμβάνουν ευρύτερα υπόψη το περιβάλλον συστημάτων και απειλών, τόσο από τεχνική όσο και από επιχειρηματική άποψη, κατά τον σχεδιασμό λύσεων προστασίας της ιδιωτικής ζωής.[115] Το χρονοδιάγραμμα παράδοσης της τυποποίησης, το κόστος υλοποίησης και η πολυπλοκότητα των δοκιμών είναι ζωτικής σημασίας ζητήματα. Ο ίδιος ο ΓΚΠΔ ενθαρρύνει το συνυπολογισμό αυτών των εκτιμήσεων. Με άλλα λόγια, πρέπει να αποφεύγεται η υπερβολική μηχανοποίηση, πράγμα που σημαίνει ότι οι τεχνικές λύσεις για την προστασία της ιδιωτικής ζωής πρέπει να είναι εφικτές, πρακτικές και κατάλληλες για τους κινδύνους. Για το σκοπό αυτό, πρέπει να λαμβάνονται υπόψη οι κατευθυντήριες γραμμές που εκπονήθηκαν από το νεοσύστατο Ευρωπαϊκό Συμβούλιο Προστασίας

[113] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[114] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[115] Nakarmi,Prajwol,Kumar, Schaefer,Christian, Casella,Dario, 2017. 5G and the EU General Data Protection Regulation.

Δεδομένων. Μέχρι σήμερα, η ομάδα εργασίας του άρθρου 29 έχει εκπονήσει κατευθυντήριες γραμμές, για το δικαίωμα στη φορητότητα των δεδομένων (WP 242), την προστασία των δεδομένων των χρηστών (WP 243) και την αξιολόγηση των επιπτώσεων της προστασίας των δεδομένων (WP 248).[116] Η ύπαρξη εικονικών στοιχείων δικτύου σημαίνει ότι οι λειτουργίες του κεντρικού δικτύου μπορούν να εκτελούνται μέσω λειτουργιών εκτός του δικτύου φορέα εκμετάλλευσης, π.χ. στο cloud, γεγονός που μπορεί να περιπλέξει την αλυσίδα εφοδιασμού και την αλυσίδα ευθύνης, αλλά μπορεί και να αποτελέσει ευκαιρία.[117] Μια εικονική αρχιτεκτονική με βάση το λογισμικό μπορεί επίσης να σημαίνει ότι στοιχεία του δικτύου μπορούν να απομονωθούν ή να μεταφερθούν σε εμπορευματοκιβώτια και ότι οι ευπάθειες μπορούν να αποκατασταθούν γρήγορα και εξ αποστάσεως. Εάν η φυσική υποδομή των δικτύων 5G επαναχρησιμοποιείται συνεχώς για νέες εικονικές διαμορφώσεις που παρέχονται από πολυάριθμους φορείς εκμετάλλευσης και ενδεχομένως διαχειρίζονται από επιχειρηματικούς οργανισμούς, θα μπορούσε να δημιουργήσει πολυπλοκότητα όσον αφορά το ποιος είναι τελικά υπεύθυνος για την ασφάλεια σε κάθε δεδομένο σημείο και ποιος είναι υπεύθυνος για τις συνέπειες των παραβιάσεων δεδομένων. Αυτό θα μπορούσε, επομένως, να επιβάλει μια πολύ πιο συνεργατική προσέγγιση για την ασφάλεια σε ολόκληρο το οικοσύστημα 5G. Το 5G θα επιτρέψει την ανάπτυξη τεράστιου αριθμού συσκευών IoT που θα μπορούσε να κατασκευάσει οποιοσδήποτε. Το δίκτυο 5G είναι πολύ πιο ετερογενές από τον επεξεργαστή του 4G. Είναι χτισμένο πάνω σε "τυποποιημένη" υποδομή που βασίζεται στο cloud (σε σύγκριση με τη σε μεγάλο βαθμό φυσική υποδομή του 4G) και θα περιλαμβάνει πολλά διακριτά ιδιωτικά δίκτυα που διαχειρίζονται αυτόνομοι οργανισμοί. Όλα αυτά καθιστούν δύσκολη την προστασία των πόρων του δικτύου με τη συμβατική "περιμετρικά προσανατολισμένη" ασφάλεια.[118] Επομένως, αν υποθέσουμε ότι οι επιτιθέμενοι και μπορούν και θα εισέλθουν σε δημόσια και ιδιωτικά δίκτυα 5G, τι αποτελεί την καλύτερη μέθοδο άμυνας; Οι ενδιαφερόμενοι φορείς του 5G πιστεύουν ότι αυτό είναι το μοντέλο ασφάλειας μηδενικής εμπιστοσύνης. Το Zero Trust[119] βασίζεται σε μια απλή υπόθεση: μην εμπιστεύεστε σε κανέναν τα πάντα. Αυτό σημαίνει ότι κάθε αίτημα πρόσβασης πρέπει να πιστοποιείται πλήρως, να εξουσιοδοτείται και να κρυπτογραφείται πριν χορηγηθεί. Έτσι

[116] Nakarmi,Prajwol,Kumar, Schaefer,Christian, Casella,Dario, 2017. 5G and the EU General Data Protection Regulation.

[117] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[118] Thales, 2021. 3 REASONS TO BE OPTIMISTIC ABOUT DATA PRIVACY IN THE 5G ERA.

[119] Thales, 2021. 3 REASONS TO BE OPTIMISTIC ABOUT DATA PRIVACY IN THE 5G ERA.

περιορίζονται οι δυνατότητες που μπορεί να έχει ένας εισβολέας, ακόμη και αν έχει αποκτήσει πρόσβαση στο δίκτυο.

Ένα βασικό σημείο του 5G σχετιζόμενο με την πυκνότητα, είναι ο υψηλής απόδοσης εντοπισμός θέσης και εντοπισμός συσκευών. Η εξαγωγή και ο εντοπισμός της ακριβούς θέσης του χρήστη της συσκευής, εκτός από την παροχή περισσότερων δυνατοτήτων για εφαρμογές βασιζόμενες στην ανίχνευση τοποθεσίας του χρήστη, θα μπορούσε σίγουρα να προκαλέσει τρωτά σημεία στο απόρρητο της τοποθεσίας, μέσω της μετάδοσης περισσότερων δεδομένων θέσης, τα οποία μέσω της διασταύρωσης πληροφοριών μπορούν επίσης να αποκαλύψουν ή να επηρεάσουν περαιτέρω προσωπικά δεδομένα.[120] Ως αποτέλεσμα, η πιθανή ταυτοποίηση των προσωπικών δεδομένων θα μπορούσε να χρησιμοποιηθεί για την κατάρτιση προφίλ και την παρακολούθηση των υποκειμένων των δεδομένων. Η αποτροπή της κατάρτισης προφίλ κρίνεται ως ζωτικής σημασίας, δεδομένης της αντιμετώπισης της αυτοματοποιημένης λήψης αποφάσεων, μέσω της κατάρτισης προφίλ σε πυκνότερα δίκτυα, τα οποία θα μπορούσαν να εντοπίσουν την ακριβή θέση των υποκειμένων των δεδομένων. Επιπλέον, κατά τη διαδικασία σχεδιασμού ή ανασχεδιασμού ενός συστήματος, οι προεπιλογές που αποσκοπούν στην προστασία των δεδομένων, θα πρέπει να λαμβάνουν υπόψη τον τρόπο με τον οποίο μια εφαρμογή ή συσκευή επεξεργάζεται τα προσωπικά δεδομένα του υποκειμένου (π.χ. δεδομένα θέσης, πρόσβαση σε αρχεία ή εφαρμογές της συσκευής, ευαίσθητα προσωπικά δεδομένα), κατά τη δημιουργία προεπιλογών προστασίας. Με άλλα λόγια, κάθε νέα δυνατότητα 5G, θα πρέπει να αναλύεται μέσω τεχνικής βάσης και να λαμβάνεται υπόψη ξεχωριστά, ειδικά όταν πρόκειται για την, απορρέουσα από την αρχή της ελαχιστοποίησης, προστασία της ιδιωτικής ζωής μέσω σχεδιασμού, η οποία είναι αυτή που ορίζει την ελάχιστη προσβασιμότητα των προσωπικών δεδομένων.

Οι υψηλότερες ταχύτητες θα είχαν ως αποτέλεσμα την εκ των πραγμάτων μη ενημέρωση του υποκειμένου των δεδομένων σχετικά με τα στοιχεία της επεξεργασίας των δεδομένων του, εξαιτίας ενός, πλέον, μη διαχειρίσιμου όγκου επεξεργασίας δεδομένων μέσω δικτύων 5G, αντί των δικτύων 4G. Οι υψηλοί ρυθμοί δεδομένων θα μπορούσαν επίσης να επηρεάσουν το δικαίωμα διόρθωσης, δικαίωμα στη λήθη, δικαίωμα περιορισμού

[120] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

της επεξεργασίας, δικαίωμα ενημέρωσης σχετικά με τη διόρθωση ή τη διαγραφή, λόγω της ταχείας μετάδοσης και ανταλλαγής δεδομένων.[121]

Επιπλέον, η υπερβολική ποσότητα επεξεργασίας δεδομένων, η οποία πραγματοποιείται χωρίς ανθρώπινη παρέμβαση, μέσω της κατάρτισης προφίλ των υποκειμένων των δεδομένων, εγείρει δραματικές ανησυχίες για την προστασία της ιδιωτικής τους ζωής. Όταν η παραβίαση δεδομένων θεωρείται ιδιαίτερα σοβαρή για τα δικαιώματα των υποκειμένων, είναι υποχρεωτική η ενημέρωση της εποπτικής αρχής αλλά και των υποκειμένων (άρθρο 34). Η προθεσμία 72 ωρών που τίθεται, αποσκοπεί μεν στη μείωση των παραβιάσεων δεδομένων, με τις νέες υψηλότερες ταχύτητες όμως η υποχρεωτική αναφορά στην εποπτική αρχή, ακόμη και μετά τη λήξη αυτής της προθεσμίας, θα επηρεάσει τον αναφερόμενο αντίκτυπο μιας παραβίασης δεδομένων, καθώς η ταχύτερη διαβίβαση προσωπικών δεδομένων, θα μπορούσε να μειώσει τη δυνητική διασφάλιση της υποχρεωτικής κοινοποίησης μιας παραβίασης δεδομένων που στοχεύει στον περιορισμό της ζημίας.

Οι αρχές της προστασίας δεδομένων του ΓΚΠΔ δεν εφαρμόζονται σε ανώνυμα δεδομένα, τα οποία δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (αιτιολογική σκέψη 26). Όσον αφορά τα ψευδωνυμοποιημένα δεδομένα, είναι ασφαλή εάν δεν μπορούν να αποδοθούν σε φυσικό πρόσωπο, εφόσον όμως παραμένουν αναγνωρίσιμα σύμφωνα με τις τρέχουσες τεχνολογικές εξελίξεις, λαμβάνοντας παράλληλα υπόψη το χρόνο και το κόστος της ταυτοποίησης. Στο πλαίσιο της ασφάλειας του 5G, ένας σημαντικός και επαρκής στόχος είναι ο διαχωρισμός του χρήστη από μια συγκεκριμένη συσκευή. Η εισαγωγή υπηρεσιών και συσκευών πρόκειται να επηρεάσει την ασφάλεια στο περιβάλλον 5G και να ανακύψουν ζητήματα προστασίας της ιδιωτικής ζωής. Τα δίκτυα 5G με τεράστιο αριθμό συσκευών πρόκειται να αντιμετωπίσουν νέα αναγνωριστικά χρηστών και νέους τύπους ταυτοτήτων συσκευών, όπως αναγνωριστικά για συσκευές IoT. Λύση για την προστασία της ιδιωτικότητας στα δίκτυα 5G για θέματα ταυτότητας συνδρομητών, αποτελεί η προστασία του μόνιμου αναγνωριστικού της συνδρομής του χρήστη από ενεργές επιθέσεις, με τη χρήση του δημόσιου κλειδιού του οικιακού δικτύου. Επιπλέον, καθώς τα δίκτυα 5G απαιτούν μέτρα από άκρο σε άκρο για την ικανοποίηση των απαιτήσεων του ΓΚΠΔ, τα πρότυπα 5G ορίζουν ότι τα αναγνωριστικά του χρήστη κρυπτογραφούνται κατά τη μετάδοση μέσω της διεπαφής αέρα

[121] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

και ότι η κρυπτογράφηση και η προστασία της ακεραιότητας εκτελούνται στο κανάλι μετάδοσης από άκρο σε άκρο, ώστε να διασφαλίζονται τα προσωπικά δεδομένα από τυχαία, μη εξουσιοδοτημένη ή παράνομη πρόσβαση, χρήση, τροποποίηση, αποκάλυψη, απώλεια, καταστροφή ή βλάβη (αιτιολογική σκέψη 39 και άρθρο 5 παράγραφος 1 ΓΚΠΔ).[122]

Οι απαιτήσεις ασφάλειας και προστασίας της ιδιωτικής ζωής βάσει των προδιαγραφών για το 5G είναι: (α) η εμπιστευτικότητα των δεδομένων χρήστη και των δεδομένων σηματοδοσίας, (β) η ακεραιότητα των δεδομένων χρήστη και των δεδομένων σηματοδοσίας, (γ) η ασφαλής αποθήκευση και επεξεργασία των διαπιστευτηρίων συνδρομής και (δ) η προστασία της ιδιωτικής ζωής των συνδρομητών. Καθίσταται σαφές ότι τα παραπάνω χαρακτηριστικά ασφαλείας δεν θα ενεργοποιηθούν όλα εξ ορισμού στον εξοπλισμό του δικτύου, καθώς ορισμένα από αυτά είναι προαιρετικά, προς υλοποίηση για τους προμηθευτές ή προς χρήση από τους φορείς εκμετάλλευσης. Κατά συνέπεια, η αποτελεσματικότητα αυτών των χαρακτηριστικών ασφαλείας εξαρτάται από τον τρόπο με τον οποίο οι φορείς εκμετάλλευσης τους επιβάλλουν και με τον οποίο διαχειρίζονται τα δίκτυά τους. Επιπλέον, οι απαιτήσεις για τα κράτη μέλη της ΕΕ, κατά την προσπάθεια εφαρμογής των δικτύων 5G στα κράτη μέλη της ΕΕ είναι οι εξής: (α) η αύξηση των μέτρων ασφαλείας για τους φορείς εκμετάλλευσης κινητών δικτύων 5G, (β) η εφαρμογή περιορισμών για τους προμηθευτές υψηλού κινδύνου σύμφωνα με την αξιολόγηση του προφίλ κινδύνου αυτών και (γ) η διασφάλιση της ύπαρξης πολλαπλών προμηθευτών για τους φορείς εκμετάλλευσης, ώστε να αποφεύγεται η εξάρτηση από έναν μόνο προμηθευτή ή από έναν προμηθευτή υψηλού κινδύνου. [123] Το Ευρωπαϊκό Συμβούλιο αναγνώρισε την ανάγκη θέσπισης ισχυρών κοινών προτύπων και μέτρων ασφαλείας, με έμφαση στην προστασία της ιδιωτικής ζωής ήδη από το σχεδιασμό, λαμβάνοντας υπόψη τα διεθνή πρότυπα για το 5G.

Συνοψίζοντας, τα μέτρα ασφαλείας 5G τα οποία θα μπορούσαν να εφαρμοστούν με βάση τον ΓΚΠΔ, έχουν σαν κύριο άξονα την ανωνυμοποίηση, την ψευδωνυμοποίηση και γενικά τη προστασία της ιδιωτικής ζωής μέσω σχεδιασμού, προκειμένου να διατηρηθεί η προστασία των δεδομένων από άκρο σε άκρο και ad hoc, αξιολογώντας και

[122] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

[123] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

επανεξετάζοντας επίσης την αποτελεσματικότητα αυτών των μέτρων, όσο αυτά εφαρμόζονται και όσο οι χρήστες των δικτύων 5G αυξάνονται.

Το 5G έχει σχεδιαστεί προκειμένου να είναι ευέλικτο. Θα είναι σε θέση να υποστηρίζει νέες εφαρμογές με διαφορετικές απαιτήσεις, όπως ρυθμούς δεδομένων Gigabit, χαμηλή καθυστέρηση και υψηλή αξιοπιστία. Αυτό επιτυγχάνεται με τη δυνατότητα διαμόρφωσης των βασικών στοιχείων των φυσικών τηλεπικοινωνιακών δικτύων, εικονικά, με τρόπο που να ανταποκρίνεται στις ιδιαίτερες ανάγκες των κάθετων βιομηχανικών κλάδων και των οργανισμών. Αυτές οι διαμορφώσεις αναφέρονται συχνά ως "φέτες δικτύου".[124] Για παράδειγμα, μια φέτα δικτύου θα μπορούσε να παρέχει αποτελεσματική υποστήριξη σε μεγάλο αριθμό συνδέσεων, ενεργοποιώντας το IoT. Ένα σύστημα ψυχαγωγίας μέσα στο αυτοκίνητο, για παράδειγμα, παρουσιάζει εντελώς διαφορετικές απαιτήσεις από τις συσκευές υποβοηθούμενης οδήγησης, που στέλνουν δεδομένα με εξαιρετικά χαμηλή καθυστέρηση στην κοντινή κυκλοφορία.

Από τη σκοπιά ενός παρόχου κινητής τηλεφωνίας, μια φέτα δικτύου είναι ένα ανεξάρτητο από άκρο σε άκρο υλικοτεχνικό δίκτυο που λειτουργεί σε μια κοινή φυσική υποδομή[125], ικανή να παρέχει την ποιότητα εξυπηρέτησης που έχει συμφωνηθεί. Είναι δυνατόν να εκτείνεται σε πολλαπλά τμήματα του δικτύου (π.χ. τερματικό, δίκτυο πρόσβασης, δίκτυο πυρήνα και δίκτυο μεταφοράς) και να αναπτύσσεται από πολλούς φορείς εκμετάλλευσης. Μια φέτα δικτύου περιλαμβάνει αποκλειστικούς ή/και κοινόχρηστους πόρους, π.χ. όσον αφορά την επεξεργαστική ισχύ, την αποθήκευση και το εύρος ζώνης, και είναι απομονωμένη από τις άλλες φέτες δικτύου.[126] Η τμηματοποίηση δικτύου οδηγεί σε αποδοτικότερη χρήση της υποδομής επικοινωνιών για όλους: οι φορείς εκμετάλλευσης δικτύων κινητής τηλεφωνίας μπορούν να χρησιμοποιούν την ίδια φυσική υποδομή για να εξυπηρετούν τους πελάτες τους με ευέλικτους τρόπους- οι καταναλωτές επωφελούνται από μεγαλύτερη ποικιλία υπηρεσιών που βελτιστοποιεί την επίδοση, ανεξαρτήτως της δραστηριότητάς τους- και οι οργανισμοί μπορούν να διαμορφώνουν τα εικονικά τους δίκτυα ώστε να ανταποκρίνονται στις συγκεκριμένες ανάγκες τους κατά παραγγελία (π.χ. διαστασιολόγηση, διαμόρφωση) μέσω διεπαφών προγραμματισμού εφαρμογών (API) που προσφέρουν οι φορείς εκμετάλλευσης κινητής τηλεφωνίας. Για παράδειγμα, ένας οργανισμός μπορεί να παρέχει έξυπνους μετρητές και έξυπνες οικιακές

[124] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[125] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[126] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

συσκευές με χαμηλές απαιτήσεις σε εύρος ζώνης και ταχύτητα, αλλά μπορεί επίσης να παρέχει ροή βίντεο, παιχνίδια και εξοπλισμό VR/AR.[127]

Η ενισχυμένη συνδεσιμότητα θα προκαλέσει τη δημιουργία νέων επιχειρηματικών μοντέλων και καινοτομιών, μεγαλύτερη σύγκλιση τομέων και τεχνολογιών. Η προσέγγιση της έξυπνης νομοθεσίας για την προστασία των προσωπικών δεδομένων χαρακτηρίζεται από κανόνες που βασίζονται σε επίπεδα κινδύνων (risk based), είναι τεχνολογικά και τομεακά ουδέτεροι και ενισχύουν την έννοια της "Λογοδοσίας".[128] Σύμφωνα με την αρχή της Λογοδοσίας, οι οργανισμοί δεν καλούνται μόνο να συμμορφώνονται, αλλά και να είναι σε θέση να αποδεικνύουν τον τρόπο συμμόρφωσής τους μέσω αποτελεσματικών πολιτικών και διαδικασιών σχετικά με τη διαχείριση των δεδομένων, για παράδειγμα, να διενεργούν εκτιμήσεις επιπτώσεων στην προστασία των προσωπικών δεδομένων, να είναι διαφανείς και να αποφεύγουν ή να μετριάζουν τον κίνδυνο βλάβης των ατόμων μέσω ορθών πρακτικών "ιδιωτικότητας εκ κατασκευής". Τέτοια καθεστώτα προστασίας του απορρήτου των δεδομένων ανέκαθεν αποδέχονταν ότι το πλαίσιο της επεξεργασίας δεδομένων, λαμβάνοντας υπόψη όλες τις σχετικές περιστάσεις, είναι αυτό που καθορίζει τον κίνδυνο και όχι η συγκεκριμένη τεχνολογία ή ο τύπος δεδομένων μεμονωμένα.

Η πρόσβαση σε μια συσκευή που συνδέεται με μια άλλη μπορεί να θέσει σε κίνδυνο τα προσωπικά δεδομένα που διαμοιράζονται. Με τη χρήση του 5G και λόγω των νέων χαρακτηριστικών, του μεγαλύτερου όγκου νέων συσκευών και της υψηλότερης συνδεσιμότητας μεταξύ των συσκευών αυτών και άρα, ως αποτέλεσμα, των μεγάλων δεδομένων, ο όγκος των δεδομένων και ο τρόπος επεξεργασίας θα αλλάξει.[129] Στο πλαίσιο αυτό, η άσκηση των δικαιωμάτων των υποκειμένων φαίνεται ιδιαίτερα περίπλοκη έως και ανέφικτη. Πιο συγκεκριμένα, τις περισσότερες φορές δεν είναι σαφές ποιος έχει το δικαίωμα διενέργειας οποιασδήποτε μορφής επεξεργασίας μέσα στο περιβάλλον του IoT και πιο συγκεκριμένα το δικαίωμα πρόσβασης και συλλογής δεδομένων από διάφορες συσκευές. Αντίστοιχα, ασαφής είναι και η δυνατότητα των υποκειμένων των δεδομένων να ασκήσουν τα δικαιώματα τους, όπως το δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης, λήθης, περιορισμού, ενημέρωσης για διαγραφή, φορητότητας των δεδομένων και το δικαίωμα αντίρρησης, λόγω του γεγονότος ότι συχνά τα υποκείμενα δεν γνωρίζουν τόσο

[127] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[128] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[129] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

το περιεχόμενο των δεδομένων και το είδος της επεξεργασίας, όσο και τον υπεύθυνο επεξεργασίας ή/και τον εκτελούντα την επεξεργασία. Σε ένα τόσο πολύπλοκο πλαίσιο, δίνεται βαρύτητα στην υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώνει τα υποκείμενα των δεδομένων, για τον ακριβή τρόπο χρήσης των δεδομένων τους. Εξίσου εύκολη και ξεκάθαρη για το υποκείμενο θα πρέπει να είναι και η δυνατότητα-δικαίωμα στην ανάκληση της συγκατάθεσης που έχει προηγουμένως δοθεί. Ωστόσο, αυτό κρίνεται δύσκολο και παράλληλα ουσιώδες για μια πλατφόρμα ανταλλαγής δεδομένων. Η συγκατάθεση των ανηλίκων, στο IoT είναι εξαιρετικά σημαντική τόσο για την προστασία της ιδιωτικής ζωής όσο και για την προστασία των παιδιών στον κυβερνοχώρο. Σε μία εποχή όπου διαφορετικά μέλη της οικογένειας κατέχουν και διαχειρίζονται, μέσω διαφορετικών λογαριασμών πληθώρα έξυπνων συσκευών, ζήτημα αποτελεί το πώς διασφαλίζεται στην πράξη η γονική συγκατάθεση (για ανηλίκους κάτω των 16 ετών ή λιγότερο, έως 13 ετών).[130]

4.1 Η Συγκατάθεση στα πλαίσια των Δικτύων τηλεπικοινωνιών 5ης γενιάς (5G) (αρ.6 παρ.1 στοιχ. α΄ ΓΚΠΔ).

Πέρα από την εγκυρότητα αυτής, τίθεται και το ερώτημα της έκτασης και του πεδίου εφαρμογής της συγκατάθεσης, επειδή η επεξεργασία προσωπικών δεδομένων μέσω παιχνιδιών με δυνατότητα IoT ή γενικά συσκευών που έχουν σχεδιαστεί με σκοπό την καταγραφή και την αποθήκευση αρχείων συνομιλιών ανηλίκων, εύκολα μπορεί να ξεπεράσει τα όρια. Τα ήδη αντιμετωπιζόμενα στα δίκτυα 4G ζητήματα γονικού ελέγχου, πρέπει να προηγούνται της γονικής συναίνεσης. Με ευθύνη του υπεύθυνου επεξεργασίας δεδομένων, η γονική συγκατάθεση πρέπει να δίνεται μετά την παροχή των απαραίτητων πληροφοριών για κάθε επεξεργασία δεδομένων, αλλά και την επαλήθευση της ηλικίας και της επιμέλειας των ανηλίκων. Η απαίτηση του GDPR για συγκατάθεση που παρέχεται με σαφήνεια και εν επιγνώσει, θα μπορούσε να αμφισβητηθεί μέσω των πολλαπλών δεδομένων και της επεξεργασίας αυτών που πραγματοποιείται μέσω το IoT. Καθώς ανάμεσα στον μαζικό αριθμό συσκευών είναι ευκολότερο, μέσω της λήψης δεδομένων από μεγαλύτερο αριθμό πηγών πληροφοριών, να διασταυρωθούν διάφορες πτυχές της προσωπικότητας, της συμπεριφοράς, των ενδιαφερόντων και των συνηθειών ενός ατόμου, οι οποίες μπορούν να αναλυθούν και να αξιολογηθούν, είναι καίριας σημασίας η

[130] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

εξασφάλιση της κατάλληλης πληροφόρησης των χρηστών του IoT, προκειμένου να κατανοήσουν τις συνέπειες της εν λόγω επεξεργασίας για αυτούς, ιδιαίτερα όσον αφορά την αυτοματοποιημένη επεξεργασία λήψης αποφάσεων.[131] Ιδιαίτερα στο πλαίσιο του IoT, είναι δυνατόν να αντιμετωπιστούν πολλαπλές παραβιάσεις δεδομένων από την ίδια αιτία, μέσω διαφορετικών συσκευών και με διαφορετικό περιεχόμενο, η διαδικασία καταγραφής κάθε παραβίασης δεδομένων ωστόσο καθίσταται περιπλοκότερη και καθυστερεί, καθώς διαφορετικοί τύποι προσωπικών δεδομένων, που παραβιάζονται με διαφορετικούς τρόπους, πρέπει να καταγράφονται ξεχωριστά, ακόμα και αν προέρχονται από την ίδια αιτία.[132]

4.2 Η Ακτίνα Σήματος στα δίκτυα 5G

Στα δίκτυα 5G αναμένεται να υπάρξει αύξηση του αριθμού των κεραιών που επιτρέπουν την αποστολή πολλαπλάσιων σημάτων. Αντί να εκπέμπει το ίδιο σήμα προς όλες τις κατευθύνσεις, το 5G θα χρησιμοποιεί διαφορετικούς συνδυασμούς κεραιών στις τοποθεσίες κυψελών για να στέλνει μια εστιασμένη ακτίνα προς την κατεύθυνση του δέκτη (συχνά αναφέρεται ως "διαμόρφωση ακτίνας").[133] MIMO (Multiple Input Multiple Output) σημαίνει ότι χρησιμοποιούνται περισσότερες από μία κεραίες για τη μετάδοση και τη λήψη ενός ραδιοσήματος, με αποτέλεσμα τη βελτίωση της ποιότητας του καναλιού επικοινωνίας.[134] Η ενίσχυση της ισχύος του σήματος αυξάνει την απόσταση που μπορεί να διανύσει το σήμα πριν εξασθενήσει, προκειμένου να φτάσει στη συσκευή. Κατά τη διαδικασία που αναφέρεται ως "αναπήδηση", το σήμα μπορεί να φτάσει στον χρήστη μέσω έμμεσης διαδρομής, αναπηδώντας σε επιφάνειες όπως τοίχοι ή δρόμοι. Συνήθως, μια επικοινωνία περιλαμβάνει πολλαπλά πακέτα πληροφοριών που μπορεί να αναπηδήσουν σε διαφορετικές επιφάνειες πριν φτάσουν στον χρήστη. Ορισμένες από αυτές τις τεχνολογίες έχουν ήδη εφαρμοστεί σε δίκτυα μη-5G και επομένως δεν είναι απολύτως καινούριες για τα δίκτυα 5G. Το σύστημα δεν έχει γνώση- και δεν χρειάζεται να έχει- της ακριβούς γεωγραφικής θέσης μιας συγκεκριμένης συσκευής. Απλώς διοχετεύει το σήμα με τρόπο που να αποδίδει ώστε η συσκευή να μπορεί να λαμβάνει το σήμα. Δεν

[131] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

[132] Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

[133] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[134] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

παράγονται ούτε αποθηκεύονται δεδομένα σχετικά με το ποιες κεραίες χρησιμοποιούνται, την κλίση τους ή την ισχύ που χρησιμοποιείται για ένα συγκεκριμένο σήμα. Καθώς τα πολλαπλά πακέτα που συνθέτουν μια επικοινωνία θα έχουν πιθανότατα "αναπηδήσει" σε διάφορες άγνωστες επιφάνειες, είναι σε κάθε περίπτωση πρακτικά αδύνατο να συναχθεί οποιοδήποτε συμπέρασμα από τέτοιες παραμέτρους, όσον αφορά την κατεύθυνση της συσκευής ή την απόσταση μεταξύ του σταθμού βάσης και της συσκευής.[135]

Οι οργανισμοί που διαμορφώνουν τα εικονικά τους δίκτυα ενδέχεται να απαιτούν λεπτομερέστερες πληροφορίες σχετικά με τα πρότυπα συμπεριφοράς των χρηστών που προέρχονται από τα δεδομένα του δικτύου με τον ίδιο τρόπο που το κάνει μια over-the-top υπηρεσία με τα δεδομένα που δεν προέρχονται από το δίκτυο.[136] Οι εν λόγω υπηρεσίες πρέπει να αντιμετωπίζονται ισότιμα βάσει της νομοθεσίας για την προστασία των δεδομένων και της ιδιωτικής ζωής και όχι να δημιουργείται ένα ξεχωριστό σύνολο κανόνων για διαφορετικούς τομείς. Ορισμένες εικονικές φέτες δικτύου μπορούν να διαμορφωθούν αποκλειστικά για τη διαχείριση διεργασιών που βασίζονται σε μηχανές χωρίς καμία επίπτωση στα άτομα (π.χ. μεταποίηση, παρακολούθηση της ρύπανσης κ.λπ.). Η διευκρίνιση ότι οι νόμοι για την προστασία των προσωπικών δεδομένων δεν θα εφαρμόζονται σε τέτοιες διαμορφώσεις θα μπορούσαν να επιτρέψουν την ανάλυση δεδομένων και την κοινή χρήση μη προσωπικών δεδομένων B2B.[137] Ο τεμαχισμός του δικτύου σημαίνει επίσης ότι ορισμένα δεδομένα μπορούν να απομονωθούν από το υπόλοιπο δίκτυο. Για παράδειγμα, ένα χρηματοπιστωτικό ίδρυμα μπορεί να αναπτύξει στοιχεία υλικού (μη εικονικά) του δικτύου που προορίζονται αποκλειστικά για τους πελάτες του, ώστε τα ευαίσθητα δεδομένα να αποθηκεύονται στις εγκαταστάσεις του χρηματοπιστωτικού ιδρύματος για μέγιστη προστασία της ιδιωτικής ζωής και ασφάλεια.

Ο πολλαπλασιασμός των συνδέσεων που επιτρέπει το 5G θα οδηγήσει σε έκρηξη του όγκου των δεδομένων που δημιουργούνται, συλλέγονται και αποθηκεύονται. Αυτό θα δημιουργήσει ατελείωτες δυνατότητες για καινοτόμες λύσεις που θα χρησιμοποιούν τα δεδομένα - καθώς και την ανάγκη για λύσεις που θα διασφαλίζουν τα δεδομένα των καταναλωτών, συμπεριλαμβανομένων των προτιμήσεών τους, του ιστορικού αγορών και των συνηθειών τους. Το 5G και το Διαδίκτυο των πραγμάτων θα εισάγουν μη δομημένα δεδομένα μηχανών, κάνοντας τα σημερινά δεδομένα να μοιάζουν μόνο με την κορυφή του

[135] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[136] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

[137] GSMA, 2020. 5G and Data Privacy: An overview for policymakers.

παγόβουνου. Πολλές εταιρείες, ωστόσο, πιθανότατα δεν θα έχουν τις γνώσεις, τις δεξιότητες και το κεφάλαιο για να αξιοποιήσουν αποτελεσματικά τα νέα δεδομένα που θα γίνουν διαθέσιμα. Με τις ικανότατες συνδεδεμένες συσκευές, το Edge computing[138] θα διαδραματίσει βασικό ρόλο για την ικανοποίηση των προσδοκιών των τελικών καταναλωτών για την άμεση παροχή πληροφοριών σε πραγματικό χρόνο. Θα επιτρέψει τη μετακίνηση των συστημάτων λήψης αποφάσεων πιο κοντά στον καταναλωτή, αλλά θα απαιτήσει επενδύσεις για την ανάλυση αιχμής[139]. Οι νέες αλληλεπιδράσεις δεδομένων που επιτρέπει το 5G, ορισμένες από τις οποίες μπορεί να συμβαίνουν χωρίς ανθρώπινη παρέμβαση (όπως η επικοινωνία μεταξύ μηχανών μέσω συσκευών που είναι πάντα ενεργοποιημένες και συνδεδεμένες), στην περίπτωση που οι πρακτικές προστασίας δεδομένων και διαφάνειας είναι αμφισβητήσιμες, ενδέχεται να υπονομεύσουν περαιτέρω την εμπιστοσύνη των καταναλωτών σε οργανισμούς, συσκευές και εμπειρίες.

4.3 Αυτοματοποίηση και Αυτοματοποιημένη λήψη αποφάσεων στα πλαίσια των Δικτύων τηλεπικοινωνιών 5ης γενιάς (5G)

Τα εικονικά περιβάλλοντα αποκτούν θεμελιώδη σημασία για τα κινητά δίκτυα 5G, στα οποία, για παράδειγμα, οι εικονικές λειτουργίες δικτύου θα ξεκινούν δυναμικά και αυτόματα, θα σταματούν, θα αυξάνονται ή θα μειώνονται[140]. Ως εκ τούτου, θα καθίσταται όλο και πιο ανέφικτο, αν όχι αδύνατο, να διασφαλισθεί χειροκίνητα το γεγονός ότι οι υποχρεώσεις προστασίας της ιδιωτικής ζωής και της ασφάλειας του ΓΚΠΔ επιβάλλονται ανά πάσα στιγμή.

Παρατηρούμε ότι η αυτοματοποίηση αποτελεί το κλειδί για τη συμμόρφωση με τον ΓΚΠΔ, κυρίως για τους φορείς εκμετάλλευσης 5G και τους παρόχους 5G και όχι τόσο για την τυποποίηση 5G[141]. Επισημαίνεται ότι οι φορείς εκμετάλλευσης και οι πάροχοι θα πρέπει να επιδιώξουν μια ενιαία προσέγγιση διαχείρισης της ασφάλειας και του απορρήτου, η οποία, με αυτοματοποιημένο τρόπο, θα διασφαλίζει την καλύτερη δυνατή προστασία του απορρήτου στα δίκτυα, θα παρακολουθεί τα κενά συμμόρφωσης με τον ΓΚΠΔ σε σχεδόν πραγματικό χρόνο, θα διασφαλίζει τη συλλογή των απαραίτητων

[138] Mastercard, 2021. What 5G means for data privacy and security?

[139] Mastercard, 2021. What 5G means for data privacy and security?

[140] Nakarmi,Prajwol,Kumar, Schaefer,Christian, Casella,Dario, 2017. 5G and the EU General Data Protection Regulation.

[141] Nakarmi,Prajwol,Kumar, Schaefer,Christian, Casella,Dario, 2017. 5G and the EU General Data Protection Regulation.

αποδεικτικών στοιχείων, σε περίπτωση παραβίασης του απορρήτου και θα πραγματοποιεί τις απαραίτητες γνωστοποιήσεις. Πρέπει επίσης να υπάρχουν αυτοματοποιημένα μέτρα για την κάλυψη των δικαιωμάτων των χρηστών, για παράδειγμα, της συγκατάθεσης, της φορητότητας των δεδομένων και της διαγραφής, μεταξύ άλλων δικαιωμάτων.

4.4 Προστασία από το σχεδιασμό στα πλαίσια των Δικτύων τηλεπικοινωνιών 5ης γενιάς (5G)

Οι απαιτήσεις του ΓΚΠΔ για την προστασία των δεδομένων προσωπικού χαρακτήρα ισχύουν άμεσα για τους φορείς εκμετάλλευσης, οι οποίοι εμπλέκονται στη διαχείριση δεδομένων προσωπικού χαρακτήρα, σε αντίθεση με τους παρόχους, οι οποίοι δεν εμπλέκονται. Παρόλα αυτά, οι πάροχοι έχουν την ευθύνη να παρέχουν κατάλληλη τεχνολογία, προϊόντα ή λύσεις που επιτρέπουν στους φορείς εκμετάλλευσης να συμμορφώνονται με τον ΓΚΠΔ.

Οι φορείς εκμετάλλευσης και οι πάροχοι πρέπει να διασφαλίζουν ότι κάθε μορφή ανάλυσης δεδομένων επί των προσωπικών δεδομένων έχει την κατάλληλη συγκατάθεση από τους χρήστες. Σε γενικές γραμμές, απαιτείται η λήψη μέτρων προστασίας των προσωπικών δεδομένων μέσω της ενίσχυσης των κόμβων, της κρυπτογράφησης και της προστασίας της ακεραιότητας των αποθηκευμένων προσωπικών δεδομένων, της ανωνυμοποίησης και της ψευδωνυμοποίησης των προσωπικών δεδομένων (κατά περίπτωση), του διαχωρισμού των δεδομένων ανάλογα με τον σκοπό, της εξουσιοδοτημένης πρόσβασης, της καταγραφής πρόσβασης και της διαγραφής των προσωπικών δεδομένων όταν δεν απαιτούνται πλέον, μεταξύ άλλων ενεργειών. Επιπλέον, θα πρέπει να συνεχιστεί η έρευνα σε θέματα όπως η καταγραφή της ιδιωτικότητας και η διαφάνεια, ως βασικός παράγοντας για την προστασία της ιδιωτικής ζωής μέσω σχεδιασμού.

III. Συμπεράσματα - Επίλογος

Σε όλο το μήκος της παρούσας εργασίας έγινε προσπάθεια να δοθεί απάντηση στο ερώτημα εάν ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679, οι αρχές και τα ρυθμιστικά εργαλεία που εισάγει, έχουν τη δυνατότητα να αντιμετωπίσουν αποτελεσματικά τις νομικές προκλήσεις της τεχνητής νοημοσύνης και να εγγυηθούν την

προστασία των δικαιωμάτων των προσώπων.[142] Η Τεχνητή Νοημοσύνη αποτελεί πρωταρχικό παράγοντα της λεγόμενης Τέταρτης Βιομηχανικής Επανάστασης, με τις αλλαγές που αυτή θα επιφέρει να προέρχονται κυρίως από την αξιοποίηση των δεδομένων των επιχειρήσεων και τη δημιουργία αξίας από αυτά. Πράγματι, τα δεδομένα φαίνεται να αποτελούν την κινητήριο δύναμη της νέας εποχής, με τις data-driven επιχειρήσεις οι οποίες χρησιμοποιούν εργαλεία ανάλυσης, να απολαμβάνουν έως και 35% μείωση χρόνου των εργασιών παραγωγής, έως και 25% μείωση αποθεμάτων και έως και 3% αύξηση εσόδων.

Τα προσωπικά δεδομένα και η Τεχνητή Νοημοσύνη αναπτύσσουν, με τον τρόπο αυτό, μία «σχέση» διπλής κατεύθυνσης, εφόσον η πρώτη επιτρέπει τη συλλογή και την αξιοποίηση μεγάλου όγκου δεδομένων αλλάζοντας συχνά τον σκοπό και τη χρήση τους. Επιπλέον, εξαιτίας των σημερινών δυνατοτήτων της τεχνητής νοημοσύνης οι οποίες περιλαμβάνουν μεταξύ άλλων όραση, ομιλία, γλώσσα και αναζήτηση, οι εφαρμογές τεχνητής νοημοσύνης χρησιμεύουν και ως προσωπικοί βοηθοί. Τα συστήματα αυτά έχουν σχεδιαστεί για να βλέπουν, να ακούν, να μιλούν, να κατανοούν και να ερμηνεύουν τις ανθρώπινες ανάγκες μέσω της χρήσης φυσικών μεθόδων επικοινωνίας. Μαθαίνοντας από και τροφοδοτώντας τα ενδιαφέροντα και τις ανάγκες των χρηστών, οι εφαρμογές AI τους ακολουθούν σε κάθε βήμα, εξάγοντας πληροφορίες και εξατομικεύοντας περιεχόμενο.

Παρόλο που τα μεγάλα δεδομένα, η τεχνητή νοημοσύνη και η μηχανική μάθηση διαδίδονται ευρέως στον δημόσιο και τον ιδιωτικό τομέα και μπορεί να θεωρούνται όλο και περισσότερο ως "συνήθης επιχειρηματική δραστηριότητα", τα βασικά χαρακτηριστικά της ανάλυσης μεγάλων δεδομένων εξακολουθούν να αντιπροσωπεύουν μια βαθμιαία αλλαγή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Έτσι, εισάγονται πλέον σημαντικές ανησυχίες και εγείρονται συζητήσεις γύρω από την ασφάλεια, την ηθική, τις ιδιωτικές και νομικές προκλήσεις που έχουν σημαντικό αντίκτυπο στην καθημερινή ζωή, καθώς οι εφαρμογές του IoT συνεχίζουν να αυξάνονται. Η τεχνολογία προφανώς εξελίσσεται πιο γρήγορα από ότι ο νόμος, η έκρηξη των εφαρμογών για κινητά ή η εισαγωγή γνωστικών υπηρεσιών και το Διαδίκτυο των Πραγμάτων είναι ίσως τα πιο εμφανή παραδείγματα.

Είναι γεγονός ότι η φύση των συστημάτων τεχνητής νοημοσύνης είναι δια μέτρου αντίθετη με ορισμένες από τις πιο βασικές αρχές του ΓΚΠΔ, καθιστώντας δύσκολη την

[142] Borras, Mitrou, 2018. Τεχνητή νοημοσύνη και προσωπικά δεδομένα Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679

προσπάθεια περιορισμού αυτών υπό το πλαίσιο του νέου κανονισμού προστασίας για τα προσωπικά δεδομένα. Τα συστήματα τεχνητής νοημοσύνης παραμένουν φύσει ασυμβίβαστα με την αρχή του περιορισμού του σκοπού, εξαιτίας της ικανότητάς τους να ανιχνεύουν μόνα τους μοτίβα και συσχετισμούς μεταξύ των δεδομένων, με σκοπό την ανάλυση αυτών. Είναι ακόμα ασυμβίβαστα με την αρχή της ελαχιστοποίησης δεδομένων, καθώς η λειτουργία τους υποστηρίζεται από τη χρήση όλων των διαθέσιμων δεδομένων, χωρίς τον περιορισμό στα απλώς απαραίτητα και σχετικά με τον σκοπό της επεξεργασίας. Η αρχή της ελαχιστοποίησης των δεδομένων έρχεται –σχεδόν από τον ορισμό της- σε αντίθεση με την ανάλυση Μεγάλων Δεδομένων και με τα συστήματα μηχανικής εκμάθησης τα οποία βασίζονται, αν δεν εξαρτώνται εξ' ολοκλήρου, στην υπερβολικά μεγάλη συλλογή δεδομένων και στην πιθανότητα αυτά να συνδυαστούν ή να χρησιμοποιηθούν εκ νέου. Παράλληλα, με τη χρήση των μεγάλων δεδομένων η ικανότητα αποθήκευσης δεδομένων αυξάνεται διαρκώς και το κόστος αποθήκευσης μειώνεται, ενώ η ικανότητα επεξεργασίας τεράστιων όγκων δεδομένων, μπορεί να ενθαρρύνει τους υπεύθυνους επεξεργασίας δεδομένων να διατηρούν ιστορικά δεδομένα για μεγάλο χρονικό διάστημα, πέραν της περιόδου που απαιτείται για τους συνήθεις επιχειρηματικούς σκοπούς. Οι αναλύσεις μεγάλων δεδομένων διαθέτουν στοιχεία που έρχονται επίσης και σε αντίθεση με τις αρχές του περιορισμού του σκοπού, την ελαχιστοποίηση των δεδομένων, την αυτοματοποιημένη λήψη αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ) και τις ειδικές κατηγορίες δεδομένων, όπως αυτές αναφέρονται στον ευρωπαϊκό κανονισμό. Αυτό συμβαίνει καθώς τα μεγάλα δεδομένα δίνουν τη δυνατότητα διατήρησης δεδομένων για μια απρόβλεπτη μελλοντική χρήση, με αποτέλεσμα την ευθεία αντίθεση με την αρχή της ελαχιστοποίησης των δεδομένων, η οποία απαιτεί τα δεδομένα να μη διατηρούνται περισσότερο από όσο είναι απαραίτητο για τον αρχικό σκοπό της συλλογής τους. Τα μεγάλα δεδομένα επιτρέπουν μεγάλη συλλογή και διατήρηση δεδομένων, ενώ η ελαχιστοποίηση των δεδομένων επιτρέπει τη συλλογή και διατήρηση δεδομένων σε μικρότερο βαθμό από τον αναγκαίο, γεγονός που καθιστά περαιτέρω ασύμβατες τις δύο έννοιες.

Ακόμα, η εξάρτηση των συστημάτων ΤΝ από τα Big Data έρχεται σε σύγκρουση με την αρχή της ακρίβειας και απαιτεί, την αντικατάσταση αυτών με δεδομένα καλύτερης ποιότητας προερχόμενα από διάφορες ομάδες ή τον δημόσιο τομέα. Ωστόσο και στις περιπτώσεις που χρησιμοποιούνται ακριβή δεδομένα, αυτά τείνουν να μένουν αποθηκευμένα για απεριόριστες περιόδους, αντίθετα με την αρχή του χρονικού

περιορισμού αποθήκευσης. Οι -κατά την αρχή της νομιμότητας- νομικές βάσεις επεξεργασίας περιορίζονται, εξαιτίας της αδυναμίας των τεχνολογιών αυτών να παράσχουν ενημέρωση για συγκατάθεση, σε συνδυασμό με την απαγόρευση της αποκλειστικά αυτοματοποιημένης λήψης αποφάσεων και την επεξεργασία δεδομένων ειδικής κατηγορίας. Η αρχή της διαφάνειας, κρίνεται μεν χρήσιμη για την αξιολόγηση της διαδικασίας που ακολουθείται από την τεχνητή νοημοσύνη, αλλά είναι δύσκολο να ευθυγραμμιστεί με τους κινδύνους χειραγώγησης, τις απειλές ασφάλειας και τις γνωστοποιήσεις πνευματικής ιδιοκτησίας.[143] Στα μεγάλα δεδομένα συναντάται επιπλέον και το λεγόμενο "παράδοξο της διαφάνειας ", καθώς τα μεγάλα δεδομένα υπόσχονται διορατικότητα σε ένα θέμα και ταυτόχρονα οι μηχανισμοί ανάλυσης μεγάλων δεδομένων είναι κρυπτικοί.

Στο IoT, τόσο η διαφανής επεξεργασία όσο και το δικαίωμα στη λήθη γίνονται πιο σύνθετα, ξεκινώντας από το γεγονός ότι τα δεδομένα ενδεχομένως θα μεταπηδούν από συσκευή σε συσκευή πολύ περισσότερες φορές από το συνηθισμένο πριν φτάσουν στον τελικό προορισμό, όπου και θα αποθηκευτούν μόνιμα. Ως εκ τούτου, για τις εταιρείες θα είναι πιο δύσκολο να παρακολουθούν πού βρίσκεται κάθε κομμάτι δεδομένων, όχι μόνο για λόγους απεικόνισης και διαφάνειας αλλά και για τους σκοπούς της διαγραφής. Πιο συγκεκριμένα, τις περισσότερες φορές δεν είναι σαφές ποιος έχει το δικαίωμα διενέργειας οποιασδήποτε μορφής επεξεργασίας μέσα στο περιβάλλον του IoT και πιο συγκεκριμένα, το δικαίωμα πρόσβασης και συλλογής δεδομένων από διάφορες συσκευές. Αντίστοιχα, ασαφής είναι και η δυνατότητα των υποκειμένων των δεδομένων να ασκήσουν τα δικαιώματα τους, όπως το δικαίωμα ενημέρωσης, πρόσβασης, διόρθωσης, λήθης, περιορισμού, ενημέρωσης για διαγραφή, φορητότητας των δεδομένων και το δικαίωμα αντίρρησης, λόγω του γεγονότος ότι συχνά τα υποκείμενα δεν γνωρίζουν τόσο το περιεχόμενο των δεδομένων και το είδος της επεξεργασίας, όσο και τον υπεύθυνο επεξεργασίας ή/και τον εκτελούντα την επεξεργασία.

Απαιτείται κάποιο επίπεδο διαφάνειας ώστε το υποκείμενο των δεδομένων να είναι σε θέση να πληροφορείται για θέματα που αφορούν την επεξεργασία των προσωπικών του δεδομένων, άλλωστε αυτό αποτελεί μέρος του δικαιώματος του υποκειμένου των δεδομένων, παρά την ύπαρξη λόγων που δικαιολογούν την ύπαρξη κρυπτογραφημένων μηχανισμών, όπως είναι περιπτώσεις προστασίας εμπορικού απορρήτου ή εθνικής

[143] Siapka, Anastasia, 2018. The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI, Διπλωματική Εργασία, Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών.

ασφάλειας. Πρέπει να δοθεί ιδιαίτερη έμφαση όχι μόνο στην τεχνολογία που χρησιμοποιείται για την επεξεργασία δεδομένων, αλλά ιδιαίτερα στους κινδύνους και τις επιπτώσεις που αυτοί έχουν για τα θεμελιώδη δικαιώματα, επιπτώσεις που πρέπει να ρυθμιστούν. Στην προσπάθεια αυτή, η έννοια της τεχνολογικής ουδετερότητας[144] εμφανίστηκε ως ρυθμιστική αρχή, ως κανόνας, με βάση τον οποίο τα κράτη προχωρούν στη διάδοση της τεχνολογικής αμεροληψίας. Η τεχνολογική ουδετερότητα του νόμου απαιτεί ο τελευταίος να παράγει τα ίδια αποτελέσματα ανεξάρτητα από το τεχνολογικό περιβάλλον στο οποίο εφαρμόζονται αυτοί οι κανόνες, μια πολιτική που προϋποθέτει, ωστόσο, ότι οι νομοθέτες λαμβάνουν υπόψη τόσο τα ζητήματα που τίθενται από τις τρέχουσες τεχνολογίες όσο και τις μελλοντικές τάσεις.[145]

Ο GDPR δεν έχει υιοθετήσει μια «ρήτρα λήξης ισχύος»[146] , η οποία θα προέβλεπε εξ ορισμού ότι ο νόμος θα λήξει μετά από μια ορισμένη περίοδο, εκτός και αν παραταθεί. Η υιοθέτηση τεχνολογικά ουδέτερων διατάξεων φαίνεται να είναι ο δρόμος για την αντιμετώπιση του απρόβλεπτου των τεχνολογικών εξελίξεων και, κατά συνέπεια, για τη διασφάλιση μιας βιώσιμης νομοθεσίας, ικανής να ανταποκρίνεται επιτυχώς σε απρόβλεπτες εξελίξεις για μια αρκετά μεγάλη περίοδο. Η συμμόρφωση με τον ΓΚΠΔ δεν είναι απλή και συχνά αυτό οφείλεται στο γεγονός ότι το κείμενό του Κανονισμού δεν έχει γραφτεί από μηχανικούς λογισμικού ή πληροφορικής, αλλά από νομικούς και υπεύθυνους χάραξης πολιτικής. Με τη γνώση ότι η τεχνολογία αναπτύσσεται ταχύτερα από το νομικό πλαίσιο που την περιβάλλει, η όποια προσπάθεια δημιουργίας νομοθετικού πλαισίου, οφείλει να βασίζεται στη συνεργασία νομικών και μηχανικών πληροφορικής. Μέσω της συνεργασίας το κείμενο θα αποκτήσει μακροβιότητα, έχοντας την ικανότητα προλάβει μελλοντικές ανησυχίες, δημιουργώντας με τον τρόπο αυτό ένα ευρύτερο και αποτελεσματικότερο φάσμα προστασίας. Σκοπός του Κανονισμού, αλλά και κάθε μελλοντικού πλαισίου, είναι να θεωρείται βοήθημα σχεδιασμού για τους μηχανικούς

[144] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[145] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[146] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

πληροφοριών που στοχεύουν στη συμμόρφωση με τον ΓΚΠΔ, αλλά και βοήθημα για την κατανόηση του κανονισμού από τους χρήστες λογισμικού. Κυρίως, οι κανόνες και οι αρχές του GDPR, όπως η έννοια της ταυτοποίησης του υποκειμένου των δεδομένων, είναι αρκετά ευέλικτοι ώστε να καλύπτουν μελλοντικές τεχνολογικές αλλαγές και να παρέχουν διαρκή προστασία. Ωστόσο, δεν πρέπει να αγνοούμε τον κίνδυνο η ασάφεια που χαρακτηρίζει ορισμένους όρους και έννοιες να οδηγήσει με την πάροδο των ετών σε μεγάλες αποκλίσεις στην ερμηνεία του νόμου και κατά συνέπεια σε νομική αβεβαιότητα.

Η ατελείωτη επιθυμία για συνέχιση της καινοτομίας έχει επιφέρει, αφενός, το λαμπρό μέλλον και τις προσδοκίες των μεγάλων δεδομένων και, αφετέρου, την ανάγκη η καινοτομία αυτή να βρίσκεται εντός των ορίων του νόμου. Αυτές οι τριβές είναι θεμελιώδεις για το όραμα της τεχνολογικής καινοτομίας της ΕΕ και μάλιστα σε ολόκληρο τον κόσμο. Αν και υπάρχουν εγγενείς τεχνολογικές λύσεις που μπορούν να ενσωματωθούν στη δυναμική των μεγάλων δεδομένων, όπως η προστασία της ιδιωτικής ζωής μέσω σχεδιασμού, εξακολουθούν να υπάρχουν αμφιβολίες για το πώς μπορεί να αμβλυνθεί πλήρως αυτή η αντίφαση. Εμφανίζεται πλέον η ανάγκη ύπαρξης παγκόσμιου νομοθετικού πλαισίου για τη ρύθμιση του IoT καθώς, ο κοινός χρήστης πρέπει να έχει τη δυνατότητα να ενημερωθεί για τις απειλές ασφάλειας, ηθικής και προστασίας της ιδιωτικής ζωής που επιβάλλονται από τις σύγχρονες συσκευές IoT. Όμως, όσο κι αν οι εφαρμογές του IoT αυξάνονται συνεχώς με την πάροδο των ετών προκειμένου να κάνουν τη ζωή μας πιο άνετη και ομαλή, η ασφάλεια του χρήστη, των προσωπικών δεδομένων του και της ιδιωτικότητας του, εξακολουθούν να αποτελούν ένα από τα μεγαλύτερα ζητήματα για το IoT μέχρι σήμερα.

Παράλληλα, η ανάλυση μεγάλων δεδομένων με τη χρήση τεχνικών που έχουν καταστεί δυνατές μέσω της ΤΝ δημιουργεί επιπτώσεις στην προστασία των δεδομένων και καθιστά δυσκολότερη την εφαρμογή των αρχών προστασίας, λόγω της χρήσης τους σε ένα πλαίσιο μεγάλων δεδομένων. Οι επιπτώσεις αυτές προκύπτουν όχι μόνο από τον όγκο των δεδομένων, αλλά και από τους τρόπους με τους οποίους αυτά παράγονται, την τάση εύρεσης νέων χρήσεων για αυτά, την πολυπλοκότητα της επεξεργασίας και την πιθανότητα απροσδόκητων συνεπειών για τα άτομα.[147] Η σημαντική αύξηση στην ανάπτυξη των δυνατοτήτων επεξεργασίας (αποθήκευση, εξόρυξη, ανίχνευση, αντιστοίχιση προφίλ) μπορεί να μεταμορφώσει πλήρως το πλαίσιο και τις συνθήκες υπό

[147] Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.

τις οποίες γίνεται η επεξεργασία των προσωπικών δεδομένων, αυξάνοντας έτσι την πληροφοριακή τους αξία με απρόβλεπτο τρόπο και αυξάνοντας τις πιθανές αρνητικές επιπτώσεις για τα άτομα.

Όπως τονίζεται από την Ευρωπαϊκή Ομάδα για την Ηθική στην Επιστήμη και τις Νέες Τεχνολογίες, «οι εφαρμογές της τεχνητής νοημοσύνης και της ρομποτικής δεν πρέπει να θέτουν απαράδεκτους κινδύνους βλάβης για τον άνθρωπο και να μην θέτουν σε κίνδυνο την ανθρώπινη ελευθερία και αυτονομία».[148] Αντίθετα, θα πρέπει να στοχεύουν στην προστασία των θεμελιωδών δικαιωμάτων και αξιών και να αναπτύσσονται με στόχο την «υπηρεσία της ανθρωπότητας» και με τρόπο που να διευκολύνει την ανθρώπινη ανάπτυξη και να μην την εμποδίζει ή να την θέτει σε κίνδυνο. Οι τεχνολογίες τεχνητής νοημοσύνης θα πρέπει να σχεδιάζονται, να αναπτύσσονται και να χρησιμοποιούνται με σεβασμό στα θεμελιώδη ανθρώπινα δικαιώματα και σύμφωνα με την αρχή της δικαιοσύνης. Η μη δέσμευση των τεχνολογιών τεχνητής νοημοσύνης με βασικές συνταγματικές αρχές θα έθετε σε κίνδυνο τη δημοκρατία. Για να μπορούμε να προστατεύσουμε τα θεμελιώδη δικαιώματα, η έρευνα, ο σχεδιασμός και η ανάπτυξη της τεχνητής νοημοσύνης, της ρομποτικής και των «αυτόνομων» συστημάτων θα πρέπει να καθοδηγούνται από ένα αυθεντικό ενδιαφέρον για την ηθική της έρευνας, την κοινωνική ευθύνη των προγραμματιστών και την παγκόσμια ακαδημαϊκή συνεργασία. Σε αυτή την προοπτική, η μηχανική με επίγνωση της ιδιωτικής ζωής ή αλλιώς η προστασία δεδομένων από το σχεδιασμό απηχεί τη συζήτηση σχετικά με την Υπεύθυνη Έρευνα και Καινοτομία (RRI) . Ένας από τους πρώτους ορισμούς RRI[149] προσφέρεται από τον von Schomberg, ο οποίος προτείνει ότι μπορεί να γίνει κατανοητό ως «μια διαφανής, διαδραστική διαδικασία μέσω της οποίας κοινωνικοί φορείς και καινοτόμοι ανταποκρίνονται αμοιβαία ο ένας στον άλλο με γνώμονα την (ηθική) αποδοχή, βιωσιμότητα και την κοινωνική επιθυμία της διαδικασίας καινοτομίας και των εμπορεύσιμων προϊόντων της (προκειμένου να επιτραπεί

[148] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[149] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

η σωστή ενσωμάτωση των επιστημονικών και τεχνολογικών προόδων στην κοινωνία μας)».[150]

Στο σημείο αυτό, οι ελεγκτικοί μηχανισμοί καθώς και οι μηχανισμοί πιστοποίησης φαίνεται να αποτελούν τη λύση και πάλι όμως εξαρτώνται από το βαθμό στον οποίο οι προγραμματιστές σχεδιάζουν τα συστήματά τους και στην προθυμία τους να αλλάξουν ολόκληρη την κουλτούρα της βιομηχανίας τους. Ομοίως, οι ενισχυμένες εξουσίες των εθνικών αρχών προστασίας δεδομένων αναμένεται να έχουν αποτρεπτικά αποτελέσματα στην αμελή επεξεργασία δεδομένων. Οι φορείς εκμετάλλευσης και οι πάροχοι πρέπει να διασφαλίζουν ότι, κάθε μορφή ανάλυσης δεδομένων επί των προσωπικών δεδομένων έχει την κατάλληλη συγκατάθεση από τους χρήστες. Σε γενικές γραμμές, απαιτείται η λήψη μέτρων προστασίας των προσωπικών δεδομένων μέσω της ενίσχυσης των κόμβων, της κρυπτογράφησης και της προστασίας της ακεραιότητας των αποθηκευμένων προσωπικών δεδομένων, της ανωνυμοποίησης και της ψευδωνυμοποίησης των προσωπικών δεδομένων (κατά περίπτωση), του διαχωρισμού των δεδομένων ανάλογα με τον σκοπό, της εξουσιοδοτημένης πρόσβασης, της καταγραφής πρόσβασης και της διαγραφής των προσωπικών δεδομένων όταν δεν απαιτούνται πλέον, μεταξύ άλλων ενεργειών. Επιπλέον, θα πρέπει να συνεχιστεί η έρευνα σε θέματα όπως η καταγραφή της ιδιωτικότητας και η διαφάνεια, ως βασικός παράγοντας για την προστασία της ιδιωτικής ζωής μέσω σχεδιασμού.

Σε ένα πλαίσιο έντονου παγκόσμιου ανταγωνισμού, απαιτείται μια σταθερή ευρωπαϊκή προσέγγιση, όπως επεδίωξε και το πλαίσιο της ευρωπαϊκής στρατηγικής για την τεχνητή νοημοσύνη που παρουσιάστηκε τον Απρίλιο του 2018. Η ευρωπαϊκή προσέγγιση για την τεχνητή νοημοσύνη στοχεύει στην προώθηση της ικανότητας καινοτομίας της Ευρώπης στον τομέα της AI, παράλληλα με την υποστήριξη της ανάπτυξης και της υιοθέτησης, ηθικής και αξιόπιστης τεχνητής νοημοσύνης σε ολόκληρη την οικονομία της ΕΕ. Αυτά τα σκέλη της Στρατηγικής για τα συστήματα Τεχνητής Νοημοσύνης συμβαδίζουν με το όραμα για ένα ευρωπαϊκό οικοσύστημα αριστείας και εμπιστοσύνης, που παρουσιάστηκε εντός του 2020 στη Λευκή Βίβλο (White Book)[151] , με τις λύσεις που προτάθηκαν στα πλαίσιά της να αποτελούν λύση για τον περιορισμό των

[150] Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) "ARTIFICIAL INTELLIGENCE-PROOF" ?

[151] European Commission, 2020. White paper in Artificial Intelligence - A European approach to excellence and trust.

επιπτώσεων όλων των προαναφερθέντων τεχνολογιών στα προσωπικά δεδομένα. Πιο συγκεκριμένα, σύμφωνα με τη Λευκή Βίβλο κρίνονται αναγκαία α) μέτρα που θα εξορθολογήσουν την έρευνα, θα ενθαρρύνουν τη συνεργασία μεταξύ των κρατών μελών και θα αυξήσουν τις επενδύσεις για την ανάπτυξη της τεχνητής νοημοσύνης και β) ορθές επιλογές πολιτικής για ένα μελλοντικό ρυθμιστικό πλαίσιο της ΕΕ που θα καθορίζει τους τύπους νομικών απαιτήσεων που θα ισχύουν για τους σχετικούς φορείς, με ιδιαίτερη έμφαση στις εφαρμογές υψηλού κινδύνου.

Καταληκτικά, η επιθυμία για πλήρη έλεγχο των αναδυόμενων τεχνολογιών οφείλει να θεωρηθεί ως μη ρεαλιστική, καθώς θα μπορούσε να παραλύσει ακόμη και τις καθημερινές ενέργειες. Η ύπαρξη υπεύθυνων επεξεργασίας δεδομένων υποστηρίζεται ως ένας πλέον αποτελεσματικότερος μηχανισμός, ιδίως όταν η ουσιαστική συγκατάθεση, η διαφάνεια ή η επεξήγηση δεν αποτελούν επιλογές. Κρίνεται επομένως, επιτακτική η ανάγκη εύρεσης μεθόδων ελαχιστοποίησης των κινδύνων προκειμένου και να επιτραπεί η επεξεργασία δεδομένων από ιδιωτικούς και δημόσιους φορείς ώστε να μπορέσουμε να αποκομίσουμε τα μέγιστα οφέλη των νέων αναδυόμενων τεχνολογιών και των αλλαγών που αυτές επιφέρουν σε πλήθος τομέων της καθημερινότητας.

Παράρτημα Α - Περί Βιβλιογραφίας

Α.1 Βιβλιογραφία

1. Bastos, Daniel, 2018. GDPR Privacy Implications for the Internet of Things.
2. Borras, Mitrou, 2018. Τεχνητή νοημοσύνη και προσωπικά δεδομένα Μια θεώρηση υπό το πρίσμα του Ευρωπαϊκού Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679
3. Bourdillon, Sophie, Stalla, Pearce, Henry, Tsakalakis, Niko., 2018. The GDPR: A game changer for electronic identification schemes? The case study of Gov.UK Verify. In: Computer Law & Security Review, Volume 34, Issue 4, pp 784-805.
4. Butterworth, M., 2018. The ICO and artificial intelligence: The role of fairness in the GDPR framework. In: Computer Law & Security Review, Volume 34, Issue 2, pp 257-268.
5. Costantinia, Federico et al. 2020. Chapter Eight - Autonomous vehicles in a GDPR era: An international comparison. In: Advances in Transport Policy and Planning, Volume 5, Pages 191-213
6. Curry, Sam, 2021. Achieving GDPR compliance post-Privacy Shield. In: Computer Fraud & Security, Volume 2021, Issue 2, pp 6-8.
7. European Commission, 2020. White paper in Artificial Intelligence - A European approach to excellence and trust.
8. Information Commissioner's Office. 2017. Big data, artificial intelligence, machine learning and data protection Version: 2.2.
9. Karageorgiou, Kaneen, Christos, Petrakis, Euripides, G.M., 2020. Towards evaluating GDPR compliance in IoT applications. In: Procedia Computer Science, Volume 176, pp. 2989-2998.
10. Karale, Ashwin, 2021. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. In: Internet of Things, Volume 15.
11. Khan, Haibat, Martin, Keith, M., 2020. A survey of subscription privacy on the 5G radio interface - The past, present and future. In: Journal of Information Security and Applications, Volume 53.
12. Kounoudes, Alexia, Dini, Kapitsaki, Georgia M., 2020. A mapping of IoT user-centric privacy preserving approaches to the GDPR. In: Internet of Things, Volume 11.

13. Kritikos,Mihalis, 2020. GDPR And AI: Making Sense Of A Complex Relationship.
14. Laurent, Maryline, et al. 2019. Authenticated and Privacy-Preserving Consent Management in the Internet of Things. In: Procedia Computer Science, Volume 151, pp 256-263.
15. Le,L.B.,Wang,X.,Bogale,T.E, 2017. Chapter 9 - mmWave communication enabling techniques for 5G wireless systems: A link level perspective. In: mmWave Massive MIMO, A Paradigm for 5G, pp195-225.
16. Loideain, Nóra Ni, Adams, Rachel, 2020. From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments. In: Computer Law & Security Review, Volume 36.
17. Meszaros, Janos, Ho, Chih-hsing, 2021. AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? In: Computer Law & Security Review, Volume 41.
18. Milossi, Maria, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2021. AI Ethics: Algorithmic Determinism or Self-Determination? The GPDR Approach.
19. Oluwayomi, A. Ajibade, 2018. A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape.
20. Plageras Andreas P and Psannis Konstantinos E., 2017. “Algorithms for Big Data Delivery over the Internet of Things”. In: 19th IEEE Conference on Business Informatics, Thessaloniki, Greece 24-26 July.
21. Prof. Doc. Mitrou, Lilian, 2019. DATA PROTECTION, ARTIFICIAL INTELLIGENCE AND COGNITIVE SERVICES: IS THE GENERAL DATA PROTECTION REGULATION (GDPR) “ARTIFICIAL INTELLIGENCE-PROOF” ?
22. Rekha, Shashi, 2021. Study of security issues and solutions in Internet of Things (IoT). In: Materials Today: Proceedings.
23. Rhahla, Mouna, Allegue, Sahar, Abdellatif, Takoua, 2021. Guidelines for GDPR compliance in Big Data systems. In: Journal of Information Security and Applications, Volume 61.
24. Rizou, Stavroula, Alexandropoulou-Egyptiadou, Eugenia, Psannis, Kostas E., 2020. GDPR interference with next generation 5G and IoT networks.

25. Seo, Junwoo, et. al. 2018. An Analysis of Economic Impact on IoT Industry under GDPR. In: Advances in Mobile Networking for IoT Leading the 4th Industrial Revolution.
26. Siapka, Anastasia, 2018. The Ethical and Legal Challenges of Artificial Intelligence: The EU response to biased and discriminatory AI, Διπλωματική Εργασία, Πάντειον Πανεπιστήμιο Κοινωνικών και Πολιτικών Επιστημών.
27. Stergiou C.L., Plageras A.P., Psannis K.E., Gupta B.B., 2019. "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network". In: Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications.
28. Stergiou C.L., Psannis K.E., Gupta B.B., 2021. "IoT-based Big Data secure management in the Fog over a 6G Wireless Network". In: IEEE Internet of Things Journal, vol. 8, issue: 7, pp 5164 – 5171.
29. Stergiou C.L., Psannis K.E., Gupta B.B., Ishibashi Y., "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", 2018. In: Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184.
30. Stergiou C.L., Psannis K.E., Kim B.-G., Gupta B.B., 2018. "Secure integration of IoT and Cloud Computing". In: Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975.
31. Stergiou C.L., Psannis K.E., Plageras A.P, Ishibashi Y., Kim B.-G., 2018. "Algorithms for efficient digital media transmission over IoT and cloud networking". In: KoreaScience, Journal of Multimedia Information System, vol. 5, issue: 1, pp. 27-34.
32. Tamburri, Damian A., 2020. Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation. In: Information Systems Volume 91.
33. Tsolka, Evaggelia, 2019. Οι νέες τεχνολογίες υπό το πρίσμα του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ). Η διαδικασία του credit scoring και profiling στην περίπτωση Ελληνικού Τραπεζικού Ιδρύματος, Διπλωματική Εργασία, Χαροκόπειο Πανεπιστήμιο.
34. Van de Waerdt,Peter J., 2020. Information asymmetries: recognizing the limits of the GDPR on the data-driven market. In: Computer Law & Security Review, Volume 38.

35. Wachter, Sandra, 2018. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, In: Computer Law & Security Review, Volume 34, Issue 3, pp 436-449.

A.2 Ηλεκτρονικές Πηγές

1. Cambridge Dictionary, URL: https://dictionary.cambridge.org/
2. Center for International Governance Innovation. 2019. The Peril and Potential of the GDPR, URL: https://www.cigionline.org/articles/peril-and-potential-gdpr/
3. Dr. Borelli, Davide, Xie, Ningxin and Neo, Eing Kai Timothy, 2018. The Internet of Things: Is it just about GDPR?, URL:https://www.pwc.co.uk/services/risk/technology-data-analytics/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html
4. European Commission, What is personal data?, URL:https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
5. GSMA, 2020. 5G and Data Privacy: An overview for policymakers, URL: https://www.gsma.com/publicpolicy/wp-content/uploads/2020/07/GSMA_5G_and_Data_Privacy_July_20.pdf
6. Lanner, 2017. Internet of Things Privacy: What GDPR Means For IoT Data, URL: https://www.lanner-america.com/latest-news/the-latest-updates-on-covid-19/
7. Mastercard, 2021. What 5G means for data privacy and security?, URL: https://www.mastercard.com/news/perspectives/2021/what-5g-means-for-data-privacy-and-security/
8. Nakarmi,Prajwol,Kumar, Schaefer,Christian, Casella,Dario, 2017. 5G and the EU General Data Protection Regulation, URL: https://www.ericsson.com/en/blog/2017/12/5g-and-the-eu-general-data-protection-regulation
9. Tech Target, What is 5G?, URL: https://www.techtarget.com/searchnetworking/definition/5G
10. Thales, 2021. 3 REASONS TO BE OPTIMISTIC ABOUT DATA PRIVACY IN THE 5G ERA, URL:https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/mobile/magazine/3-reasons-be-optimistic-about-data-privacy