ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Ο ΑΝΤΙΚΤΥΠΟΣ ΤΟΥ GDPR ΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Ανυφαντή Ζωή

Α.Μ:00523

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Επιβλέπων καθηγητής
Γεώργιος Σταμούλης

Λαμία, 2019

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

The impact of GDPR Regulation to Artificial Intelligence

Anifanti Zoi

A.M:00523

Master thesis

Georgios Stamoulis

Lamia
2019

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»
ΡΟΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ο ΑΝΤΙΚΤΥΠΟΣ ΤΟΥ GDPR ΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Ανυφαντή Ζωή

Α.Μ:00523

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων καθηγητής
Γεώργιος Σταμούλης
Λαμία, 2019

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «Ο αντίκτυπος του GDPR στην Τεχνητή Νοημοσύνη» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Η ΔΗΛΟΥΣΑ

27/06/2019

Υπογραφή

Ο ΑΝΤΙΚΤΥΠΟΣ ΤΟΥ GDPR ΣΤΗ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

Ανυφαντή Ζωή

Α.Μ: 00523

Τριμελής Επιτροπή:

Σταμούλης Γεώργιος,

Βαβουγιός Διονύσιος,

Κοζύρη Μαρία

Επιστημονικός Σύμβουλος:

Κίκιρας Παναγιώτης

ΕΥΧΑΡΙΣΤΙΕΣ

Η διπλωματική αυτή εργασία αποτελεί έργο προσωπικής μου προσπάθειας. Για να ολοκληρωθεί και να φτάσει στο επιθυμητό αυτό σημείο απαιτήθηκαν ώρες μελέτης, συγκέντρωσης και συλλογής πληροφοριών. Ευχαριστώ όλους όσους με βοήθησαν καθ' όλη την περίοδο εκπόνησης και συγγραφής δίνοντάς μου κουράγιο και στήριξη. Επίσης, ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, κύριο Γεώργιο Σταμούλη και τον επιστημονικό σύμβουλο κύριο Παναγιώτη Κίκιρα, για τις πολύτιμες συμβουλές, τις συστάσεις και τις κατευθυντήριες γραμμές που μου έδινε. Τέλος, ευχαριστώ την τριμελή εξεταστική επιτροπή που μου κάνει την τιμή να αξιολογήσει την εργασία μου.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία ασχολείται με τον αντίκτυπο του GDPR στην Τεχνητή Νοημοσύνη. Πιο συγκεκριμένα, στην εργασία πραγματοποιείται αρχικά μια εισαγωγή στην προστασία δεδομένων και στο GDPR, όπου περιγράφονται οι αρχές προστασίας δεδομένων, το πεδίο εφαρμογής του GDPR και η Νομοθεσία – Διατάξεις που το διέπουν. Επίσης γίνεται αναφορά στην προστασία της ιδιωτικής ζωής από τεχνική άποψη. Στη συνέχεια, πραγματοποιείται αναφορά στην Τεχνητή Νοημοσύνη, τη λειτουργία της, τις εφαρμογές της και τις Δημόσιες και Ιδιωτικές χρήσεις της. Ακολούθως η εργασία πραγματεύεται το βασικό ζήτημα διερεύνησης που είναι ο αντίκτυπος του GDPR στην Τεχνητή Νοημοσύνη. Πιο αναλυτικά, γίνεται αναφορά στα προβλήματα του GDPR στην Τεχνητή Νοημοσύνη και αναφέρεται η πολυπλοκότητα του GDPR που αναμένεται να αυξήσει το κόστος χρήσης της Τεχνητής Νοημοσύνης. Ακόμα, αποτυπώνονται οι απόψεις ότι το GDPR θα αυξήσει το κόστος εργασίας, ότι είναι νομικά επικίνδυνο για τις εταιρείες που χρησιμοποιούν Τεχνητή Νοημοσύνη και ότι το GDPR θα επιδεινώσει την ευρωπαϊκή ανταγωνιστικότητα περιορίζοντας τη χρήση Τεχνητής Νοημοσύνης στην Ευρωπαϊκή Ένωση. Τελειώνοντας, στην εργασία παρουσιάζονται συστάσεις – μελλοντικές προοπτικές, μεταξύ των οποίων είναι η απλούστευση του GDPR, η θέσπιση του δικαιώματος της κατάργησης, η τροποποίηση δικαιωμάτων φορητότητας δεδομένων, η παρουσίαση σαφέστερων κατευθυντήριων γραμμών για την αποσύνδεση δεδομένων, η επιβολή προστίμων για την παραβίαση του GDPR ανάλογα με τη ζημιά και την υπαιτιότητα και η εξουσιοδότηση χρήσης της Τεχνητής Νοημοσύνης για το δημόσιο συμφέρον.

ABSTRACT

This paper deals with the impact of GDPR on Artificial Intelligence. More specifically, it offers an introduction to data protection and the GDPR, which describes the data protection principles, the scope of the GDPR and the Legislation - Provisions that govern it. Reference is also made to the protection of privacy from a technical point of view. Subsequently, reference is made to Artificial Intelligence, its operation, its applications and its Public and Private uses. The paper then deals with the basic question of the GDPR impact on Artificial Intelligence. More specifically, reference is made to GDPR's problems in Artificial Intelligence, and the complexity of GDPR is expected to increase the cost of using Artificial Intelligence. Still, there are views that the GDPR will increase labor costs, that it is legally hazardous to companies using Artificial Intelligence and that GDPR will worsen European competitiveness by limiting the use of Artificial Intelligence in the European Union. Finally, recommendations are made, including the simplification of the GDPR, the introduction of the right of withdrawal, the modification of data portability rights, the introduction of clearer guidelines for data unbundling, the imposition of fines for breaching the GDPR depending on the damage and fault and the authorization to use Artificial Intelligence for the public interest.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

Στην αναδυόμενη οικονομία δεδομένων, η καινοτομία σε πολλές βιομηχανίες θα εξαρτηθεί σε μεγάλο βαθμό από το τι κάνουν οι εταιρείες με τη διαχείριση των δεδομένων (Castro & Korte, 2013). Αυτή η τάση έχει καταστήσει την Τεχνητή Νοημοσύνη (Artificial Intelligence - AI) - ένα σύνολο τεχνολογιών που επιτρέπει στους υπολογιστές να εκτελούν καθήκοντα όπως ο άνθρωπος - ένα από τα πιο πολύτιμα εργαλεία που διαθέτουν οι επιχειρήσεις. Η Τεχνητή Νοημοσύνη επιτρέπει στους οργανισμούς να χρησιμοποιούν δεδομένα για να δημιουργήσουν νέες υπηρεσίες, να βελτιώσουν υπάρχουσες υπηρεσίες και να κάνουν πιο αποτελεσματικές πολλές υπάρχουσες διαδικασίες. Η Τεχνητή Νοημοσύνη μπορεί να αναλύσει τα μεγάλα σύνολα δεδομένων πολύ ταχύτερα από ό, τι ο άνθρωπος, επιτρέποντάς της να κάνει γρήγορες και ακριβείς παρατηρήσεις σχετικά με τις τάσεις των δεδομένων και να αντλήσει συμπεράσματα από αυτές τις παρατηρήσεις, να κάνει προβλέψεις, να συμβάλλει στην αυτοματοποίηση μηχανών και στις αλληλεπιδράσεις μεταξύ μηχανών και να βοηθήσει τους ανθρώπους να αλληλεπιδρούν με τα μηχανήματα με νέους τρόπους (Castro & New, 2016). Η Τεχνητή Νοημοσύνη μπορεί όχι μόνο να εκτελεί πολλά καθήκοντα πιο αποτελεσματικά από τους ανθρώπους, αλλά μπορεί και να κάνει τα πράγματα που ο άνθρωπος δεν μπορεί, όπως είναι η ανάλυση ποσοτήτων δεδομένων που είναι πολύ μεγάλες για να τις επεξεργαστεί ο ανθρώπινος νους. Οι εταιρείες πρέπει να έχουν πρόσβαση σε δεδομένα - και συχνά σε μεγάλου όγκου - για να χρησιμοποιήσουν με επιτυχία την Τεχνητή Νοημοσύνη. Επομένως, οι κανονισμοί που ελέγχουν τη χρήση των δεδομένων έχουν σοβαρές επιπτώσεις στην Τεχνητή Νοημοσύνη.

Καθώς οι επιχειρήσεις παγκοσμίως και σχεδόν σε κάθε κλάδο αρχίζουν να βελτιώνουν την παραγωγικότητά τους με χρήση της τεχνολογίας Τεχνητής Νοημοσύνης, η ευρωπαϊκή οικονομία θα μπορέσει να παραμείνει ανταγωνιστική μόνο εάν οι επιχειρήσεις της κάνουν το ίδιο. Οι ευρωπαϊκές εταιρείες τεχνολογίας, για παράδειγμα, έχουν μια τεράστια ευκαιρία στην αγορά να αναπτύξουν την Τεχνητή Νοημοσύνη για πολλές διαφορετικές περιπτώσεις χρήσης. Οι υπεύθυνοι για τη χάραξη πολιτικής της ΕΕ έχουν αναγνωρίσει την οικονομική σημασία της AI και έχουν δεσμεύσει εκατοντάδες εκατομμύρια ευρώ για έρευνα στην Τεχνητή Νοημοσύνη (European Commission, 2017). Η συμβουλευτική εταιρεία PwC εκτιμά ότι η Τεχνητή Νοημοσύνη θα μπορούσε να προσθέσει έως και 2,5 τρισεκατομμύρια δολάρια στο ευρωπαϊκό ΑΕΠ μέχρι το 2030 (PwC, 2017). Το GDPR επιβάλλει αυστηρούς κανόνες για τον τρόπο με τον οποίο οι επιχειρήσεις μπορούν να χρησιμοποιούν τα προσωπικά δεδομένα όσων ζουν στην ΕΕ - ένας περιορισμός που αναμφισβήτητα θα παρεμποδίσει την ανάπτυξη και τη χρήση της Τεχνητής Νοημοσύνης στην Ευρώπη. Αυτοί οι περιορισμοί επηρεάζουν ουσιαστικά όλες τις ευρωπαϊκές εταιρείες, καθώς οι περισσότερες επιχειρήσεις επεξεργάζονται προσωπικά δεδομένα σχετικά με τους εργαζομένους τους, όπως πληροφορίες μισθοδοσίας. Και ενώ δεν χρησιμοποιούνται όλες οι χρήσεις της Τεχνητής Νοημοσύνης με προσωπικά δεδομένα, πολλοί το κάνουν. Για παράδειγμα, οι εταιρείες χρησιμοποιούν την Τεχνητή Νοημοσύνη για να αυτοματοποιήσουν τις οικονομικές συμβουλές, να επεξεργαστούν τις πιστωτικές εφαρμογές και να αναλύσουν τα αποτελέσματα των ιατρικών δοκιμών. Το GDPR περιέχει κανόνες που περιορίζουν άμεσα και έμμεσα την ανάπτυξη και τη χρήση της Τεχνητής Νοημοσύνης (Castro & Wallace, 2018):

- Οι εταιρείες πρέπει να έχουν ανθρώπους να αναθεωρήσουν ορισμένες αλγοριθμικές αποφάσεις, οι οποίες αυξάνουν το κόστος εργασίας με τη χρήση εξελιγμένων συστημάτων Τεχνητής Νοημοσύνης.

- Οι εταιρείες που πρέπει να εξηγήσουν τη λογική πίσω από τις αλγοριθμικές αποφάσεις τους είναι μια αμφίσημη απαίτηση που θα μπορούσε να αναγκάσει τις εταιρείες να κάνουν αντισταθμίσεις μεταξύ ακρίβειας και ερμηνείας των μοντέλων υπολογιστών τους

- Το δικαίωμα διαγραφής δεδομένων μπορεί να μειώσει την ακρίβεια ορισμένων αλγοριθμικών μοντέλων.

- Η μη συμμόρφωση με το εξαιρετικά περίπλοκο σύνολο κανόνων του GDPR οδηγεί σε αυστηρές κυρώσεις που καθιστούν μια προηγμένη επεξεργασία δεδομένων νομικά και οικονομικά επικίνδυνη. Επειδή οι απαιτήσεις του GDPR θα ήταν ανέφικτες - και σε ορισμένες περιπτώσεις αδύνατες - να εκπληρωθούν, πολλές εταιρείες θα περιορίσουν τελικά τη χρήση της Τεχνητής Νοημοσύνης.

Ορισμένες πτυχές του GDPR παραμένουν ανοιχτές στην ερμηνεία, τόσο από τις ρυθμιστικές αρχές όσο και από τα δικαστήρια, όπως ποια τεχνικά μέτρα μπορεί να ικανοποιήσουν την απαίτηση να «σβήσουν» τα δεδομένα και ποιο είναι το δικαίωμα σε «ουσιαστικές πληροφορίες σχετικά με τη σχετική λογική» σε μια αλγοριθμική απόφαση . Αυτή η ασάφεια παρουσιάζει τόσο μια ευκαιρία όσο και ένα πρόβλημα. Από τη μια πλευρά, δημιουργεί περιθώρια για τους υπεύθυνους χάραξης πολιτικής να περιορίζουν τις πιο επιβλαβείς παρενέργειες του GDPR χωρίς να το τροποποιούν. Για παράδειγμα, οι ρυθμιστικές αρχές μπορούν να ερμηνεύουν ανεπαρκώς καθορισμένες διατάξεις όπως το δικαίωμα σε «ουσιαστικές πληροφορίες» σχετικά με τους

αλγορίθμους με τρόπο που δεν θα αναγκάσει απαραιτήτως την επένδυση στην Τεχνητή Νοημοσύνη (Castro & Wallace, 2018).

Από την άλλη πλευρά όμως, η αμφιλεγόμενη νομοθεσία επιτρέπει την ασυνήθιστη επιβολή της νομοθεσίας, γεγονός που αποτελεί πρόβλημα που η ΕΕ μπορεί να αντιμετωπίσει μόνο με την τροποποίηση του GDPR. Πολλές εταιρείες πιθανόν θα λειτουργούν σύμφωνα με τις αυστηρότερες ερμηνείες του GDPR, ώστε να μην υποστούν τα σοβαρά πρόστιμα του GDPR, ιδίως επειδή η συμβουλευτική ομάδα της ΕΕ για την προστασία των δεδομένων, η ομάδα εργασίας του άρθρου 29 (WP29), τείνει να χρησιμοποιεί απαγορευτικές ερμηνείες στις κατευθυντήριες γραμμές του νόμου, ακόμη και όταν αυτό συμβαίνει εις βάρος της καινοτομίας. Αυτή η αβεβαιότητα πιθανώς θα εμποδίσει την ανάπτυξη και τη χρήση της Τεχνητής Νοημοσύνης (Castro & Wallace, 2018).

ΚΕΦΑΛΑΙΟ 2: GENERAL DATA PROTECTION REGULATION (GDPR)

2.1 Εισαγωγή στην προστασία δεδομένων

Ως προστασία των δεδομένων ορίζεται συνήθως ο νόμος που έχει σχεδιαστεί για την προστασία των προσωπικών δεδομένων. Στις σύγχρονες κοινωνίες, προκειμένου να είναι εφικτός ο έλεγχος των δεδομένων και η προστασία από τις καταχρήσεις, είναι απαραίτητο οι νόμοι για την προστασία των δεδομένων να περιορίσουν και να διαμορφώσουν τις δραστηριότητες των εταιρειών και των κυβερνήσεων. Αυτά τα θεσμικά όργανα έχουν επανειλημμένα δείξει ότι αν δεν υπάρχουν κανόνες που περιορίζουν τις ενέργειές τους, θα προσπαθήσουν να τα συγκεντρώσουν όλα αυτά, να τα αποθηκεύσουν όλα, να τα μοιραστούν με άλλους, χωρίς να τα γνωστοποιούν (Privacy International, 2018).

Κάθε φορά που κάποιος χρησιμοποιεί μια υπηρεσία, αγοράζει ένα προϊόν στο διαδίκτυο, εγγράφεται στο ηλεκτρονικό ταχυδρομείο, πηγαίνει στο γιατρό, πληρώνει τους φόρους ή συμμετέχει σε οποιαδήποτε σύμβαση ή αίτηση παροχής υπηρεσιών, πρέπει να παραδίνει μερικά από τα προσωπικά του δεδομένα. Ακόμη και χωρίς τη συγκατάθεση κάποιου, τα δεδομένα και οι πληροφορίες του δημιουργούνται και συλλαμβάνονται από εταιρείες και πρακτορεία που πιθανώς δεν έχει ενσυνείδητα αλληλεπιδράσει. Ο μόνος τρόπος για τους πολίτες και τους καταναλωτές να έχουν εμπιστοσύνη τόσο στην κυβέρνηση όσο και στις επιχειρήσεις είναι μέσω ισχυρών πρακτικών προστασίας δεδομένων, με αποτελεσματική νομοθεσία που συμβάλλει στην ελαχιστοποίηση της κρατικής και εταιρικής επιτήρησης και της εκμετάλλευσης των δεδομένων.

Από τη δεκαετία του 1960 και την επέκταση των δυνατοτήτων της τεχνολογίας της πληροφορίας, οι επιχειρήσεις και οι κυβερνήσεις έχουν αποθηκεύσει αυτά τα προσωπικά δεδομένα σε βάσεις δεδομένων. Οι βάσεις δεδομένων μπορούν να αναζητηθούν, να επεξεργασθούν, να διασταυρωθούν και τα δεδομένα τους να μοιραστούν σε άλλους οργανισμούς ανά τον κόσμο. Μόλις η συλλογή και επεξεργασία δεδομένων έγινε ευρέως διαδεδομένη, οι άνθρωποι άρχισαν να θέτουν ερωτήσεις σχετικά με τα δεδομένα τους. Ποιος είχε δικαίωμα πρόσβασης στα δεδομένα; Διατηρήθηκαν με ακρίβεια; Είχαν συλλεχθεί και διαδοθεί χωρίς τη συγκατάθεσή τους; Θα μπορούσε να χρησιμοποιηθεί για τη διάκριση ή παραβίαση άλλων θεμελιωδών δικαιωμάτων; Από όλα αυτά τα ερωτήματα και εν μέσω αυξανόμενου δημόσιου ενδιαφέροντος, οι αρχές προστασίας δεδομένων σχεδιάστηκαν μέσω πολυάριθμων εθνικών και διεθνών διαβουλεύσεων. Το Γερμανικό ομόσπονδο κρατίδιο της Έσσης πέρασε τον πρώτο νόμο το 1970, ενώ ο αμερικανικός Νόμος Fair Credit Reporting Act το 1970 περιείχε επίσης στοιχεία προστασίας δεδομένων (Gellman, 2017).

Η καθοδηγούμενη από τις ΗΠΑ ανάπτυξη ενός «κώδικα ορθών πρακτικών πληροφόρησης» στις αρχές της δεκαετίας του 1970 εξακολουθεί να διαμορφώνει σήμερα το δίκαιο προστασίας δεδομένων. Ωστόσο, η ΕΕ είναι εκείνη που κυριαρχεί στα θέματα privacy. Οι εθνικοί νόμοι προέκυψαν σύντομα, αρχίζοντας από τη Σουηδία, τη Γερμανία και τη Γαλλία. Μέχρι τον Ιανουάριο του 2018, πάνω από 100 χώρες είχαν θεσπίσει νόμους για την προστασία των δεδομένων, ενώ εκκρεμούν νομοσχέδια ή πρωτοβουλίες για τη θέσπιση νόμου σε άλλες 40 (Banisar, 2018).

Με την πάροδο του χρόνου υιοθετήθηκαν επίσης περιφερειακά νομικά πλαίσια. Το 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) ανέπτυξε τις κατευθυντήριες γραμμές του, οι οποίες περιλάμβαναν «αρχές

προστασίας της ιδιωτικής ζωής». Λίγο αργότερα, τέθηκε σε ισχύ η Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία των προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα - εκσυγχρονίστηκε το 2018 (128th Session of the Committee of Ministers, 2018).

Ο τεράστιος όγκος των δεδομένων που παράγονται και η ταχεία ανάπτυξη της τεχνολογίας, συμπεριλαμβανομένης της εξελιγμένης μορφοποίησης και παρακολούθησης, καθώς και η τεχνητή νοημοσύνη, σημαίνει ότι ορισμένοι υφιστάμενοι νόμοι για την προστασία των δεδομένων είναι ξεπερασμένοι και ακατάλληλοι για να αντιμετωπίσουν τη διαδικασία επεξεργασίας. Τα πλαίσια δεν αντικατοπτρίζουν το νέο δυναμικό επεξεργασίας δεδομένων που προέκυψε με την πρόοδο των τεχνολογιών που αναπτύχθηκαν και ενσωματώθηκαν στα συστήματα διακυβέρνησης και στα επιχειρηματικά μοντέλα. Έχει αναφερθεί ότι το 90% των δεδομένων στον κόσμο σήμερα δημιουργήθηκε τα τελευταία δύο χρόνια και κάθε δύο ημέρες δημιουργούμε τόσο πολλά δεδομένα όσα κάναμε από την αρχή μέχρι το 2013 (Singlehurst et al., 2017).

Όταν καταρτίστηκαν πολλά πλαίσια προστασίας δεδομένων, ο κόσμος ήταν ένα πολύ διαφορετικό μέρος. Για παράδειγμα, υιοθετήθηκαν πολλοί νόμοι προτού δημιουργηθεί η Google, το Facebook ή τα smartphones. Ένα πλαίσιο προστασίας δεδομένων μπορεί να έχει τους περιορισμούς του, αλλά παρέχει ένα σημαντικό και θεμελιώδες σημείο εκκίνησης για να διασφαλιστεί η εφαρμογή ισχυρών κανονιστικών και νομικών διασφαλίσεων για την προστασία των προσωπικών δεδομένων. Ένα ισχυρό πλαίσιο προστασίας δεδομένων μπορεί να ενισχύσει τα άτομα, να περιορίσει τις πρακτικές επιβλαβών δεδομένων και να περιορίσει την εκμετάλλευση των δεδομένων. Είναι απαραίτητο να παρασχεθούν τα απαιτούμενα πλαίσια διακυβέρνησης σε εθνικό και παγκόσμιο επίπεδο για να διασφαλιστεί ότι τα

άτομα θα έχουν ισχυρά δικαιώματα επί των δεδομένων τους, θα επιβάλλονται αυστηρές υποχρεώσεις σε όσους επεξεργάζονται προσωπικά δεδομένα (τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα) έναντι εκείνων που παραβιάζουν αυτές τις υποχρεώσεις και προστασίες.

Συνολικά, η προστασία δεδομένων πρέπει να εξασφαλίζει τα εξής (Privacy International, 2018):

- Πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων και πρέπει να λαμβάνονται με νόμιμα και δίκαια μέσα, καθώς και να γίνονται με διαφανή τρόπο.

- Οι σκοποί για τους οποίους πρόκειται να χρησιμοποιηθούν τα δεδομένα και οι πληροφορίες πρέπει να προσδιορίζονται (το αργότερο) κατά τη στιγμή της συλλογής και πρέπει να χρησιμοποιούνται μόνο για τους συμφωνημένους σκοπούς. Τα προσωπικά δεδομένα μπορούν να αποκαλυφθούν, να χρησιμοποιηθούν ή να διατηρηθούν για τους αρχικούς σκοπούς (δηλ. Ο σκοπός κατά τη στιγμή της συλλογής).

- Τα δεδομένα προσωπικού χαρακτήρα, καθώς δημιουργούνται και υφίστανται επεξεργασία, πρέπει να είναι επαρκή, συναφή και να περιορίζονται στην αναγκαιότητα των σκοπών για τους οποίους πρόκειται να χρησιμοποιηθούν.

- Τα δεδομένα πρέπει να είναι ακριβή και πλήρη και πρέπει να λαμβάνονται μέτρα για να εξασφαλιστεί ότι είναι ενημερωμένα.

- Πρέπει να χρησιμοποιούνται εύλογες διασφαλίσεις ασφάλειας για την προστασία προσωπικών δεδομένων από απώλεια, μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή αποκάλυψη.

- Δεν πρέπει να υπάρχουν μυστικοί επεξεργαστές δεδομένων, πηγών ή επεξεργασίας. Τα άτομα πρέπει να έχουν επίγνωση της συλλογής και επεξεργασίας των δεδομένων τους, καθώς και του σκοπού της χρήσης τους.

- Τα άτομα έχουν μια σειρά δικαιωμάτων τα οποία τους επιτρέπουν να ελέγχουν τα προσωπικά τους δεδομένα και οποιαδήποτε επεξεργασία.

- Εκείνοι που χρησιμοποιούν προσωπικά δεδομένα πρέπει να λογοδοτούν και να αποδεικνύουν την τήρηση των παραπάνω αρχών και να διευκολύνουν και να εκπληρώνουν την άσκηση αυτών των δικαιωμάτων, τηρώντας τους ισχύοντες νόμους που κατοχυρώνουν αυτές τις αρχές.

Οι κανόνες προστασίας δεδομένων πρέπει να επιβληθούν από ρυθμιστικό φορέα ή αρχή, που ονομάζεται συχνά Επίτροπος προστασίας δεδομένων. Η ισχύς αυτών των αρχών ποικίλλει από χώρα σε χώρα και η ανεξαρτησία της εξαρτάται από την εκάστοτε κυβέρνηση. Αυτές οι εξουσίες, για παράδειγμα, μπορεί να περιλαμβάνουν την ικανότητα διεξαγωγής ερευνών, ενεργούντων καταγγελιών και επιβολής προστίμων όταν ανακαλύπτουν ότι ένας οργανισμός έχει παραβιάσει τον νόμο.

Εκτός από την εφαρμογή μέσω ρυθμιστικών μέσων, οι τεχνολογίες μπορούν να διαδραματίσουν σημαντικό ρόλο στην τήρηση των κανόνων προστασίας δεδομένων. Μέσω τεχνολογικών μέσων και προσεκτικού σχεδιασμού, είναι δυνατό να περιοριστεί η συλλογή δεδομένων, να περιοριστεί μαθηματικά η περαιτέρω

επεξεργασία δεδομένων, προκειμένου να περιοριστεί οπωσδήποτε η περιττή πρόσβαση, μεταξύ άλλων μέτρων προστασίας της ιδιωτικής ζωής. Οι νόμοι μπορούν να επηρεάσουν και, όταν είναι απαραίτητο, να επιβάλουν τέτοιες εξελίξεις. Αν και η υιοθέτησή τους είναι αργή, ωστόσο οι εταιρείες και οι κυβερνήσεις είναι ανθεκτικές στο να περιορίσουν τις μελλοντικές δυνατότητές τους ή τις προσδοκίες τους να εξορύσσουν τις πληροφορίες, ακόμη και αν νομικά υποτίθεται ότι περιορίζουν την ερμηνεία του σκοπού.

Σε γενικές γραμμές, οι προσωπικές πληροφορίες σημαίνουν κάθε είδους πληροφορίες (ένα μόνο κομμάτι πληροφοριών ή ένα σύνολο πληροφοριών) που μπορούν να αναγνωρίσουν προσωπικά ένα άτομο ή να τα αναδείξουν ως άτομο. Τα προφανή παραδείγματα είναι το όνομα, η διεύθυνση, ο αριθμός ταυτότητας, η ημερομηνία γέννησης ή η εικόνα του προσώπου. Μερικά ίσως λιγότερο εμφανή παραδείγματα περιλαμβάνουν τους αριθμούς πινακίδων κυκλοφορίας οχημάτων, τους αριθμούς πιστωτικών καρτών, τα δακτυλικά αποτυπώματα, τη διεύθυνση IP ενός υπολογιστή ή τα αρχεία υγείας. Ένα άτομο μπορεί να ξεχωρίσει από άλλα άτομα, ακόμη και αν το όνομά του δεν είναι γνωστό. Για παράδειγμα, οι εταιρίες δημιουργίας προφίλ σε απευθείας σύνδεση εκχωρούν έναν μοναδικό αριθμό και χρησιμοποιούν τεχνικές παρακολούθησης για να ακολουθήσουν τα άτομα γύρω από το δίκτυο και να δημιουργήσουν ένα προφίλ της συμπεριφοράς και των συνηθειών τους προκειμένου να τους παρουσιάσουν τις ανάλογες διαφημίσεις. Ορισμένες προσωπικές πληροφορίες θεωρούνται πιο ευαίσθητες από άλλες και επομένως υπόκεινται σε αυστηρότερους κανόνες. Αυτές περιλαμβάνουν τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τη θρησκεία, την υγεία και τη σεξουαλική ζωή. Τέτοιες πληροφορίες δεν μπορούν να συλλέγονται ή να χρησιμοποιούνται καθόλου χωρίς τη συγκεκριμένη συγκατάθεση των ατόμων (Privacy International, 2018).

2.1.1 Αρχές προστασίας δεδομένων

Όταν υπάρχει συγκεκριμένος νόμος για την προστασία δεδομένων, οι οργανισμοί, δημόσιοι ή ιδιωτικοί, που συλλέγουν και χρησιμοποιούν προσωπικά στοιχεία έχουν υποχρέωση να χειρίζονται αυτά τα δεδομένα σύμφωνα με τον νόμο περί προστασίας δεδομένων. Από τα περιφερειακά και διεθνή πλαίσια, θα πρέπει να τηρούνται ορισμένες αρχές κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

1. Δικαιοσύνη, νομιμότητα, διαφάνεια

Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε νόμιμη και δίκαιη επεξεργασία. Αυτή η αρχή είναι βασική για την αντιμετώπιση πρακτικών όπως η πώληση ή / και η μεταφορά προσωπικών δεδομένων που αποκτήθηκαν δόλια. Η «δικαιοσύνη και διαφάνεια» είναι ουσιαστικής σημασίας για τη διασφάλιση ότι τα δεδομένα των ανθρώπων δεν χρησιμοποιούνται με τρόπους που δεν θα περίμενε κανείς. Ως «νόμιμο» νοείται ότι τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να σέβεται το κράτος δικαίου και να πληροί ένα νομικό υπόβαθρο για τη μεταποίηση. Ένας «νόμιμος λόγος» είναι μια περιορισμένη αιτιολόγηση για τη διεκπεραίωση των δεδομένων του ανθρώπου που αναφέρονται στο νόμο (π.χ. συγκατάθεση) - που συζητείται στο παρακάτω τμήμα με τίτλο «Νόμιμοι λόγοι επεξεργασίας».

Αυτή η αρχή έχει σημαία καθώς, είναι ζωτικής σημασίας το άτομο να είναι σαφώς ενημερωμένο και να έχει επίγνωση του τρόπου επεξεργασίας των δεδομένων του και από ποιον. Αν υπάρχει πρόθεση να μοιραστούν τα δεδομένα ενός ατόμου με

ένα τρίτο μέρος, αλλά ο υπεύθυνος επεξεργασίας δεδομένων δεν είναι διαφανής για αυτό το γεγονός και το υποκείμενο των δεδομένων δεν έχει σαφώς ενημερωθεί, είναι πιθανό ότι τα προσωπικά του δεδομένα να λήφθηκαν άδικα, και η διαδικασία να μην θεωρείται διαφανής. Για παράδειγμα, στην Ιρλανδία, μια ασφαλιστική εταιρεία επικοινώνησε με έναν από τους πελάτες της για να τον ενημερώσει για μια νέα πιστωτική κάρτα, αλλά δεν ήταν σαφές στον πελάτη ότι δεν ήταν η ασφαλιστική εταιρεία που θα έδινε τη νέα κάρτα, αλλά ότι τα δεδομένα θα μεταφέρονταν στην τράπεζα για να τα επεξεργαστεί - δηλαδή η τράπεζα ήταν ο υπεύθυνος επεξεργασίας δεδομένων, αλλά αυτό δεν είχε καταστεί σαφές στο άτομο στην ανακοίνωση που έλαβε από την ασφαλιστική εταιρεία. Ως εκ τούτου, κρίθηκε ότι υπέστη αδικαιολόγητη επεξεργασία (Data Protection Commission, 2019).

2. Περιορισμός στόχου

Όλα τα προσωπικά δεδομένα θα πρέπει να συλλέγονται για καθορισμένο, συγκεκριμένο και νόμιμο σκοπό. Οποιαδήποτε περαιτέρω επεξεργασία δεν πρέπει να είναι ασυμβίβαστη με τους σκοπούς που καθορίζονται στην αρχή (δηλ. Το σημείο συλλογής). Αυτό ουσιαστικά σημαίνει ότι δεν είναι αποδεκτό να δηλώνεται ότι χρειάζονται δεδομένα ενός ατόμου για ένα σκοπό και στη συνέχεια να χρησιμοποιούνται για κάτι άλλο χωρίς προειδοποίηση ή δικαιολογία.

Οι τεχνολογικές εξελίξεις (και η μαζική παραγωγή, η συλλογή και η ανάλυση των δεδομένων που τις συνοδεύουν) σημαίνουν ότι αυτές οι αρχές είναι όλο και πιο σημαντικές. Ο σκοπός της επεξεργασίας και η προτεινόμενη χρήση των δεδομένων πρέπει να προσδιορίζονται σαφώς και να εξηγούνται στο υποκείμενο των δεδομένων. Εάν τα δεδομένα πρόκειται να χρησιμοποιηθούν για σκοπό διαφορετικό από τον

αρχικό σκοπό, τότε το υποκείμενο των δεδομένων πρέπει να είναι επαρκώς ενημερωμένο για αυτό. Είναι ιδιαίτερα σημαντικό τα ευαίσθητα προσωπικά δεδομένα να μην υποβάλλονται σε επεξεργασία για σκοπούς διαφορετικούς από αυτούς που καθορίστηκαν αρχικά. Αυτό είναι ιδιαίτερα σημαντικό για τις μεγάλες διαδικασίες επεξεργασίας δεδομένων και άλλων δεδομένων. Για παράδειγμα, η βιομηχανία των χρηματιστών δεδομένων ευδοκιμεί από την επαναδιάθεση δεδομένων (Privacy International, 2019). Συγκεντρώνουν δεδομένα από μια τεράστια ποικιλία πηγών, στη συνέχεια συλλέγουν και αναλύουν προφίλ και μοιράζονται ιδέες με τους πελάτες τους. Αυτό σημαίνει ότι πολλά δεδομένα που μοιράζονται για ένα σκοπό επαναπροσδιορίζονται με τρόπους που δεν αναμένονται, συμπεριλαμβανομένης και της στοχοθετημένης διαφήμισης.

Τα προσωπικά δεδομένα δεν πρέπει να αποκαλύπτονται, να διατίθενται ή να χρησιμοποιούνται με άλλο τρόπο για σκοπούς διαφορετικούς από αυτούς που καθορίζονται, σύμφωνα με την αρχή του περιορισμού του σκοπού. Υπάρχουν, ωστόσο, δύο κοινές εξαιρέσεις από την αρχή αυτή: είναι αποδεκτό αν γίνει:

α) με τη συγκατάθεση του υποκειμένου των δεδομένων

β) από την αρχή του νόμου

Παρόλο που πρόκειται για δύο ευρέως αναγνωρισμένες εξαιρέσεις στις αρχές περιορισμού της χρήσης, συχνά χρησιμοποιούνται για κατάχρηση. Στην περίπτωση του στοιχείου α), η συγκατάθεση πρέπει να είναι έγκυρη. Δεν πρέπει να υπόκειται σε όρους, να λαμβάνονται μέσω προκαθορισμένων πλαισίων ή να αποκρύπτονται οι λεπτομέρειες αυτών των άλλων σκοπών σε μικρές εκτυπώσεις ή σε μη νόμιμη μορφή. Στην περίπτωση του στοιχείου β), αυτό χρησιμοποιήθηκε για να επιτρέψει ευρείες ρυθμίσεις για την κοινοχρησία δεδομένων από κρατικούς φορείς και ιδρύματα κατά

την άσκηση των καθηκόντων τους, για παράδειγμα με τη χρήση δεδομένων που παρέχονται για λόγους υγειονομικής περίθαλψης ή εκπαίδευσης ή για λόγους μετανάστευσης. Τέτοιες γενικές εξαιρέσεις απειλούν να αποδυναμώσουν την προστασία που προσφέρει ο νόμος περί προστασίας των δεδομένων, οπότε είναι ζωτικής σημασίας οι διατάξεις που προβλέπουν εξαιρέσεις να κατασκευαστούν στενά, έτσι ώστε η αρχή του περιορισμού των σκοπών να μην είναι περιττή και μη εφαρμόσιμη όταν πρόκειται για το κράτος και τις λειτουργίες του.

Επιπλέον, σε σχέση με τον περιορισμό του σκοπού, το κείμενο ενός νόμου θα μπορούσε να προβλέπει διάφορους σκοπούς οι οποίοι δεν πρέπει να είναι ασυμβίβαστοι με την αρχή αυτή. Αυτά θα μπορούσαν να περιλαμβάνουν, αλλά δεν περιορίζονται σε:

- σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον

- Επιστημονικοί, στατιστικοί ή ιστορικοί σκοποί

Είναι σημαντικό οι στόχοι αυτοί να περιορίζονται στο πεδίο εφαρμογής τους και οι ανωτέρω όροι να ορίζονται περαιτέρω ώστε να παρέχουν σαφήνεια ως προς το τι μπορεί να συνεπάγεται.

Εάν δεν υπάρχουν σαφείς περιορισμοί στο σημείο συλλογής όσον αφορά τις χρήσεις των δεδομένων, υπάρχουν ανησυχίες ότι τα δεδομένα θα μπορούσαν να χρησιμοποιηθούν για άλλους σκοπούς κατά τη διάρκεια του κύκλου ζωής των δεδομένων, γεγονός που θα μπορούσε να έχει επιζήμιες επιπτώσεις για τα άτομα και να οδηγήσει σε κατάχρηση. Υπάρχει ένας αυξανόμενος αριθμός περιπτώσεων στις οποίες η αρχή του περιορισμού του σκοπού υπονομεύεται και παρακάμπτεται. Για παράδειγμα, η Aadhaar, η εθνική βιομετρική βάση δεδομένων της Ινδίας,

δημιουργήθηκε αρχικά το 2009 με στόχο την τυποποίηση κυβερνητικών βάσεων δεδομένων. Ωστόσο, με την πάροδο του χρόνου, το σχέδιο έχει γίνει πιο φιλόδοξο και τώρα χρησιμοποιείται για μια σειρά σκοπών από τις σχολικές εισαγωγές έως την απόκτηση πιστοποιητικών θανάτου (The Centre for Internet and Society, 2016).

Το Eurodac (eur-lex.europa.eu), μια βιομετρική βάση δεδομένων που δημιουργήθηκε το 2000 για να επιτρέψει στα κράτη μέλη της ΕΕ να ελέγξουν εάν ένας αιτών άσυλο είχε προηγουμένως ζητήσει άσυλο σε άλλη ευρωπαϊκή χώρα ή είχε λάβει κοινωνικές παροχές από άλλη χώρα της ΕΕ, χρησιμοποιείται τώρα για νέο σκοπό. Ο επικαιροποιημένος κανονισμός Eurodac, ο οποίος τέθηκε σε ισχύ τον Ιούλιο του 2015, επιτρέπει πλέον τη "χρήση της βάσης δεδομένων Eurodac για τα δακτυλικά αποτυπώματα των αιτούντων άσυλο για την πρόληψη, ανίχνευση και διερεύνηση τρομοκρατικών εγκλημάτων και άλλων σοβαρών εγκλημάτων".

3. Ελαχιστοποίηση

Η ελαχιστοποίηση των δεδομένων είναι μια βασική έννοια στην προστασία δεδομένων, τόσο από τα δικαιώματα ενός ατόμου όσο και από την άποψη της ασφάλειας των πληροφοριών. Ο νόμος θα πρέπει να ορίζει σαφώς ότι θα πρέπει να διεκπεραιώνονται μόνο τα δεδομένα που είναι απαραίτητα και συναφή για το σκοπό που αναφέρεται. Οποιεσδήποτε εξαιρέσεις πρέπει να είναι πολύ περιορισμένες και σαφώς καθορισμένες.

- Ανάγκη: Πρέπει να διασφαλιστεί ότι τα συλλεγόμενα δεδομένα δεν προορίζονται να είναι πιο εκτεταμένα από τα αναγκαία για τους σκοπούς για τους οποίους θα χρησιμοποιηθούν τα δεδομένα. Η δοκιμή πρέπει να είναι ότι

η λιγότερο παρεμβατική μέθοδος που χρησιμοποιείται για την επίτευξη ενός νόμιμου στόχου.

- Σχετικότητα: Τα δεδομένα που επεξεργάζονται πρέπει να είναι σχετικά με τους καθορισμένους σκοπούς.

Αυτές οι αρχές απαιτούν από τα άτομα που επεξεργάζονται τα δεδομένα να εξετάσουν ποιο είναι το ελάχιστο ποσό των δεδομένων που είναι απαραίτητα για την επίτευξη του σκοπού. Οι επεξεργαστές θα πρέπει να το τηρούν αυτό, χωρίς να είναι αποδεκτό να συλλέγουν επιπλέον δεδομένα επειδή μπορεί να είναι χρήσιμα αργότερα ή απλά επειδή δεν έχει δοθεί καμία σκέψη για το αν είναι απαραίτητα σε ένα συγκεκριμένο σενάριο (Commission National Informatique & Libertes, 2019).

Η αρχή της ελαχιστοποίησης των δεδομένων είναι ακόμα πιο ολοκληρωμένη στην εποχή των μεγάλων δεδομένων, όπου η πρόοδος στην τεχνολογία έχει ριζικά βελτιώσει τις αναλυτικές τεχνικές για την αναζήτηση, τη συγκέντρωση και τη διασταύρωση μεγάλων συνόλων δεδομένων, προκειμένου να αναπτυχθεί η νοημοσύνη και οι πληροφορίες (Privacy International, 2019).

Με την υπόσχεση και την ελπίδα ότι η κατοχή περισσότερων δεδομένων θα επιτρέψει την ακριβή κατανόηση της ανθρώπινης συμπεριφοράς, υπάρχει ένα ενδιαφέρον και μια σταθερή προσπάθεια να συγκεντρωθούν τεράστια ποσά δεδομένων. Υπάρχει επείγουσα ανάγκη να αμφισβητηθεί αυτή η άποψη και να διασφαλιστεί ότι θα πρέπει να υποβάλλονται σε επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα και χρήσιμα για συγκεκριμένο σκοπό.

4. Ακρίβεια

Τα προσωπικά δεδομένα πρέπει να είναι ακριβή κατά τη διάρκεια της επεξεργασίας και πρέπει να λαμβάνεται κάθε εύλογο μέτρο για να διασφαλιστεί αυτό. Αυτό περιλαμβάνει τα ακόλουθα στοιχεία:

- Ακρίβεια: Όλα τα επεξεργασμένα δεδομένα πρέπει να είναι ακριβή καθ 'όλη τη διάρκεια του κύκλου ζωής των δεδομένων.

- Πληρότητα: Οποιαδήποτε κατηγορία δεδομένων πρέπει να είναι πλήρης στο μέτρο του δυνατού, ώστε η παράλειψη των σχετικών δεδομένων να μην οδηγεί σε συμπεράσματα διαφορετικών πληροφοριών στις πληροφορίες που θα μπορούσαν να ληφθούν εάν τα δεδομένα ήταν πλήρη.

- Ενημέρωση: Όλα τα δεδομένα που διατηρούνται και μπορούν να υποστούν περαιτέρω επεξεργασία σύμφωνα με τις διατάξεις που προβλέπονται στον νόμο περί προστασίας δεδομένων πρέπει να ενημερώνονται.

- Περιορισμός: Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία (και να διατηρούνται) μόνο για το χρονικό διάστημα που απαιτείται για το σκοπό για τον οποίο συλλέχθηκαν και αποθηκεύτηκαν.

Τα ανωτέρω στοιχεία επιβεβαιώνουν τα δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα να έχουν πρόσβαση στα προσωπικά τους δεδομένα και να διορθώνουν ελλιπή, ανακριβή ή παρωχημένα δεδομένα τα οποία πρέπει να προβλέπονται σε νόμο περί προστασίας δεδομένων. Όλο και περισσότερο, οι διαδικασίες λήψης αποφάσεων και χάραξης πολιτικής βασίζονται σε δεδομένα. Ωστόσο, υπάρχει μεγάλος κίνδυνος, εάν τα δεδομένα δεν είναι ακριβή και

ενημερωμένα, το αποτέλεσμα της διαδικασίας λήψης αποφάσεων να είναι επίσης ανακριβές. Στα πιο σοβαρά σενάρια, αυτό θα μπορούσε να οδηγήσει σε μια απόφαση ότι ένα άτομο δεν έχει πρόσβαση σε δημόσιες υπηρεσίες ή σε προγράμματα κοινωνικής πρόνοιας, ούτε έχει λάβει δάνειο. Για παράδειγμα, υπήρξαν περιπτώσεις ατόμων που αρνήθηκαν αδικαιολογήτως δάνειο ή υποθήκη στο σπίτι τους επειδή η εταιρεία που ήταν υπεύθυνη για την αναθεώρηση του πιστωτικού τους σκοπού είχε ανακριβείς πληροφορίες οι οποίες μείωσαν την βαθμολογία τους από το «Άριστη» στο «Κακή» ή επειδή ήταν ανακριβείς οι πληροφορίες καταγράφηκαν από τα τραπεζικά ιδρύματα που καθιστούσαν ένα άτομο ανεπιθύμητο πελάτη (LaMagna, 2017).

5. Περιορισμένη αποθήκευση

Τα προσωπικά δεδομένα θα πρέπει να διατηρούνται μόνο για το χρονικό διάστημα που απαιτούνται τα δεδομένα για το σκοπό για τον οποίο συλλέχθηκαν και αποθηκεύθηκαν αρχικά. Αυτό θα ενισχύσει και θα διευκρινίσει την υποχρέωση διαγραφής δεδομένων στο τέλος της επεξεργασίας, η οποία θα πρέπει να συμπεριληφθεί σε άλλη διάταξη. Ο νόμος πρέπει να ορίζει σαφώς ότι τα δεδομένα δεν θα πρέπει να φυλάσσονται για περισσότερο από το αναγκαίο για το σκοπό για τον οποίο είχαν αρχικά ληφθεί. Οποιεσδήποτε εξαιρέσεις πρέπει να είναι πολύ περιορισμένες και σαφώς καθορισμένες.

Προκειμένου τα άτομα να είναι ενημερωμένα σχετικά με την επεξεργασία των δεδομένων τους, πρέπει να ενημερώνονται για το χρονικό διάστημα που θα διατηρούνται τα δεδομένα τους. Είναι συνεπώς απαραίτητο η νομοθεσία να ενθαρρύνει τους ελεγκτές να εφαρμόσουν την αρχή της ελαχιστοποίησης των

δεδομένων, ελαχιστοποιώντας τη συλλογή προσωπικών δεδομένων και όχι αποθηκεύοντας τα περισσότερο από το απαραίτητο. Οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να καταρτίσουν χρονοδιαγράμματα διατήρησης που να καθορίζουν τις περιόδους διατήρησης για όλα τα δεδομένα που κατέχουν. Αυτά πρέπει να επανεξετάζονται τακτικά. Αυτό διαφέρει από τη διαγραφή των δεδομένων προσωπικού χαρακτήρα σχετικά με το αίτημα του υποκειμένου των δεδομένων, το οποίο πρέπει επίσης να προβλέπεται στη νομοθεσία. Μετά την απαραίτητη χρονική περίοδο, τα προσωπικά δεδομένα θα πρέπει να διαγράφονται με ασφάλεια. Εάν τα δεδομένα πρόκειται να αποθηκευτούν πέρα από την περίοδο διατήρησης με ανώνυμη (και όχι ψευδονομία) μορφή, οι συνέπειες στην ιδιωτική ζωή για τα υποκείμενα των δεδομένων πρέπει να εξεταστούν προσεκτικά.

Ακόμη και αν τα δεδομένα έχουν υποβληθεί σε δίκαιη, νόμιμη και διαφανή επεξεργασία και σε σχέση με τις αρχές του περιορισμού του σκοπού, της ελαχιστοποίησης και της ακρίβειας, είναι απαραίτητο να διασφαλιστεί ότι τα δεδομένα δεν αποθηκεύονται για περισσότερο από το απαιτούμενο και αναγκαίο για τον σκοπό που συλλέχθηκαν. Κάθε παρέμβαση στο δικαίωμα στην προστασία της ιδιωτικής ζωής και των δεδομένων πρέπει να είναι αναγκαία και αναλογική (Court of Justice of the European Union, 2014).

Η αόριστη διατήρηση δεδομένων δεν αποτελεί μόνο παραβίαση των δικαιωμάτων ενός ατόμου, αλλά και κίνδυνο για όσους την επεξεργάζονται. Η απουσία περιορισμού της χρονικής περιόδου για την οποία αποθηκεύονται τα δεδομένα αυξάνει τους κινδύνους ασφαλείας και εγείρει ανησυχίες ότι θα μπορούσε να χρησιμοποιηθεί για νέους σκοπούς απλώς και μόνο επειδή εξακολουθεί να είναι διαθέσιμος και προσβάσιμος. Υπάρχουν κίνδυνοι που, αν είναι ξεπερασμένοι, θα μπορούσαν να οδηγήσουν σε κακές διαδικασίες λήψης αποφάσεων που θα

μπορούσαν να έχουν σοβαρές επιπτώσεις. Στην εποχή της εκτεταμένης, ανεξέλεγκτης κρατικής και εταιρικής επιτήρησης, είναι σημαντικό να τεθούν αυστηροί περιορισμοί στη διατήρηση δεδομένων για να μετριαστούν πιθανές παράνομες παρεμβάσεις στο δικαίωμα στην ιδιωτική ζωή (Privacy International, 2019).

6. Ακεραιότητα και εμπιστευτικότητα

Τα προσωπικά δεδομένα, σε κατάσταση ανάπαυσης και διαμετακόμισης, καθώς και η υποδομή που χρησιμοποιείται για επεξεργασία πρέπει να προστατεύονται από διασφαλίσεις ασφαλείας έναντι κινδύνων όπως παράνομη ή μη εξουσιοδοτημένη πρόσβαση, χρήση και αποκάλυψη, καθώς και απώλεια ή καταστροφή δεδομένων.

Οι διασφαλίσεις ασφάλειας θα μπορούσαν να περιλαμβάνουν:

- Φυσικά μέτρα, δηλαδή κλειδωμένες πόρτες και κάρτες αναγνώρισης.
- Οργανωτικά μέτρα, δηλαδή έλεγχοι πρόσβασης.
- Πληροφοριακά μέτρα, δηλαδή κρυπτογράφηση (μετατροπή κειμένου σε κωδικοποιημένη μορφή) και παρακολούθηση απειλών.
- Τεχνικά μέτρα, δηλαδή κρυπτογράφηση, ανωνυμοποίηση.

Άλλα οργανωτικά μέτρα περιλαμβάνουν τακτικούς ελέγχους της επάρκειας αυτών των μέτρων, εφαρμογή πολιτικών προστασίας δεδομένων και ασφάλειας πληροφοριών, κατάρτιση και τήρηση εγκεκριμένων κωδίκων δεοντολογίας.

Εάν δεν ληφθούν μέτρα ασφαλείας για την προστασία δεδομένων και για την ασφάλεια και ακεραιότητα της υποδομής, τα δεδομένα παραμένουν ευάλωτα σε απειλές και διατρέχουν κίνδυνο παραβίασης και παράνομης πρόσβασης. Έχουν υπάρξει πολλαπλά παραδείγματα παραβιάσεων δεδομένων ως αποτέλεσμα αδύναμης ασφάλειας. Για παράδειγμα, τον Μάρτιο του 2016, οι προσωπικές πληροφορίες των 55 εκατομμυρίων ψηφοφόρων των Φιλιππίνων διαρρέουν μετά από παραβίαση της βάσης δεδομένων της Επιτροπής σχετικά με τις εκλογές (COMELEC). Τον Σεπτέμβριο του 2016, η Εθνική Επιτροπή Προστασίας Προσωπικών Δεδομένων κατέληξε στο συμπέρασμα ότι υπήρξε παραβίαση της ασφάλειας που επέτρεψε την πρόσβαση στη βάση δεδομένων COMELEC που περιείχε τόσο προσωπικά όσο και ευαίσθητα δεδομένα και άλλες πληροφορίες (Foundation for Media Alternatives, 2019).

7. Ευθύνη

Μια οντότητα που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, υπό την ιδιότητά τους ως υπεύθυνων επεξεργασίας δεδομένων ή επεξεργαστών, θα πρέπει να λογοδοτεί για τη συμμόρφωση με τα πρότυπα και να λαμβάνει μέτρα τα οποία θέτουν σε εφαρμογή τις διατάξεις που προβλέπονται σε έναν νόμο για την προστασία των δεδομένων. Οι υπεύθυνοι για την επεξεργασία δεδομένων πρέπει να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τη νομοθεσία περί προστασίας δεδομένων, συμπεριλαμβανομένων των αρχών, των υποχρεώσεών τους και τα δικαιώματα των ατόμων.

Η αρχή της λογοδοσίας είναι το κλειδί για ένα αποτελεσματικό πλαίσιο προστασίας δεδομένων. Συγκεντρώνει όλες τις άλλες αρχές και θέτει την ευθύνη σε

όσους επεξεργάζονται τα δεδομένα των ανθρώπων (είτε πρόκειται για μια εταιρεία είτε για μια δημόσια αρχή) ώστε να είναι υπεύθυνοι και να αποδείξουν την τήρηση των υποχρεώσεών τους. Στην πράξη, αυτό σημαίνει ότι όσοι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι πιο ανοικτοί και ενεργοί όσον αφορά τον τρόπο με τον οποίο χειρίζονται δεδομένα σύμφωνα με τις υποχρεώσεις τους. Πρέπει να είναι σε θέση να εξηγήσουν, να δείξουν και να αποδείξουν ότι σέβονται το απόρρητο των πολιτών - τόσο στους ρυθμιστές όσο και στους ιδιώτες. Η σπουδαιότητα της αρχής της λογοδοσίας είναι σαφέστερη όταν εξετάζεται το πλαίσιο στο οποίο δεν υπάρχουν μηχανισμοί λογοδοσίας - δηλαδή όταν δεν υπάρχει δομή για την αναφορά παραβιάσεων του νόμου.

Οι μηχανισμοί λογοδοσίας διαδραματίζουν σημαντικό ρόλο στη διερεύνηση των παραβάσεων και στην κατοχή οντοτήτων που υπόκεινται στον νόμο για λογοδοσία.

2.2 Τι είναι το GDPR

Ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation - GDPR) είναι η νέα νομοθεσία για την προστασία δεδομένων που καταστάθηκε επιβεβλημένη σε όλη την Ευρωπαϊκή Ένωση τον Μάιο του 2018. Το GDPR ενισχύει την προστασία των προσωπικών δεδομένων των ατόμων στην Ευρωπαϊκή Ένωση και απλοποιεί το δίκαιο των δεδομένων στην Ευρωπαϊκή Ένωση. Αυτό έγινε τη χρονική περίοδο κατά την οποία οι αναδυόμενες τεχνολογίες (όπως το Cloud Computing, τα μεγάλα δεδομένα, το

Διαδίκτυο των πραγμάτων, η τεχνητή νοημοσύνη, το VR / AR) παράγουν ένα τεράστιο όγκο δεδομένων και οι συνέπειες για την προστασία δεδομένων είναι σημαντικές, αλλά ασαφείς. Ο αντίκτυπος του GDPR στους ευρωπαϊκούς και μη ευρωπαϊκούς οργανισμούς είναι σημαντικός. Ωστόσο, μέχρι σήμερα πολλοί οργανισμοί δεν γνωρίζουν ακόμη τη νέα νομοθεσία και την πολυπλοκότητά της, ενώ άλλοι εξακολουθούν να εστιάζουν στο πρώτο στάδιο υλοποίησης. Ένας μεγάλος αριθμός οργανισμών αναμένεται να μην είναι συμβατοί με το GDPR και, ως εκ τούτου, ενδέχεται να εκτεθούν στις νέες υψηλές κυρώσεις που εισήχθησαν (Addis & Kutar, 2018).

Το GDPR εγκρίθηκε τον Απρίλιο του 2016 μετά από τέσσερα χρόνια συζητήσεων. Καταστάθηκε εκτελέσιμο στις 25 Μαΐου 2018 παρέχοντας ενιαία προστασία δεδομένων εντός της Ευρωπαϊκής Ένωσης και αποτελεί την πρώτη επικαιροποίηση των κανονισμών για την προστασία δεδομένων από τον νόμο περί προστασίας δεδομένων / DPA 1998 (Gov.UK, 1998) (Οδηγία 95/46 / EC του Ευρωπαϊκού Κοινοβουλίου, 1995). Το GDPR αναμένεται να επηρεάσει τόσο την ασφάλεια των δεδομένων όσο και τα αποτελέσματα των επιχειρήσεων. Η εφαρμογή του μπορεί να είναι δαπανηρή και χρονοβόρα όταν οι οργανισμοί πρέπει να εφαρμόσουν λύσεις για την πρόληψη επιθέσεων, την ανάλυση και την ταχεία αντίδραση σε παραβιάσεις, αν και το κόστος εξαρτάται από τα σημερινά επίπεδα οργανωτικής συμμόρφωσης με τη νομοθεσία προστασίας δεδομένων. Σύμφωνα με το Dell Software (2016), οι εταιρείες ψηφιακής τεχνολογίας / πληροφορικής δεν είχαν γενική ευαισθητοποίηση σχετικά με το GDPR: το 97% των εταιρειών δεν είχε σχέδιο προετοιμασίας για το GDPR και μόνο το 9% των επαγγελματιών πληροφορικής και επιχειρήσεων ήταν πεπεισμένοι ότι θα είναι πλήρως έτοιμοι το Μάιο 2018 (Addis & Kutar, 2018).

Μια πρόσφατη έρευνα που διεξήχθη από τη διεθνή δικηγορική εταιρεία Paul Hastings και δημοσιεύθηκε από την Computer Week (Ashford, 2018) υποδεικνύει ότι πάνω από το 90% των αμερικανικών και βρετανικών εταιρειών πιστεύουν ότι θα συμμορφωθούν τον Μάιο του 2018. Ωστόσο, η ίδια έρευνα δείχνει άλλα ανησυχητικά δεδομένα. Μόνο το 39% των εταιρειών του Ηνωμένου Βασιλείου και το 47% των εταιρειών των υπολοίπων κρατών έχουν υλοποιήσει έργα GDPR, ενώ μόνο το ένα τρίτο λαμβάνει συγκεκριμένη υποστήριξη από τρίτους για την εφαρμογή του GDPR (Addis & Kutar, 2018).

Σύμφωνα με το Άρθρο 1 ΓΚΠΔ/ Άρθρο 1 Οδηγίας 2016/680/ΕΕ, αντικείμενο του παρόντος νόμου είναι η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων και ιδίως του δικαιώματος προστασίας προσωπικών δεδομένων.

2.3 Πεδίο εφαρμογής

Σύμφωνα με το Άρθρο 2 του ΓΚΠΔ/Άρθρο 2 Οδηγίας 680, σχετικά με το πεδίο εφαρμογής ισχύουν τα εξής: «Οι ρυθμίσεις του Κανονισμού (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων- εφεξής Κανονισμός) και του παρόντος νόμου

εφαρμόζονται στην, εν όλω η εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται η πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Οι ρυθμίσεις του Κανονισμού και του Κεφαλαίου Β' εφαρμόζονται με την επιφύλαξη της εφαρμογής ειδικότερων ρυθμίσεων των άρθρων 16 έως 19 του κεφαλαίου Β' του παρόντος νόμου.

Οι ρυθμίσεις της Οδηγίας 2016/680/ΕΕ και του κεφαλαίου Γ' του παρόντος εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της διακρίβωσης η της δίωξης εγκλημάτων η της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

Οι ρυθμίσεις του κεφαλαίου Γ' τους παρόντος εφαρμόζονται και στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις κατά περίπτωση αρμόδιες αρχές για τους σκοπούς της εθνικής ασφάλειας.

Όταν τα δεδομένα προσωπικού χαρακτήρα υφίστανται επεξεργασία από τις αρμόδιες αρχές για σκοπούς διαφορετικούς από τους αναφερόμενους στις παραγράφους 3 και 4 του παρόντος άρθρου , όπως η αρχειοθέτηση προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς , εφαρμόζεται ο Κανονισμός και οι ρυθμίσεις του Κεφαλαίου Β.

Οι ρυθμίσεις του Κανονισμού, της Οδηγίας 2016/680/ΕΕ και των Κεφαλαίων Β' και Γ' του παρόντος νόμου εφαρμόζονται και ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από τα δικαστήρια και τις

εισαγγελικές αρχές. Δεν εφαρμόζονται οι ρυθμίσεις που αφορούν την άσκηση των εξουσιών και καθηκόντων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όταν τα δικαστήρια και οι εισαγγελικές αρχές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο της άσκησης της δικαιοδοτικής αρμοδιότητάς τους .

Ο Κανονισμός και ο παρών νόμος δεν εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας. Ως τέτοια δραστηριότητα νοείται εκείνη που αναφέρεται στο ιδιωτικό πεδίο δράσης ενός προσώπου ή μιας οικογένειας, δηλαδή εκείνη που δεν εμπίπτει στην επαγγελματική ή/και εμπορική δραστηριότητα και δεν έχει ως σκοπό η ως αποτέλεσμα τη συστηματική διαβίβαση ή τη διάδοση δεδομένων σε τρίτους.

Οι ρυθμίσεις του Κανονισμού και του παρόντος νόμου εφαρμόζονται ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπεύθυνο επεξεργασίας ή/και εκτελούντα επεξεργασία, εφόσον αυτή λαμβάνει χώρα στην ελληνική επικράτεια ή στο πλαίσιο εγκατάστασης στην ελληνική επικράτεια, ακόμη και εάν η εν λόγω επεξεργασία λαμβάνει χώρα εκτός ελληνικής επικράτειας».

2.4 Νομοθεσία – Διατάξεις

Το GDPR επισημοποιεί ορισμένες έννοιες που έχουν ήδη αναπτυχθεί μέσω των δικαστηρίων και παρέχει μεγαλύτερη υπευθυνότητα και διαφάνεια (Kolah &

Foss). Στη συνέχεια περιγράφονται οι τομείς αλλαγών απέναντι στην ισχύουσα νομοθεσία.

1. *Παγκόσμια εμβέλεια*

Η νέα νομοθεσία για την προστασία δεδομένων έχει παγκόσμια εφαρμογή. Εφαρμόζεται σε οντότητες και υποκείμενα που εδρεύουν στην ΕΕ και σε οντότητες που εδρεύουν εκτός ΕΕ και χειρίζονται τους πολίτες της ΕΕ και τα δεδομένα των κατοίκων (άρθρο 3). Επομένως, οι μη κοινοτικοί οργανισμοί που επεξεργάζονται δεδομένα ατόμων που βρίσκονται στην Ευρωπαϊκή Ένωση και δραστηριοποιούνται στην Ευρώπη πρέπει να συμμορφώνονται με τον νέο κανονισμό.

2. *Ορισμός των προσωπικών δεδομένων*

Σύμφωνα με το άρθρο 4 παράγραφος 1 [...] κάθε πληροφορία σχετικά με αναγνωρισμένο ή αναγνωρίσιμο (ζωντανό) φυσικό πρόσωπο («υποκείμενο των δεδομένων») ... μπορεί να προσδιοριστεί, άμεσα ή έμμεσα ... με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, ένας αριθμός αναγνώρισης, ένα ηλεκτρονικό αναγνωριστικό ή ένας ή περισσότεροι παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, πνευματική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου. Ο ορισμός περιλαμβάνει ψηφιακά αποτυπώματα, όπως διευθύνσεις IP και cookies, τα οποία είναι εξαιρετικά σημαντικά για το μάρκετινγκ βάσει τοποθεσίας και την ασφάλεια των δεδομένων.

Σύμφωνα με το άρθρο 9, ο ορισμός των Ευαίσθητων Προσωπικών Δεδομένων (ειδικές κατηγορίες προσωπικών δεδομένων) διευρύνεται επίσης, με τη συμπερίληψη των γενετικών και βιομετρικών δεδομένων. Η παράγραφος 51 προβλέπει, για παράδειγμα, ότι η επεξεργασία των φωτογραφιών δεν πρέπει συστηματικά να

θεωρείται επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι καλύπτονται από τον ορισμό των βιομετρικών δεδομένων μόνον όταν υποβάλλονται σε επεξεργασία μέσω ειδικών τεχνικών μέσων που επιτρέπουν τη μοναδική αναγνώριση ή επικύρωση φυσικού προσώπου. Αυτά τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να υποβάλλονται σε επεξεργασία, εκτός εάν επιτρέπεται η επεξεργασία σε συγκεκριμένες περιπτώσεις που ορίζονται στον παρόντα κανονισμό (π.χ. όταν είναι προς το δημόσιο συμφέρον των κρατών μελών).

3. *Συγκατάθεση*

Σε περίπτωση που δοθεί συγκατάθεση για τη συλλογή, επεξεργασία και διαγραφή δεδομένων, πρέπει να είναι συγκεκριμένη, ενημερωμένη, ελεύθερη, σαφής και καταφατική (η σιωπή ή τα τετραγωνίδια δεν μπορούν να χρησιμοποιηθούν για τη λήψη συγκατάθεσης και η συγκατάθεση πρέπει να καταγράφεται και να αποθηκεύεται για σκοπούς ελέγχου) . Η συγκατάθεση μπορεί να αποσυρθεί ανά πάσα στιγμή και είναι επίσης εύκολη η ανάκληση της έγκρισης (άρθρο 7).

4. *Αιτήματα πρόσβασης υποκειμένων (Subject Access Requests - SAR)*

Τα υποκείμενα δεδομένων μπορούν να ζητήσουν πρόσβαση σε προσωπικά δεδομένα. Υπάρχει μια νέα, συντομότερη προθεσμία για τους οργανισμούς να απαντήσουν (30 ημέρες και όχι 40) και μπορεί να ζητηθεί όχι μόνο εγγράφως.

5. *Φορητότητα δεδομένων*

Παρέχεται ένα νέο δικαίωμα εξαγωγής δεδομένων σε μηχανικά αναγνώσιμο μορφότυπο και μεταφορά σε άλλο ελεγκτή (άρθρο 20).

6. Εκτεταμένο δικαίωμα για διαγραφή

Το δικαίωμα των υποκειμένων των δεδομένων να ζητούν από τις οντότητες (τόσο ελεγκτές όσο και επεξεργαστές) να διαγράψουν και να καταστρέψουν τα προσωπικά τους δεδομένα επεκτείνεται και μπορεί να ζητηθεί όχι μόνο για σελίδες αναζήτησης (σύμφωνα με την οδηγία 95) αλλά και σε άλλες περιπτώσεις (Άρθρο 18). Το δικαίωμα αυτό δεν είναι απόλυτο δικαίωμα αλλά μπορεί να ζητηθεί σε συγκεκριμένη περίπτωση, για παράδειγμα όταν: τα δεδομένα υποβλήθηκαν σε παράνομη επεξεργασία ή η διατήρηση των δεδομένων δεν είναι πλέον απαραίτητη (σε σχέση με τον αρχικό σκοπό) ή είναι απαραίτητη για να συμμορφωθεί με νομική υποχρέωση. Σύμφωνα με το GDPR, η παρούσα αδικαιολόγητη και ουσιαστική ζημία ή αγωνία δεν αποτελεί απαραίτητη προϋπόθεση για την άσκηση αυτού του δικαιώματος. Ωστόσο, εάν η επεξεργασία προκαλεί ζημιά ή αγωνία, αυτό είναι πιθανό να καταστήσει την περίπτωση για διαγραφή ισχυρότερη. Τα Υποκείμενα Δεδομένων μπορούν επίσης να αντιταχθούν στη μεταποίηση (όπου δεν υπάρχει νόμιμο έννομο συμφέρον να συνεχίσουν να το κάνουν) ή να αποσύρουν τη συγκατάθεσή τους. (ICO, 2017, σελ. 19)

7. Αυτοματοποιημένες αποφάσεις, προφίλ και δικαιώματα στην επεξήγηση

Το GDPR εισάγει νέες απαιτήσεις για μεγαλύτερη διαφάνεια και πιο ατομικό έλεγχο. Το GDPR εισάγει τον ορισμό του προφίλ (συλλογή πληροφοριών για ένα άτομο ή ομάδα ατόμων και ανάλυση των χαρακτηριστικών τους ή των προτύπων συμπεριφοράς ώστε να τοποθετηθούν σε μια συγκεκριμένη κατηγορία ή ομάδα και / ή να προβούν σε προβλέψεις ή εκτιμήσεις σχετικά με την ικανότητά τους να εκτελούν νέα δικαιώματα), νέα δικαιώματα για τα πρόσωπα στα οποία αναφέρονται τα

δεδομένα και υποχρεώσεις των ελεγκτών (δικαιώματα εξήγησης και δικαίωμα να ζητηθεί η παρέμβαση του ανθρώπου).

8. Ελεγκτής και επεξεργαστής

Στο πλαίσιο του GDPR και οι δύο έχουν συγκεκριμένες ευθύνες, μια επέκταση στην τρέχουσα κατάσταση.

9. Υπεύθυνος προστασίας δεδομένων (Data Protection Officer - DPO)

Ο Υπεύθυνος προστασίας δεδομένων είναι ένας ανεξάρτητος ρόλος του GDPR σε έναν οργανισμό για την ενημέρωση, την παροχή συμβουλών και την παρακολούθηση της συμμόρφωσης. Ορισμένες οργανώσεις πρέπει να έχουν έναν υπεύθυνο προστασίας δεδομένων (DPO): εάν είναι δημόσια αρχή (εκτός από τα δικαστήρια που ενεργούν υπό την ιδιότητά τους ως δικαστές), εάν πραγματοποιούν μεγάλης κλίμακας συστηματική παρακολούθηση ατόμων (για παράδειγμα, παρακολούθηση συμπεριφορών στο διαδίκτυο), εάν διεξάγουν επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων ή δεδομένων σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις.

10. Υποχρέωση αναφοράς παραβιάσεων εντός 72 ωρών

Οι παραβιάσεις δεδομένων (π.χ. cyberattacks ή απώλειες φορητών υπολογιστών ή κινητών τηλεφώνων) πρέπει να δηλώνονται εντός 72 ωρών από την ενημέρωσή τους τόσο για τους ρυθμιστές όσο και για τους ιδιώτες "εκτός εάν η παραβίαση προσωπικών δεδομένων είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων "(άρθρο 33) ή αν" τα δεδομένα είναι ανώνυμα ή κρυπτογραφημένα ". Εάν ο οργανισμός δεν αναφέρει

παραβίαση, αυτό θα έχει ως αποτέλεσμα ένα διπλό πρόστιμο (για παραβίαση και επικοινωνία που λείπει).

11. Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων (Data Protection Impact Assessments - DPIA)

Οι οργανισμοί πρέπει να εκτελούν ένα έγγραφο DPIA προκειμένου να κατανοήσουν τους πιθανούς κινδύνους από την επεξεργασία δεδομένων (άρθρο 35). Απαιτούνται στις εξής περιπτώσεις:

- Συστηματικές και εκτεταμένες δραστηριότητες επεξεργασίας, συμπεριλαμβανομένης της μορφοποίησης και, σε περίπτωση αποφάσεων που παράγουν έννομα αποτελέσματα για τους ιδιώτες (άρθρο 35 α)

- επεξεργασία μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων ή προσωπικών δεδομένων σε σχέση με ποινικές καταδίκες ή αδικήματα, συμπεριλαμβανομένης της επεξεργασίας σημαντικού αριθμού προσωπικών δεδομένων σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο ... που πλήττει μεγάλο αριθμό ατόμων και συνεπάγεται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες (αιτιολογική σκέψη 91).

- Μεγάλη κλίμακα, συστηματική παρακολούθηση των δημόσιων χώρων (δηλ. Μέσω της χρήσης CCTV) (ICO, 2017)

12. Προστασία απορρήτου από το σχεδιασμό και από προεπιλογή

Η προστασία των δεδομένων πρέπει να λαμβάνεται υπόψη από την αρχή κάθε έργου (άρθρο 25.1) και ο υπεύθυνος της επεξεργασίας πρέπει να διασφαλίζει ότι,

"τυγχάνουν επεξεργασίας μόνο δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό της επεξεργασίας" (άρθρο 25.2).

Από προεπιλογή, η υψηλότερη ρύθμιση απορρήτου θα πρέπει να εφαρμόζεται αυτόματα σε ένα νέο προϊόν και, από προεπιλογή, τα προσωπικά δεδομένα θα πρέπει να διατηρούνται μόνο για τον απαιτούμενο χρόνο.

13. Υψηλές κυρώσεις

Οι οργανισμοί καλούνται να αποδείξουν τον τρόπο συμμόρφωσής τους με το GDPR και οι αρχές προστασίας δεδομένων μπορούν να αξιολογήσουν τον τρόπο με τον οποίο χρησιμοποιούν προσωπικά δεδομένα (έλεγχος). Τα διοικητικά πρόστιμα σε περίπτωση μη συμμόρφωσης έχουν αυξηθεί σημαντικά.

Οι ρυθμιστικές αρχές μπορούν να επιβάλλουν:

- Πρόστιμα έως 10 εκατ. Ευρώ ή έως 2% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως σε περιπτώσεις ελαφρών παραβάσεων (άρθρο 83 παράγραφος 4).

- Πρόστιμα πάνω από € 20 εκατ. ή μέχρι 4% του συνολικού ετήσιου κύκλου εργασιών παγκοσμίως σε περίπτωση μεγάλων παραβάσεων (άρθρο 83.5) και σε περίπτωση μη συμμόρφωσης με εντολή της εποπτικής αρχής.

Μπορούμε να διαπιστώσουμε ότι στο πλαίσιο του GDPR υπάρχουν ορισμένες πρόσθετες απαιτήσεις για τους οργανισμούς και έχουν ενισχυθεί ορισμένοι υφιστάμενοι τομείς.

2.5 Προστασία της ιδιωτικής ζωής από τεχνική άποψη

Στον σημερινό κόσμο των ψηφιακών υπηρεσιών, της κοινωνικής δικτύωσης και του Διαδικτύου των πραγμάτων βιώνουμε μια άνευ προηγουμένου συλλογή μεγάλης κλίμακας και περαιτέρω επεξεργασία προσωπικών δεδομένων. Αυτή η νέα κοινωνία που βασίζεται στα δεδομένα εισάγει ορισμένες σοβαρές ανησυχίες όσον αφορά την προστασία της ιδιωτικής ζωής, συμπεριλαμβανομένων των εκτεταμένων δυνατοτήτων ηλεκτρονικής επιτήρησης, μορφοποίησης προφίλ και γνωστοποίησης ιδιωτικών πληροφοριών.

Η προστασία της ιδιωτικής ζωής από το σχεδιασμό παρουσιάστηκε για πρώτη φορά από τον Επίτροπο Πληροφοριών και Προστασίας Προσωπικών Δεδομένων του Οντάριο και αφορούσε την ενσωμάτωση των μέτρων προστασίας της ιδιωτικής ζωής και των τεχνολογιών ενίσχυσης της ιδιωτικής ζωής (PETs) απευθείας στο σχεδιασμό των τεχνολογιών και των συστημάτων πληροφορικής. Σήμερα, η προστασία της ιδιωτικής ζωής από το σχεδιασμό ή η προστασία των δεδομένων της από τη σχεδίασή της ως παραλλαγή θεωρείται ως μια πολύπλευρη έννοια, η οποία περιλαμβάνει διάφορα τεχνολογικά και οργανωτικά στοιχεία, τα οποία εφαρμόζουν αρχές προστασίας προσωπικών δεδομένων και δεδομένων σε συστήματα και υπηρεσίες.

Ο κανονισμός για την γενική προστασία δεδομένων (GDPR) αντιμετωπίζει για πρώτη φορά την προστασία δεδομένων από το σχεδιασμό ως νομική υποχρέωση για τους υπεύθυνους επεξεργασίας δεδομένων και επεξεργαστές δεδομένων, αναφέροντας ρητά την ελαχιστοποίηση των δεδομένων και την πιθανή χρήση ψευδωνυμοποίησης. Εκτός αυτού, εισάγει την υποχρέωση προστασίας των δεδομένων από προεπιλογή, προχωρώντας σε περαιτέρω πρόβλεψη της προστασίας

των προσωπικών δεδομένων ως περιουσιακού στοιχείου των συστημάτων και των υπηρεσιών.

Ο γενικός κανονισμός για την προστασία των δεδομένων (GDPR), αποσκοπεί στην αντιμετώπιση αυτών των κινδύνων ενισχύοντας τα δικαιώματα των ατόμων στην ψηφιακή εποχή και επιτρέποντάς τους να ελέγχουν καλύτερα τα προσωπικά τους δεδομένα στο διαδίκτυο. Παράλληλα, οι εκσυγχρονισμένοι και ενοποιημένοι κανόνες θα επιτρέψουν στις επιχειρήσεις να αξιοποιήσουν στο έπακρο τις ευκαιρίες της ψηφιακής ενιαίας αγοράς (DSM) που επωφελείται επίσης από την αυξημένη εμπιστοσύνη των καταναλωτών.

Ωστόσο, η ρύθμιση από μόνη της δεν μπορεί να εγγυηθεί προστασία στο εξελισσόμενο μεγάλο περιβάλλον επεξεργασίας δεδομένων, εάν δεν εφαρμόζεται σωστά, παρακολουθείται και επιβάλλεται. Αυτό πραγματοποιείται όπου η τεχνολογία μπορεί να διαδραματίσει καθοριστικό ρόλο προσφέροντας πρακτικά εργαλεία προστασίας της ιδιωτικής ζωής και υποστηρίζοντας την εφαρμογή των νομικών διατάξεων.

Ο ENISA εργάζεται στον τομέα των τεχνολογιών προστασίας της ιδιωτικής ζωής τα τελευταία χρόνια, ακολουθώντας μια προσέγγιση μηχανικής. Ο ENISA εργάζεται ακριβώς σε αυτή τη γραμμή τεχνολογίας για την προστασία της ιδιωτικής ζωής στον κόσμο του διαδικτύου και του κινητού. Για το σκοπό αυτό, εστιάζει ιδιαίτερα στην έννοια της ιδιωτικής ζωής από τη σχεδίαση ως θεμελιώδη αρχή της ενσωμάτωσης των εγγυήσεων προστασίας δεδομένων στο επίκεντρο των νέων ηλεκτρονικών προϊόντων και υπηρεσιών. Σε αυτό το πλαίσιο, εξετάζονται επίσης τεχνολογίες βελτίωσης της ιδιωτικής ζωής (PETs) που μπορούν να υποστηρίξουν την ενσωμάτωση της ιδιωτικής ζωής σε συστήματα και υπηρεσίες. Επιπλέον, αναλύονται

και προτείνονται μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων, ακολουθώντας μια προσέγγιση βασισμένη στον κίνδυνο. Ιδιαίτερη έμφαση δόθηκε στα κρυπτογραφικά πρωτόκολλα και εργαλεία και στην πιθανή εφαρμογή τους σε πραγματικές εφαρμογές. Οι παραβιάσεις προσωπικών δεδομένων είναι ένας άλλος τομέας εστίασης, ο οποίος αντιμετωπίζει ιδιαίτερα τις μεθόδους και τα εργαλεία αναφοράς και διαχείρισης αναφορών. Τέλος, εξετάζονται πιθανοί μηχανισμοί για την προστασία των online δεδομένων, συμπεριλαμβανομένων των εργαλείων διαφάνειας και ελέγχου, μηχανισμών λογοδοσίας, τεχνικών διαγραφής δεδομένων και φορητότητας, ηλεκτρονικών σφραγίδων, καθώς και συστημάτων φήμης (www.enisa.europa.eu).

2.5.1 Αρχές σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υφίστανται επεξεργασία με νόμιμο, δίκαιο και διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, δικαιοσύνη και διαφάνεια»), να συλλέγονται για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασυμβίβαστο προς τους σκοπούς αυτούς. Η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης για λόγους γενικού συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1, δεν θεωρείται ασυμβίβαστη με τους αρχικούς σκοπούς («περιορισμός του σκοπού»).

Επίσης τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή, σχετικά και περιορισμένα σε ό, τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους

οποίους υποβάλλονται σε επεξεργασία («ελαχιστοποίηση των δεδομένων»). Πρέπει να είναι ακριβή και, όπου χρειάζεται, ενημερωμένα. Πρέπει να λαμβάνεται κάθε εύλογο μέτρο ώστε να διασφαλίζεται ότι τα δεδομένα που είναι ανακριβή, λαμβανομένων υπόψη των σκοπών για τους οποίους υποβάλλονται σε επεξεργασία, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση («ακρίβεια»).

Επιπροσθέτως, τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό των προσώπων στα οποία αναφέρονται τα δεδομένα για χρονικό διάστημα που δεν υπερβαίνει το χρονικό διάστημα που είναι αναγκαίο για τους σκοπούς για τους οποίους διεκπεραιώνονται τα δεδομένα προσωπικού χαρακτήρα. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερες χρονικές περιόδους, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία αποκλειστικά για σκοπούς αρχειοθέτησης για λόγους δημόσιου συμφέροντος, επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1, με την επιφύλαξη της εφαρμογής των κατάλληλων τεχνικών και οργανωτικών μέτρων που απαιτούνται από τον παρόντα κανονισμό για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων («περιορισμός της αποθεματοποίησης»).

Τέλος, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται με τρόπο που εξασφαλίζει την κατάλληλη ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και κατά τυχαίας απώλειας, καταστροφής ή ζημίας, χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα («ακεραιότητα και εμπιστευτικότητα»). Ο υπεύθυνος της επεξεργασίας είναι υπεύθυνος και μπορεί να αποδείξει την τήρηση της παραγράφου 1 («λογοδοσία») (gdpr-info.eu).

2.5.2 Νομιμότητα της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι νόμιμη μόνον εάν και στο βαθμό που ισχύει τουλάχιστον ένα από τα ακόλουθα:

- το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους ειδικούς σκοπούς.

- η επεξεργασία είναι απαραίτητη για την εκτέλεση μιας σύμβασης στην οποία συμμετέχει το πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή για τη λήψη μέτρων κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη της σύμβασης.

- η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με μια νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας.

- η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

- η επεξεργασία είναι αναγκαία για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή για την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

- η επεξεργασία είναι αναγκαία για τους σκοπούς των έννομων συμφερόντων που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο, εκτός εάν τα συμφέροντα ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του προσώπου στο

οποίο αναφέρονται τα δεδομένα απαιτούν προστασία των δεδομένων προσωπικού χαρακτήρα.

Το τελευταίο στοιχείο από τα παραπάνω δεν εφαρμόζεται στην περίπτωση επεξεργασίας που πραγματοποιείται από δημόσιες αρχές κατά την εκτέλεση των καθηκόντων τους.

Ο σκοπός της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που καθορίζεται σε αυτή τη νομική βάση, είναι αναγκαίος για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή για την άσκηση επίσημης αρχής που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Αυτή η νομική βάση μπορεί να περιέχει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τους γενικούς όρους που διέπουν τη νομιμότητα της επεξεργασίας από τον υπεύθυνο επεξεργασίας, τα είδη δεδομένων που υπόκεινται στη μεταποίηση, τα ενδιαφερόμενα πρόσωπα, τις οντότητες και τους σκοπούς για τους οποίους μπορούν να δημοσιοποιηθούν τα προσωπικά δεδομένα, ο περιορισμός του σκοπού, οι περίοδοι αποθήκευσης, καθώς και οι διαδικασίες επεξεργασίας, συμπεριλαμβανομένων μέτρων για τη διασφάλιση νόμιμης και δίκαιης επεξεργασίας.

Όταν η επεξεργασία για σκοπό διαφορετικό από εκείνον για τον οποίο συλλέχθηκαν τα προσωπικά δεδομένα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή σε νόμο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των στόχων στους οποίους αναφέρεται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος της επεξεργασίας, για να διαπιστώσει κατά πόσο η μεταποίηση για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέχθηκαν αρχικά τα προσωπικά δεδομένα, λαμβάνει υπόψη, μεταξύ άλλων:

- κάθε σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα προσωπικά δεδομένα και των σκοπών της προβλεπόμενης περαιτέρω επεξεργασίας,

- το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των προσώπων στα οποία αναφέρονται τα δεδομένα και του υπεύθυνου επεξεργασίας,

- τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως κατά πόσον οι ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα υφίστανται επεξεργασία σύμφωνα με το άρθρο 9 ή κατά πόσον τα δεδομένα προσωπικού χαρακτήρα σχετικά με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

- τις πιθανές συνέπειες της προβλεπόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

- την ύπαρξη κατάλληλων διασφαλίσεων, οι οποίες μπορεί να περιλαμβάνουν κρυπτογράφηση (gdpr-info.eu).

ΚΕΦΑΛΑΙΟ 3: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

3.1 Τι είναι η Τεχνητή Νοημοσύνη

Ο όρος «Τεχνητή Νοημοσύνη» (Artificial Intelligence) περιγράφει τον ευρύτερο στόχο της ενδυνάμωσης των συστημάτων ηλεκτρονικών υπολογιστών να εκτελούν καθήκοντα που συνήθως απαιτούν ανθρώπινη νοημοσύνη, όπως η οπτική αντίληψη, η αναγνώριση ομιλίας, η λήψη αποφάσεων και η μετάφραση μεταξύ των γλωσσών (English Oxford Living Dictionaries). Αυτός ο όρος περιλαμβάνει μια ευρεία ποικιλία τεχνικών καινοτομιών, καθεμιά από τις οποίες μπορεί να παρουσιάσει ξεχωριστές προκλήσεις στα υφιστάμενα εργαλεία προστασίας δεδομένων. Τα περισσότερα συστήματα Τεχνητής Νοημοσύνης που χρησιμοποιούνται σήμερα αφορούν συστήματα υπολογιστών που εκτελούν διακριτές εργασίες - για παράδειγμα, παίζοντας παιχνίδια, αναγνωρίζοντας εικόνες ή επαληθεύοντας ταυτότητα - προσδιορίζοντας πρότυπα σε μεγάλες ποσότητες δεδομένων. Η μαθηματική έννοια της Τεχνητής Νοημοσύνης χρονολογείται από τη δεκαετία του 1950, αλλά έχει βρει εφαρμογές πραγματικού κόσμου τα τελευταία χρόνια λόγω των προόδων της επεξεργαστικής ισχύος και των τεράστιων ποσοτήτων ψηφιακών δεδομένων που είναι διαθέσιμα για ανάλυση. Ως αποτέλεσμα, η Τεχνητή Νοημοσύνη συνήθως συνδέεται με "μεγάλα δεδομένα".

Υπάρχουν πολλά παραδείγματα narrow artificial intelligence - Τεχνητή Νοημοσύνη που έχει σχεδιαστεί για να εκτελεί μία εργασία ή σειρά καθηκόντων. Η στενή Τεχνητή Νοημοσύνη είναι ακόμα περίπλοκη. Όπως σημειώνουν οι New York Times, ακόμη και τα narrow εργαλεία Τεχνητής Νοημοσύνης μπορεί να είναι

αδιαφανή και μη κατανοητά επειδή περιλαμβάνουν μια χιονοστιβάδα στατιστικής πιθανοφάνειας (Kuang, 2017).

Πιο αμφισβητούμενες είναι οι ανησυχίες για την «γενική τεχνητή νοημοσύνη» που παρουσιάζουν προφανώς έξυπνη συμπεριφορά τουλάχιστον τόσο προχωρημένη όσο ένα άτομο σε ολόκληρο το φάσμα των γνωστικών καθηκόντων (Executive Office of the President of the United States, 2016). Όταν ένα σύστημα μπορεί να συμπεριφερθεί με τέτοιο τρόπο ώστε ένας παρατηρητής να μην μπορεί να το διακρίνει από αυτόν ενός ανθρώπου, λέγεται ότι περνάει τη λεγόμενη "δοκιμασία Turing", που εκδόθηκε από τον Alan Turing το 1950.

Συλλογικά, οι τεχνολογίες αυτές περιγράφουν όλο και περισσότερο την πραγματικότητα των σύγχρονων υπολογιστών και τα έθνη σε όλο τον κόσμο έχουν επιδείξει δέσμευση να βρίσκονται στην πρώτη γραμμή της Τεχνητής Νοημοσύνης με την ανακοίνωση φιλόδοξων θεμάτων για την προώθηση της ανάπτυξης τεχνολογιών Τεχνητής Νοημοσύνης. Όπως ανέφερε η Ευρωπαϊκή Επιτροπή στην πρόσφατη έκθεσή της για την Τεχνητή Νοημοσύνη για την Ευρώπη: «Η τεχνητή νοημοσύνη είναι ήδη μέρος της ζωής μας - δεν είναι επιστημονική φαντασία. Από τη χρήση ενός εικονικού προσωπικού βοηθού για να οργανώσουμε την εργάσιμη μέρα μας, για να ταξιδέψουμε σε ένα αυτοκαθοδηγούμενο όχημα, για τα τηλέφωνά μας που προτείνουν τραγούδια ή εστιατόρια που θα θέλαμε, η Τεχνητή Νοημοσύνη είναι πραγματικότητα». Η έκθεση συνεχίζει να σημειώνει το σημαντικό γεγονός ότι «πέρα από το να κάνουμε τη ζωή μας πιο εύκολη, η Τεχνητή Νοημοσύνη μας βοηθά να λύσουμε μερικές από τις μεγαλύτερες προκλήσεις στον κόσμο: από τη θεραπεία χρόνιων παθήσεων ή τη μείωση των ποσοστών θανάτων σε τροχαία ατυχήματα στην καταπολέμηση της κλιματικής αλλαγής ή στην πρόβλεψη απειλών στον κυβερνοχώρο» (Communication from the European Commission, 2018).

Η Τεχνητή Νοημοσύνη και οι σχετικές τεχνολογίες προχωρούν γρήγορα. Όπως και η ατμομηχανή ή η ηλεκτρική ενέργεια στο παρελθόν, η Τεχνητή Νοημοσύνη μετασχηματίζει τον κόσμο μας, την κοινωνία μας και τη βιομηχανία μας (Communication from the European Commission, 2018).

Η Τεχνητή Νοημοσύνη είναι ένας τομέας της επιστήμης των υπολογιστών που αφιερώνεται στην επιδίωξη συστημάτων πληροφορικής που εκτελούν πράξεις ανάλογες με τη μάθηση και τη λήψη αποφάσεων. Τα συστήματα Τεχνητής Νοημοσύνης μιμούνται διάφορες ανθρώπινες λειτουργίες όπως μάθηση, κατανόηση, συλλογιστική και αλληλεπίδραση με ανθρώπους, μηχανές και περιβάλλον (Castro & New, 2016). Ορισμένες μορφές τεχνητής νοημοσύνης που μπορούν να μάθουν να εκτελούν συγκεκριμένα καθήκοντα πολύ καλύτερα από τους ανθρώπους, αλλά η ικανότητά τους για τη μάθηση και την αυτοπεποίθηση περιορίζονται πάντοτε σε ένα εξαιρετικά περιορισμένο εύρος δυνατοτήτων.

Παρόλο που το πεδίο της έρευνας της Τεχνητής Νοημοσύνης χρονολογείται από το τέλος του Δεύτερου Παγκοσμίου Πολέμου, και παρά τα αξιοσημείωτα επιτεύγματα σε τόσους άλλους τομείς της Πληροφορικής, η πρόοδος στην Τεχνητή Νοημοσύνη δεν κατάφερε να συμβαδίσει με τις προσδοκίες. Κατά τη διάρκεια της δεκαετίας του 1950, της δεκαετίας του 1960 και της δεκαετίας του 1970, οι εμπειρογνώμονες της Τεχνητής Νοημοσύνης προέβλεπαν την άνοδο των μηχανών με ανθρώπινη νοημοσύνη που θα συνέβαινε μέσα σε λίγες δεκαετίες ή τουλάχιστον σε μία περίπτωση μέσα σε λίγους μήνες (Castro & New, 2016). Η πρόοδος επιτέλους επιταχύνθηκε κατά τη διάρκεια των τελευταίων χρόνων χάρη στις πρόσφατες εξελίξεις στον αλγοριθμικό σχεδιασμό, τις βελτιώσεις στις δυνατότητες επεξεργασίας δεδομένων και την άνοδο του cloud computing. Το βασικό επίτευγμα ήταν η μηχανική μάθηση, όπου οι αλγόριθμοι χρησιμοποιούν δεδομένα για την αυτόματη και

επαναληπτική κατασκευή νέων αναλυτικών μοντέλων, επιτρέποντάς τους έτσι να μάθουν πώς να επιλύουν τα προβλήματα μέσα σε στενά καθορισμένα πλαίσια χωρίς να προγραμματιστούν ρητά για μια συγκεκριμένη λύση (Castro & Wallace, 2018).

3.2 Λειτουργία

Η Τεχνητή Νοημοσύνη είναι ο τομέας της μελέτης που περιγράφει την ικανότητα της μηχανικής μάθησης ακριβώς όπως οι άνθρωποι και την ικανότητα να ανταποκρίνεται σε ορισμένες συμπεριφορές γνωστές. Η ανάγκη της Τεχνητής Νοημοσύνης αυξάνεται καθημερινά. Από τη στιγμή που η Τεχνητή Νοημοσύνη εισήχθη για πρώτη φορά στην αγορά, υπήρξε η αιτία της ταχείας αλλαγής στον τομέα της τεχνολογίας και των επιχειρήσεων. Οι επιστήμονες των υπολογιστών προβλέπουν ότι μέχρι το 2020, "το 85% των αλληλεπιδράσεων με τους πελάτες θα αντιμετωπιστεί χωρίς άνθρωπο". (Khaled AlSedrah, 2017).

Η Τεχνητή Νοημοσύνη προσφέρει αξιοπιστία, αποδοτικότητα κόστους, επιλύει πολύπλοκα προβλήματα και λαμβάνει αποφάσεις. Επιπλέον, η Τεχνητή Νοημοσύνη περιορίζει τα δεδομένα από το να χαθούν. Η Τεχνητή Νοημοσύνη εφαρμόζεται σήμερα στα περισσότερα πεδία, είτε πρόκειται για επιχειρήσεις είτε για μηχανικούς. Ένα από τα σπουδαία εργαλεία της Τεχνητής Νοημοσύνης ονομάζεται "μάθηση ενίσχυσης", το οποίο βασίζεται στην επιτυχία και την αποτυχία στην πραγματική ζωή για να αυξήσει την αξιοπιστία των εφαρμογών. Δυστυχώς, η Τεχνητή Νοημοσύνη είναι περιορισμένη με τις ικανότητές της και τη λειτουργικότητά της.

Η Τεχνητή Νοημοσύνη βασίζεται κυρίως σε αλγόριθμους και μοντέλα, ως τεχνική που έχει σχεδιαστεί με βάση επιστημονικά ευρήματα όπως τα μαθηματικά, τη στατιστική και τη βιολογία (Khaled AlSedrah, 2017). Η Τεχνητή Νοημοσύνη λειτουργεί με βάση διάφορα μοντέλα όπως: Fuzzy Algorithm, Decision Tree, Genetic Algorithm, Cluster Algorithm, Neural Network, deep learning.

3.3 Εφαρμογές - Δυνατότητες

Η Τεχνητή Νοημοσύνη μπορεί να σχεδιαστεί χρησιμοποιώντας πολλούς αλγορίθμους. Αυτοί οι αλγόριθμοι βοηθούν το σύστημα να προσδιορίσει την αναμενόμενη απόκριση, η οποία βασικά θα πει στον υπολογιστή τι πρέπει να αναμένει και να εργαστεί αναλόγως. Εδώ είναι μερικές από τις μεγαλύτερες εφαρμογές Τεχνητής Νοημοσύνης που πιθανώς χρησιμοποιούμε στην καθημερινή μας ζωή χωρίς να γνωρίζουμε:

- Φωνητική αναγνώριση
- Εικονικοί πράκτορες
- Πλατφόρμα εκμάθησης μηχανών
- Διαχείριση αποφάσεων
- Πλατφόρμα βαθιάς μάθησης
- Biomatters

- Αυτοματοποίηση ρομποτικής διαδικασίας
- Ανάλυση κειμένου (Khaled AlSedrah, 2017).

Η "μηχανική μάθηση" είναι ένα υποσύνολο της Τεχνητής Νοημοσύνης που ο καθηγητής Andrew Ng του Πανεπιστημίου του Stanford έχει ορίσει ως "την επιστήμη της λήψης των ηλεκτρονικών υπολογιστών χωρίς να έχουν προγραμματιστεί ρητά" (www.coursera.org). Ενώ οι όροι μηχανική μάθηση και Τεχνητή Νοημοσύνη χρησιμοποιούνται συχνά εναλλακτικά, νοούνται ως μία μέθοδος για την επίτευξη της Τεχνητής Νοημοσύνης. Η μηχανική μάθηση χρησιμοποιεί στατιστικές τεχνικές για να δώσει στους υπολογιστές τη δυνατότητα να "μαθαίνουν" - να βελτιώνουν προοδευτικά την απόδοση του μηχανήματος δημιουργώντας νέους μαθηματικούς αλγορίθμους - από μεγάλους όγκους δεδομένων χωρίς να έχουν προγραμματιστεί ρητά. Αντί να ακολουθεί απλώς τις οδηγίες, όπως κάνουν οι παραδοσιακοί υπολογιστές, η μηχανική μάθηση κάνει προβλέψεις και συστάσεις βασισμένες σε πρότυπα που ανιχνεύονται σε σύνολα δεδομένων εκπαίδευσης. Η μηχανική μάθηση αποτελεί τη βάση άλλων εργαλείων και χρησιμοποιείται ευρέως σήμερα για την εκτέλεση πολυάριθμων εργασιών, όπως ανίχνευση απάτης, φιλτράρισμα ηλεκτρονικού ταχυδρομείου, ανίχνευση cyberthreats όπως εισβολείς δικτύου, συνιστώμενα βιβλία ή ταινίες κτλ. Η μηχανική μάθηση είναι η τεχνολογία πίσω από το Cue, το ρομποτικό παίκτη μπάσκετ της Toyota που έχει τέλεια γυρίσματα με ακρίβεια και ξεπερνά τα μεγαλύτερα ονόματα του NBA (Camparo, 2018).

Η deep learning είναι ένας τύπος μηχανικής μάθησης, εμπνευσμένος από τα νευρωνικά δίκτυα του ανθρώπινου εγκεφάλου, για να επεξεργάζεται κρυμμένα επίπεδα πληροφοριών και να καταλήγει σε ένα συμπέρασμα. Η βαθιά εκμάθηση χρησιμοποιεί πολλαπλά στρώματα τεχνητών νευρωνικών δικτύων για την

προσομοίωση της λήψης αποφάσεων ενός ανθρώπου. Αυτή η τεχνολογία βρίσκεται στην καρδιά πολλών εφαρμογών Τεχνητής Νοημοσύνης που αναπτύσσονται σήμερα και επιτρέπει τεχνολογίες όπως η όραση μέσω υπολογιστή, η ταξινόμηση κειμένων, η αναγνώριση προτύπων, η κατανόηση ομιλίας και οι προγνωστικές συστάσεις. Η βαθιά εκμάθηση κατέστησε δυνατή την ύπαρξη τεχνολογιών φωνητικής αναγνώρισης σε όλη την καθημερινότητά μας - σε smartphones, ψηφιακούς βοηθούς, συστήματα οικιακής ασφάλειας που λειτουργούν με Τεχνητή Νοημοσύνη και άλλες έξυπνες συσκευές. Συχνά, η deep learning χρησιμοποιεί μεγαλύτερα σύνολα δεδομένων για τη δημιουργία μεγαλύτερων μοντέλων και την άριστη εκπαίδευση αυτών των μοντέλων.

Η deep learning επέτρεψε την αύξηση της τεχνολογίας που είναι γνωστή ως όραση στον υπολογιστή, όπου οι μηχανές που είναι εξειδικευμένες στην αναγνώριση εικόνας, τη σύγκριση και τον προσδιορισμό μοτίβου "βλέπουν" με ίση ή πολύ μεγαλύτερη οξύτητα από τα ανθρώπινα μάτια, και στη συνέχεια συνδέουν αυτό που βλέπουν με τα δεδομένα που εξετάστηκαν προηγουμένως. Η όραση των υπολογιστών έχει δημιουργήσει προόδους στον τομέα της υγειονομικής περίθαλψης, της εθνικής ασφάλειας, της βοηθητικής περίθαλψης και άλλων διαφόρων τομέων. Για παράδειγμα, στην υγειονομική περίθαλψη, οι αλγόριθμοι σήμερα είναι σε θέση να εκτιμήσουν τον κίνδυνο καρδιακών παθήσεων σε ασθενείς με την ανάλυση των αιμοφόρων αγγείων με σάρωση αμφιβληστροειδούς, ανίχνευση καρκινικών όγκων εξετάζοντας τις CT ανιχνεύσεις, διάγνωση της πνευμονίας με εξέταση των ακτίνων X στο στήθος και να εντοπίζουν τον διαβήτη σε έναν ενήλικα με την εμφάνιση των προβλημάτων του αμφιβληστροειδούς (Timmer, 2018).

Μια άλλη εφαρμογή βοηθά τα άτομα με προβλήματα όρασης να κατανοούν τις εικόνες ή να αντιλαμβάνονται καλύτερα το περιβάλλον τους, περιγράφοντάς τα ως κείμενο ή βοηθώντας τους ανθρώπους που επικοινωνούν με την ακοή,

μεταφράζοντας ομιλούμενες λέξεις στο κείμενο σε μια οθόνη (Microsoft Accessibility Blog, 2017) Ίσως η πιο κοινή καθημερινή εφαρμογή της όρασης υπολογιστή είναι η αναγνώριση προσώπου, η οποία χρησιμοποιείται για να ξεκλειδώνουν έξυπνα τηλέφωνα, στην πρόσθεση ετικετών σε φίλους σε κοινωνικά μέσα δικτύωσης και στην αναζήτηση εικόνων. Η όραση των υπολογιστών έχει επίσης αποδείξει τη χρήση της στον αθλητισμό, καθώς ο αγωνιστικός εξοπλισμός αυτοκινήτων τη χρησιμοποιεί για να βελτιώσει την ασφάλεια των οδηγών. Το γκολφ τη χρησιμοποιεί για να βελτιώσει τις εμπειρίες και την ανάλυση των παικτών και επίσης η Διεθνής Ομοσπονδία Γυμναστικής σκοπεύει να την ενσωματώσει στους Ολυμπιακούς Αγώνες του Τόκιο του 2020 για να βοηθήσει τους κριτές (Zee, 2017; Greenberg, 2018).

Μια άλλη μορφή τεχνολογίας Τεχνητής Νοημοσύνης, η επεξεργασία φυσικής γλώσσας (NLP) κάνει ακριβώς όπως υποδηλώνει το όνομα της - ερμηνεύει και αλληλεπιδρά με το διάλογο σε πραγματικό χρόνο. Ο στόχος του NLP, ο οποίος συχνά συνδυάζεται με τεχνολογίες αναγνώρισης ομιλίας, είναι να αλληλοεπιδρά με τα άτομα μέσω διαλόγου, είτε να αντιδρά σε προτροπές είτε να παρέχει μετάφραση σε πραγματικό χρόνο μεταξύ των γλωσσών. Αυτή η τεχνολογία στηρίζει πολλές συναλλαγές εξυπηρέτησης πελατών. Ο μεταφραστής Τεχνητής Νοημοσύνης της Microsoft είναι σε θέση να μεταφράσει τα κινέζικα στα αγγλικά με "ακρίβεια συγκρίσιμη με αυτή ενός δίγλωσσου προσώπου" (Del Bello, 2018). Αυτοί οι μεταφραστές έχουν πολυάριθμες εφαρμογές που καλύπτουν διάφορους τομείς, γεωγραφικά όρια και πολιτιστικά εμπόδια. Τα κυριότερα μέσα ενημέρωσης βασίστηκαν σε τεχνολογίες βασισμένες στο NLP για τη δημιουργία χιλιάδων ειδήσεων, αθλημάτων και οικονομικών ιστοριών τα τελευταία δύο χρόνια, συμπεριλαμβανομένων περισσότερων από 500 αναφορών στην Washington Post σχετικά με τις εκλογές του 2017 (Keohane, 2017). Επιπρόσθετα, οι εξετάσεις GRE

που χρησιμοποιήθηκαν για εισαγωγή να αποφοιτήσουν τη μελέτη σε πολλούς κλάδους βαθμολογούνται σήμερα από τα συστήματα NLP (Hardesty, 2012).

3.4 Δημόσιες και Ιδιωτικές χρήσεις της Τεχνητής Νοημοσύνης

Οι αξιοσημείωτες εξελίξεις στις εφαρμογές της Τεχνητής Νοημοσύνης έχουν οδηγήσει σε αξιοσημείωτη χρήση της Τεχνητής Νοημοσύνης στον δημόσιο και τον ιδιωτικό τομέα. Όπως η Βρετανική Βουλή των Λόρδων σημείωσε στην πρόσφατη έκθεσή της για την Τεχνητή Νοημοσύνη, η Τεχνητή Νοημοσύνη είναι ένα εργαλείο που είναι ήδη βαθιά ενσωματωμένο στις ζωές μας (publications.parliament.uk). Ως εργαλείο υπολογισμού που μπορεί να ενισχύσει οποιαδήποτε διαδικασία λήψης αποφάσεων, η Τεχνητή Νοημοσύνη δίνει τη δυνατότητα σε εμπειρογνώμονες σε κάθε τομέα να προσφέρουν βελτιωμένες υπηρεσίες και να επιτύχουν πρωτοφανείς ανακαλύψεις. Οι τεχνολογίες της Τεχνητής Νοημοσύνης διευκολύνουν τις εμπορικές αλληλεπιδράσεις και εξατομικευμένες υπηρεσίες και προϊόντα. Τα οφέλη της Τεχνητής Νοημοσύνης καλύπτουν ένα μεγάλο αριθμό τομέων, μερικοί από τους οποίους περιγράφονται παρακάτω.

- Τεχνητή Νοημοσύνη στην Υγεία και την Ιατρική- η Τεχνητή Νοημοσύνη στην υγειονομική περίθαλψη βοηθά στην έρευνα και την πρόληψη των ασθενειών, καθώς και τη διάγνωση και τη θεραπεία των ασθενών. Το Collaborative Cancer Cloud της Intel έχει σχεδιαστεί για να βοηθήσει τους ερευνητές να ανακαλύψουν νέους βιοδείκτες που σχετίζονται με τις διαγνώσεις και την εξέλιξη του καρκίνου (Intel, 2017). Η Τεχνητή Νοημοσύνη χρησιμοποιείται όλο και περισσότερο για εφαρμογές στην ιατρική - αυτό βοηθά τους γιατρούς να βρουν τη σωστή θέση για να λειτουργούν κατά

τη διάρκεια χειρουργικών επεμβάσεων και στην έγκαιρη ανίχνευση ασθενειών (Project InnerEye, 2008).

- Τεχνητή Νοημοσύνη στις μεταφορές - Πολλά σύγχρονα οχήματα περιλαμβάνουν τεχνολογίες Τεχνητής Νοημοσύνης που παρέχουν βοήθεια όταν δημιουργούν αντίγραφα ασφαλείας ή αλλάζουν λωρίδες. Αυτά τα εργαλεία βρίσκονται σε τρένα, πλοία και αεροπλάνα, καθώς και σχεδόν οτιδήποτε κινείται.

- Τεχνητή Νοημοσύνη στις Χρηματοπιστωτικές Υπηρεσίες – η Τεχνητή Νοημοσύνη είναι απαραίτητη για την ανίχνευση και την πρόληψη της απάτης και χρησιμοποιείται από οργανισμούς χρηματοπιστωτικών υπηρεσιών και επιχειρήσεις χρηματοοικονομικής τεχνολογίας, συμπεριλαμβανομένων τραπεζών, πιστωτικών καρτών και άλλων παρόχων υπηρεσιών πληρωμών, για την καταπολέμηση της απάτης και της οικονομικής εγκληματικότητας. Χρησιμοποιείται σήμερα ευρέως για να εντοπίσει τα πρότυπα συνήθων και ασυνήθιστων συμπεριφορών, να εντοπίσει έγκαιρους δείκτες απάτης, να επιτρέψει ταχύτερες και ακριβέστερες οικονομικές αποφάσεις και να παράσχει στους επαγγελματίες των χρηματοπιστωτικών υπηρεσιών βασικές πληροφορίες που ενσωματώνονται ουσιαστικά από μια ποικιλία πηγών.

- Τεχνητή Νοημοσύνη στο Marketing- η Τεχνητή Νοημοσύνη έχει αποδειχθεί χρήσιμη για πιο αποτελεσματικό μάρκετινγκ, βοηθώντας τις εταιρείες να παράγουν στοχευμένες διαφημίσεις σε καταναλωτές που είναι πιθανότερο να ενδιαφέρονται για συγκεκριμένα προϊόντα (και, αντίθετα, να μην επιβαρύνουν τους καταναλωτές με διαφημίσεις για προϊόντα για τα οποία δεν έχουν ενδιαφέρον) .

- Τεχνητή Νοημοσύνη στη γεωργία - Ο γεωργικός τομέας ήταν πρώιμος βιομηχανικός χρήστης της Τεχνητής Νοημοσύνης, βρίσκοντας πολλές εφαρμογές Τεχνητής Νοημοσύνης. Για παράδειγμα, μια ομάδα ερευνητών συνεργάστηκε με τη Microsoft για την ανάπτυξη αλγορίθμων που βοηθούν τους κτηνοτρόφους, προσδιορίζοντας και αναλύοντας πρότυπα για κάθε ζώο (Spencer, 2017).

- Τεχνητή Νοημοσύνη στην Εκπαίδευση και την Κατάρτιση - η Τεχνητή Νοημοσύνη ασχολείται όλο και περισσότερο με την εκπαίδευση και την κατάρτιση. Από μικρή ηλικία, η ρομποτική διδασκαλία είναι διαθέσιμη για να βοηθήσει τα παιδιά να μάθουν αλληλεπιδραστικά. Οι εταιρείες διδασκαλίας σε απευθείας σύνδεση χρησιμοποιούν την Τεχνητή Νοημοσύνη για να αναλύσουν, να αναθεωρήσουν και να προσαρμόσουν τις εμπειρίες ατομικής μάθησης με βάση τεχνικές όπου ο κάθε μαθητής φαίνεται πιο ευαίσθητος (Devlin, 2016). Η Τεχνητή Νοημοσύνη σε ένα έξυπνο σύστημα διδασκαλίας είναι σε θέση να χρησιμοποιήσει τη μηχανική μάθηση για να προσαρμοστεί και να ανταποκριθεί στις ανάγκες των μαθητών σε πραγματικό χρόνο . Η Τεχνητή Νοημοσύνη χρησιμοποιείται επίσης σήμερα για να βοηθήσει στην ταξινόμηση των εξετάσεων και την πρόληψη της λογοκλοπής.

- Τεχνητή Νοημοσύνη στην ηλεκτρονική προστασία- η Τεχνητή Νοημοσύνη βοηθά τους οργανισμούς να παρακολουθούν, εντοπίζουν και μετριάζουν τις απειλές στον κυβερνοχώρο που αντιμετωπίζουν ολοένα και περισσότερο οι κυβερνήσεις, η βιομηχανία και τα άτομα. Αυτό βοηθά στα μακροχρόνια ζητήματα ασφάλειας του κυβερνοχώρου, όπως φίλτρα ανεπιθύμητης αλληλογραφίας, ανίχνευση κακόβουλων αρχείων και σάρωση κακόβουλων ιστοτόπων (Tully, 2018).

- Τεχνητή Νοημοσύνη για τις δημόσιες αρχές και τις δημόσιες υπηρεσίες - Οι εφαρμογές της Τεχνητής Νοημοσύνης χρησιμοποιούνται συστηματικά για την παροχή αποτελεσματικότερων κυβερνητικών υπηρεσιών και για την ενίσχυση της δημόσιας ασφάλειας. Οι εφαρμογές της Τεχνητής Νοημοσύνης βοηθούν την επιβολή του νόμου με την ανίχνευση της απάτης, τον έλεγχο της κυκλοφορίας και τους αλγορίθμους για την πρόβλεψη της υποτροπής και των κινδύνων πτήσης. Χρησιμοποιώντας αναλυτικά στοιχεία πρόβλεψης της εγκληματικότητας, η Τεχνητή Νοημοσύνη έχει συμβάλει στην αποτελεσματική ανάπτυξη της επιβολής του νόμου σε περιοχές όπου είναι πιθανότερο να εμφανιστούν εγκλήματα σε συγκεκριμένες χρονικές στιγμές (Rieland, 2018).

- Τεχνητή Νοημοσύνη για την Προστασία των Δεδομένων - Ενώ κάποιοι μελετητές υποστήριξαν ότι η Τεχνητή Νοημοσύνη αποτελεί απειλή για την προστασία των δεδομένων, άλλοι ισχυρίστηκαν ότι η Τεχνητή Νοημοσύνη μπορεί να προσφέρει ευκαιρίες για περαιτέρω ενίσχυση. Για παράδειγμα, η Τεχνητή Νοημοσύνη μπορεί να βοηθήσει τις εταιρείες να περιορίσουν ή να ελέγξουν ποιος εξετάζει τα δεδομένα ενός ατόμου και να απαντά σε πραγματικό χρόνο για να αποτρέψει την ακατάλληλη χρήση ή κλοπή των δεδομένων. Οι εταιρείες αναπτύσσουν εργαλεία απορρήτου βασισμένα σε Τεχνητή Νοημοσύνη, όπως τα bots για την προστασία της ιδιωτικής ζωής, τα οποία θυμούνται τις προτιμήσεις απορρήτου και προσπαθούν να τα καταστήσουν συνεπή σε διάφορους ιστότοπους, καθώς και τους σαρωτές πολιτικών απορρήτου που προσπαθούν να διαβάσουν και να απλοποιήσουν τις πολιτικές προστασίας προσωπικών δεδομένων. Η Polisis, η οποία σημαίνει «ανάλυση της πολιτικής απορρήτου», είναι Τεχνητή Νοημοσύνη που

χρησιμοποιεί τη μηχανική μάθηση για να «διαβάσει μια πολιτική απορρήτου» που δεν έχει ξαναδεί ποτέ και να εξαγάγει μια ευανάγνωστη περίληψη, που εμφανίζεται σε μια γραφική ροή, για το είδος των δεδομένων που συλλέγει μια υπηρεσία και αν ο χρήστης μπορεί να εξαιρεθεί από αυτή τη συλλογή ή κοινή χρήση (Greenberg, 2018). Η Τεχνητή Νοημοσύνη χρησιμοποιείται επίσης για την προειδοποίηση χρηστών ύποπτων ιστοτόπων, διαφημίσεων και άλλων κακόβουλων δραστηριοτήτων. Τέλος, η Τεχνητή Νοημοσύνη επιτρέπει στις εταιρείες να αναπτύσσουν τεχνολογίες που προστατεύουν περισσότερο την ιδιωτική ζωή των χρηστών. Για παράδειγμα, οι ερευνητές προσπαθούν να αναπτύξουν τεχνικές εκμάθησης μηχανών που αξιολογούν τα κρυπτογραφημένα δεδομένα, βελτιώνοντας έτσι την ιδιωτική ζωή των χρηστών.

ΚΕΦΑΛΑΙΟ 4: Ο ΑΝΤΙΚΤΥΠΟΣ ΤΟΥ GDPR ΣΤΗΝ ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ

4.1 Εισαγωγή

Ο νόμος για την προστασία της ιδιωτικής ζωής και των δεδομένων φαίνεται να είναι ο βασικός τομέας του δικαίου που ασχολείται με τις επιπτώσεις των μηχανών στην κοινωνία (Butterworth, 2018). Η γέννηση της προστασίας των δεδομένων στην Ευρώπη, ιδίως η οδηγία 95/46 / ΕΚ για την προστασία των δεδομένων, συνδέθηκε με τις εντυπωσιακές εξελίξεις της δεκαετίας του '70 (Simitis, 2014). Ήδη από τη θέσπιση της οδηγίας, τα μέσα της δεκαετίας του '90, η ταχεία επέκταση της χρήσης του Διαδικτύου και η εμφάνιση πολλών ηλεκτρονικών υπηρεσιών θέτουν νέες προκλήσεις για τις ρυθμιστικές αρχές. Πέρα από τα οφέλη των ψηφιακών τεχνολογιών, η πραγματικότητα της συλλογής, της επεξεργασίας, της αποθήκευσης και της χρήσης αλλαγών έχει φέρει νέους, πολύ άγνωστους κινδύνους (Burri & Schär, 2016).

Το αυστηρό πλαίσιο προστασίας δεδομένων θεωρήθηκε ξεπερασμένο και δυσκίνητο σε ένα περιβάλλον Internet (πράγματι, Web 2.0), το οποίο είναι "πιο ευάλωτο από ό, τι οι περισσότεροι άνθρωποι πίστευαν" (Hustinx, 2013). Η εξελισσόμενη τεχνολογία και η πανταχού παρούσα φύση της πληροφορικής δημιούργησαν αμέτρητα προβλήματα για την προστασία των προσωπικών δεδομένων, καθώς θέτουν σε κίνδυνο τις θεμελιώδεις αρχές του «παραδοσιακού» νόμου περί προστασίας δεδομένων, όπως η αρχή της παραγραφής ή το μοντέλο προειδοποίησης και συγκατάθεσης (Mantelero, 2014). Η προσαρμογή των νομικών αρχών στη σύγκλιση των "πραγματικών και ψηφιοποιημένων" κόσμων σε έναν απρόσκοπτο χώρο για τα άτομα, μια σύγκλιση που διευκολύνεται από τον συνεχώς

αυξανόμενο αριθμό γεφυρών που δημιουργούνται τόσο από την καινοτόμο χρήση των υφιστάμενων τεχνολογιών όσο και από την ανάπτυξη νέων και αναδυόμενων τεχνολογιών, ήταν η πρόκληση που αντιμετωπίζουν οι ευρωπαίοι νομοθέτες (Mitrou, 2011).

Η σύλληψη του GDPR αποσκοπούσε στην αντιμετώπιση του κινδύνου αύξησης της απώλειας της συνάφειας και της αποτελεσματικότητας της νομοθεσίας της 3ης γενιάς. Εκτός από μια απλή αναθεώρηση της οδηγίας για την προστασία των δεδομένων και λιγότερο από μια αλλαγή κανονιστικού παραδείγματος, ο κανονισμός προσπαθεί να διατηρήσει την πορεία του με τις τεχνολογικές και κοινωνικοοικονομικές αλλαγές, διασφαλίζοντας ταυτόχρονα τα θεμελιώδη δικαιώματα των ατόμων και επιτρέποντας τον έλεγχο των δεδομένων τους. Το GDPR δεν απευθύνεται ειδικά σε AI. Παρόλο που οι δυσκολίες και η πολυπλοκότητα του ψηφιακού περιβάλλοντος έχουν ληφθεί υπόψη από το σχεδιασμό της ρυθμιστικής στρατηγικής για την προστασία δεδομένων, η ρυθμιστική επιλογή στο GDPR συνίσταται περισσότερο σε αυτό που αντιλαμβανόμαστε ως "ανεξάρτητη από τεχνολογία νομοθεσία".

Το GDPR εφαρμόζεται τόσο στη φάση ανάπτυξης της AI όσο και σε σχέση με τη χρήση της για την ανάλυση και τη λήψη αποφάσεων σχετικά με τα άτομα. Το GDPR περιέχει σημαντικά δικαιώματα για τους χρήστες σχετικά με οποιαδήποτε επεξεργασία των προσωπικών τους δεδομένων, καθώς και υποχρεώσεις των μεταποιητών που θα διαμορφώσουν τον τρόπο με τον οποίο θα αναπτυχθεί και θα εφαρμοστεί η AI. Ιδιαίτερα σχετικές με το περιβάλλον AI είναι οι διατάξεις σχετικά με το πεδίο εφαρμογής, τους νομικούς λόγους, τις αρχές προστασίας δεδομένων και την αυτοματοποιημένη λήψη αποφάσεων (Niemitz, 2018).

4.2 Προβλήματα του GDPR στην Τεχνητή Νοημοσύνη

Το GDPR θέτει τρία βασικά προβλήματα στις επιχειρήσεις που χρησιμοποιούν την Τεχνητή Νοημοσύνη: υψηλότερο κόστος, πρακτικούς περιορισμούς και νομικούς κινδύνους. Το υψηλότερο κόστος και οι νομικοί κίνδυνοι δυνητικά θα αποτρέψουν τη χρήση της Τεχνητής Νοημοσύνης εντελώς, ενώ οι πρακτικοί περιορισμοί θα δυσκολέψουν τη χρήση και θα υπονομεύσουν την αποτελεσματικότητά του. Πολλές διατάξεις του GDPR επιβάλλουν άμεσο ή έμμεσο κόστος στη χρήση της Τεχνητής Νοημοσύνης. Για παράδειγμα, η απαίτηση να έχουμε μια ανθρώπινη κριτική σε ορισμένες αλγοριθμικές αποφάσεις επιβάλλει άμεσα σημαντικό κόστος στις επιχειρήσεις που χρησιμοποιούν την Τεχνητή Νοημοσύνη, καθώς το πέρασμα από κάθε λεπτομέρεια μιας αλγοριθμικής απόφασης είναι περίπλοκη και χρονοβόρα εργασία που απαιτεί ιδιαίτερες δεξιότητες. Το δικαίωμα στη φορητότητα των δεδομένων δεν στοχεύει άμεσα την Τεχνητή Νοημοσύνη, αλλά επιβάλλει έμμεσες δαπάνες δημιουργώντας μια υποχρέωση για τις επιχειρήσεις που χρησιμοποιούν την Τεχνητή Νοημοσύνη να επεξεργάζονται και να προμηθεύουν μεγάλα και πολύπλοκα σύνολα δεδομένων σε επαναχρησιμοποιήσιμη μορφή.

Ανάλογα με το πώς ερμηνεύουν οι ρυθμιστικές αρχές και τα δικαστήρια, το GDPR θα μπορούσε να επιβάλει σημαντικούς πρακτικούς περιορισμούς. Για παράδειγμα, το δικαίωμα στην επεξήγηση είναι προβληματικό επειδή, όπως έδειξε η έρευνα, υπάρχει μια ανταλλαγή μεταξύ της ακρίβειας και της διαφάνειας στους αλγορίθμους. Ο περιορισμός του σκοπού είναι επίσης μη πρακτικός για την Τεχνητή Νοημοσύνη, επειδή απαιτεί από τις εταιρείες να λαμβάνουν την άδεια κάθε υποκείμενου δεδομένων προτού κάνει οτιδήποτε καινούργιο με τα δεδομένα τους

χρησιμοποιώντας Τεχνητή Νοημοσύνη, ανεξάρτητα από το αν η επαναδιάταξη θα έχει οποιεσδήποτε επιπτώσεις στην ιδιωτική ζωή ή την ευημερία των καταναλωτών.

Το GDPR κάνει επίσης την Τεχνητή Νοημοσύνη μια νομικά επικίνδυνη προσπάθεια, η οποία θα μετατρέπει ορισμένες εταιρείες μακριά από τη χρήση της σε όλα. Η πολυπλοκότητα του GDPR σημαίνει ότι υπάρχει ένας τεράστιος αριθμός πιθανών σημείων αποτυχίας, όπου οι εταιρείες θα μπορούσαν να παραβιάσουν κατά λάθος το GDPR και έτσι να αντιμετωπίσουν σοβαρά πρόστιμα (Castro & Wallace, 2018).

4.3 Η πολυπλοκότητα του GDPR θα αυξήσει το κόστος χρήσης της Τεχνητής Νοημοσύνης

Στο Ανοικτό Πανεπιστήμιο των Βρυξελλών, ένας οικονομολόγος καλεί το GDPR ως το "πιο περίπλοκο κομμάτι της νομοθεσίας που η ΕΕ έχει παράξει ποτέ" (Siegle, 2018). Το GDPR περιέχει τόσους κανόνες που πρακτικά όλες οι εταιρείες που επεξεργάζονται προσωπικά δεδομένα θα πρέπει να προσλάβουν επαγγελματίες για να τους κρατήσει στη δεξιά πλευρά του νόμου, αποτρέποντας έτσι πόρους που διαφορετικά θα μπορούσαν να δαπανηθούν για την καινοτομία (Wallace, 2017). Οι επιχειρήσεις που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη πιθανότατα θα αντιμετωπίσουν το μεγαλύτερο κόστος εξαιτίας της ιδιαίτερης προσοχής που αποδίδει το GDPR στην αυτοματοποιημένη επεξεργασία και τις προκλήσεις, όπως το δικαίωμα διαγραφής ιδιαίτερα για την Τεχνητή Νοημοσύνη. Αυτά τα κόστη θα εμποδίσουν την προώθηση της Τεχνητής Νοημοσύνης στην Ευρώπη με την εκτόπιση των επενδύσεων

στην έρευνα και την ανάπτυξη, καθιστώντας έτσι πιο δύσκολη την απογείωση των ευρωπαϊκών επιχειρήσεων Τεχνητής Νοημοσύνης και την αποθάρρυνση των ξένων εταιρειών Τεχνητής Νοημοσύνης να εισέλθουν στην ευρωπαϊκή αγορά. Η ΕΕ θα πρέπει να αναθεωρήσει και να απλουστεύσει το GDPR έτσι ώστε, τουλάχιστον, ο καθένας να γνωρίζει πώς να το ακολουθήσει (Castro & Wallace, 2018).

4.4 Το GDPR θα αυξήσει το κόστος εργασίας

Οι εταιρείες της ΕΕ που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη θα πρέπει να προσλάβουν ειδικούς στο δίκαιο της ΕΕ για την προστασία των δεδομένων ώστε να αποκτήσουν τις καλύτερες πιθανότητες να συμμορφωθούν πλήρως με το GDPR. Ο ίδιος ο κανονισμός απαιτεί από τις επιχειρήσεις να ορίσουν υπεύθυνο προστασίας δεδομένων (Data Protection Officer - DPO) ο οποίος θα είναι υπεύθυνος για την παρακολούθηση της συμμόρφωσης και την επαφή με τις αρχές. Αυτό σημαίνει ότι οι εταιρείες που χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα στην Τεχνητή Νοημοσύνη θα αφιερώσουν χρόνο και χρήμα προστατεύοντας τους εαυτούς τους από τους νομικούς κινδύνους που θα μπορούσαν διαφορετικά να δαπανούν για την καινοτομία που ωφελεί τους πελάτες τους και την προώθηση της Τεχνητής Νοημοσύνης γενικά (56). Η Διεθνής Ένωση Επαγγελματιών Προστασίας Προσωπικών Δεδομένων (International Association of Privacy Professionals - IAPP) υποστηρίζει, "αυτό δεν είναι έργο ενός διαχειριστή συμμόρφωσης χαμηλού επιπέδου. Αυτός είναι σαφώς ένας καταλαβαίνων χειριστής στο επιχειρηματικό ή δημόσιο όργανο, κάποιος που μπορεί να αξιολογήσει τον κίνδυνο και να δώσει προτεραιότητα στις προσπάθειες" (International Association of Privacy Specialists, 2016).

Η πρόσληψη ενός υπεύθυνου προστασίας δεδομένων που έχει τα προσόντα για τη διασφάλιση της συμμόρφωσης με το GDPR σε μια εταιρεία που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα με συστήματα Τεχνητής Νοημοσύνης σε μεγάλη κλίμακα αποτελεί σημαντική πρόκληση. Ο σωστός υποψήφιος πρέπει όχι μόνο να κατανοήσει μια ποικιλία εξελιγμένων χρήσεων των τεχνολογιών που βασίζονται σε δεδομένα και τον τρόπο με τον οποίο σχετίζονται όχι μόνο με τις διατάξεις του ίδιου του GDPR αλλά και με τις διάφορες αποχρώσεις του εθνικού δικαίου όπως είναι ο αντίκτυπος των εθνικών νόμων για τη διατήρηση δεδομένων και το δικαίωμα διαγραφής. Οι επαγγελματίες με αυτού του είδους την τεχνογνωσία είναι δύσκολο να βρεθούν και η ζήτηση για αυτούς θα αυξηθεί με την έναρξη ισχύος του GDPR, δημιουργώντας έτσι μια σοβαρή έλλειψη αυτών των εργαζομένων στο εγγύς μέλλον. Για να θέσει το πρόβλημα στο πλαίσιο, το IAPP, η μεγαλύτερη ένωση επαγγελματιών στον τομέα της ιδιωτικής ζωής στον κόσμο, έχει 30.000 μέλη σε 100 χώρες, εκ των οποίων όλοι, ενδεχομένως, ειδικεύονται στο ευρωπαϊκό δίκαιο. Αυτός ο αριθμός είναι πολύ μικρότερος από τους 75.000 αξιωματικούς προστασίας δεδομένων που εκτιμά ο IAPP ότι θα χρειαστούν εταιρείες ανά τον κόσμο για να συμμορφωθούν με το GDPR μόνο (International Association of Privacy Specialists, 2016).

4.5 Το GDPR είναι νομικά επικίνδυνο για τις εταιρείες που χρησιμοποιούν Τεχνητή Νοημοσύνη

Η πολυπλοκότητα του GDPR κάνει επίσης τη χρήση της Τεχνητής Νοημοσύνης νομικά επικίνδυνη. Οι εταιρείες που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη είναι πολύ πιθανότερο να βρεθούν οι ίδιες ο στόχος της νομικής

δράσης μετά την έναρξη ισχύος του GDPR. Με τόσα πολλά πιθανά σημεία αποτυχίας, πολλές εταιρείες που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη θα μπορούσαν να υποστούν ισχυρά πρόστιμα απλά επειδή δεν κατανοούν επαρκώς την πολυπλοκότητα του GDPR - όχι επειδή προσπαθούν να κάνουν κάτι παράνομο ή ακόμη και να βλάψουν τους καταναλωτές. Τα πρόστιμα αυτά θα είναι επίσης πολύ μεγαλύτερα από ό, τι στο προηγούμενο καθεστώς προστασίας δεδομένων. Το κόστος και η πιθανότητα ακούσιας μη συμμόρφωσης θα μπορούσε να αποδειχθεί ακόμη πιο ισχυρό αντικίνητρο στη χρήση της Τεχνητής Νοημοσύνης στην Ευρώπη από το κόστος συμμόρφωσης, επειδή ορισμένες επιχειρήσεις, ιδίως οι μικρές και μεσαίες επιχειρήσεις, μπορούν να αποφασίσουν ότι η επένδυση στην Τεχνητή Νοημοσύνη στην ΕΕ δεν αξίζει το ρίσκο. Ως εκ τούτου, η ΕΕ θα πρέπει να τροποποιήσει το GDPR ώστε να καταστήσει πρόστιμα ανάλογα με τη ζημία που έχει προκληθεί όσο και με την ευθύνη της επιχείρησης (Castro & Wallace, 2018).

4.6 Η τοποθέτηση δεδομένων θα αυξήσει το κόστος Τεχνητής Νοημοσύνης

Το Κεφάλαιο 5 του GDPR καθιστά παράνομο τα κράτη μέλη της ΕΕ να παρεμποδίζουν τις ροές δεδομένων σε άλλα κράτη μέλη για λόγους προστασίας της ιδιωτικής ζωής. Η απαγόρευση αυτή είναι μια θετική εξέλιξη, επειδή θα επέτρεπε σε εταιρείες που χρησιμοποιούν την Τεχνητή Νοημοσύνη να έχουν πρόσβαση στις υπηρεσίες ανταγωνιστικών παρόχων υπηρεσιών cloud σε ολόκληρη την ΕΕ, αντί σε μία μόνο χώρα, δημιουργώντας έτσι μια μεγαλύτερη, πιο ανταγωνιστική αγορά υπηρεσιών cloud. Η ανταγωνιστική τιμολόγηση για τις υπηρεσίες cloud καθιστά πιο προσιτό για τις εταιρείες να χρησιμοποιούν την Τεχνητή Νοημοσύνη για να

αποθηκεύουν και να αναλύουν μεγάλα σύνολα δεδομένων. Αλλά το GDPR διατηρεί την υπάρχουσα γενική απαγόρευση των μεταφορών δεδομένων προσωπικού χαρακτήρα από την Ευρωπαϊκή Ένωση, επιτρέποντας μόνο μεταφορές εκτός Ένωσης σε συγκεκριμένες περιστάσεις, όπως σε χώρες των οποίων οι νόμοι περί προστασίας δεδομένων της Ευρωπαϊκής Επιτροπής θεωρούνται «επαρκείς» ή όταν υπάρχουν συγκεκριμένες διασφαλίσεις ή δεσμευτικοί εταιρικοί κανόνες που διασφαλίζουν ότι το GDPR παραμένει εκτελεστό από τις αρχές της ΕΕ (Castro & Wallace, 2018).

Συνεπώς, θα είναι ακόμη δύσκολο για τις εταιρείες της ΕΕ που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη να χρησιμοποιούν ανταγωνιστικές υπηρεσίες cloud εκτός της ΕΕ (Regulation 2016/679). Παρόλο που οι κανόνες του GDPR για τον εντοπισμό δεδομένων είναι προτιμότεροι από το status quo, εξακολουθούν να μην αντιμετωπίζουν το θεμελιώδες πρόβλημα της ευρωπαϊκής νομοθεσίας περί ιδιωτικού απορρήτου, περιορίζοντας περιττές περιπτώσεις όπου οι οργανισμοί μπορούν να αποθηκεύουν δεδομένα. Ως εκ τούτου, η ΕΕ πρέπει να καταργήσει όλους τους νόμους για τον εντοπισμό δεδομένων. Οι κανόνες εντοπισμού δεδομένων είναι άσκοπες στρεβλώσεις που δεν παρέχουν προστασία της ιδιωτικής ζωής αλλά αυξάνουν το κόστος της Τεχνητής Νοημοσύνης καθιστώντας τις υπηρεσίες cloud λιγότερο ανταγωνιστικές (Cory, 2017). Εάν μια εταιρεία είναι νομικά υπεύθυνη στα ευρωπαϊκά δικαστήρια τότε οι κίνδυνοι για την προστασία της ιδιωτικής ζωής των δεδομένων των Ευρωπαίων σε άλλη χώρα δεν είναι μεγαλύτεροι από την προστασία στην ΕΕ, επειδή η εταιρεία θα έπρεπε να χειρίζεται τα δεδομένα σύμφωνα με το δίκαιο της ΕΕ, ενώ τα δικαστήρια της ΕΕ θα κατέχουν την ευθύνη της εταιρείας για τυχόν αποτυχίες από μέρους της ή των εργολάβων της.

4.7 Η διαθεσιμότητα των δεδομένων θα ενισχύσει την ανταγωνιστικότητα της Τεχνητής Νοημοσύνης, αλλά με κόστος

Το δικαίωμα των υποκειμένων των δεδομένων να μεταφέρουν τα προσωπικά τους δεδομένα σε άλλους παρόχους υπηρεσιών είναι μία από τις λίγες διατάξεις του GDPR που πιθανόν να έχουν τουλάχιστον ορισμένες αντισταθμιστικές θετικές επιπτώσεις στην Τεχνητή Νοημοσύνη, τουλάχιστον βραχυπρόθεσμα, επειδή θα αυξηθεί και θα διαφοροποιηθεί το ποσό των διαθέσιμων δεδομένων για νέες υπηρεσίες Τεχνητής Νοημοσύνης. Ωστόσο, το κόστος της πρόσβασης των χρηστών σε εξαιρετικά μεγάλα, πολύπλοκα και διαφορετικά σύνολα δεδομένων που έχουν συσσωρευτεί εδώ και πολλά χρόνια θα μπορούσε να αποδυναμώσει τα κίνητρα των εταιρειών να συλλέγουν και να αποθηκεύουν αυτά τα δεδομένα στην πρώτη θέση. Όταν οι εταιρείες μπορούν να αποδείξουν στις ρυθμιστικές αρχές ότι το κόστος ενός συγκεκριμένου αιτήματος μεταφοράς φορητότητας δεδομένων είναι υπερβολικό, ο νόμος πρέπει να επιτρέπει εναλλακτικές λύσεις, όπως ο πελάτης να πληρώνει ένα εύλογο ποσό, όπως συμβαίνει με τα δαπανηρά αιτήματα ελευθερίας πληροφόρησης (Castro & Wallace, 2018).

4.8 Το GDPR θα επιδεινώσει την ευρωπαϊκή ανταγωνιστικότητα περιορίζοντας τη χρήση Τεχνητής Νοημοσύνης στην ΕΕ

Η βασική οικονομική αξία της Τεχνητής Νοημοσύνης έγκειται στην ικανότητά της να αυτοματοποιεί πολύπλοκες διαδικασίες, οι οποίες, όπως και τα

προηγούμενα κύματα αυτοματοποίησης, υπόσχονται να βελτιώσουν δραματικά την οικονομική παραγωγή, να αυξήσουν τον κοινωνικό πλούτο και να αυξήσουν το βιοτικό επίπεδο. Ωστόσο, οι περιορισμοί του GDPR για την Τεχνητή Νοημοσύνη θα καταστήσουν πολύ πιο δύσκολο για την ΕΕ να ενισχύσει την οικονομία της χρησιμοποιώντας Τεχνητή Νοημοσύνη, επιτρέποντας έτσι σε άλλα μέρη του κόσμου να αγωνιστούν περισσότερο. Εκτός από την υπονόμευση των πλεονεκτημάτων της χρήσης της Τεχνητής Νοημοσύνης στην ευρωπαϊκή βιομηχανία, οι περιορισμοί της ΕΕ για Τεχνητή Νοημοσύνη θα καταστήσουν επίσης πολύ δύσκολο για τις ευρωπαϊκές επιχειρήσεις Τεχνητής Νοημοσύνης να καταστούν ηγέτες στην ανάπτυξη και την παροχή υπηρεσιών Τεχνητής Νοημοσύνης.

Η Τεχνητή Νοημοσύνη καθιστά τις επιχειρηματικές διαδικασίες πιο αποτελεσματικές με αυτοματοποίηση εργασιών, οι οποίες μειώνουν το κόστος παραγωγής και απελευθερώνουν την ανθρώπινη εργασία. Εκτός από την εξοικονόμηση και την αποδοτικότητα της αυτοματοποίησης αυτών των εργασιών, μακροπρόθεσμα, η Τεχνητή Νοημοσύνη αυξάνει επίσης την παραγωγικότητα με την εκτροπή της ανθρώπινης εργασίας σε πιο οικονομικά χρήσιμες δραστηριότητες που προηγουμένως δεν είχαν το χρόνο να αντιμετωπίσει, βελτιώνοντας περαιτέρω την οικονομική παραγωγή και τη δημιουργία πλούτου. Το συνακόλουθο αποτέλεσμα της αυτοματοποίησης και της τεχνολογικής προόδου στην ευρωπαϊκή βιομηχανία τους τελευταίους δύο αιώνες ήταν να αυξήσει δραστικά το βιοτικό επίπεδο ακόμη και των φτωχότερων Ευρωπαίων. Η Τεχνητή Νοημοσύνη είναι ένα άλλο κύμα βιομηχανικού αυτοματισμού που υπόσχεται να συνεχίσει τις ευεργετικές επιπτώσεις της τεχνολογίας στην οικονομία.

Η δυνητική αξία της πνευματικής ιδιοκτησίας σε μια προηγμένη και υψηλής εξειδίκευσης οικονομία, όπως αυτή της ΕΕ, είναι διττή: εκτός από τη συνολική

ανταγωνιστική τιμή ενίσχυσης της αποτελεσματικότητας στις ευρωπαϊκές βιομηχανίες, η αξία της πνευματικής ιδιοκτησίας σε αυτές τις βιομηχανίες δημιουργεί μια αγορά για τις επιχειρήσεις που μπορούν να αναπτύξουν και να προμηθεύσουν τα εργαλεία Τεχνητής Νοημοσύνης που χρειάζονται παγκοσμίως για το επόμενο κύμα βιομηχανικού αυτοματισμού. Η Ευρώπη μπορεί να είναι μια οικονομική δύναμη, αλλά δεν κατάφερε να παράγει πραγματικά μεγάλους γίγαντες του διαδικτύου. Η ανάπτυξη της Τεχνητής Νοημοσύνης θα μπορούσε να αποτελέσει μια ακόμη ευκαιρία για την Ευρώπη να παράγει μερικούς σημαντικούς παράγοντες σε αυτό το διάστημα και να ανταποκριθεί στην παγκόσμια ζήτηση για Τεχνητή Νοημοσύνη, αλλά λόγω του GDPR, οι ευρωπαϊκές επιχειρήσεις Τεχνητής Νοημοσύνης πρέπει να ανταγωνίζονται με το ένα χέρι δεμένο (Castro & Wallace, 2018).

4.9 Το GDPR είναι λανθασμένο πλαίσιο για την Τεχνητή Νοημοσύνη;

Εάν οι υπεύθυνοι χάραξης πολιτικής της ΕΕ επιθυμούν να επιταχύνουν την ευρωπαϊκή παραγωγικότητα και ανταγωνιστικότητα μέσω της Τεχνητής Νοημοσύνης, τότε η Επιτροπή θα πρέπει να υποβάλει πρόταση για την τροποποίηση του GDPR. Δυστυχώς, δεδομένου του χρόνου και της ενέργειας που χρειάστηκε αρχικά για την οριστικοποίηση του GDPR (το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης υιοθέτησαν τελικά τον κανονισμό τέσσερα έτη μετά την υποβολή της αρχικής πρότασης από την Επιτροπή), το επιχείρημα ότι οι φορείς χάραξης πολιτικής πρέπει να το αναθεωρήσουν λίγο μετά την έναρξη ισχύος του είναι απίθανο να είναι δημοφιλές. Ωστόσο, η τροποποίηση του GDPR είναι ο μόνος τρόπος αντιμετώπισης όλων των επιβλαβών συνεπειών που έχει ο κανονισμός

για την Τεχνητή Νοημοσύνη. Ως εκ τούτου, αντί να επιτύχει μια νίκη για μια τελείως εσφαλμένη νομοθετική πράξη, η Επιτροπή θα πρέπει να ξεκινήσει άμεσα τις εργασίες για το GDPR 2.0.

Το GDPR έχει σημαντικά διδάγματα για τους υπεύθυνους χάραξης πολιτικής σε άλλα μέρη του κόσμου, ιδίως εκείνων των περιφερειακών εμπορικών συνασπισμών. Όπως όλες οι ρυθμίσεις της ΕΕ για την ενιαία αγορά, το GDPR βασίζεται στην αρχή ότι είναι καλύτερο για την ΕΕ να έχει ένα δίκαιο προστασίας δεδομένων, διότι ο ρυθμιστικός κατακερματισμός εμποδίζει τη ροή των ψηφιακών υπηρεσιών. Αυτή είναι μια υγιής αρχή, αλλά δεν σημαίνει ότι ο υπόλοιπος κόσμος πρέπει να αντιγράψει το GDPR προκειμένου να συμμετάσχει στο ψηφιακό εμπόριο με την ΕΕ. Η αντιγραφή του GDPR θα ήταν αβάσιμη, διότι ο κανονισμός περιλαμβάνει περιττούς περιορισμούς, οι οποίοι θα ήταν εξίσου επιζήμιοι οπουδήποτε αλλού, καθώς υπόσχονται να βρίσκονται στην Ευρώπη.

Το GDPR ασκεί πιέσεις σε άλλες χώρες να αντιγράψουν τους κανονισμούς της ΕΕ υπό την προϋπόθεση ότι διευκολύνουν το εμπόριο με τη μεγαλύτερη ενιαία αγορά στον κόσμο (Beattie, 2017). Ωστόσο, οι χώρες δεν χρειάζεται να υιοθετήσουν το GDPR για να αποκτήσουν δωρεάν ροές δεδομένων με την ΕΕ, καθώς το άρθρο 46 του GDPR επιτρέπει την ελεύθερη ροή δεδομένων όταν υπάρχουν μηχανισμοί για την επιβολή της νομοθεσίας της ΕΕ για δεδομένα της ΕΕ, όπως η συμφωνία Ασπίδα προστασίας με τις Ηνωμένες Πολιτείες. Στο βαθμό που οι κυβερνήσεις αντιστέκονται στην υιοθέτηση του GDPR, θα μειώσουν επίσης τις πιέσεις στις εταιρείες να κάνουν το GDPR το de facto σύνολο κανόνων για τις παγκόσμιες δραστηριότητές τους.

Το GDPR είναι το λανθασμένο πλαίσιο για την Τεχνητή Νοημοσύνη και την ψηφιακή οικονομία - τόσο στην Ευρώπη όσο και παντού. Ο κανονισμός υπό τη

σημερινή του μορφή θα καταστήσει πολύ δύσκολο για την ΕΕ να ανταγωνιστεί άλλες περιφέρειες στις οποίες οι επιχειρήσεις έχουν ελεύθερα χέρια στην ανάπτυξη και τη χρήση της Τεχνητής Νοημοσύνης. Η ΕΕ θα πρέπει να απλουστεύσει το GDPR και να περιορίσει τους περιορισμούς που απειλούν να δεσμεύσουν την ψηφιακή οικονομία της για τα επόμενα χρόνια (Castro & Wallace, 2018).

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ – ΣΥΣΤΑΣΕΙΣ - ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΟΠΤΙΚΕΣ

5.1 Συμπεράσματα

Το GDPR δημιουργεί σημαντικούς επιχειρηματικούς κινδύνους για οργανισμούς που πραγματοποιούν επεξεργασία δεδομένων. Η τεχνολογία Τεχνητής Νοημοσύνης μπορεί να συμβάλει στην άμβλυνση των κινδύνων αυτών, υποστηρίζοντας τις αξιολογήσεις κινδύνου, την παρακολούθηση και τον έλεγχο συμμόρφωσης με τις γνώσεις των βέλτιστων πρακτικών, με εξοικονόμηση χρόνου στη διαθεσιμότητα συμβουλών και ζητώντας όλες τις σχετικές πληροφορίες. Τα συστήματα που βασίζονται στη συμμόρφωση απαιτούν την τήρηση καλά τεκμηριωμένων κανόνων και τη ρητή αιτιολογία για αυτό ή την επιλογή να μην το πράξουν. Επίσης, το GDPR απαιτεί τακτικά επεξηγήσεις σχετικά με τη συλλογιστική ή οι οργανισμοί επεξεργασίας δεδομένων ενδέχεται να απαιτούν εξηγήσεις σχετικά με το σκεπτικό ενός συστήματος Τεχνητής Νοημοσύνης για να τους πείσουν ότι τα νομικά επιχειρήματα που προβάλλουν πρέπει να αντεπεξέλθουν σε έλεγχο. Για το λόγο αυτό, η τεχνολογία βασισμένη σε κανόνες είναι περισσότερο κατάλληλη από την τεχνολογία μηχανικής μάθησης στα περισσότερα. Ωστόσο, σε μία πτυχή του GDPR που απαιτεί πράγματι επεξηγήσεις λογικής που πρέπει να δοθούν στα υποκείμενα των δεδομένων που το ζητούν, μπορεί να είναι ανεπιθύμητη η παροχή πλήρων εξηγήσεων για λόγους επιχειρηματικού απορρήτου. Ορισμένες από τις αποφάσεις που απαιτούνται από το GDPR είναι αποφάσεις που λαμβάνονται μονομερώς για έναν οργανισμό επεξεργασίας δεδομένων, πράγμα που σημαίνει ότι οι μόνοι οργανισμοί που ενδέχεται να κάνουν επιχειρηματική υπόθεση για ένα σύστημα

Τεχνητής Νοημοσύνης για να υποστηρίξουν αυτές τις αποφάσεις είναι συμβούλια που συμβουλεύουν πολλούς οργανισμούς σχετικά με τη συμμόρφωση με το GDPR.

Ωστόσο, όλοι οι οργανισμοί καλούνται να παρακολουθούν συνεχώς τις παραβιάσεις της ασφάλειας και, σε περίπτωση πιθανής ή πραγματικής παραβίασης, να εκτιμούν γρήγορα εάν πρέπει να ενημερώσουν την αρμόδια εποπτική αρχή. Τα καθήκοντα παρακολούθησης μπορούν να υλοποιηθούν καλύτερα με μηχανική μάθηση παρά με τεχνολογία βασισμένη σε κανόνες, ειδικά εάν υπάρχει ανάγκη ανίχνευσης απρόβλεπτων γεγονότων.

5.2 Συστάσεις – μελλοντικές προοπτικές

Οι διατάξεις GDPR που στοχεύουν στους αλγορίθμους όχι μόνο εμποδίζουν την Τεχνητή Νοημοσύνη χωρίς να προστατεύουν τους χρήστες από αθέμιτες αποφάσεις, αλλά καταπνίγουν την ανάπτυξη της Τεχνητή Νοημοσύνης συνολικά στην ΕΕ και εξαφανίζουν τις ξένες εταιρείες Τεχνητής Νοημοσύνης, με αποτέλεσμα λιγότερες επιλογές για τους ευρωπαίους καταναλωτές και τις επιχειρήσεις που τους εξυπηρετούν. Υπάρχουν, ωστόσο, άλλοι τρόποι με τους οποίους η ΕΕ μπορεί να προστατεύσει τα δεδομένα των καταναλωτών χωρίς να καταπνίγει την τεχνητή νοημοσύνη.

Αντί να θέτουν άμεσους περιορισμούς στους αλγορίθμους, οι υπεύθυνοι χάραξης πολιτικής θα μπορούσαν να ελέγξουν τις αποφάσεις σχετικά με τους καταναλωτές με βάση τη σοβαρότητα και το πλαίσιο των αποφάσεων αυτών και όχι την τεχνολογία που χρησιμοποιήθηκε για την παραγωγή τους. Γενικότερα, ο νόμος

για την προστασία των δεδομένων πρέπει να απαγορεύει τις ενέργειες που είναι γνωστό ότι είναι επιβλαβείς και να τιμωρούν τα λάθη που έχουν επιβλαβείς συνέπειες, χωρίς να αντιμετωπίζουν κάθε επαναδιάταξη δεδομένων ως πιθανή απειλή για την προστασία της ιδιωτικής ζωής, όπως κάνει τώρα το GDPR. Πράγματι, περιορίζοντας την ανάπτυξη της Τεχνητής Νοημοσύνης, το GDPR ενδέχεται να διαβρώσει την ιδιωτική ζωή των καταναλωτών, καθώς η Τεχνητή Νοημοσύνη έχει τη δυνατότητα να μειώσει την απειλή άλλων ατόμων που έχουν μη εξουσιοδοτημένη πρόσβαση σε προσωπικές πληροφορίες.

Υπάρχουν αποχρώσεις στο GDPR που θα μπορούσαν να παράσχουν κάποια ελευθερία στις ρυθμιστικές αρχές και τα δικαστήρια να ερμηνεύσουν το νόμο με τρόπους που θα μπορούσαν να είναι λιγότερο επιβλαβείς για την ανάπτυξη και τη χρήση της Τεχνητής Νοημοσύνης στην ΕΕ. Ωστόσο, αυτές οι ερμηνείες θα μπορούσαν επίσης να καταλήξουν να είναι πιο επιβλαβείς για την Τεχνητή Νοημοσύνη, οπότε στην πραγματικότητα πρόκειται για τον ίδιο κίνδυνο. Ο μόνος τρόπος για την εξάλειψη αυτών των αναμφίβολα ζημιογόνων πτυχών του GDPR είναι οι υπεύθυνοι χάραξης πολιτικής να τροποποιήσουν τον κανονισμό. Ωστόσο, δεδομένου τόσο του τεράστιου χρόνου όσο και της προσπάθειας που καταβάλλεται για τη δημιουργία του GDPR και της γενικά δυσχερούς φύσης της νομοθεσίας της ΕΕ, η τροποποίηση του GDPR θα είναι μια δύσκολη υπόθεση. Ωστόσο, είναι ο καλύτερος και ίσως μόνο τρόπος για την Ευρώπη να εξαλείψει αυτό το ανταγωνιστικό μειονέκτημα και να γίνει ηγέτης στην Τεχνητή Νοημοσύνη (Castro & Wallace, 2018).

5.2.1 Απλούστευση του GDPR

Ενώ αρκετές διατάξεις του GDPR θέτουν συγκεκριμένα προβλήματα για την Τεχνητή Νοημοσύνη, η συνολική πολυπλοκότητα του κανονισμού καθιστά τον επιβλαβή αντίκτυπό του στην Τεχνητή Νοημοσύνη χειρότερο από το άθροισμα των πλέον επιβλαβών τμημάτων του. Οι έρευνες από συμβούλους και επιχειρήσεις για την ασφάλεια στον κυβερνοχώρο υποδεικνύουν ότι οι εταιρείες γενικά δεν κατανοούν τις υποχρεώσεις τους όσον αφορά το GDPR, με πολλές επιχειρήσεις να βρίσκονται σε λάθος πλευρά (van der Meulen, 2017). Όταν οι νόμοι είναι πολύ δύσκολο να ακολουθηθούν, οι ρυθμιστικές αρχές καταλήγουν να μην επιβάλλουν τα πρότυπα συμπεριφοράς που φαινομενικά γράφτηκαν για να δημιουργήσουν. Κατά ειρωνικό τρόπο, το GDPR ζητά από τις επιχειρήσεις να δημοσιεύουν σαφείς και συνοπτικές ειδοποιήσεις περί απορρήτου, ωστόσο οι εταιρείες δικαίου που πρέπει να συμμορφώνονται με αυτές είναι πάνω από 250 σελίδες νομικής φύσης. Εάν η ΕΕ θέλει σοβαρά να δημιουργήσει μια ενιαία αγορά βασισμένη σε κανόνες με υψηλά πρότυπα, θα πρέπει να απλουστεύσει δραστικά το GDPR, μειώνοντάς το σε ένα σύνολο ευκόλως κατανοητών κανόνων που εστιάζονται αποκλειστικά στην πρόληψη των ζημιών των καταναλωτών, αντί να προσπαθούν να ελέγχουν αυστηρά τον τρόπο με τον οποίο οι εταιρείες πραγματοποιούν διαχείριση και χρήση δεδομένων, εις βάρος της καινοτομίας (Castro & Wallace, 2018).

5.2.2 Αφαίρεση του δικαιώματος της ανθρώπινης αναθεώρησης

Το δικαίωμα σε μια ανθρώπινη αναθεώρηση των αλγοριθμικών αποφάσεων θα καταστήσει την Τεχνητή Νοημοσύνη πιο ακριβή και θα αναγκάσει τις εταιρείες να χρησιμοποιούν λιγότερο ακριβή συστήματα Τεχνητής Νοημοσύνης, χωρίς να προστατεύουν τους καταναλωτές από βλαβερές ή άδικες αποφάσεις - σε μεγάλο βαθμό επειδή οι άνθρωποι μπορούν να είναι περισσότερο προκατειλημμένοι και μεροληπτικοί προς τους αλγορίθμους. Αντ 'αυτού, οι υπεύθυνοι χάραξης πολιτικής θα πρέπει να ενθαρρύνουν τη χρήση εργαλείων όπως μια ανισομερή ανάλυση επιπτώσεων που αναπτύχθηκε για την καταπολέμηση της μεροληψίας έναντι προστατευόμενων κατηγοριών ατόμων (Korte & Castro, 2015).

5.2.3 Θέσπιση δικαιωμάτων για την επανεξέταση και την επεξήγηση της τεχνολογίας Neutral

Οποιεσδήποτε απαιτήσεις για διαφάνεια, αποδείξεις, εποπτεία ή εξήγηση πρέπει να είναι τεχνολογικά ουδέτερες. Η ΕΕ πρέπει να διασφαλίσει ότι το δικαίωμα του ατόμου σε αναθεώρηση ή μια εξήγηση μιας συγκεκριμένης απόφασης πρέπει να εξαρτάται από τη φύση και τη σοβαρότητα της εν λόγω αποφάσεως, δεν είναι απλώς αν η απόφαση έγινε από έναν άνθρωπο ή έναν αλγόριθμο. Η εφαρμογή αυτών των δικαιωμάτων αποκλειστικά στις αποφάσεις που λαμβάνονται από τους αλγόριθμους δημιουργεί αντικίνητρο για τις εταιρείες να χρησιμοποιούν Τεχνητή Νοημοσύνη, καθώς αντιπροσωπεύει ένα επιπλέον κόστος συμμόρφωσης και καθιστά τη χρήση της τεχνολογίας λιγότερο αποδοτική. Επιπλέον, μια τέτοια απαίτηση θα επέτρεπε να

ληφθούν αθέμιτες αποφάσεις από ανθρώπους, οι οποίες τείνουν να είναι περισσότερο ανοικτές στην προκατάληψη, για να αποφευχθούν παρόμοια επίπεδα ελέγχου και λογοδοσίας. Τέλος, η ΕΕ πρέπει να λάβει υπόψη ότι είναι δυνατόν να απαιτούνται διαφορετικοί κανόνες για διαφορετικούς κλάδους και να αποφεύγονται οι γενικές απαιτήσεις (Castro & Wallace, 2018).

5.2.4 Επεξήγηση «ενημερωτικών πληροφοριών»

Η ΕΕ πρέπει να τροποποιήσει το GDPR για να διευκρινίσει ότι, στο πλαίσιο αλγοριθμικών αποφάσεων, η παροχή «σημαντικών πληροφοριών» σημαίνει ότι ο επεξεργαστής δεδομένων πρέπει να παρουσιάσει στο υποκείμενο των δεδομένων μια περιγραφή των δεδομένων που χρησιμοποιεί ο αλγόριθμος και μια βασική εξήγηση για τον τρόπο με τον οποίο λαμβάνει αποφάσεις. Ωστόσο, η απαίτηση να εξηγεί κάθε πιθανή απόχρωση κάθε ξεχωριστής απόφασης θα ήταν δαπανηρή και θα αποθάρρυνε τη χρήση της Τεχνητής Νοημοσύνης. Επιπλέον, πολύπλοκες εξηγήσεις είναι απίθανο να είναι χρήσιμες για τον μέσο καταναλωτή (Castro & Wallace, 2018).

5.2.5 Θέσπιση του δικαιώματος της κατάργησης

Ανάλογα με τον τρόπο με τον οποίο οι ρυθμιστικές αρχές εφαρμόζουν το νόμο, αναγκάζοντας τις εταιρείες να διαγράψουν δεδομένα από αλγοριθμικά μοντέλα

θα μπορούσαν να βλάψουν τον αλγόριθμο και να υπονομεύσουν τα οφέλη του για τους χρήστες. Οι ρυθμιστικές αρχές θα πρέπει να λαμβάνουν ως φιλελεύθερη μια ερμηνεία "διαγραφής" όπως μπορούν και να επιτρέπουν στις εταιρείες να διαγράφουν πληροφορίες με τον συμβατικό τρόπο, χωρίς να αλλοιώνουν αλγοριθμικά μοντέλα. Ωστόσο, επειδή η διάκριση μεταξύ των όρων "διαγραφή" και "κατάργηση" είναι τόσο ξεκάθαρη, η καλύτερη λύση είναι η ΕΕ να τροποποιήσει το GDPR για να αντικαταστήσει την προηγούμενη λέξη με αυτή. Επιπλέον, ανεξάρτητα από το ποια λέξη ισχύει, τα δικαιώματα των πελατών να διαγράφουν τα δεδομένα τους δεν πρέπει να παραβιάζουν τη λειτουργικότητα των αλγορίθμων όσον αφορά την εργασία για άλλους πελάτες. Για το σκοπό αυτό, αντί του δικαιώματος διαγραφής, οι καταναλωτές πρέπει να έχουν δικαίωμα στην ανωνυμία, όπου μπορούν να απαιτούν από τις εταιρείες να διαγράφουν τις πληροφορίες τους κατά τρόπο που να μην παρεμβαίνει στη συμπεριφορά ενός αλγορίθμου. Δεδομένου ότι η "ανωνυμοποίηση" σημαίνει διατήρηση μόνο εκείνου που δεν είναι προσωπικά αναγνωρίσιμο, η εκπλήρωση του δικαιώματος διαγραφής μέσω ανωνυμίας μπορεί να είναι νομικά αποδεκτή στο πλαίσιο της τρέχουσας διατύπωσης του GDPR. Η τροποποίηση του GDPR για να διευκρινιστεί αυτό θα βοηθούσε αναμφίβολα στην άρση της αβεβαιότητας.

Το δικαίωμα κατάργησης δεν πρέπει επίσης να ισχύει για δεδομένα που έχουν τεθεί νόμιμα στο κοινό - δηλαδή, η λεγόμενη διάταξη "δικαίωμα να λησμονηθεί" πρέπει να καταργηθεί εντελώς. Οι πληροφορίες στον δημόσιο τομέα είναι ένα δημόσιο αγαθό που είναι επίσης ένα πολύτιμο στοιχείο των αλγοριθμικών εργαλείων, όπως η αναζήτηση ή η μετάφραση (Castro & Wallace, 2018).

5.2.6 Αδειοδότηση των δεδομένων που δεν αποτελούν κίνδυνο για το υποκείμενο των δεδομένων

Το GDPR αντιμετωπίζει όλες τις επαναδημιουργίες δεδομένων πέραν του αρχικού του σκοπού ως σοβαρό αδίκημα, για το οποίο επιβάλλει ανώτατα πρόστιμα που περιορίζουν σοβαρά την παράνομη ικανότητα των εταιρειών Τεχνητής Νοημοσύνης να πειραματίζονται και να καινοτομούν χρησιμοποιώντας προσωπικά δεδομένα. Αλλά δεν είναι όλες οι επαναχρησιμοποιήσεις δεδομένων επιβλαβείς. Στην πραγματικότητα, πολλές είναι εξαιρετικά επωφελείς για την κοινωνία της ΕΕ. Ως εκ τούτου, η ΕΕ θα πρέπει να τροποποιήσει το GDPR ώστε να προβαίνει στη μεταστροφή των δεδομένων χωρίς να ζητεί τη συγκατάθεσή τους ως νόμιμη, υπό την προϋπόθεση ότι δεν δημιουργεί κίνδυνο για το υποκείμενο των δεδομένων ούτε μεταφέρει δεδομένα σε άλλο ελεγκτή. Όταν μια τέτοια μεταφορά είναι απλώς αποτέλεσμα συγχώνευσης ή εξαγοράς, η κοινοποίηση πρέπει να είναι επαρκής (Castro & Wallace, 2018).

5.2.7 Τροποποίηση δικαιωμάτων φορητότητας δεδομένων

Τα περιορισμένα δικαιώματα φορητότητας δεδομένων μπορούν να είναι χρήσιμα για επιχειρήσεις που χρησιμοποιούν την Τεχνητή Νοημοσύνη, διευκολύνοντας την πρόσβαση σε μεγαλύτερα και πιο ποικίλα σύνολα δεδομένων. Αλλά η επιβολή αυτού του δικαιώματος χωρίς εύλογους περιορισμούς θα επιβάλει τεράστιο κόστος που θα μπορούσε να αποθαρρύνει ορισμένες μορφές συλλογής δεδομένων, με επακόλουθους περιορισμούς για την Τεχνητή Νοημοσύνη.

Οι πελάτες θα πρέπει να βοηθήσουν στην κάλυψη ενός μέρους του ιδιαίτερα υψηλού κόστους μεταφοράς - όπως και οι πολίτες που ασκούν το δικαίωμά τους σε πληροφορίες από την κυβέρνηση συχνά πρέπει να πληρώσουν ένα μικρό τέλος για αιτήματα ελευθερίας πληροφόρησης, οι οποίες είναι εξαιρετικά δαπανηρές για τον φορολογούμενο (Castro & Wallace, 2018).

5.2.8 Παρουσίαση σαφέστερων κατευθυντήριων γραμμών για την αποσύνδεση δεδομένων

Οι αρμόδιοι για τη χάραξη πολιτικής είχαν δίκιο να συμπεριλάβουν εξαιρέσεις στο GDPR για ψευδονομικά και ανώνυμα δεδομένα, καθώς ενθαρρύνει τις εταιρείες που αναπτύσσουν ή χρησιμοποιούν την Τεχνητή Νοημοσύνη να κάνουν περισσότερα με δεδομένα που δεν αποτελούν απειλή για την ιδιωτική ζωή. Ωστόσο, οι ισχύοντες κανόνες για την εξακρίβωση της ταυτότητας είναι ασαφείς, έτσι οι σαφέστερες κατευθυντήριες γραμμές θα διευκόλυναν τις επιχειρήσεις να απομακρύνουν τα δεδομένα με εμπιστοσύνη. Οι ρυθμιστικές αρχές προστασίας δεδομένων στην ΕΕ θα πρέπει να καταρτίσουν σαφέστερες οδηγίες σχετικά με τον τρόπο με τον οποίο οι εταιρείες μπορούν νομίμως να διατηρούν τα δεδομένα ανώνυμα, καθώς αυτό θα ενθάρρυνε τις εταιρείες να αναπτύσσουν ή να χρησιμοποιούν την Τεχνητή Νοημοσύνη για να απομακρύνουν περισσότερα δεδομένα, γνωρίζοντας τη νομική ευθύνη τους σχετικά με τις ενέργειές τους και όχι με τα ενδεχόμενα πέρα από τον έλεγχό τους. Συνολικά, θα χαρακτήριζαν ως ανώνυμα περισσότερα δεδομένα για χρήση σε Τεχνητή Νοημοσύνη, επιτρέποντας έτσι μια ευρύτερη περιοχή

δραστηριοτήτων επεξεργασίας δεδομένων από ό, τι οι άδειες GDPR για προσωπικά δεδομένα.

Στις Ηνωμένες Πολιτείες, το άρθρο 164.514 του Κώδικα Απορρήτου Ασφάλειας για την Ασφάλεια της Υγείας (Health Insurance Portability and Accountability Act - HIPAA) θέτει πρότυπα για τον αποχαρακτηρισμό των δεδομένων, σε αντίθεση με το GDPR (U.S. Department for Health and Human Services, 2017). Παρόλο που ο υποστηρικτικός ορισμός αποχαρακτηρισμού του HIPAA είναι ουσιαστικά ο ίδιος με τον ορισμό του GDPR για την ανωνυμοποίηση, όπως επισημαίνει το IAPP, μια εταιρεία που ακολουθεί τις κατευθυντήριες γραμμές της HIPAA στην ΕΕ δεν μπορεί να είναι αρκετά σίγουρη ότι πληροί τις απαιτήσεις του GDPR για ψευδονομία - πόσο μάλλον για ανωνυμοποίηση.

Είναι αλήθεια ότι η HIPAA ασχολείται με ένα περιορισμένο είδος δεδομένων, ενώ το GDPR σχετίζεται με όλα τα προσωπικά δεδομένα - κάτι που σημαίνει ότι είναι ευκολότερο για την HIPAA να προσφέρει στις εταιρείες συγκεκριμένα βήματα για την ικανοποιητική ανωνυμοποίηση των δεδομένων. Εντούτοις, οι κατευθυντήριες γραμμές που λαμβάνουν τουλάχιστον υπόψη αυτά τα μέτρα και, όπως η HIPAA, επιτρέπουν την πιστοποίηση εμπειρογνωμόνων για ανώνυμα δεδομένα, θα επιτρέψουν στις εταιρείες που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη στην ΕΕ να αποκομίσουν εμπιστοσύνη για τα πλεονεκτήματα των ανωνυμοποιημένων δεδομένων που μπορούν να υποστούν επεξεργασία εκτός του GDPR (Wes, 2017).

5.2.9 Επιβολή προστίμων για την παραβίαση του GDPR ανάλογα με τη ζημιά και την υπαιτιότητα

Το GDPR επιβάλλει εξαιρετικά μεγάλα πρόστιμα για παραβιάσεις στις διατάξεις που θεωρούνται ιδιαίτερα επιβλαβείς για την Τεχνητή Νοημοσύνη, όπως το δικαίωμα στην εξήγηση και η γενική απαγόρευση της επαναπροώθησης δεδομένων. Τα πρόστιμα για παραβιάσεις δεδομένων θα πρέπει να είναι ανάλογα με την έκταση τόσο της βλάβης που προκαλείται από την παραβίαση όσο και της υπαιτιότητας της επιχείρησης γι 'αυτήν (Castro & McQuinn, 2015). Στις εταιρείες δεν πρέπει να επιβάλλονται πρόστιμα για δραστηριότητες που δεν προκαλούν κακό.

Για παράδειγμα, η αφήγηση των στοιχείων της πιστωτικής κάρτας των καταναλωτών σε λάθος χέρια μπορεί να οδηγήσει σε σημαντικό κόστος τόσο για τους καταναλωτές όσο και για τους παρόχους πιστωτικών καρτών τους. Εάν η παραβίαση οφείλεται σε πρακτικές αμέλειας στον κυβερνοχώρο, εκτός από την ευθύνη για το κόστος, οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να αντιμετωπίσουν μεγάλα πρόστιμα ως κίνητρο για συμπεριφορά με μεγαλύτερη υπευθυνότητα στο μέλλον. Και όποτε μια απρόβλεπτη επίθεση στον κυβερνοχώρο επιτύχει παρά τις καλύτερες προσπάθειες του υπεύθυνου της επιχείρησης, η επιχείρηση πρέπει να φέρει ευθύνη μόνο για τα έξοδα και να μην αντιμετωπίσει πρόσθετα πρόστιμα.

Από την άλλη πλευρά, κάθε φορά που μια εταιρεία χρησιμοποιεί προσωπικά δεδομένα για να δοκιμάσει έναν νέο αλγόριθμο και το κάνει με τρόπο που να μην βλάπτει τους καταναλωτές, δεν θα πρέπει να επιβάλλονται καθόλου κυρώσεις. Οι εταιρείες που αναπτύσσουν ή χρησιμοποιούν Τεχνητή Νοημοσύνη θα πρέπει να μπορούν να πειραματιστούν με νέους αλγόριθμους χωρίς πρώτα να ζητήσουν άδεια από κάθε υποκείμενο δεδομένων επειδή φοβούνται ότι θα επιβληθούν πρόστιμα, γιατί

αυτή η δραστηριότητα δεν αποτελεί απειλή για τα υποκείμενα των δεδομένων (Castro & Wallace, 2018).

5.2.10 Εξουσιοδότηση χρήσης της Τεχνητής Νοημοσύνης για το δημόσιο συμφέρον

Μια από τις νομικές βάσεις για την επεξεργασία δεδομένων στο GDPR εκτελεί καθήκοντα προς το δημόσιο συμφέρον ή στην άσκηση δημόσιας εξουσίας και, ως εκ τούτου, οι χρήσεις δεδομένων που βασίζονται σε αυτή τη νομική βάση δεν υπόκεινται σε όλους τους ίδιους περιορισμούς όπως και άλλοι χρήσεις. Οι ευρωπαϊκές εθνικές κυβερνήσεις θα πρέπει να εφαρμόσουν ελευθέρως αυτή την εξουσιοδότηση για να απαλλάξουν τις χρήσεις της Τεχνητή Νοημοσύνη που εξυπηρετούν το δημόσιο συμφέρον, συμπεριλαμβανομένων τομέων όπως η υγειονομική περίθαλψη, η εκπαίδευση και το περιβάλλον.

Για παράδειγμα, η Τεχνητή Νοημοσύνη έχει σημαντικές εφαρμογές στον τομέα της υγειονομικής περίθαλψης, όπου μπορεί να βοηθήσει τους γιατρούς να εντοπίσουν νωρίς τις ασθένειες και να εντοπίσουν πιθανές αποτελεσματικές θεραπείες (Wallace, 2017, 2018). Αυτή η εξουσιοδότηση δημιουργεί μια ευκαιρία για τις ευρωπαϊκές κυβερνήσεις να οδηγήσουν σε Τεχνητή Νοημοσύνη και να αποδείξουν τη χρησιμότητά τους αναπτύσσοντας Τεχνητή Νοημοσύνη στο δημόσιου τομέα. Οι ευρωπαϊκές εθνικές κυβερνήσεις πρέπει να χρησιμοποιούν την Τεχνητή Νοημοσύνη για να καταστήσουν τις δημόσιες υπηρεσίες πιο αποτελεσματικές και να

επιτύχουν τα καλύτερα δυνατά αποτελέσματα για τους ανθρώπους που τα χρησιμοποιούν (Castro & Wallace, 2018).

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση

Addis C., & Kutar M. (2018). The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. Available at: https://www.ukais.org/resources/Documents/ukais%202018%20proceedings%20papers/paper_39.pdf.

Ashford, W. (2018). Top UK and US firms still overestimating GDPR readiness. Available at: http://www.computerweekly.com/news/450432510/TopUK-and-US-firms-still-overestimating-GDPR-readiness.

Banisar D. (2018) 'National Comprehensive Data Protection/Privacy Laws and Bills 2018', Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

Beattie A. (2017). "Why the Whole World Feels the 'Brussels Effect,'" Financial Times. Available at: https://www.ft.com/content/7059dbf8-a82a-11e7-ab66-21cc87a2edde.

Castro D., & Korte T. (2013). Data Innovation 101, Center for Data Innovation. Available at: https://www.datainnovation.org/2013/11/data-innovation-101/.

Castro D. & McQuinn A. (2015). "How and When Regulators Should Intervene," Information Technology and Innovation Foundation. Available at: http://www2.itif.org/2015-how-whenregulators-intervene.pdf.

Castro D., & New J. (2016). The Promise of Artificial Intelligence, Center for Data Innovation. Available at: http://www2.datainnovation.org/2016-promise-of-ai.pdf.

Castro D., & Wallace N. (2018). The Impact of the EU's New Data Protection Regulation on AI, Center for Data Innovation.

Cory N. (2017). "Cross Border Data Flows: Where Are the Barriers, and What Do They Cost?", Information Technology and Innovation Foundation. Available at: http://www2.itif.org/2017-cross-border-data-flows.pdf.

Dell. (2016). GDPR: Perceptions and Readiness. A Global Survey of Data Privacy Professionals at companies with European Customers. Available at: http://www.eurocloud.fr/wp-content/uploads/2016/10/gdpr.pdf

European Commission (2017). "Making the Most of Robotics and Artificial Intelligence in Europe" Available at: https://ec.europa.eu/commission/commissioners/2014-2019/ansip/blog/making-most-robotics-and-artificial- intelligenceeurope_en.

Gellman R. (2017). 'Fair Information Practices: A Basic History', April 2017. Available at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

Gov.UK. Data Protection Act 1998 (1998). Available at: https://www.gov.uk/dataprotection/the-data-protection-act

ICO. (2016). Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now. Available at: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf.

International Association of Privacy Specialists (2016). "The GDPR Demands 75k DPOs: Where Will They Come From?". Available at: https://iapp.org/media/pdf/DPAWhitepaper.pdf.

Khaled AlSedrah M. (2017). Artificial Intelligence, Advanced Analysis and Design, American University of Middle East.

Kolah, A., & Foss, B. (2015). Unlocking the power of data under the new EU general data protection regulation. Journal of Direct, Data and Digital Marketing Practice, 16(4), 270–274.

Korte T. & Castro D. (2015). "Disparate Impact Analysis is Key to Ensuring Fairness in the Age of the Algorithm," Center for Data Innovation. Available at: https://www.datainnovation.org/2015/01/disparateimpact-analysis-is-key-to-ensuring-fairness-in-the-age-of-the-algorithm/.

LaMagna M. (2017). ' The reason your loan application is rejected may have nothing to do with your credit score', MarketWatch', available at: https://www.marketwatch.com/story/the-reason-your-loan-application-is-rejected-may-havenothing-to-do-with-your-credit-score-2017-03-29

Privacy International (2018). The Keys to Data Protection, A Guide for Policy Engagement on Data Protection, London. Available at: https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

PwC (2017). "Potential Global Regional Gains from AI". Available at: https://press.pwc.com/News-releases/ai-to-drive-gdpgains-of--15.7-trillion-with-productivity-personalisationimprovements/s/3cc702e4-9cac-4a17-85b9-

71769fba82a6, and https://press.pwc.com/Multimedia/News-releases/All/potential-globalregional-gains-from-ai/a/a070cb3b-fd32-4a38-a59a-468d7d378af5.

Regulation 2016/679 (General Data Protection Regulation), Chapter V, (see page L 119/60-65). Available at: http://ec.europa.eu/justice/dataprotection/reform/files/regulation_oj_en.pdf.

Siegle L. (2018). "New EU Data Rules Will Get Tough on Privacy," The Economist: The World in 2018. Available at: http://www.theworldin.com/edition/2018/article/14563/dodd-frank-data.

Singlehurst T. et al. (2017). 'ePrivacy and Data Protection', CitiGroup, p4. Available at: https://www.citibank.com/commercialbank/insights/assets/docs/ePrivacyandData.pdf

U.S. Department for Health and Human Services (2017). "Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,". Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/specialtopics/de-identification/index.html.

van der Meulen R. (2017). "Top 5 Priorities to Prepare for EU GDPR," Gartner. Available at: https://www.gartner.com/smarterwithgartner/top-five-priorities-to-preparefor-eu-gdpr/.

Wallace N. (2017). "Overzealous EU Data Protection Regulations More Likely to Take Your Job Than a Robot," City A.M.. Available at: http://www.cityam.com/260087/overzealous-eu-data-protectionregulations-more-likely-take

Wallace N. (2018). "5 Q's for Ben Marthappu, Co-Founder of Cera," Center for Data Innovation. Available at: https://www.datainnovation.org/2018/01/5-qs-for-ben-maruthappu-cofounder-of-cera/;

Wallace N. (2017). "UK Regulations Need an Update to Make Way for Medical AI," Center for data Innovation. Available at: https://www.datainnovation.org/2017/08/uk-regulations-need-an-updateto-make-way-for-medical-ai/

Wallace N. (2017). "5 Q's for Matteo Carli, Chief Technology Officer and Founder of Xbird," Center for Data Innovation. Available at: https://www.datainnovation.org/2017/06/5qs-for-matteo-carlichief-technology-officer-and-founder-of-xbird/

Wallace N. (2017). "5 Q's for Eyal Toledano, Co-Founder of Zebra Medical Vision," Center for Data Innovation. Available at: https://www.datainnovation.org/2017/06/5qs-for-eyaltoledano-co-founder-of-zebra-medical-vision/.

Wes M. (2017). "Looking to Comply With GDPR? Here's a Primer on Anonymization and Pseudonymization," International Association of Privacy Professionals. Available at: https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-onanonymization-and-pseudonymization/.

128th Session of the Committee of Ministers (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018)2-final. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

Πηγές από το Διαδίκτυο

www.enisa.europa.eu

www.gdpr-info.eu

Data Protection Commission (Ireland) (2019). 'Case Study 1/01', available at: https://www.dataprotection.ie/docs/Case-Study-1-01-Bank-and-Insurance-Company/121.htm

Privacy International (2019). 'How do companies get our data?' available at: https://www.privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

The Centre for Internet and Society (2016). 'Aadhaar Act and its Non-compliance withData Protection Law in India'. available at: https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protectionlaw-in-india

Commission National Informatique & Libertes (2019). Compliance Package: Connected Vehicles and Personal Data, available (PDF) at: https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

Privacy International (2019). Big Data - Explainer, available at: https://privacyinternational.org/explainer/1310/big-data

Communication from the Commission (2018). Artificial Intelligence for Europe, COM (2018) 237 final. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625.

Court of Justice of the European Union (2014). 'The Court of Justice declares the Data Retention Directive to be invalid', Curia, available (PDF) at https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Executive Office of the President of the United States (2016). National Science and Technology Council Committee on Technology, Preparing for the Future of Artificial Intelligence. Available at: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

Foundation for Media Alternatives (2019). 'National Privacy Commission to issue findings on Comelec breach' available at: http://www.fma.ph/?p=399

Greenberg N. (2018). "PGA Tour Is Embracing Artificial Intelligence, And It Could Change How You Watch Golf," The Roanoke Times. available at https://www.roanoke.com/washingtonpost/sports/pga-touris-embracing-artificial-intelligence-and-it-could-change/article_f46d97b1-0b99-5495-a9e9-a015d0b9620b.html.

Del Bello, L. (2018). AI Translates News Just as Well as a Human Would, futurism.com. available at https://futurism.com/ai-translator-microsoft/.

Keohane, J. (2017). "What News-Writing Bots Mean for the Future of Journalism," Wired. available at https://www.wired.com/2017/02/robots-wrote-this-story/.

Hardesty, L. (2012). "Is MIT Giving Away the Farm?," MIT Technology Review. available at https://www.technologyreview.com/s/428698/is-mit-giving-away-the-farm/.

Kuang, C. (2017). "Can A.I. Be Taught to Explain Itself?," New York Times Magazine. Available at: https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html?_r=0. 5

Privacy International (2019). Contesting Surveillance, available at https://www. privacyinternational.org/programmes/contesting-surveillance

Machine Learning, Coursera. Available at: https://www.coursera.org/learn/machine-learning.

Camparo A. (2018). This basketball-playing robot is so good it could outshoot Stephen Curry, nbcnews.com. Available at: https://www.nbcnews.com/mach/science/basketball-playing-robot-so-good-it-couldoutshoot-stephen-curry-ncna858011.

Timmer, J. (2018). AI trained to spot heart disease risks using retina scan, arstechnica.com. Available at https://arstechnica.com/science/2018/02/ai-trained-to-spot-heart-disease-risks-using-retina-scan/.

Seeing AI App, Microsoft Accessibility Blog (2017). Available at https://blogs.msdn.microsoft.com/accessibility/2017/07/12/seeing-ai-app-is-now-available-in-the-ios-app-store/;

Zee, S. (2017). Whose Sign Is It Anyway? AI Translates Sign Language Into Text, blogs.nvidia.com. available at https://blogs.nvidia.com/blog/2017/05/11/ai-translates-sign-language/.

House of Lords Select Committee in Artificial Intelligence (2018). AI in the UK: Ready, Willing and Able?, HL Paper 100. available at: https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf.

Intel (2017), Artificial Intelligence, The Public Policy Opportunity, available at: https://blogs.intel.com/policy/files/2017/10/Intel-artificial-Intelligence-Public-Policy-White-Paper-2017.pdf.

Project InnerEye (2008)—Medical Imaging AI to Empower Clinicians, Microsoft Project InnerEye. available at https://www.microsoft.com/en-us/research/project/medical-image-analysis/.

Spencer, G. (2017), Buffaloes and the Cloud: Students turn to tech to save poor farming families, news.microsoft.com. available at: https://news.microsoft.com/apac/features/saving-farmingfamilies-tech-one-cow-goat-buffalo-time/.

Devlin, H. (2016), "Could online tutors and artificial intelligence be the future of teaching?," The Guardian. available at: https://www.theguardian.com/technology/2016/dec/26/could-online-tutors-and-artificialintelligence-be-the-future-of-teaching.

Tully, P. (2018), Using defensive AI to strip cyberattackers of their advantage, venturebeat.com. available at: https://venturebeat.com/2018/03/06/using-defensive-ai-to-strip-cyberattackers-of-their-advantage/.

Rieland, R. (2018), "Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased?," Smithsonian. available at: https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crimeis-it-biased-180968337/.

Greenberg, A. (2018), "An AI That Reads Privacy Policies So That You Don't Have To," Wired. available at: https://www.wired.com/story/polisis-ai-reads-privacy-policies-so-you-dont-have-to/.

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

S. Simitis, Kommentar zum Bundesdatenschutzgesetz (2014) p. 82 ff, 134 ff.

Burri, M., & Schär, R. (2016). The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. Journal of Information Policy, 6, pp. 479-511.

Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2013.

A. Mantelero, The future of consumer data protection in the EU Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Computer Law & Security Review 30(6) 2014, pp. 643-660, 645.

L. Mitrou, Privacy Challenges and Perspectives in Europe in M. Bottis (ed.) An Information Law for the 21st Century (Proceedings of Third International Seminar on Information Law), Athens 2011, pp. 220-236.

P. Niemitz, Constitutional Democracy and Technology in the age of Artificial Intelligence. Accepted for publication in Royal Society Philosophical Transactions A 2018.