ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα

με Διεθνή Προσανατολισμό

«Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα»

ΝΟΤΟΠΟΥΛΟΥ ΦΩΤΕΙΝΗ

Επιβλέπουσα Καθηγήτρια: Δελούκα-Ιγγλέση Κορνηλία

Διπλωματική Εργασία υποβληθείσα στο Τμήμα Οργάνωσης και Διοίκησης Επιχειρήσεων του Πανεπιστημίου Πειραιώς για την απόκτηση

Μεταπτυχιακού Διπλώματος Ειδίκευσης στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με Διεθνή Προσανατολισμό.

Πειραιάς, 2022

ΠΑΡΑΡΤΗΜΑ Δ : **ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ**

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

Μεταπτυχιακό Πρόγραμμα Σπουδών

στη «Διοίκηση Επιχειρήσεων – Ολική Ποιότητα» με διεθνή προσανατολισμό

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή [δεύτερη] σελίδα στο σώμα της διπλωματικής εργασίας)

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων - Ολική Ποιότητα με διεθνή προσανατολισμό με τίτλο:

Σύγχρονα ζητήματα γύρω από την προστασία δεδομένων προσωπικού χαρακτήρα,

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Υπογραφή Μεταπτυχιακού Φοιτητή/τριας .....

Ονοματεπώνυμο Νατσιούλου Φωτεινή

Ημερομηνία 12-12-2022

Αφιέρωση

Η παρούσα πτυχιακή εργασία είναι αφιερωμένη στους γονείς μου,
για την στήριξη, τα εφόδια και την αγάπη τους από την πρώτη μέρα.

Ευχαριστίες

Με τις σελίδες που ακολουθούν, ολοκληρώνεται ένας εκτενής, έντονος και πολύ σημαντικός κύκλος στη ζωή μου. Δοθείσης της ευκαιρίας θα ήθελα να εκφράσω τις ειλικρινείς και θερμές μου ευχαριστίες σε όλους όσους ήταν μαζί μου σ' αυτό το ταξίδι,

το Πανεπιστήμιο Πειραιώς και το τμήμα Οργάνωσης και Διοίκησης Επιχειρήσεων, τους καθηγητές και τους διοικητικούς υπαλλήλους, για την υποδειγματική πραγματοποίηση του προγράμματος, την καθοδήγηση και την προτροπή να ανακαλύψουμε νέους ορίζοντες,

ιδιαιτέρως, την κ. Δελούκα-Ιγγλέση, που ως επιβλέπουσα της παρούσας διπλωματικής, με συμβούλευσε, με καθοδήγησε και με ενθάρρυνε να εξελίξω την κριτική μου σκέψη,

τους συναδέλφους μου για την υποστήριξη, τη συμπαράσταση και την κατανόηση που έδειξαν όλους αυτούς τους μήνες,

και τέλος την οικογένεια και τους φίλους μου, που όντας παρόντες σε κάθε εύκολη και δύσκολη στιγμή, με βοηθάνε να εξελίσσομαι στην καλύτερη έκδοση του εαυτού μου.

Περίληψη

Μία από τις μεγαλύτερες προκλήσεις της εποχής είναι η προστασία των προσωπικών δεδομένων, η ενημέρωση, η ευαισθητοποίηση και η ανάγκη για τον σεβασμό αυτών. Στα επόμενα κεφάλαια, παρουσιάζεται το ουσιαστικό πρόβλημα και γίνεται αναφορά στους νόμους που έχουν τεθεί σε ισχύ στην Ευρωπαϊκή Ένωση, αλλά και στην Ελλάδα. Η αρχική οδηγία (95/46/ΕΚ) δημοσιεύθηκε το 1995, πριν περίπου 30 χρόνια. Η ραγδαία εξέλιξη των τεχνολογιών, οδήγησε σε συστάσεις για ανάγκη θέσπισης ειδικής νομοθεσίας και εκτεταμένη έρευνα σχετικά με το ζήτημα. Το 2016 το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο δημοσίευσαν τον ν. 2016/679 σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, ορίζοντας μια περίοδο εφαρμογής για τα κράτη μέλη περίπου δύο ετών. Στην Ελλάδα, η Ελληνική Αρχή Προστασίας Προσωπικών Δεδομένων, κατέληξε στην ισχύουσα μέχρι σήμερα νομοθεσία με τον ν. 4624/2019, δημιουργώντας παράλληλα πολλές προκλήσεις, κινδύνους αλλά και ευκαιρίες στον επιχειρηματικό κόσμο. Στη συνέχεια, γίνεται μια αναφορά στην εφαρμογή της ισχύουσας νομοθεσίας στον χώρο εργασίας και δίδονται κάποια παραδείγματα, διεθνή και εγχώρια, σχετικά με καταγγελίες παράβασης που κατέληξαν σε κυρώσεις και σε πρόστιμα εκατομμυρίων ευρώ. Τέλος, γίνεται λόγος για καίρια ζητήματα γύρω από τα προσωπικά δεδομένα στα πλαίσια των μέσων κοινωνικής δικτύωσης, εμπορευματοποίσησης των προσωπικών δεδομένων, καθώς και σε ζητήματα υγείας με αφορμή την παγκόσμια επιδημία του Covid-19.

Πίνακας Περιεχομένων

Πίνακας Συντομεύσεων

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔικΕΕ	Δίκαιο Επιχειρήσεων & Εταιριών
ΕΚ	Ευρωπαϊκό Κοινοβούλιο
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΣΛΕΕ	Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης
DPA	Data Protection Authority
GDPR	General Data Protection Regulation

Κεφάλαιο 1 : Εισαγωγή

Η ραγδαία πρόοδος της πληροφορικής και της τεχνολογίας δίνουν τη δυνατότητα αλόγιστης και αθέμιτης επεξεργασίας και χρήσης δεδομένων προσωπικού χαρακτήρα σε οικονομικούς, πολιτικούς, κοινωνικούς και άλλους τομείς. Μάλιστα, σύμφωνα με την ευρωπαϊκή νομοθεσία για την προστασία των δεδομένων, συγκεκριμένα προσωπικά δεδομένα[1] θεωρούνται «ειδικά» — με άλλα λόγια, ευαίσθητα -και ως εκ τούτου, άξια ακόμη μεγαλύτερης νομικής προστασίας. Καθημερινά, κατά την περιήγηση στο διαδίκτυο εμφανίζονται αναδυόμενα παράθυρα με την είσοδο σε μία ιστοσελίδα που ζητούν τη συγκατάθεση του χρήστη στην επεξεργασία των προσωπικών του δεδομένων. Συνήθως το κείμενο ζητά τη συγκατάθεση του χρήστη για τη συλλογή προσωπικών δεδομένων, αναγνωριστικών χαρακτηριστικών της συσκευής πρόσβασης, γεωγραφικές συντεταγμένες, καθώς και πληροφορίες σχετικές με την περιηγήση, με σκοπό τη δημιουργία εξατομικευμένων διαφημίσεων και προώθησης περιεχόμενου και προϊόντων με βάση το ιστορικό του χρήστη. Δίνεται, κατά κανόνα, η επιλογή στον χρήστη αν θα αποδεχθεί τη συγκεκριμένη επιλογή και επεξεργασία πλήρως ή μερικώς, με την επιλογή ορισμένων κατηγοριών ή σκοπών επεξεργασίας, καθώς και να αρνηθεί την επεξεργασία. Ωστόσο, δεν είναι λίγες οι φορές που η επιλογή της άρνησης δε βρίσκεται σε ευδιάκριτο σημείο ενώ η επιλογή της συγκατάθεσης είναι εμφανώς πιο διακριτή. Σε κάθε περίπτωση ο χρήστης θα πρέπει να έχει την επιλογή ανάκλησης της συγκατάθεσής του.

---

[1] Με κριτήριο τη βαρύτητα των δεδομένων και το βαθμό διείσδυσή τους στη σφαίρα της ιδιωτικότητας και εν γένει της ψυχικής και σωματικής υπόστασης του προσώπου, τα Προσωπικά Δεδομένα διακρίνονται σε απλά και ευαίσθητα. Τα ευαίσθητα προσωπικά δεδομένα απαριθμούνται στο άρθρο 9 του Κανονισμού και είναι τα εξής: δεδομένα που αποκαλύπτουν την εθνοτική ή φυλετική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, τα γενετικά και βιομετρικά δεδομένα, δεδομένα που αφορούν την υγεία και δεδομένα που αφορούν τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός προσώπου. Τα προσωπικά δεδομένα που δεν ανήκουν στις ειδικές κατηγορίες του άρθρου 9 αποτελούν απλά προσωπικά δεδομένα. Η ειδοποιός διαφορά μεταξύ των δύο βασικών κατηγοριών προσωπικών δεδομένων είναι ότι για τα ευαίσθητα το επίπεδο προστασίας είναι υψηλότερο, η επεξεργασία τους επιτρέπεται μόνο κατ' εξαίρεση και οι όροι της νόμιμης επεξεργασίας τους ορίζονται ειδικώς στις διατάξεις του άρθρου 9 του Κανονισμού.

Ουσιαστικά, δηλώνοντας συμφωνία με το κείμενο, ο χρήστης συμφωνεί στη συλλογή, επεξεργασία και αποθήκευση δεδομένων προσωπικού χαρακτήρα κυρίως για εμπορικούς σκοπούς. Αυτό συνεπάγεται, ότι συλλέγονται, κωδικοποιούνται και ομαδοποιούναι δεδομένα σχετικά με τα ενδιαφέροντα του χρήστη, και στη συνέχεια χρησιμοποιούνται για να γίνεται προώθηση σχετικών διαφημίσεων.

Η ζήτηση της συγκατάθεσης αυτής, προκύπτει από τη σχετική νομοθεσία περί προστασίας των προσωπικών δεδομένων. Στα πλαίσια της ανάγκης για προστασία της ιδιωτικής ζωής του ατόμου και του σεβασμού των θεμελιωδών δικαιωμάτων και ελευθεριών, γίνεται όλο και πιο αισθητή η ανάγκη για την υπάρξη νομοθεσίας σχετικά με την προστασία προσωπικών δεδομένων. Πριν σχεδόν τρεις δεκαετίες, τον Οκτώβριο του 1995, τέθηκε σε ισχύ η οδηγία 95/46/ΕΚ περί προστασίας προσωπικών δεδομένων. Ωστόσο, η ραγδαία τεχνολογική εξέλιξη, η παγκοσμιοποίηση, η γιγάντωση των κοινωνικών δικτύων και η με εκθετικούς ρυθμούς αυξανόμενη χρήση του διαδικτύου στο πλαίσιο προσωπικών και επαγγελματικών δραστηριοτήτων, κατέστησαν την Οδηγία 95/46/ΕΚ ξεπερασμένη. Έτσι, στις 16 Απριλίου 2016 ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο ο υπ' αριθμό 2016/679/ΕΕ Γενικός Κανονισμός προσωπικών δεδομένων, που αντικατέστησε την εν λόγω Οδηγία. Ο ορισμός που δίνεται σχετικά με την έννοια των προσωπικών δεδομένων έχει ώς εξής:

> *«δεδομένα προσωπικού χαρακτήρα: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»* [2].

[2] Άρθρο 4, του Κανονισμού 2016/679. Στην Ελλάδα, ο ορισμός των δεδομένων προσωπικού χαρακτήρα διατυπώνεται στο άρθρο 44 παρ.1 περ. α του Ν. 4624/2019 , ο οποίος είναι κατ' ουσίαν ίδιος με αυτόν του Κανονισμού 2016/679/ΕΕ. Από την άλλη μεριά, σύμφωνα με τον προισχύσαντα ν. 2472/1997, ως δεδομένα προσωπικού χαρακτήρα οριζόταν: *«κάθε πληροφορία*

Όπως διαπιστώνουμε, η έννοια των προσωπικών δεδομένων είναι ευρύτατη, αφού οι πληροφορίες οι οποίες δύνανται να ταυτίζονται με ένα άτομο είναι ανεξάντλητες αλλά με πολλαπλές εκφάνσεις σε όλους τους τομείς της ζωής του προσώπου, όπως τη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή και κοινωνική[3].

Ήδη, δεν είναι ούτε λίγες ούτε σπάνιες οι περιπτώσεις παραβίασης των δεδομένων προσωπικού χαρακτήρα με αθέμιτη και άνομη συλλογή και επεξεργασία αυτών. Η αλόγιστη και ανάρμοστη χρήση τους από εταιρίες, για παράδειγμα τηλεφωνίας, έχει βρεθεί κατά καιρούς στο επίκεντρο των ειδήσεων. Τα τελευταία χρόνια, οι αρχές έχουν επιστήσει την προσοχή τους στην ενημέρωση και την ευαισθητοποίηση των υποκείμενων και των εταιριών σχετικά με τη σημασία συμμόρφωσης με το κανονισμό αναφορικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, προκειμένου να αποφευχθεί περιττή και απερίσκεπτη χρήση τους.

Ένα φλέγον ζήτημα των τελευταίων χρόνων είναι η προστασία προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης, που αποκτούν όλο και περισσότερο έδαφος στην καθημερινότητα των ανθρώπων παγκοσμίως. Η αυξανόμενη δημοτικότητα των κοινωνικών μέσων έχει προσελκύσει έναν τεράστιο αριθμό ανθρώπων να συμμετάσχουν σε πολλές διαδικτυακές δραστηριότητες σε καθημερινή βάση. Ο τεράστιος όγκος πληροφοριών κάθε χρήστη αποτελούν ελκυστικό στόχο για οργανισμούς που επιδιώκουν να συλλέξουν και να συγκεντρώσουν αυτές τις πληροφορίες είτε για νόμιμους σκοπούς είτε για κακόβουλους στόχους. Για παράδειγμα, ο χρήστης δημιουργεί τα δεδομένα παρέχοντας ευκαιρίες σε ερευνητές και επιχειρηματικούς εταίρους να μελετήσουν και να κατανοήσουν άτομα σε πρωτοφανείς κλίμακες.[4] Αυτές οι πληροφορίες είναι επίσης ζωτικής

που αναφέρεται στο υποκείμενο των δεδομένων». Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων».

[3] Εξ αντιδιαστολής καθίσταται φανερό ότι εκτός του πεδίου του ΓΚΠΔ παραμένουν τα δεδομένα εκείνα που δεν ταυτοποιούνται ή δεν μπορούν να ταυτοποιηθούν με συγκεκριμένο άτομο.

[4] Ghazaleh Beigi, Kai Shu, Yanchao Zhang, and Huan Liu. 2018. Securing social media user data: An adversarial approach. In Proceedings of the 29th Conference on Hypertext and Social Media. ACM.

σημασίας για την παροχή εξατομικευμένων υπηρεσιών, ιδίως της χρυσοφόρας «στοχευμένης διαφήμισης» (βλ. και «Data as currency/Data as asset»)[5],[6] και η έλλειψή τους θα είχε ως αποτέλεσμα την υποβάθμιση της ποιότητας των διαδικτυακών υπηρεσιών εξατομίκευσης.

Από την άλλη, τεράστιες ποσότητες δεδομένων που δημιουργούνται από χρήστες κινδυνεύουν να εκθέσουν το απόρρητο των ατόμων λόγω του πλούτου του περιεχομένου, συμπεριλαμβανομένων των σχέσεων ενός χρήστη και άλλων προσωπικών πληροφοριών. Αυτά τα δεδομένα καθιστούν επίσης τους διαδικτυακούς χρήστες ανιχνεύσιμους και, κατά συνέπεια, οι χρήστες είναι ιδιαίτερα ευάλωτοι σε πιθανούς κινδύνους που κυμαίνονται από διώξεις από κυβερνήσεις έως στοχευμένη απάτη. Για παράδειγμα, δεν είναι λίγοι οι χρήστες που μοιράζονται τα ταξιδιωτικά τους σχέδια δημόσια στα μέσα κοινωνικής δικτύωσης χωρίς να γνωρίζουν ότι αυτό οι πληροφορίες θα μπορούσαν να χρησιμοποιηθούν εναντίον τους για διαρρήξεις και κλοπές. Επιπλέον ευαίσθητες πληροφορίες που συνήθως δεν αποκαλύπτουν ρητά οι χρήστες μπορούν εύκολα να συναχθούν από τις δραστηριότητες στα μέσα κοινωνικής δικτύωσης, όπως η τοποθεσία, η ηλικία και οι σχέσεις εμπιστοσύνης με κοντινά τους πρόσωπα.

---

[5] Παραδοσιακά, τα "cookies", ήτοι οι ψηφιακοί κώδικες που καταγράφουν συγκεκριμένη συμπεριφορά χρήστη, χρησιμοποιούνται για την παρακολούθηση της διαδικτυακής συμπεριφοράς μέσω προγραμμάτων περιήγησης ενός υπολογιστή. Περαιτέρω, οι συλλεγείσες πληροφορίες των χρηστών, με τη χρήση των κατάλληλων αλγορίθμων, χρησιμοποιούνται για την εμφάνιση ατομικών στοχευμένων διαφημίσεων, είτε σε επιτραπέζιους υπολογιστές, είτε σε κινητές συσκευές. Εννοείται ότι οι ποσότητες δεδομένων καταναλωτών που συλλέγονται στο Διαδίκτυο είναι τεράστιες. Άλλωστε, η στοχευμένη διαφήμιση τροφοδοτείται καθοριστικά και από το γεγονός ότι οι χρήστες, δημοσιεύοντας το «προφίλ» τους, κοινοποιούν σημαντικές πληροφορίες για τα ενδιαφέροντά τους, τα hobbies τους, κλπ.

[6] Σύμφωνα με το Άρθρο 4 παρ. 4 του ΓΚΠΔ, η «κατάρτιση προφίλ» αναφέρεται ως «οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου».

Η αρχική, θεμελιώδης οδηγία περί προστασίας προσωπικών δεδομένων, ήρθε το 1995 (οδηγία 95/46/ΕΚ) εντός της Ευρωπαϊκής Ένωσης. Στη συνέχεια, το 2016, με τον Κανονισμό (ΕΕ) 2016/679 (ευρύτερα γνωστός και ως: «GDPR»)[7], ο οποίος κατήργησε την οδηγία, ορίστηκε νέο, πιο εξειδικευμένο αλλά και πιο αυστηρό νομικό πλαίσιο σχετικα. Η ευρεία εφαρμογή και διάδοσή του, έφερε καταλυτικές αλλαγές εντός των οργανισμών, δημιουργώντας παράλληλα νέες ανάγκες και νέες επιχειρηματικές ευκαιρίες στην αγορά. Για παράδειγμα, από τη στιγμή που όλες οι εταιρίες έπρεπε να συμμορφωθούν με τον κανονισμό, δημιουργήθηκε επιτακτική ανάγκη για ύπαρξη συμβούλων και εκπαιδευτών, καθώς και τροποποιήσεων στα τεχνολογικά συστήματα.

Η προστασία των δεδομένων έχει αποκτήσει υψηλή θέση στην ΕΕ με τις νομοθεσίες του κοινοβουλίου της ΕΕ για την προστασία των δεδομένων να αποδεικνύουν επαρκώς την πρόθεση της ΕΕ. Το τεράστιο μέγεθος των δεδομένων που παράγονται, διαβιβάζονται και υποβάλλονται σε επεξεργασία σήμερα είναι ένας από τους παράγοντες που απαιτούν την έγκριση του ΓΚΠΔ και η ΕΕ επιδιώκει να διασφαλίσει «ένα ισχυρό και πιο συνεκτικό πλαίσιο προστασίας δεδομένων στην Ένωση». Η παραγωγή μαζικών δεδομένων και η επεξεργασία τους που καθίστανται τόσο εύκολα δυνατές σε σύντομο χρονικό διάστημα από τις τεχνολογικές εξελίξεις καθιστούν την έκδοση του παρόντος κανονισμού πιο ορθολογική.

Είναι σημαντικό να τονισθεί ότι, καταρχήν, το άρθρο 16 της Συνθήκης για τη Λειτουργία της ΕΕ (ΣΛΕΕ) θεσπίζει ρητά την προστασία των προσωπικών δεδομένων στην ΕΕ. Στην §2 του ίδιου άρθρου προβλέπεται η αρμοδιότητα του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου να θεσπίζουν κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων από την Ένωση και τα κράτη-μέλη και σχετικά με την ελεύθερη

[7] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, ΚΑΝΟΝΙΣΜΟΣ (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).

κυκλοφορία αυτών, οι οποίοι κανόνες θα υπόκεινται στον έλεγχο ανεξάρτητων αρχών και δε θα θίγουν του ειδικούς κανόνες που προβλέπονται στο άρθρο 39 της ΣΛΕΕ [8].

Τέλος, σύμφωνα με το άρθρο 8 του Χάρτη των Θεμελιωδών Διακιωμάτων της Ευρωπαϊκής Ένωσης, ορίζεται ότι κάθε φυσικό πρόσωπο, ως υποκείμενο των δεδομένων, έχει το δικαίωμα στην προστασία των προσωπικών του δεδομένων.[9] Επίσης, θα πρέπει να σημειωθεί ότι, η Συνταγματική κατοχύρωση του δικαιώματος στην προστασία των προσωπικών δεδομένων, στην Ελλάδα, προβλέπεται στο άρθρο 9Α Σ[10]. Το άρθρο αυτό εξειδικεύει το περιεχόμενο της παρ. 1 του άρθρου 5 του Συντάγματος, στο οποίο κατοχυρώνεται η προστασία της προσωπικότητας[11].

Όσον αφορά τη χώρα μας, η προστασία των προσωπικών δεδομένων ρυθμίστηκε αρχικά με την ενσωμάτωση της Οδηγίας 95/46/ΕΚ με το Ν. 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα» (όπως αυτός τροποποιήθηκε και ίσχυε) μέχρι την κατάργησή του από τον προσφάτως ψηφισθέντα Ν.4624/2019. Ο Ν. 2472/1997 απετέλεσε το βασικό και αρκούντως αποτελεσματικό εργαλείο προστασίας των προσωπικών δεδομένων στην Ελλάδα, για σχεδόν μία εικοσαετία.

Κλείνοντας, θα ήταν παράληψη να μην αναφερθούμε και στην πλέον πρόσφατη Οδηγία 2019/770/ΕΕ, το άρθρο 3 § 1 εδ.β' της οποίας προβλέπει τη δυνατότητα να συμφωνηθεί, στο

---

[8] Βλ. Ιγγλεζάκη, Ι., Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, εκδόσεις Interactive Books, 2018

[9] Βλ. άρθρο 16 παρ.1 ΣΛΕΕ, αρθ.8 παρ.1 Χάρτη Θεμελιωδών Δικαιωμάτων.

[10] Βλ. 9Α Συντάγματος : *«Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».*

[11] Βλ. Λ. Μήτρου, Άρθρο 9 Α Συντάγματος, σε Φ. Σπυρόπουλο/Ξ. Κοντιάδη/Χ. Ανθόπουλο/Γ. Γεραπετρίτη (επιμ.), Σύνταγμα, Κατ' άρθρο Ερμηνεία, 2017, σελ. 214-233.

πλαίσιο μιας σύμβασης προμήθειας ψηφιακού περιεχομένου ή υπηρεσίας, ότι "ο καταναλωτής θα παράσχει δεδομένα προσωπικού χαρακτήρα αντί για τη συνήθη χρηματική παροχή"[12].

Κεφάλαιο 2: Η οδηγία 95/46/ΕΚ και ιστορική αναδρομή

2.1. Η οδηγία 95/46/ΕΚ και τα κριτήρια σύννομης επεξεργασίας προσωπικών δεδομένων

Αρχικά, η ανάγκη για προστασία των προσωπικών δεδομένων των ατόμων οδήγησε στην έκδοση της οδηγίας 95/46/ΕΚ[13] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995. Η οδηγία αυτή τέθηκε σε εφαρμογή σε δεδομένα που επεξεργάζονται είτε με αυτοματοποιημένα μέσα, όπως μια ηλεκτρονική βάση δεδομένων χρηστών ή πελατών είτε σε δεδομένα που αποτελούν μέρος μη αυτοματοποιημένων συστημάτων αρχειοθέτησης όπως τα παραδοσιακά έντυπα αρχεία. Αξίζει να αναφερθεί ότι όταν πρόκειται για θέματα εθνικής άμυνας, δημόσιας ασφάλειας ή δραστηριότητες του κράτους στα πλαίσια του ποινικού δικαίου , ο σκοπός της οδηγίας 95/46/ΕΚ ήταν να καθοριστούν βασικά κριτήρια για τη νομιμότητα της επεξεργασίας έτσι ώστε να επιτευχθεί η προστασία των θεμελιωδών δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.[14]

Λόγω της σπουδαιότητος της οδηγίας αυτής, η οποία διαμόρφωσε διαχρονικά το βασικό κορμό του δικαίου της προστασίας των προσωπικών δεδομένων, θεωρήθηκε σκόπιμο να γίνει μια σύντομη αναφορά στα βασικά σημεία της.

Η επεξεργασία των δεδομένων είναι σύννομη μόνο εάν: [15]

---

[12] Μαργαρίτης Ε., Πληρωμή με αντίτιμο Προσωπικά Δεδομένα: Είναι πράγματι τα προσωπικά δεδομένα το «νέο νόμισμα»; Διαθέσιμο σε: https://www.lawspot.gr/nomika-blogs/eyaggelos_margaritis/pliromi-me-antitimoprosopika-dedomena-einai-pragmati-ta-prosopika?lspt_destination=upgrade

[13] ΟΔΗΓΙΑ 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ, διαθέσιμη: https://www.lawspot.gr/nomikes-plirofories/nomothesia/odigia-95-46-ek-toy-eyropaikoy-koinovoylioy-kai-toy-symvoylioy-tis

[14] Άρθρο 1, 95/46/ΕΚ

[15] Άρθρο 7, 95/46/ΕΚ

i) για την επεξεργασία έχει δοθεί ρητή συγκατάθεση από το υποκείμενο πρόσωπο που αφορούν τα δεδομένα ή

ii) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος· ή

iii) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας· ή

iv) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων· ή

v) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας ή σε τρίτο· ή

vi) η επεξεργασία είναι απαραίτητη για τους σκοπούς του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων που χρήζουν προστασίας.

Οι αρχές της ποιότητας των δεδομένων, οι οποίες πρέπει να εφαρμόζονται για όλες τις νόμιμες δραστηριότητες επεξεργασίας δεδομένων, είναι δύο. Πρώτον, τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε θεμιτή και νόμιμη επεξεργασία και να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς. Πρέπει επίσης να είναι κατάλληλα και όχι υπερβολικά, ακριβή και, εφόσον απαιτείται, ενημερωμένα, να μην αποθηκεύονται για μεγαλύτερο χρονικό διάστημα από το αναγκαίο και μόνο για τους σκοπούς για τους οποίους συλλέχθηκαν. Δεύτερον, απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση και την επεξεργασία δεδομένων που αφορούν την υγεία ή τη

σεξουαλική ζωή[16]. Η διάταξη αυτή συνοδεύεται από ορισμένες εξαιρέσεις που αφορούν, για παράδειγμα, περιπτώσεις όπου η επεξεργασία είναι απαραίτητη για την προστασία ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή για σκοπούς προληπτικής ιατρικής διάγνωσης.

2.2. Τα δικαιώματα του υποκειμένου σχετικά με την επεξεργασία των προσωπικών του δεδομένων

Το πρόσωπο του οποίου τα δεδομένα υποβάλλονται σε επεξεργασία, το υποκείμενο των δεδομένων, μπορεί να ασκήσει τα ακόλουθα δικαιώματα:

2.2.1. Το δικαίωμα λήψης πληροφοριών

Θα πρέπει να γνωστοποιείται στο υποκείμενο πρόσωπο η ταυτότητα του υπεύθυνου επεξεργασίας ή/και του εκπροσώπου του, ποιοι θα είναι οι αποδέκτες των δεδομένων όπως επίσης και ο σκοπός για το οποίο γίνεται η επεξεργασία των δεδομένων του. Επιπρόσθετα, θα πρέπει το υποκείμενο να ενημερώνεται σε ποιο βαθμό είναι απαραίτητη η παροχή και η επεξεργασία των δεδομένων του καθώς και αν υπάρχει δυνατότητα άρνησης και ποιες είναι οι προβλεπόμενες κυρώσεις. Τέλος, θα πρέπει να είναι ενήμερος για την δυνατότητα πρόσβασης στα καταχωρημένα δεδομένα και κατά πόσο είναι εφικτή η διόρθωσή τους.[17]

2.2.2. Το δικαίωμα πρόσβασης

Εγγυάται ότι το υποκείμενο πρόσωπο θα λαμβάνει ανά ορισμένα χρονικά διαστήματα την επιβεβαίωση επεξεργασίας ή μη των δεδομένων του, τους σκοπούς για τους οποίους χρησιμοποιούνται, τους αποδέκτες αυτών. Επίσης, οποιαδήποτε διόρθωση, διαγραφή ή κλείδωμα

[16] Άρθρο 8, 95/46/ΕΚ

[17] Άρθρο 10, 95/46/ΕΚ

των δεδομένων λόγω μη έγκυρης ή μη σύννομης επεξεργασίας αυτών θα πρέπει να γνωστοποείται.[18]

2.2.3. Το δικαίωμα εναντίωσης στην επεξεργασία δεδομένων

Το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να αντιτάσσεται, για νόμιμους λόγους, στην επεξεργασία των δεδομένων που το αφορούν. Θα πρέπει επίσης να έχει το δικαίωμα να αντιτάσσεται, κατόπιν δωρεάν αιτήματος, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα τα οποία ο υπεύθυνος επεξεργασίας αναμένει ότι θα υποβληθούν σε επεξεργασία για σκοπούς άμεσης εμπορικής προώθησης. Θα πρέπει τέλος, να ενημερώνεται πριν από την αποκάλυψη δεδομένων προσωπικού χαρακτήρα σε τρίτους για σκοπούς άμεσης εμπορικής προώθησης και να του παρέχεται ρητά το δικαίωμα να αντιτάσσεται σε τέτοιες γνωστοποιήσεις.[19]

2.2.4. Περιορισμοί άσκησης των δικαιωμάτων και εξαιρέσεις

Ωστόσο, ένα άλλο σημαντικό στοιχείο της οδηγίας 95/46/ΕΚ είναι οι εξαιρέσεις και οι περιορισμοί από τα δικαιώματα του υποκειμένου που αναφέρθηκαν στις προηγούμενες υποενότητες: το δικαίωμα της ενημέρωσης του προσώπου στο οποίο αναφέρονται τα δεδομένα, το δικαίωμα πρόσβασης και τη δημοσιότητα της επεξεργασίας. Ορίζονται περιπτώσεις, όπως η ασφάλεια του κράτους, η δημόσια ασφάλεια, η εθνική άμυνα όπου μπορεί τα δικαιώματα του υποκειμένου να περιορίζονται. Άλλες τέτοιες περιπτώσεις είναι δημοσιονομικά, νομισματικά ή φορολογικά και άλλα θέματα που έχουν άμεση επιρροή στο οικονομικό συμφέρον κράτους μέλους ή για την πρόληψη ή/και δίωξη παραβάσεων ποινικού νόμου.[20]

---

[18] Άρθρο 12, 95/46/ΕΚ

[19] Άρθρο 14, 95/46/ΕΚ

[20] Άρθρο 13, 95/46/ΕΚ

2.3. Η ασφάλεια της επεξεργασίας και η κοινοποίηση σε αρχή ελέγχου

Η ασφάλεια και η εμπιστευτικότητα της επεξεργασίας των ευαίσθητων προσωπικών δεδομένων έχουν αναμφίβολα ύψιστη σημασία καθώς, κάθε πρόσωπο που του έχει παρασχεθεί πρόσβαση στα δεδομένα προσωπικού χαρακτήρα (μόνο μέσω σύμβασης ή δικαιοπραξίας) πρέπει να τα επεξεργάζεται υπό την εποπτεία και μόνον κατ' εντολή του υπευθύνου της επεξεργασίας. Πρέπει να εφαρμόζονται τα κατάλληλα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα από τυχαία ή παράνομη καταστροφή ή τυχαία απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση, ιδίως όταν τα δεδομένα είναι διαθέσιμα σε κάποιο δίκτυο.[21]

Τέλος, η κοινοποίηση της επεξεργασίας σε αρχή ελέγχου είναι σημαντική και υποχρεωτική. Πρέπει να ενημερώνεται η εθνική εποπτική αρχή από τον υπεύθυνο επεξεργασίας πριν από την εκτέλεση οποιασδήποτε επεξεργασίας. Μετά την παραλαβή της κοινοποίησης, η εκάστοτε εποπτική αρχή θα πρέπει να διενεργεί προηγούμενους ελέγχους για τον προσδιορισμό συγκεκριμένων κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων Πρέπει να λαμβάνονται μέτρα για να εξασφαλίζεται η δημοσιότητα των επεξεργασιών και οι αρχές ελέγχου πρέπει να τηρούν μητρώο των κοινοποιούμενων επεξεργασιών.[22]

2.4. Η εισαγωγή του Γενικού Κανονισμού για την Προστασία Δεδομένων

Έπειτα από την οδηγία 95/46/ΕΚ το 1995 σχετικά με την προστασία των προσωπικών δεδομένων, και την πάροδο των ετών που έφερε ραγδαίες τεχνολογικές εξελίξεις αλλάζοντας τη ζωή των ανθρώπων σε εξαιρετικά απόβλεπτο βαθμό, το 2011 ο επόπτης προστασίας δεδομένων έκανε λόγο για την επιτακτική ανάγκη αναθεώρησης της οδηγίας του 1995. Στις αρχές του 2012 το Ευρωπαϊκό Συμβούλιο προτείνει την αναδιάρθρωση της οδηγίας έτσι ώστε να ενδυναμώσει τα δικαιώματα ιδιωτικότητας στο διαδίκτυο και να ωθήσει την ψηφιακή οικονομία της Ευρώπης. Στις 12 Μαρτίου 2014, το Ευρωπαϊκό Κοινοβούλιο ψηφίζει υπέρ του Γενικού Κανονισμού για την Προστασία Δεδομένων (από εδώ και στο εξής ΓΚΠΔ) με 621 θετικές ψήφους. Στη συνέχεια, το

---

[21] Άρθρο 17, 95/46/ΕΚ

[22] Άρθρο 18, 95/46/ΕΚ

καλοκαίρι της επόμενης χρονιάς, το Συμβούλιο έχει διαμορφώσει το μεγαλύτερο ποσοστό του ΓΚΠΔ, ενώ τον Δεκέμβριο του 2015 το Ευρωπαϊκό κοινοβούλιο και το Συμβούλιο καταλήγουν σε συμφωνία σχετικά με το ολοκληρωμένο πλέον κείμενο του ΓΚΠΔ. Τον Φεβρουάριο του 2016 δημιουργείται το πλάνο υλοποίησης του κανονοσμου, όπου στις 27 Απριλίου 2016 δημοσιεύεται ο Κανονισμός 2016/679/ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και για την κατάργηση της Οδηγίας 95/46/ΕΚ. Ο ΓΚΠΔ ακολουθεί τα βασικά σημεία της Οδηγίας, όμως, εισάγει και αρκετές καινοτομίες. Το δικαίωμα στα προσωπικά δεδομένα θεωρείται θεμελιώδες δικαίωμα, γι' αυτό και στο άρθρο 1 του ΓΚΠΔ ορίζεται ότι ο Κανονισμός «προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα». Σύμφωνα δε με το άρθρο 2, ο Κανονισμός εφαρμόζεται σε κάθε μορφή επεξεργασίας, είτε αυτή είναι αυτοματοποιημένη είτε όχι και ανεξάρτητα από το εάν η επεξεργασία λαμβάνει χώρα εντός της Ε.Ε. (άρθρο 3).Σκοπός του ΓΚΠΔ, μεταξύ άλλων, είναι να ενισχύσει ένα ευρύ φάσμα υφιστάμενων δικαιωμάτων και να θεσπίσει νέα για τα άτομα.[23]

Ο Κανονισμός, αποτελούμενος από 99 άρθρα, τέθηκε σε ισχύ την 26η Μαΐου του 2018, ενόσω τα κράτη - μέλη της ΕΕ υποχρεούνται να εφαρμόσουν κατά ομοιόμορφο τρόπο τον Κανονισμό, προκειμένου τα υποκείμενα των δεδομένων να προστατεύονται υπό ένα κοινό νομικό πλαίσιο. Ας σημειωθεί ότι, η επιλογή του Κανονισμού ως νομοθετικού εργαλείου απέβλεπε ακριβώς στη συνεκτικότητα της ρύθμισης δεδομένου ότι παράγει άμεσα αποτελέσματα στα κράτη-μέλη ανεξάρτητα από το εθνικό δίκαιο και υπερισχύει τυχόν αντίθετων εθνικών κανόνων[24]. Περαιτέρω, ο νέος Κανονισμός ορίζει ότι οι εταιρείες με έδρα εκτός ΕΕ, οφείλουν να εφαρμόζουν τους ίδιους κανόνες με τις εταιρείες με έδρα στην ΕΕ, εφόσον προσφέρουν αγαθά και υπηρεσίες που

[23]«The History of the General Data Protection Regulation», διαθέσιμο στην ιστοσελίδα: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[24] Βλ. Μήτρου, Λ., Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων Νέο Δίκαιο – Νέες Υποχρεώσεις – Νέα Δικαιώματα», τεύχος 29 σειράς Δίκαιο και Κοινωνία στον 21ο Αιώνα, ΕΚΔΟΣΕΙΣ ΣΑΚΚΟΥΛΑ ΑΘΗΝΑ – ΘΕΣΣΑΛΟΝΙΚΗ 2017 σελ. 33 επ.

σχετίζονται με δεδομένα προσωπικού χαρακτήρα ή παρακολουθούν τη συμπεριφορά φυσικών προσώπων στην ΕΕ.

2.5. Προκλήσεις σχετικά με την εφαρμογή του ΓΚΠΔ

Στο σημείο αυτό αξίζει να παρατεθεί το σημείο της αιτιολογικής έκθεσης του Κανονισμού: «Οι ραγδαίες τεχνολογικές εξελίξεις και η παγκοσμιοποίηση δημιούργησαν νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Η κλίμακα της συλλογής και της ανταλλαγής δεδομένων προσωπικού χαρακτήρα αυξήθηκε σημαντικά. Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους. Τα φυσικά πρόσωπα ολοένα και περισσότερο δημοσιοποιούν προσωπικές πληροφορίες και τις καθιστούν διαθέσιμες σε παγκόσμιο επίπεδο. Η τεχνολογία έχει αλλάξει τόσο την οικονομία όσο και την κοινωνική ζωή και θα πρέπει να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης και τη διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα».

Συνακόλουθα, με την επιβολή του νέου αυτού Κανονισμού, οι υπεύθυνοι επεξεργασίας κλήθηκαν να αντιμετωπίσουν πολλές προκλήσεις για την εκπλήρωση των νομικών απαιτήσεων. Παρά τις μακροχρόνιες συζητήσεις, διαπραγματεύσεις και αναθεωρήσεις σχετικά με το τελικό κείμενο του ΓΚΠΔ και τον επαρκή χρόνο που δόθηκε στους οργανισμούς για να εφαρμόσουν τις απαιτούμενες αλλαγές στις διαδικασίες, τα προϊόντα και τις υπηρεσίες τους, λίγοι οργανισμοί ήταν σε θέση να συμμορφωθούν πλήρως με τον ΓΚΠΔ.

Ένας από τους κύριους λόγους γι' αυτό είναι ότι ο ΓΚΠΔ είναι ως επί το πλείστον ένα νομικό έγγραφο, παρέχοντας λίγες τεχνικές οδηγίες προς τις οντότητες που υποχρεούνται να τον εφαρμόσουν. Αν και αυτή ήταν μια σκόπιμη επιλογή, προκειμένου να μη δεσμεύσουν τον ΓΚΠΔ με ρητές τεχνολογίες που θα ευνοούσαν συγκεκριμένες πλατφόρμες και λύσεις, αυτή η τεχνολογική άγνωστη προσέγγιση προκάλεσε απρόβλεπτες επιπλοκές σε οργανισμούς που προσπαθούσαν να να προσαρμόσουν τις εσωτερικές τους διαδικασίες στις διατάξεις του ΓΚΠΔ. Για παράδειγμα, μία από τις πιο βαθιές δυσκολίες θα ήταν η συμμόρφωση με τις υπάρχουσες

διαδικασίες δημιουργίας αντιγράφων ασφαλείας. Τα ιδρύματα είναι υποχρεωμένα να διατηρούν τακτικά αντίγραφα ασφαλείας των δεδομένων τους σε περίπτωση συμβάντων που θέτουν σε κίνδυνο την ασφάλεια ή φυσικές καταστροφές. Ένα μεγάλο ερώτημα που προκύπτει από τον ΓΚΠΔ, είναι ο τρόπος με τον οποίο οι οργανισμοί πρέπει να χειρίζονται τα αντίγραφα ασφαλείας τους μόλις ένας χρήστης ζητήσει να καταργήσει τα δεδομένα του. Προφανώς, σύμφωνα με τον ΓΚΠΔ, αυτή η ενέργεια διαγραφής πρέπει να εκτελεστεί και στα αντίγραφα ασφαλείας, ανοίγοντας έτσι την πόρτα σε πιθανές καταχρήσεις δεδομένων, σκόπιμες εκμεταλλεύσεις ή ακόμα και τυχαία λάθη.[25]

Ένα έτος μετά την έναρξη ισχύος του πρωτοποριακού γενικού κανονισμού της ΕΕ για την προστασία δεδομένων, οι Financial Times δημοσίευσαν ένα άρθρο σχετικά με ενδείξεις ότι ο Κανονισμός έχει ελλείψεις και ακούσιες συνέπειες που πλήττουν τις επιχειρήσεις, τους καταναλωτές και την καινοτομία. Οι υποστηρικτές υποστηρίζουν ότι ο Κανονισμός, ο οποίος περιορίζει τον τρόπο με τον οποίο οι εταιρείες μπορούν να χρησιμοποιούν πληροφορίες που αγγίζουν την εθνικότητα, τις πολιτικές απόψεις, τις θρησκευτικές πεποιθήσεις ή τον σεξουαλικό προσανατολισμό κάποιου, είναι το κλειδί για την ανάπτυξη της εμπιστοσύνης των χρηστών και των πελατών προς τις εταιρίες. Ωστόσο, από την άλλη πλευρά, υποστηρίζεται ότι ο ΓΚΠΔ δημιουργεί δυσκολίες για τις ευρωπαϊκές επιχειρήσεις. Για παράδειγμα, ο νόμος απαιτεί από τους οργανισμούς να εξηγούν πώς χρησιμοποιούν τα δεδομένα προσωπικού χαρακτήρα σε συστήματα τεχνητής νοημοσύνης και σε άλλες αυτοματοποιημένες διαδικασίες λήψης αποφάσεων που έχουν σημαντικό αντίκτυπο στα άτομα, όπως εάν θα προσφέρουν ενυπόθηκο δάνειο. Η πολυπλοκότητα των συστημάτων τεχνητής νοημοσύνης τα καθιστά πιο ακριβή, αλλά καθιστά επίσης δυσκολότερη την εξήγηση των αποφάσεών τους. Οι επιχειρήσεις που δεν είναι σε θέση να συμμορφωθούν, θα καταλήξουν να αποφεύγουν εντελώς τα προηγμένα συστήματα τεχνητής νοημοσύνης.[26]

---

[25] Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy001, Διαθέσιμο στο: https://doi.org/10.1093/cybsec/tyy001

[26] J. Espinoza, «EU admits it has been hard to implement GDPR», Financial Times, 23/06/2020 Διαθέσιμο στο: https://www.ft.com/content/66668ba9-706a-483d-b24a-18cfbca142bf

Κεφάλαιο 3: Γενικός Κανονισμός για την Προστασία Δεδομένων 2016/679

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, στις 27 Απριλίου 2016 στις Βρυξέλλες, δημοσιεύτηκε ο Κανονισμός 2016/679 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 του 1995 (βλ. Κεφάλαιο 2). Ο νέος αυτός Κανονισμός[27] τέθηκε σε ισχύ στις 25 Μαϊου 2018 για όλα τα κράτη μέλη και άλλαξε ριζικά το τοπίο στον χώρο της προστασίας των προσωπικών δεδομένων επιβάλλοντας πρόσθετες υποχρεώσεις, όχι μόνο σε υπεύθυνους επεξεργασίας αλλά πλέον και στους εκτελούντες την επεξεργασία προσωπικών δεδομένων.

Το ουσιαστικό πεδίο εφαρμογής του Κανονισμού καθορίζεται στο άρθρο 2 ΓΚΠΔ. Έτσι, εφαρμόζεται στην, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης, δηλ. σε ένα διαρθρωμένο σύνολο προσωπικών δεδομένων, τα οποία είναι προσβάσιμα με βάση συγκεκριμένα κριτήρια, ήτοι περισσότερα από ένα κριτήρια (άρθρο 2 παρ. 1 και άρθρο 4 αριθ. 6 ΓΚΠΔ)[28].

Ειδικότερα, ο Κανονισμός βρίσκει εφαρμογή στην επεξεργασία προσωπικών δεδομένων, ενώ η έννοια της επεξεργασίας ορίζεται ευρύτατα, ήτοι: «Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση

---

[27] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ, διαθέσιμος: https://www.lawspot.gr/nomikes-plirofories/nomothesia/genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr

[28] Ιγγλεζάκης, Ι., Ο Γενικός κανονισμός Προστασίας προσωπικών Δεδομένων – Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, 2018, σελ. 29.

πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή» (βλ. άρθρο 4 σημ. 2)

3.1. Βασικές αρχές και στοιχεία που διέπουν την επεξεργασία προσωπικών δεδομένων

Υπάρχουν κάποιες βασικές αρχές πάνω στις οποίες στηρίζεται η επεξεργασία των προσωπικών δεδομένων. Η επεξεργασία γίνεται κατά τρόπο τέτοιο έτσι ώστε να διατηρείται η νομιμότητα, η αντικειμενικότητα και η διαφάνεια προς το υποκείμενο. Η επεξεργασία των δεδομένων θεωρείται σύννομη εάν είναι σύμφωνη με το νόμο, επιδιώκει θεμιτό σκοπό και είναι απαραίτητη σε μια δημοκρατική κοινωνία για την επίτευξη ενός νόμιμου σκοπού. Όσον αφορά την αρχή της διαφάνειας, αφορά τον υπεύθυνο επεξεργασίας που εξηγεί στο υποκείμενο των δεδομένων τον τρόπο με τον οποίο τα δεδομένα χρησιμοποιούνται/υποβάλλονται σε επεξεργασία. Θα πρέπει η πληροφορήση να είναι απλή, συνοπτική, εύκολα κατανοητή, σαφής και προσβάσιμη. Η συλλογή των δεδομένων θα πρέπει να έχει σαφής και νόμιμους σκοπούς, οι οποίοι είναι καθορισμένοι από την αρχή και τα δεδομένα δε θα πρέπει να υπόκεινται σε περαιτέρω επεξεργασία, ενώ θα πρέπει να συλλέγονται μόνο τα αναγκαία για τους σκοπούς δεδομένα. Επίσης, τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται όταν είναι απαραίτητο και να διορθώνεται οποιαδήποτε ανακρίβεια. Τέλος, είναι αναγκαία η ασφαλής και προστατευμένη αποθήκευσή τους και η αποφυγή οποιασδήποτε παράνομης επεξεργασίας, καταστροφής ή απώλειας. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη για την τήρηση των βασικών αυτών αρχών. [29]

Σκοπός των βασικών αυτών αρχών είναι τα υποκείμενα των δεδομένων να μην εξαπατώνται ή παραπλανώνται όσον αφορά την επεξεργασία των δεδομένων τους. Οι αρχές της δίκαιης και διαφανούς επεξεργασίας απαιτούν να ενημερώνεται το υποκείμενο των δεδομένων για την ύπαρξη της πράξης επεξεργασίας και τους σκοπούς της. Ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα κάθε περαιτέρω πληροφορία που είναι αναγκαία για τη διασφάλιση δίκαιης και διαφανούς επεξεργασίας, λαμβάνοντας υπόψη τις ειδικές περιστάσεις και το πλαίσιο εντός του οποίου τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται

[29] Άρθρο 5, 2016/679 του ΓΚΠΔ.

σε επεξεργασία. Επιπλέον, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται για την ύπαρξη κατάρτισης προφίλ και τις συνέπειες της εν λόγω κατάρτισης προφίλ. Η δικαιοσύνη των πληροφοριών συνδέεται επίσης με τη λογοδοσία, δεδομένου ότι τεκμαίρεται ότι οι πληροφορίες που πρέπει να παρέχονται καθιστούν δυνατό τον έλεγχο της συμμόρφωσης. Η πληροφοριακή δικαιοσύνη εγείρει συγκεκριμένα ζητήματα σε σχέση με την τεχνητή νοημοσύνη και τα μαζικά δεδομένα, λόγω της πολυπλοκότητας της επεξεργασίας που εμπλέκεται στις εφαρμογές τεχνητής νοημοσύνης, της αβεβαιότητας του αποτελέσματός της και της πολλαπλότητας των σκοπών της. Λόγω της αυξημένης χρήσης τεχνητής νοημοσύνης για επεξεργασία και ανάλυση δεδομένων, θα πρέπει ο υπεύθυνος επεξεργασίας να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα κατάλληλα ώστε να διασφαλίζεται, ιδίως, ότι διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες στα δεδομένα προσωπικού χαρακτήρα και ότι ο κίνδυνος σφαλμάτων ελαχιστοποιείται. Επίσης, πρέπει να διασφαλίζεται ότι προστατεύονται τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που λαμβάνει υπόψη τους δυνητικούς κινδύνους που ενέχουν για τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και αποτρέπει, μεταξύ άλλων, τις διακρίσεις εις βάρος φυσικών προσώπων λόγω φυλετικής ή εθνοτικής καταγωγής, πολιτικών πεποιθήσεων, θρησκείας ή πεποιθήσεων, συμμετοχής σε συνδικαλιστική οργάνωση, γενετικής κατάστασης ή κατάστασης υγείας ή γενετήσιου προσανατολισμού, ή που έχουν ως αποτέλεσμα τη λήψη μέτρων με τέτοιο αποτέλεσμα. [30] Τα μέτρα που πρέπει να ληφθούν από τον υπεύθυνο επεξεργασίας εξαρτώνται από το πεδίο εφαρμογής, το πλαίσιο και τον σκοπό της διαδικασίας· σχετικά με τη σοβαρότητα και την πιθανότητα επέλευσης κινδύνων για τα δικαιώματα των υποκειμένων των δεδομένων· και για την ανάγκη να είναι «κατάλληλο» και «κατάλληλο». Ουσιαστικά, δεν υπάρχει γενική μέθοδος καθορισμού μέτρων που μπορεί να λάβει κάθε υπεύθυνος επεξεργασίας χωρίς να εξετάσει το πλαίσιο και τις ιδιαιτερότητές του. [31]

---

[30] Sartor G., Lagiola F.,: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service, ISBN: 978-92-846-6771-0

[31] Christian Kurtz, Florian Wittner, Martin Semmann, Wolfgang Schulz, Tilo Böhmann, Accountability of platform providers for unlawful personal data processing in their ecosystems–A

Ο υπεύθυνος επεξεργασίας θα πρέπει να έχει λάβει σαφή συγκατάθεση από το υποκείμενο για τη συλλογή και επεξεργασία των δεδομένων και να μπορεί να το αποδείξει. Ακόμα και στην περίπτωση που η συγκατάθεση δίνεται στα πλαίσια κάποιας γενικότερης δήλωσης-αποδοχής, θα πρέπει το σκέλος της επεξεργασίας των προσωπικών δεδομένων να παρουσιάζεται διακριτά. Σκοπός αυτού είναι το υποκείμενο να είναι ενήμερο για την επεξεργασία των προσωπικών του δεδομένων. Ωστόσο, το υποκείμενο, οποιαδήποτε στιγμή μπορεί να ανακαλέσει τη συγκατάθεσή του και από τη στιγμή της ανάκλησης και έπειτα ο υπεύθυνος επεξεργασίας δε θα έχει το δικαίωμα να συνεχίσει να επεξεργάζεται τα δεδομένα. Όση επεξεργασία έχει πραγματοποιηθεί πριν τη στιγμή της ανάκλησης, θεωρείται, νόμιμη.[32] Στην περίπτωση που το υποκείμενο είναι παιδί ηλικίας κάτω των δεκαέξι (16) ετών, η συγκατάθεση θα πρέπει να δοθεί από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού, του οποίου τα στοιχεία είναι απαραίτητο να επαληθεύονται.[33] Αυτό σημαίνει ότι μόνο τα παιδιά από δεκαέξι (16) ετών και πάνω μπορούν να δώσουν τη συγκατάθεσή τους.

Είναι σημαντικό να αναφερθεί ότι για να θεωρηθεί έγκυρη η συγκατάθεση θα πρέπει το υποκείμενο να μη βρίσκεται υπό πίεση, να έχει ενημερωθεί πλήρως για το αντικείμενο και τις συνέπειες της συγκατάθεσης και τέλος ο σκοπός της συγκατάθεσης να είναι εύλογος και συγκεκριμένος.[34]

Στο Άρθρο 9 αναφέρονται κάποιες περιπτώσεις όπου απαγορεύεται η επεξεργασία προσωπικών δεδομένων (βλ. ευαίσθητα προσωπικά δεδομένα) [35]. Τέτοια δεδομένα αφορούν την εθνοτική

---

socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR, Journal of Responsible Technology, Volume 9, 2022

[32] Άρθρο 7, 2016/679 του ΓΚΠΔ.

[33] Άρθρο 8, 2016/679 του ΓΚΠΔ.

[34] FRA/COE, Handbook on European Data Protection Law, Belgium, 2014, page 56. Διαθέσιμο στο: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

[35] Βλ. και υποσ. 1 της παρούσης διπλωματικής εργασίας.

καταγωγή, πολιτικές πεποιθήσεις, τη θρησκεία, τον συνδικαλισμό, την υγεία τη σεξουαλική ζωή του υποκειμένου και γενετικά ή βιομετρικά δεδομένα που αποσκοπούν στην αδιαμφισβήτητη ταυτοποίηση του προσώπου.[36] Το σκεπτικό πίσω από την επιλογή αυτών των κατηγοριών δεδομένων είναι ότι οποιαδήποτε κατάχρηση αυτών των δεδομένων προσωπικού χαρακτήρα θα είχε πολύ σημαντικές επιπτώσεις στα ατομικά δικαιώματα και ελευθερίες και ίσως μη-αναστρέψιμες και μακροπρόθεσμες στο κοινωνικό περιβάλλον του υποκειμένου.[37]

3.2. Τα δικαιώματα του υποκειμένου των δεδομένων

3.2.1. Το δικαίωμα της πληροφόρησης

Το άρθρο 13 απαριθμεί ορισμένες πληροφορίες που πρέπει να παρέχονται στο υποκείμενο των δεδομένων όταν λαμβάνονται δεδομένα προσωπικού χαρακτήρα από το υποκείμενο των δεδομένων, όπως: την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας ή του εκπροσώπου του, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, τους σκοπούς και τη νομική βάση της επεξεργασίας, τα έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, τους αποδέκτες των δεδομένων προσωπικού χαρακτήρα (κατά περίπτωση), τον υπεύθυνο επεξεργασίας που προτίθεται να διαβιβάσει δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό και τη νομική βάση για τη διαβίβαση αυτή. Άλλες πληροφορίες που πρέπει να παρέχονται περιλαμβάνουν την περίοδο αποθήκευσης των δεδομένων προσωπικού χαρακτήρα, την ύπαρξη του δικαιώματος του υποκειμένου των δεδομένων για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας, καθώς και το δικαίωμα στη φορητότητα των δεδομένων, την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης ανά πάσα στιγμή χωρίς να θίγεται η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της, το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή, κατά πόσον η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική

---

[36] Άρθρο 9, 2016/679 του ΓΚΠΔ.

[37] Salami, Emmanuel, An Analysis of the General Data Protection Regulation (EU) 2016/679 (May 10, 2017). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=2966210

απαίτηση και τις συνέπειες της μη παροχής των εν λόγω δεδομένων, την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ. Ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει πληροφορίες σχετικά με την πρόθεσή του να επεξεργαστεί προσωπικά δεδομένα για σκοπούς άλλους από αυτούς που αποκτήθηκαν. [38]

3.2.2.Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Ο υπεύθυνος επεξεργασίας θα πρέπει να επιβεβαιώνει στο υποκείμενο σχετικά με την επεξεργασία στην οποία υπόκεινται τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και να του παρέχεται πρόσβαση μεταξύ άλλων, στους σκοπούς που αφορά η επεξεργασία, στους αποδέκτες, στο χρονικό διάστημα για το οποίο διατηρούνται τα δεδομένα στα αρχεία και να είναι ενημερωμένο σχετικά με υπάρχουσες εποπτικές αρχές και το δικαίωμα υποβολής καταγγελίας καθώς και για την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων.[39] Το δικαιωμα στην πρόσβαση των δεδομένων αποτελεί βασική πτυχή της διαφάνειας. Στο άρθρο 15 παράγραφος 1 στοιχείο η) αφορά ειδικά την αυτοματοποιημένη λήψη αποφάσεων, απαιτώντας από τον υπεύθυνο επεξεργασίας να παρέχει υποχρεωτικά πληροφορίες που αφορούν την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων και καθοριστικές πληροφορίες αναφορικά με τον τρόπο χρήσης των δεδομένων σε προγράμματα τεχνητής νοημοσύνης που οδηγούν στην αυτοματοιποιημένη λήψη αποφάσεων, καθώς και τη λογική και τα κριτήρια που χρησιμοποιούνται προκειμένου να ληφθεί η απόφαση.

Έχει υπάρξει ευρεία συζήτηση σχετικά με το κατά πόσον το άρθρο 15 θα πρέπει να ερμηνευθεί υπό την έννοια ότι παρέχει στα υποκείμενα των δεδομένων το δικαίωμα να λαμβάνουν εξατομικευμένη επεξήγηση των αυτοματοποιημένων αξιολογήσεων και αποφάσεων. Δυστυχώς, η διατύπωση του εν λόγω άρθρου 15 θεωρείται διφορούμενη. Ειδικότερα, δεν διευκρινίζεται αν η υποχρέωση παροχής πληροφοριών σχετικά με τη «λογική που διέπεται» αφορά μόνο την παροχή γενικών πληροφοριών σχετικά με τις μεθόδους που υιοθετούνται στο σύστημα ή συγκεκριμένες

[38] Άρθρο 13, 2016/679 του ΓΚΠΔ.

[39] Άρθρο 15, 2016/679 του ΓΚΠΔ.

πληροφορίες σχετικά με τον τρόπο με τον οποίο οι μέθοδοι αυτές εφαρμόζονται στο υποκείμενο των δεδομένων (δηλαδή, μια ατομική εξήγηση). [40]

Ο τρόπος με τον οποίο θα πρέπει να εφαρμόζεται το δικαίωμα πρόσβασης στην πράξη δεν είναι απολύτως σαφής, ιδίως στο πλαίσιο της επεξεργασίας δεδομένων που περιλαμβάνει αλγόριθμους ή αυτοματοποιημένες αποφάσεις, η οποία είναι όλο και πιο συχνή στην επεξεργασία δεδομένων προσωπικού χαρακτήρα. Μεγάλος όγκος δεδομένων προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία από πολλούς υπεύθυνους επεξεργασίας δεδομένων, γεγονός που δημιουργεί την ανάγκη για αυτοματοποιημένη επεξεργασία και ανάλυση των εν λόγω δεδομένων. Μια τέτοια αυτοματοποιημένη επεξεργασία μπορεί να είναι πολύ εξελιγμένη, χρησιμοποιώντας εργαλεία εξόρυξης δεδομένων και μηχανικής μάθησης για την ανακάλυψη μοτίβων και σχέσεων σε μεγάλα σύνολα δεδομένων. Τα εργαλεία κατάρτισης προφίλ μπορούν να κατηγοριοποιήσουν και να ομαδοποιήσουν τα υποκείμενα των δεδομένων, προβλέποντας και αποδίδοντάς τους ιδιαίτερα χαρακτηριστικά. [41]

Ο ΓΚΠΔ αναγνωρίζει ότι αυτές οι πρακτικές ενέχουν διάφορους κινδύνους για τα υποκείμενα των δεδομένων. Ορισμένες διατάξεις είναι προσαρμοσμένες ώστε να παρέχουν στα υποκείμενα των δεδομένων περαιτέρω προστασία, όπως το δικαίωμα εναντίωσης στην αυτοματοποιημένη ατομική λήψη αποφάσεων[42] και το δικαίωμα να μην υπόκεινται σε αποφάσεις που βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία[43], τα οποία αναφέρονται σε επόμενες ενότητες.

---

[40] Wachter, S., B. Mittelstadt, and L. Floridi (2016). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law 7, 76–99. & Edwards, L. and Veale, M. (2019). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law and Technology Review, 16-84.

[41] Bart Custers, Anne-Sophie Heijne, The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice, Computer Law & Security Review, Volume 46, 2022

[42] Άρθρο 21, 2016/679 του ΓΚΠΔ

[43] Άρθρο 22, 2016/679 του ΓΚΠΔ

Ωστόσο, η αποτελεσματική επίκληση αυτών των δικαιωμάτων είναι δυνατή μόνο εάν τα υποκείμενα των δεδομένων γνωρίζουν την ύπαρξη, τη λειτουργία και τις συνέπειες αυτών των πρακτικών. Το άρθρο 15 παράγραφος 1 του GDPR ορίζει ρητά ότι όταν χρησιμοποιείται αυτοματοποιημένη λήψη αποφάσεων (συμπεριλαμβανομένης της κατάρτισης προφίλ), το δικαίωμα πρόσβασης για τα υποκείμενα των δεδομένων περιλαμβάνει πρόσβαση σε σημαντικές πληροφορίες σχετικά με τη λογική, τη σημασία και τις προβλεπόμενες συνέπειες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων. Σε σημείωσή του ο ΓΚΠΔ εξειδικεύει περαιτέρω αυτό το δικαίωμα σε σημαντικές πληροφορίες δηλώνοντας ότι δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, συμπεριλαμβανομένων των εμπορικών απορρήτων, ιδίως του λογισμικού προστασίας πνευματικών δικαιωμάτων. [44]

3.2.3.Δικαίωμα διόρθωσης και διαγραφής (δικαίωμα στη λήθη)

Στις διατάξεις των άρθρων 16 και 17 του ΓΚΠΔ κατοχυρώνονται το δικαίωμα διόρθωσης και το δικαίωμα διαγραφής των δεδομένων. Ειδικότερα, σύμφωνα με το άρθρο 16 του ΓΚΠΔ, το υποκείμενο των δεδομένων έχει δικαίωμα διόρθωσης ανακριβών προσωπικών δεδομένων του και δικαίωμα συμπλήρωσης ελλιπών προσωπικών δεδομένων, μεταξύ άλλων μέσω της παροχής συμπληρωματικής δήλωσης. [45] Μπορούμε, συνεπώς, να θεωρήσουμε ότι η διάταξη αυτή υλοποιεί την αρχή της ακρίβειας που κατοχυρώνεται στο άρθρο 5 παρ. 1 στοιχ. δ΄ ΓΚΠΔ[46].

Περαιτέρω, κατοχυρώνεται το δικαίωμα διαγραφής που είναι γνωστό και ως «δικαίωμα στη λήθη». Ειδικότερα, το άρθρο 17 του ΓΚΠΔ προβλέπει το δικαίωμα διαγραφής που αναφέρεται ευρέως ως δικαίωμα στη λήθη. Πρόκειται κατ' ουσίαν για το δικαίωμα του υποκειμένου των δεδομένων να ζητάει από τον υπεύθυνο επεξεργασίας τη διαγραφή προσωπικών δεδομένων που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση, εφόσον ισχύει μια από τις ακόλουθες προϋποθέσεις (άρθρο 17 §§ 1, 2 του Κανονισμού): α) τα δεδομένα προσωπικού χαρακτήρα δεν

---

[44] Σημείωση 63, 2016/679 του ΓΚΠΔ

[45] Άρθρο 16, 2016/679 του ΓΚΠΔ.

[46] Ιγγλεζάκης, (2018) ό. π. σελ. 99.

είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία, β) το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία, γ) το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία, δ) τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα, ε) τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν, ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας, στ) τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί σε σχέση με την προσφορά υπηρεσιών της κοινωνίας των πληροφοριών σε παιδί.

Όπως διαπιστώνουμε, η ουσία του δικαιώματος αυτού είναι ότι οι πληροφορίες του υποκειμένου των δεδομένων πρέπει να διαγράφονται με την παρουσία ορισμένων προϋποθέσεων όπως είναι: ότι τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τον σκοπό της συλλογής τους, ανάκληση της συγκατάθεσης του υποκειμένου των δεδομένων, παράνομη επεξεργασία, τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν για συμμόρφωση με νομική υποχρέωση που υποστηρίζεται από το νόμο κ.α. Εάν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και υποχρεούται να διαγράψει τα δεδομένα αυτά, τότε, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, ενημερώνει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα ότι το υποκείμενο των δεδομένων έχει ζητήσει τη διαγραφή τυχόν συνδέσμων ή αντιγράφων ή αναπαραγωγών. Το δικαίωμα στη λήθη είναι ένα δικαίωμα που, λογικά, θα τύχει τεράστιας υποστήριξης από τα δικαστήρια. [47]

Αξίζει να σημειωθεί ότι το δικαίωμα στη λήθη, ειδικότερα, στις μηχανές αναζήτησης στο διαδίκτυο αναγνωρίσθηκε από το ΔικΕΕ όταν δέχθηκε ότι το δικαίωμα αυτό ερείδεται στη βάση του άρθρου 12 της οδηγίας 95/46/ΕΚ. Ειδικότερα, με την απόφαση C-131/12, αναγνωρίσθηκε το δικαίωμα του υποκειμένου των δεδομένων να διαγράφονται προσωπικά δεδομένα που το αφορούν

[47] Άρθρο 17, 2016/679 του ΓΚΠΔ.

και τα οποία περιλαμβάνονται σε λίστες αποτελεσμάτων των μηχανών αναζήτησης πληροφοριών στο Διαδίκτυο, μετά από μια έρευνα, βάσει του ονοματεπωνύμου του υποκειμένου των δεδομένων[48].

Ωστόσο στο άρθρο 17 αναφέρονται και κάποιες εξαιρέσεις στο δικαίωμα της λήθης. Προβλέπεται ότι το εν λόγω δικαίωμα δεν ισχύει όταν η επεξεργασία είναι απαραίτητη: για την άσκηση του δικαιώματος της ελεύθερης έκφρασης και της πληροφόρησης, για τη συμμόρφωση με νομική υποχρέωση ή για την εκτέλεση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, για σκοπούς που σχετίζονται με το δημόσιο συμφέρον εντός του τομέα της δημόσιας υγείας, για λόγους αρχειοθέτησης προς το δημόσιο συμφέρον ή επιστημονικής ή ιστορικής έρευνας· για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων.

3.2.4. Δικαίωμα περιορισμού της επεξεργασίας

Το υποκείμενο των δεδομένων έχει το δικαίωμα να περιορίσει την επεξεργασία όταν ισχύει ένα από τα ακόλουθα: το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων προσωπικού χαρακτήρα, η επεξεργασία θα περιοριστεί εν αναμονή της επαλήθευσης της εν λόγω γνησιότητας, το υποκείμενο θεωρεί παράνομη την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και αντιτίθεται στη διαγραφή τους, ενώ αντ' αυτής ζητά τον περιορισμό της χρήσης τους, τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον χρήσιμα για τους σκοπούς της επεξεργασίας, αλλά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, άσκηση ή υπεράσπιση νομικών αξιώσεων ή τέλος, το υποκείμενο των δεδομένων έχει αντιταχθεί στην επεξεργασία εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερισχύουν εκείνων του υποκειμένου των δεδομένων. Στην περίπτωση δεδομένων που περιορίζονται βάσει των ανωτέρω, τα εν λόγω δεδομένα υποβάλλονται σε επεξεργασία μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων για τη θεμελίωση, άσκηση, υπεράσπιση νομικών αξιώσεων ή για την προστασία των δικαιωμάτων άλλου φυσικού ή νομικού προσώπου ή

---

[48] Ιγγλεζάκης, Ι., Το δικαίωμα στην ψηφιακή λήθη και οι μηχανές αναζήτησης στο Διαδίκτυο. Παρουσίαση της απόφασης Google Spain του ΔΕΕ της 13ης Μαίου 2014 (υπόθεση C-131/12), ΔτΑ 2015 (66), σελ. 827 επ.·

δημόσιου συμφέροντος. Το υποκείμενο των δεδομένων ενημερώνεται πριν από την άρση του περιορισμού της επεξεργασίας.[49]

3.2.5. Δικαίωμα στη φορητότητα των δεδομένων

Ένα, επίσης, νέο δικαίωμα που θεσπίζεται με τον Κανονισμό είναι το δικαίωμα στη φορητότητα των δεδομένων, σύμφωνα με το άρθρο 20 ΓΚΠΔ. Έτσι, ο Κανονισμός προβλέπει ότι το υποκείμενο του οποίου τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί, έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας τα εν λόγω δεδομένα σε δομημένη και αναγνώσιμη μορφή. Επιπρόσθετα, έχει το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας που πρώτος σύλλεξε τα δεδομένα ή ακόμη και να αιτείται την απευθείας διαβίβαση αυτών εφόσον το επιτρέπουν τα διαθέσιμα τεχνικά μέσα. Οι προϋποθέσεις για την εφαρμογή της είναι ότι η επεξεργασία να βασίζεται σε συγκατάθεση, όπως αναφέρεται στο άρθρο 6 του ΓΚΠΔ και η επεξεργασία να πραγματοποιείται με αυτοματοποιημένα μέσα.[50]

Δεν υπόκεινται όλα τα προσωπικά δεδομένα στο δικαίωμα φορητότητας. Μόνο προσωπικά δεδομένα για τα οποία η επεξεργασία βασίζεται σε συγκατάθεση ή μια συμβατική σχέση. Αυτός ο περιορισμός αντιστοιχεί σε μεγάλο βαθμό στην απαίτηση ότι τα προσωπικά δεδομένα που τίθενται υπό επεξεργασία παρασχέθηκαν από το υποκείμενο των δεδομένων. Κατά συνέπεια, μόνο ένα μέρος από τα προσωπικά δεδομένα καλύπτονται από το δικαίωμα στη φορητότητα, τα παρεχόμενα δεδομένα, τα οποία εξ ορισμού, παρέχονται απευθείας από το υποκείμενο των δεδομένων. Ωστόσο, τα παραγόμενα δεδομένα, αυτά που είτε προέρχονται είτε συνάγονται από αναλύσεις, δεν θεωρούνται πως παρέχονται από το υποκείμενο των δεδομένων ως εκ τούτου δεν υπόκεινται στο δικαίωμα της φορητότητας. Ο ΓΚΠΔ παρέχει ένα σχετικά ισχυρό δικαίωμα στη φορητότητα των δεδομένων του υποκειμένου. Η φορητότητα των δεδομένων εξετάζεται από την οπτική γωνία του υποκειμένου των δεδομένων, με έμφαση σχετικά με την προστασία των

---

[49] Άρθρο 18, 2016/679 του ΓΚΠΔ.

[50] Άρθρο 20, 2016/679 του ΓΚΠΔ.

δεδομένων. Η δημιουργία ενός ολοκληρωμένου καθεστώτος για τη φορητότητα κάθε είδους προσωπικών δεδομένων δεν ήταν η προτεραιότητα του νομοθέτη της ΕΕ, όπως φαίνεται από τον αποκλεισμό της κατηγορίας των παραγόμενων προσωπικών δεδομένων.[51]

Σε αυτό το σημείο αξίζει να αναφερθεί ότι η άσκηση του δικαιώματος της φορητότητας των δεδομένων δεν θίγει την άσκηση του δικαιώματος στη λήθη. Ως εκ τούτου, οι πληροφορίες που έχουν «ξεχαστεί» σύμφωνα με το άρθρο 17 του ΓΚΠΔ δεν μπορούν να αποτελέσουν αντικείμενο τέτοιας διαβίβασης. Ο υπεύθυνος επεξεργασίας παρέχει τα δεδομένα στο υποκείμενο των δεδομένων σε «δομημένο, κοινώς χρησιμοποιούμενο, αναγνώσιμο από μηχανήματα και διαλειτουργικό μορφότυπο...». Έχει προταθεί ότι το δικαίωμα στη φορητότητα των δεδομένων θα βοηθήσει ορισμένες επιχειρήσεις, καθώς το δικαίωμα μεταφοράς προσωπικών δεδομένων μεταξύ υπευθύνων επεξεργασίας δημιουργεί μια σημαντική ευκαιρία για την προσέλκυση πελατών από ανταγωνιστές (π.χ. οι διαδικτυακές επιχειρήσεις και τα δίκτυα κοινωνικών μέσων μπορούν να προσελκύσουν χρήστες που προηγουμένως ήταν απρόθυμοι να μετακινηθούν από έναν ανταγωνιστή, λόγω των δυσκολιών που σχετίζονται με τη δημιουργία νέου λογαριασμού. Επομένως, τούτο θα ενθαρρύνει τον ανταγωνισμό μεταξύ των εταιριών αυτών και θα έχει ως αποτέλεσμα την καλύτερη παροχή υπηρεσιών.[52]

3.2.6. Το δικαίωμα εναντίωσης

Περαιτέρω, ο Κανονισμός κατοχυρώνει το δικαίωμα εναντίωσης, όπως και το δικαίωμα εναντίωσης σε αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης και της κατάρτισης προφίλ.

Το άρθρο 21 του ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων το δικαίωμα να αντιταχθεί στην επεξεργασία δεδομένων που το αφορούν, εκτός εάν υπάρχει δημόσιο συμφέρον ή έννομο

---

[51] Zufall, F., & Zingg, R. (2021). Data Portability in a Data-Driven World. In S. Peng, C. Lin, & T. Streinz (Eds.), Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration (pp. 215-234). Cambridge: Cambridge University Press.

[52] Salami, Emmanuel, An Analysis of the General Data Protection Regulation (EU) 2016/679 (May 10, 2017). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=2966210

συμφέρον του υπευθύνου επεξεργασίας ή τρίτου που καθιστά αδύνατη την εν λόγω αντίρρηση. Σε τέτοια περίπτωση, ο υπεύθυνος επεξεργασίας πρέπει να είναι σε θέση να αποδείξει την ύπαρξη τέτοιων παραγόντων που συνιστούν εξαίρεση από το δικαίωμα εναντίωσης. Το υποκείμενο των δεδομένων έχει, επίσης, δικαίωμα αντίρρησης για την επεξεργασία των προσωπικών του δεδομένων για σκοπούς άμεσου μάρκετινγκ και η εν λόγω αντίρρηση σηματοδοτεί τον τερματισμό της επεξεργασίας των δεδομένων για τέτοιους σκοπούς.[53] Το αποτέλεσμα του δικαιώματος εναντίωσης βάσει του ΓΚΠΔ θα εξαρτηθεί σε μεγάλο βαθμό από τις συγκεκριμένες περιστάσεις αυτής της αντίρρησης. Πρώτον, όταν ένα υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία των δεδομένων του, ο υπεύθυνος επεξεργασίας πρέπει να περιορίσει την επεξεργασία των δεδομένων αυτών έως ότου κριθεί το βάσιμο της προβαλλόμενης αντίρρησης. Δεύτερον, όταν η επεξεργασία πραγματοποιείται με σκοπό την άμεση εμπορική προώθηση, η αντίρρηση αυτή καθίσταται αυτομάτως έγκυρη και δεσμευτική χωρίς εξαιρέσεις.

3.3. Ασφάλεια των δεδομένων και γνωστοποίηση παραβάσεων

Σύμφωνα με τον Κανονισμό, κρίνεται απαραίτητη η εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων από τον υπεύθυνο επεξεργασίας και τον εκτελών την επεξεργασία για να διασφαλιστεί ορισμένο επίπεδο ασφάλειας με σκοπό την αποφυγή κινδύνων, συμπεριλαμβανομένης της ψευδωνυμοποίησης και της κρυπτογράφησης προσωπικών δεδομένων. την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την ανθεκτικότητα των συστημάτων επεξεργασίας, τη δυνατότητα έγκαιρης αποκατάστασης από φυσικές ή τεχνικές βλάβες και την επαναφορά της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα.[54]

Μόλις δημιουργηθούν δεδομένα, υπάρχουν προφανή ζητήματα σχετικά με τη φύλαξή τους και γύρω από τη διατήρηση της ιδιωτικής ζωής εκείνων που τα έχουν παραδώσει. Όλοι γνωρίζουν το έγκλημα στον κυβερνοχώρο, είτε αυτό στρέφεται κατά οργανισμών (για παράδειγμα, μέσω της

[53] Άρθρο 21, 2016/679 του ΓΚΠΔ.

[54] Άρθρο 32 2016/679 του ΓΚΠΔ.

χρήσης «ransomware» για την απόσπαση οικονομικού κέρδους ή εναντίον ατόμων μέσω των διαφόρων τύπων κακόβουλου λογισμικού που μπορούν να μολύνουν υπολογιστές). Όλα τα προσωπικά δεδομένα που έχουν αποθηκευτεί ενδέχεται να επιτεθούν από χάκερ. Για παράδειγμα, μια επίθεση σχετικά με τον οργανισμό Sony το 2011 είχε ως αποτέλεσμα την κλοπή των «ονομάτων, διευθύνσεων, διευθύνσεις ηλεκτρονικού ταχυδρομείου, ημερομηνίες γέννησης, ονόματα χρήστη, κωδικούς πρόσβασης, συνδέσεις, ερωτήσεις ασφαλείας και περισσότερα» από τους λογαριασμούς των χρηστών στο Sony PlayStation Network. Ανεξάρτητα από το πόσο προσεκτικά αυτά τα δεδομένα μπορεί να προστατεύονται, θα κινδυνεύουν πάντα, οπότε το λογισμικό ασφαλείας πρέπει να ενημερώνεται συνεχώς για να παραμένει ένα βήμα μπροστά από τους χάκερ. Επίσης, σε ορισμένες περιπτώσεις, τα δεδομένα που διατηρούνται για ένα άτομο μπορεί να είναι ανώνυμα (ή «αποχαρακτηρισμένα»), κάτι που μπορεί να φαίνεται αξιόπιστος τρόπος προστασίας της ιδιωτικής ζωής αυτού του ατόμου. Ωστόσο, έχει αποδειχθεί ότι όταν συνδυάζονται πολλά αποχαρακτηρισμένα σύνολα δεδομένων, είναι δυνατή η παραβίαση της ανωνυμίας ατόμων με τριγωνισμό μεταξύ αυτών των συνόλων δεδομένων. Για παράδειγμα, στο Αμερικανικό πλαίσιο έχει επισημανθεί ότι «γνωρίζοντας τον ταχυδρομικό κώδικα ενός ατόμου εντοπίζει αυτό το άτομο σε έναν στους 30.000 (ο μέσος πληθυσμός ενός ταχυδρομικού κώδικα). Η σύνδεση ενός ταχυδρομικού κώδικα με μια ημερομηνία γέννησης μειώνει το εύρος πιθανής ταυτοποίησης σε περίπου μία στις 80 ενώ η περαιτέρω σύνδεση του φύλου και του έτους γέννησης είναι επαρκής, κατά μέσο όρο, για να προσδιορίζουν με μοναδικό τρόπο ένα άτομο. Φαίνεται, λοιπόν, ότι τα δεδομένα τα οποία οι χρήστες παραδίδουν στην υπηρεσία διαδικτύου δεν μπορεί να διασφαλιστεί ότι οι πάροχοι προστατεύονται από κλοπή από τρίτους· και ότι τα δεδομένα αυτά, τα οποία θα μπορούσαν καταρχήν να θεωρηθούν ότι προστατεύονται μέσω διαδικασίες ανωνυμοποίησης στην πράξη δεν είναι. [55]

Η εποπτική αρχή θα πρέπει να ενημερώνεται από τον υπεύθυνο επεξεργασίας για οποιαδήποτε παραβίαση δεδομένων προσωπικού χαρακτήρα εντός 72 ωρών από τη στιγμή που έλαβε γνώση της εν λόγω παραβίασης, εκτός εάν η παραβίαση δεν είναι πιθανό να οδηγήσει σε κίνδυνο για τα

[55] S. E. Koonin and M. J. Holland, 'The value of big data for urban science' in Lane, Privacy, Big Data, and the Public Good, Cambridge University Press (2014)

δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η εν λόγω κοινοποίηση περιγράφει μεταξύ άλλων, βασικά στοιχεία της παραβίασης, όπως ο κατά προσέγγιση αριθμός των υποκειμένων των δεδομένων που παραβιάστηκαν καθώς και τις κατηγορίες δεδομένων, γνωστοποιούνται τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, περιγράφει τις πιθανές συνέπειες της παραβίασης και περιγράφει τα μέτρα που έχει λάβει ή προτίθεται να λάβει ο υπεύθυνος επεξεργασίας για την αντιμετώπιση της παραβίασης. Ορίζεται επίσης ότι ο υπεύθυνος επεξεργασίας υποχρεούται τεκμηρίωσης για τυχόν παραβιάσεις δεδομένων προσωπικού χαρακτήρα, αναφέροντας τα πραγματικά γεγονότα, τα αποτελέσματά της παραβίασης και τα όποια μέτρα πρόκειται να ληφθούν με σκοπό τη διόρθωση ή/και τον μετριασμό της παραβίασης.[56] Η διάταξη αυτή αποτελεί νέα εισαγωγή στον ΓΚΠΔ και θεωρείται ότι βασίζεται στο άρθρο 4 παράγραφος 3 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες 2002/58/ΕΚ[57].

Πέραν της εποπτικής αρχής, σαφή ενημέρωση πρέπει να λαμβάνει και το υποκείμενο του οποίου τα προσωπικά δεδομένα παραβιάστηκαν, όταν η παραβίαση υπάρχει σημαντική πιθανότητα να προκαλέσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η κοινοποίηση αυτή δεν απαιτείται εάν: ο υπεύθυνος επεξεργασίας αποδεδειγμένα έχει χρησιμοποιήσει κατάλληλα και επαρκή τεχνικά και οργανωτικά μέτρα προστασίας ή ο υπεύθυνος επεξεργασίας έχει λάβει μεταγενέστερα μέτρα τα οποία διασφαλίζουν ότι δεν είναι πλέον πιθανό να επέλθει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα ή θα απαιτούσε δυσανάλογη προσπάθεια. Στην τελευταία περίπτωση, θα υπήρχε δημόσια ανακοίνωση ή παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων θα ενημερώνονται αντίστοιχα αποτελεσματικό τρόπο.[58] Ενώ η κοινοποίηση στην εποπτική αρχή που απαιτείται βάσει του άρθρου 33 του ΓΚΠΔ είναι υποχρεωτική «εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις

---

[56] Άρθρο 33 του ΓΚΠΔ.

[57]Οδηγία 2002/58/ΕΚ

[58] Άρθρο 34 του ΓΚΠΔ.

ελευθερίες των φυσικών προσώπων.», η κοινοποίηση που πρέπει να γίνει στο υποκείμενο των δεδομένων σύμφωνα με το άρθρο 34 του ΓΚΠΔ πρέπει να γίνεται μόνο όταν υπάρχει πιθανότητα υψηλού κινδύνου. Ως εκ τούτου, οι υπεύθυνοι επεξεργασίας που μπορούν να αποδείξουν την έλλειψη κινδύνου κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα ενδέχεται να είναι σε θέση να αποφύγουν την εν λόγω διάταξη σχετικά με τις κοινοποιήσεις. Αξίζει επίσης να σημειωθεί ότι, ενώ το επίπεδο κινδύνου που απαιτείται για την κοινοποίηση στην εποπτική αρχή είναι απλώς «οποιοδήποτε επίπεδο κινδύνου», αυτό που απαιτείται για την κοινοποίηση στο υποκείμενο των δεδομένων είναι «υψηλού κινδύνου», με την έννοια ότι το μεγαλύτερο μέρος της παραβίασης δεδομένων για την οποία θα ειδοποιηθεί ο υπεύθυνος επεξεργασίας πιθανότατα δε θα κοινοποιηθεί στο υποκείμενο των δεδομένων.

3.4. Εποπτική Αρχή

Το άρθρο 51 του ΓΚΠΔ προβλέπει τη σύσταση μίας ή περισσότερων ανεξάρτητων εποπτικών αρχών με ευθύνη την παρακολούθηση και την προστασία των διατάξεων του παρόντος κανονισμού.[59] Στο επόμενο άρθρο, το 52, προβλέπονται λεπτομέρειες για την πλήρη ανεξαρτησία των εποπτικών αρχών, συμπεριλαμβανομένου του κράτους, παρέχοντας παράλληλα στην εποπτική αρχή το ανθρώπινο κεφάλαιο και πόρους, τόσο τεχνικής φύσεως όσο και οικονομικής, όπως επίσης και εγκαταστάσεις και τις κατάλληλες υποδομές που απαιτούνται για την αποτελεσματική εκτέλεση των καθηκόντων.

Το άρθρο 57 του ΓΚΠΔ απαριθμεί τα καθήκοντα της εποπτικής αρχής, συμπεριλαμβανομένης της παρακολούθησης και της επιβολής της εφαρμογής του κανονισμού, της παροχής συμβουλών στα διάφορα κυβερνητικά σκέλη σχετικά με την προστασία του δικαιώματος στην ιδιωτική ζωή των υποκειμένων των δεδομένων και του χειρισμού καταγγελιών που υποβάλλονται από υποκείμενα δεδομένων. Επιπλέον, η εποπτική αρχή οφείλει να συνεργάζεται με άλλες εποπτικές αρχές με σκοπό τη διασφάλιση της συνέπειας της εφαρμογής και της επιβολής του ΓΚΠΔ, να διεξάγει έρευνες σχετικά με την εφαρμογή του, να παρακολουθεί τις τυχόν εξελίξεις οι οποίες σχετίζονται

[59] Άρθρο 51, 2016/679 του ΓΚΠΔ.

και πιθανόν να έχουν αντίκτυπο στην προστασία των δεδομένων προσωπικού χαρακτήρα, να προωθεί την κατάρτιση κώδικα δεοντολογίας ενώ παράλληλα να γνωμοδοτεί και να εγκρίνει τον εν λόγω κώδικα δεοντολογίας. Τέλος, η εποπτική αρχή ενθαρρύνει τη δημιουργία μηχανισμών πιστοποίησης της προστασίας των δεδομένων και σφραγίδων και σημάτων προστασίας δεδομένων.[60]

Στη συνέχεια του Κανονισμού, στο άρθρο 58 απαριθμούνται οι εξουσίες της εποπτικής αρχής οι οποίες χωρίζονται σε ερευνητικές, διορθωτικές, εξουσιοδοτικές/συμβουλευτικές εξουσίες. Ορισμένες από τις εξουσίες που διαπερνούν και τους τρεις επικεφαλής των εξουσιών περιλαμβάνουν την εξουσία να ζητούν πληροφορίες από τον ελεγκτή/εκτελούντα την επεξεργασία και τους εκπροσώπους τους, εξουσίες έρευνας, επανεξέταση των πιστοποιήσεων, εξουσίες έκδοσης προειδοποιήσεων, επιπλήξεων, απαγορεύσεων, προστίμων, απαγορεύσεων επεξεργασίας κ.λπ.[61] Όταν υπάρχουν περισσότερες από μία εποπτικές αρχές, σύμφωνα με τον μηχανισμό της συνεκτικότητας, οι εν λόγω εποπτικές αρχές θα πρέπει να συνεργάζονται μεταξύ τους με σκοπό την επίτευξη των στόχων του ΓΚΠΔ.[62]

Ο ΓΚΠΔ προβλέπει στο άρθρο 31, ότι τόσο ο υπεύθυνος όσο και ο εκτελών την επεξεργασία πρέπει να είναι διαθέσιμοι στην εποπτική αρχή, να συνεργάζονται και να συμβάλουν και να διευκολύνουν την εκτέλεση των καθηκόντων της.[63]

3.4.1. Η Αρχή Προστασίας Προσωπικών Δεδομένων στην Ευρωπαϊκή Ένωση

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ), το οποίο έχει νομική προσωπικότητα, συστάθηκε σύμφωνα με τις διατάξεις του άρθρου 68 του ΓΚΠΔ.[64] Το ΕΣΠΔ απαρτίζεται από τον

---

[60] Άρθρο 57, 2016/679 του ΓΚΠΔ.

[61] Άρθρο 58, 2016/679 του ΓΚΠΔ.

[62] Άρθρο 63, 2016/679 του ΓΚΠΔ.

[63] Άρθρο 31, 2016/679 του ΓΚΠΔ.

[64] Άρθρο 68, 2016/679 του ΓΚΠΔ.

επικεφαλής μιας εποπτικής αρχής κάθε κράτους μέλους και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ή τους εκπροσώπους τους. Κατά την αιτιολογική σκέψη 139 του ΓΚΠΔ, το ΕΣΠΔ αντικαθιστά την ομάδα προστασίας που συστάθηκε με την οδηγία 95/46/ΕΚ. Το ΕΣΠΔ αναμένεται να ενεργεί ανεξάρτητα και να μην λαμβάνει οδηγίες από κανέναν, παρά μόνο να παρέχει συμβουλές στην Επιτροπή για την τροποποίηση του ΓΚΠΔ, όπως μπορεί να ζητηθεί.[65]

Στο άρθρο 70 επισημαίνονται τα καθήκοντα του ΕΣΠΔ, τα οποία περιλαμβάνουν: την παρακολούθηση της ορθής εφαρμογής του ΓΚΠΔ, όπως απαιτείται βάσει του ΓΚΠΔ, την εξέταση κάθε ζητήματος που καλύπτει την εφαρμογή του Κανονισμού και την έκδοση σχετικών κατευθυντήριων γραμμών, συστάσεων και βέλτιστων πρακτικών, την παροχή γνώμης στην Επιτροπή σχετικά με τις απαιτήσεις πιστοποίησης, την τήρηση προσβάσιμου στο κοινό ηλεκτρονικού μητρώου των αποφάσεων που λαμβάνονται από εποπτικές αρχές και δικαστήρια σχετικά με ζητήματα που διεκπεραιώνονται στο πλαίσιο του μηχανισμού συνεκτικότητας κ.λπ.[66] Οι συζητήσεις του ΕΣΠΔ πρέπει να είναι εμπιστευτικές όταν κρίνεται αναγκαίο.[67]

3.4.2. Η Αρχή Προστασίας Προσωπικών Δεδομένων στην Ελλάδα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι ανεξάρτητη δημόσια αρχή κατά το άρθρο 9Α του Συντάγματος και εδρεύει στην Αθήνα. Η ΑΠΔΠΧ είναι αρμόδια για την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), του Ν. 4624/2019, του Ν. 3471/2006 και άλλων κανονισμών που σχετίζονται με την προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, καθώς και για την άσκηση των καθηκόντων που της ανατίθενται κάθε φορά, όπως αναφέρεται σε προηγούμενες παραγράφους.

---

[65] Άρθρο 69, 2016/679 του ΓΚΠΔ.

[66] Άρθρο 70, 2016/679 του ΓΚΠΔ.

[67] Άρθρο 76, 2016/679 του ΓΚΠΔ.

3.5. Προσφυγές, ευθύνη και κυρώσεις

Ο ΓΚΠΔ παρέχει στα υποκείμενα των δεδομένων προσωπικού χαρακτήρα το δικαίωμα, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, να υποβάλουν καταγγελία σε εποπτική αρχή, ιδίως στο κράτος μέλος της διαμονής τους ή του τόπου εργασίας τους ή του τόπου της εικαζόμενης παράβασης. Ορίζεται, επίσης, ότι η εποπτική αρχή ενημερώνει τον καταγγέλλοντα σχετικά με την πρόοδο και την έκβαση της καταγγελίας.[68] Επιπλέον, προβλέπεται το δικαίωμα των φυσικών και νομικών προσώπων σε ένδικα μέσα κατά νομικά δεσμευτικών αποφάσεων εποπτικής αρχής εναντίον τους.[69] Τέλος, μέσω του κανονισμού, ορίζεται ότι κάθε υποκείμενο των δεδομένων έχει δικαίωμα πραγματικής δικαστικής προσφυγής κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία όταν θεωρεί ότι έχει γίνει παραβίαση των δικαιωμάτων του, όπως αυτά ορίζονται στον ΓΚΠΔ, κατά τη διάρκεια της επεξεργασίας των προσωπικών του δεδομένων.[70]

Το άρθρο 80 του ΓΚΠΔ προβλέπει ότι το υποκείμενο των δεδομένων δικαιούται την ανάθεση σε έναν μη κερδοσκοπικό φορέα ή οργανισμό (ο οποίος έχει καταστατικούς σκοπούς που είναι προς το δημόσιο συμφέρον και ασκεί δραστηριότητες στον τομέα της προστασίας των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων) να ασκήσει τα ένδικα μέσα για λογαριασμό του.[71] Η διάταξη αυτή θα διασφαλίσει ότι τα υποκείμενα των δεδομένων θα εξακολουθήσουν να μπορούν να ασκήσουν ένδικα μέσα (μέσω μη κερδοσκοπικού φορέα) χωρίς η πιθανή οικονομική δυσχέρεια να αποτελεί εμπόδιο να ασκήσουν τέτοια ένδικα μέσα. Προβλέπεται ότι το υποκείμενο των δεδομένων διατηρεί το δικαίωμα να αξιώσει αποζημίωση από τους υπευθύνους

---

[68] Άρθρο 77, 2016/679 του ΓΚΠΔ.

[69] Άρθρο 78, 2016/679 του ΓΚΠΔ.

[70] Άρθρο 79, 2016/679 του ΓΚΠΔ.

[71] Άρθρο 80, 2016/679 του ΓΚΠΔ.

επεξεργασίας/εκτελούντες την επεξεργασία για υλικές ή μη υλικές ζημίες ως αποτέλεσμα παραβίασης του κανονισμού.[72]

Οι εποπτικές αρχές είναι εξουσιοδοτημένες να επιβάλουν διοικητικά πρόστιμα όταν εντοπίζεται παραβίαση του Κανονισμού. Παραβάσεις των υποχρεώσεων του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, των υποχρεώσεων του οργανισμού πιστοποίησης, των υποχρεώσεων του φορέα παρακολούθησης επιβαρύνονται με διοικητικό πρόστιμο που μπορεί να ανέλθει έως και σε 10 εκατομμύρια ευρώ ή στο 2% του παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους όταν πρόκειται για επιχειρήσεις. Οι παραβιάσεις των βασικών αρχών επεξεργασίας, συμπεριλαμβανομένης της συγκατάθεσης, των δικαιωμάτων του υποκειμένου των δεδομένων, τα οποία περιλαμβάνουν το δικαίωμα στη φορητότητα των δεδομένων, το δικαίωμα στη λήθη κ.λπ., της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα αποδέκτη ή διεθνή οργανισμό, των υποχρεώσεων που απορρέουν από το δίκαιο του κράτους μέλους, της μη συμμόρφωσης με οποιαδήποτε εντολή της εποπτικής αρχής για περιορισμό της επεξεργασίας ή αναστολή των ροών δεδομένων μπορεί να επιφέρουν διοικητικό πρόστιμο έως 20 εκατομμύρια ευρώ ή 4% του παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους όταν πρόκειται για επιχειρήσεις. Τα κριτήρια που πρέπει να λαμβάνονται υπόψη από την αρχή ελέγχου πριν από τη λήψη απόφασης σχετικά με το ύψος του προστίμου που πρέπει να καταβάλει μια εταιρεία ή οργανισμός που σφάλλει περιλαμβάνουν: τη φύση, τη σοβαρότητα και τη διάρκεια της παράβασης, τον εκ προθέσεως ή εξ αμελείας χαρακτήρα της παράβασης, τις ενέργειες που προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για τον μετριασμό των ζημιών, προηγούμενες παραβάσεις, κατηγορίες ειδικών δεδομένων που παραβιάστηκαν κ.λπ.[73]

Οι προϋποθέσεις που απαριθμούνται κατ' αυτόν τον τρόπο παρέχουν στις εποπτικές αρχές κάποια μορφή διακριτικής ευχέρειας για να αποφασίσουν πόσα μπορεί να καταβληθούν ως πρόστιμα. Ως εκ τούτου, οι εταιρείες στις οποίες επιβάλλονται πρόστιμα μπορούν να ασκήσουν έφεση κατά των

---

[72] Άρθρο 82, 2016/679 του ΓΚΠΔ.

[73] Άρθρο 83, 2016/679 του ΓΚΠΔ.

εν λόγω προστίμων στα δικαστήρια. Το άρθρο 83 του GDPR περιέχει πολύ βαριά διοικητικά πρόστιμα αρκετά για να προκαλέσει ακόμη και στις μεγαλύτερες εταιρείες προβλήματα. Κατα συνέπεια, αναμένεται ότι οι εταιρείες εναντίον των οποίων επιβάλλονται τέτοια πρόστιμα πιθανότατα θα αμφισβητήσουν τέτοιες επιβολές στο δικαστήριο. Τέλος, αυτές οι διατάξεις σχετικά με τα διοικητικά πρόστιμα θα κάνουν τις εταιρείες να λάβουν πολύ σοβαρά υπόψη τον κανονισμό, ειδικά στην πρόσληψη ατόμων με εμπειρία στους σχετικούς τομείς της προστασίας δεδομένων. Τα διοικητικά πρόστιμα έχουν το πλεονέκτημα ότι είναι τόσο βαριά ώστε να χρησιμεύουν ως αποτρεπτικός παράγοντας για τις εταιρείες και να ενθαρρύνουν τη συμμόρφωση με τον ΓΚΠΔ.

Τα κράτη μέλη επιτρέπεται επίσης να θεσπίζουν κυρώσεις για παραβάσεις που δεν καλύπτονται από τον ΓΚΠΔ και οι κυρώσεις αυτές πρέπει να κοινοποιούνται στην Επιτροπή έως τις 25 Μαΐου 2018.[74]

3.6. Ο ν. 4624/2019 σχετικά με τα μέτρα εφαρμογής του Κανονισμού 2016/679

Στις 26 Αυγούστου 2019, ψηφίστηκε από τη Βουλή των Ελλήνων, ο νόμος 4624/2019, ο οποίος είναι αναπόσπαστα συνδεδεμένος με τον ΓΚΠΔ. Ο νόμος έχει ως πεδίο εφαρμογής δημόσιους και ιδιωτικούς φορείς μεταξύ των οποίων γίνεται διαχωρισμός με έμφαση στους δημόσιους φορείς.[75] Ο νόμος 4624/2019 αποτελεί συνέπεια της ευρωπαϊκής μεταρρύθμισης για την προστασία των δεδομένων προσωπικού χαρακτήρα και της προσαρμογής του εθνικού δικαίου που προκάλεσε. Ο νόμος που εγκρίθηκε αποσκοπεί στη διασφάλιση της ελεύθερης ροής των δεδομένων προσωπικού χαρακτήρα τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα, με σκοπό τη διαμόρφωση της ευρωπαϊκής «ψηφιακής ενιαίας αγοράς» και την προστασία των φυσικών προσώπων από την παράνομη επεξεργασία των προσωπικών τους δεδομένων από τις εθνικές αρχές επιβολής του νόμου.

---

[74] Άρθρο 84, 2016/679 του ΓΚΠΔ.

[75] Άρθρο 2, 4624/2019 του ΓΚΠΔ.

Ως δημόσιος φορέας ορίζεται:[76]

> *«οι δημόσιες αρχές, οι ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, τα νομικά πρόσωπα δημοσίου δικαίου, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δεύτερου βαθμού και τα νομικά πρόσωπα και οι επιχειρήσεις αυτών, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό»*

Ενώ, ως ιδιωτικός τομέας ορίζεται οποιοσδήποτε φορέας, φυσικό ή νομικό πρόσωπο που δεν εμπίπτει στην κατηγορία του δημοσίου.

Αξίζει να σημειωθεί, πως ενώ ο Κανονισμός τέθηκε σε ισχύ τον Μάιο του 2016 από το Ευρωπαϊκό Κοινοβούλιο και σχεδόν άμεσα Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων στην Ελλάδα εκκίνησε τις διαδικασίες για την ενσωμάτωση σε εθνικό επίπεδο με αρχική ημερομηνία περάτωσης τον Μάιο του 2017, η διαδικασία έπειτα από διάφορες αναβολές ολοκληρώθηκε τον Αύγουστο του 2019. Θεωρείται ότι αυτή η καθυστέρηση οφείλεται στο γεγονός ότι ο Έλληνας νομοθέτης επέλεξε να στραφεί σε μια άλλη έννομη τάξη, τη γερμανική νομοθεσία, η οποία έχει περισσότερη εμπειρία στον τομέα της προστασίας των προσωπικών δεδομένων, από την οποία θα μπορούσε να αντλήσει σημαντικά στοιχεία.[77]

Ως εκ τούτου, η διάκριση μεταξύ δημόσιου και ιδιωτικού τομέα βασίζεται σε μια δογματική εξήγηση. Ειδικότερα, ο νόμος για την προστασία των δεδομένων προσωπικού χαρακτήρα θα πρέπει, αφενός, να προστατεύει τον πολίτη από την επεξεργασία δεδομένων από δημόσιους φορείς

---

[76] Άρθρο 4, 4624/2019 του ΓΚΠΔ.

[77] Γριβοκωστόπουλος Ι., «Κριτική ανάλυση του Ν. 4624/2019», Επιθεώρηση Δικαίου Πληροφορικής, Τεύχος 1 2021, Διαθέσιμο στο: http://ejournals.lib.auth.gr/infolawj/

και, ως εκ τούτου, να τον εξοπλίζει με ένα «αμυντικό δικαίωμα» και, αφετέρου, να παρέχει προστασία έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από ιδιωτικούς φορείς.[78]

[78] Karyda, Spyridoula, Law No. 4624/2019: Shedding Light on the Greek Adaptation of the GDPR (March 11, 2022). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=4055464 or http://dx.doi.org/10.2139/ssrn.4055464

Κεφάλαιο 4: Σύγχρονα θέματα και προκλήσεις σχετικά με τον ΓΚΠΔ

4.1 Η έννοια της συγκατάθεσης και κύρια ζητήματα

Η συγκατάθεση διαδραματίζει καίριο ρόλο στην παραδοσιακή κατανόηση της προστασίας των δεδομένων. Όπως αναφέρθηκε και σε προηγούμενη παράγραφο, το υποκείμενο, προκειμένου να τεθούν υπό επεξεργασία τα δεδομένα του, παρέχει τη συγκατάθεσή του. Στο άρθρο 4, παράγραφο 11 του ΓΚΠΔ, δίδεται ο ορισμός της συγκατάθεσης, ως οποιαδήποτε πράξη ενδεικνύει την ελεύθερη και ρητή συφμωνία του υποκειμένου να συλλεχθούν και να επεξεργαστούν τα προσωπικά του δεδομένα. Στηριζόμενοι στο μοντέλο «ειδοποίησης και συγκατάθεσης», σύμφωνα με το οποίο η προστασία των δεδομένων αποσκοπεί στην προστασία του δικαιώματος στην «πληροφοριακή αυτοδιάθεση». Το δικαίωμα αυτό ασκείται πράγματι με τη συγκατάθεση ή την άρνηση περιεχομένου στην επεξεργασία των δεδομένων κάποιου, αφού έχει λάβει επαρκή ειδοποίηση. Ωστόσο, υπάρχουν δύο βασικά ζητήματα τα οποία δε θα πρέπει να αποσιωπηθούν.

Το πρώτο ζήτημα είναι ότι η συγκατάθεση τις περισσότερες φορές δεν βασίζεται σε πραγματική γνώση της επεξεργασίας που διακυβεύεται, ούτε σε μια πραγματική ευκαιρία επιλογής. Αφενός, η σημερινή επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι τόσο περίπλοκη που τα περισσότερα υποκείμενα των δεδομένων δεν έχουν τις δεξιότητες να τα κατανοήσουν και να προβλέψουν τους σχετικούς κινδύνους.

Σύμφωνα με την έννοια της συγκατάθεσης , όταν ένα άτομο παρέχει τη συγκατάθεση του, εισέρχεται οικειοθελώς σε μια συμφωνία με την οποία θέτει τον εαυτό του σε κάθε είδους κίνδυνο, και το άτομο ή ο οργανισμός που είναι υπεύθυνος για τη συλλογή και επεξεργασία των δεδομένων υποχρεούται να διασφαλίζει ότι το πρόσωπο έχει δώσει την εν επιγνώσει συγκατάθεσή του πριν από τη σύναψή της, σε ποια περίπτωση, όμως θα μπορούσε ευλόγως να χαρακτηριστεί η συγκατάθεσή ως «εν επιγνώσει»; Όταν οι χρήστες χρησιμοποιούν μια διαδικτυακή υπηρεσία, είτε το Facebook, είτε το Google, είτε έναν ιστότοπο λιανικού εμπορίου υποχρεούνται να αναγνωρίσουν ότι έχουν διαβάσει τους «όρους και προϋποθέσεις» που ισχύουν για την εν λόγω υπηρεσία. Αυτά καλύπτουν ζητήματα όπως η προστασία της ιδιωτικής ζωής και το βαθμό στον οποίο τα δεδομένα που παραδίδονται από τους χρήστες μπορούν να επαναχρησιμοποιηθούν από τον πάροχο υπηρεσιών. Η αναγνώριση των όρων και προϋποθέσεων είναι ο τρόπος με τον οποίο

η συναίνεση των χρηστών κατόπιν ενημέρωσης λαμβάνεται από τον πάροχο υπηρεσιών. Ωστόσο, η περίπτωση ειδοποίησης και συγκατάθεσης προϋποθέτει ότι οι πολίτες είναι σε θέση να αξιολογήσουν τις πιθανά οφέλη και το κόστος της απόκτησης δεδομένων με επαρκή ακρίβεια ώστε να γίνονται συνειδητές επιλογές. Αυτό ωστόσο, καθίσταται εξαιρετικά δύσκολο για διάφορους λόγους, συμπεριλαμβανομένου την αυξανόμενη χρήση σύνθετων και αδιαφανών τεχνικών προγνωστικής εξόρυξης δεδομένων, την αλληλεξάρτηση των προσωπικών δεδομένων και το εύρος των πιθανών βλαβών που μπορεί να προκληθούν. Η κατάσταση περιπλέκεται περαιτέρω από το γεγονός ότι αυτοί που συλλέγουν τα δεδομένα συνήθως προσπαθούν να ελαχιστοποιήσουν την ικανότητα του προσώπου για το οποίο τα δεδομένα συλλέγονται για να κατανοήσουν το εύρος των δεδομένων και τη χρήση τους, μέσω ενός μείγματος προηγμένου σχεδιασμού και ειδικευμένης νομικής ορολογίας.[79] Με απλά λόγια, αυτό οδηγεί σε καταστάσεις στις οποίες οι άνθρωποι συναινούν στη συλλογή, χρήση και αποκάλυψη των προσωπικών τους δεδομένων όταν δεν είναι προς το συμφέρον τους να το πράξουν.

Επιπλέον, ακόμη και αν τα υποκείμενα των δεδομένων διέθεταν τέτοιες δεξιότητες, δεν θα είχαν το χρόνο και την ενέργεια να μελετήσουν τις λεπτομέρειες κάθε πολιτικής απορρήτου. Το πιο κοινό παράδειγμα αποτελεί η περιήγηση στο διαδίκτυο. Η πλειοψηφία, αν όχι όλες, οι ιστοδελιδες, πλέον, κατά την είσοδο του χρήστη στη σελίδα, ζητούν τη συγκατάθεσή του για επεξεργασία προσωπικών δεδομένων. Αξίζει να αναφερθεί, επίσης, η διαδικασία δημιουργίας ενός λογαριασμού, για παράδειγμα σε ένα ηλεκτρονικό κατάστημα για την παραγγελία ενός προϊόντος ή μιας υπηρεσίας. Στο τελευταίο στάδιο της δημιουργίας του λογαριασμού, ζητάται από τον χρήστη να συμφωνήσει με όρους, προϋποθέσεις και πολιτική απορρήτου, ένα κείμενο που περιλαμβάνει πληθώρα νομικών όρων και περιπτώσεων που ο μέσος χρήστης, δε διαβάζει σχολαστικά και πολύ πιθανό να μην είναι σε θέση να κατανοήσει. Από την άλλη, η άρνηση συγκατάθεσης μπορεί να συνεπάγεται αδυναμία χρήσης (ή περιορισμό στη χρήση) υπηρεσιών που είναι σημαντικές ή ακόμη και απαραίτητες για τα υποκείμενα των δεδομένων.

---

[79] Strandburg, Katherine J.. "Privacy, Big Data, and the Public Good: Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context." (2014).

Το δεύτερο ζήτημα είναι ότι η συγκατάθεση, όταν στοχεύει σε συγκεκριμένους σκοπούς, δεν περιλαμβάνει (και, ως εκ τούτου, αποκλείει, όταν θεωρείται αναγκαία βάση της επεξεργασίας) μελλοντικές, συχνά άγνωστες, χρήσεις των δεδομένων, ακόμη και όταν οι χρήσεις αυτές είναι κοινωνικά επωφελείς. Έτσι, η απαίτηση συγκατάθεσης μπορεί να «επηρεάσει τα μελλοντικά οφέλη και να εμποδίσει πολύτιμες νέες ανακαλύψεις», όπως φαίνεται σε «μυριάδες παραδείγματα», συμπεριλαμβανομένης της «εξέτασης αρχείων υγείας και εργαστηριακών αποτελεσμάτων για ιατρική έρευνα, της ανάλυσης δισεκατομμυρίων αρχείων αναζήτησης στο Διαδίκτυο για τη χαρτογράφηση επιδημιών γρίπης και τον εντοπισμό επικίνδυνων αλληλεπιδράσεων φαρμάκων, της αναζήτησης οικονομικών αρχείων για τον εντοπισμό και την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της παρακολούθησης οχημάτων και πεζών για να βοηθήσει στον σχεδιασμό υποδομών».

Ωστόσο, αυτά τα ζητήματα για τη συγκατάθεση έχουν αντικρουστεί παρατηρώντας ότι είναι εφικτό να εφαρμοστούν οι αρχές της συγκατάθεσης και του περιορισμού του σκοπού. Πρώτον, υποστηρίχθηκε ότι οι ανακοινώσεις πρέπει να επικεντρώνονται στο πιο σημαντικό ζήτημα και ότι πρέπει να είναι φιλικές προς τον χρήστη και άμεσες. Ειδικότερα, θα πρέπει να παρέχονται απλές και σαφείς πληροφορίες σχετικά με τον τρόπο συμμετοχής ή εξαίρεσης σε σχέση με την επεξεργασία, όπως εκείνες που αφορούν την παρακολούθηση των χρηστών ή τη διαβίβαση δεδομένων σε τρίτους. Περαιτέρω κουμπιά εξαίρεσης ή επιλογής θα μπορούσαν να παρουσιαστούν σε όλους τους χρήστες, για να παρέχουν τρόπους έκφρασης των προτιμήσεών τους σχετικά με την παρακολούθηση, τη δημιουργία προφίλ κ.λπ. Δεύτερον, ο ΓΚΠΔ επιτρέπει την επεξεργασία των δεδομένων που συλλέχθηκαν για ορισμένους σκοπούς για περαιτέρω σκοπούς, εφόσον οι τελευταίοι σκοποί είναι συμβατοί με τους αρχικούς.[80]

[80]Sartor G., Lagiola F.,: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, Scientific Foresight Unit (STOA) EPRS | European Parliamentary Research Service, ISBN: 978-92-846-6771-0

4.2. Η προστασία προσωπικών δεδομένων στο χώρο εργασίας

Η σχέση μεταξύ εργοδοτών και εργαζομένων ήταν πάντα περίπλοκη. Έχει υποστηριχθεί ότι σε κανέναν άλλο τομέα τα υποκείμενα των δεδομένων δεν εκτίθενται τόσο όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν όσο στο πλαίσιο της απασχολήσεως. Οι τεχνολογίες αιχμής (π.χ. τεχνητή νοημοσύνη) και τα εργαλεία βιντεοεπιτήρησης/παρακολούθησης που απευθύνονται στους εργαζομένους προσφέρουν ορισμένες νέες εξαιρετικά εξελιγμένες ευκαιρίες για παραβίαση της νομοθεσίας περί προστασίας των δεδομένων εκ μέρους των εργοδοτών. Από την άλλη, οι ίδιες τεχνολογίες εξοπλίζουν και τα δύο μέρη με εξαιρετικά χρήσιμα μέσα για την κατάλληλη διαφύλαξη και εξισορρόπηση των αντικρουόμενων συμφερόντων τους.[81]

Στον ΓΚΠΔ αναφέρεται στο άρθρο 88, ότι η Ένωση δεν προβλέπει ειδικούς κανόνες για τον χώρο απασχόλησης, οπότε τα κράτη μέλη μπορούν να θεσπίσουν το δικό τους νομικό πλαίσιο που να διέπει την επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης.[82] Ο ΓΚΠΔ παρέχει στα κράτη μέλη μια «ρήτρα ανοίγματος» που τους επιτρέπει είτε να θεσπίσουν περαιτέρω ειδικούς εθνικούς κανόνες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της απασχόλησης είτε να διατηρήσουν τις ήδη υφιστάμενες εθνικές νομοθεσίες. Κατά συνέπεια, οι κανόνες σχετικά με την προστασία των δεδομένων και της ιδιωτικής ζωής στο πλαίσιο της απασχόλησης εφαρμόστηκαν με διάφορους τρόπους στα διάφορα κράτη μέλη της ΕΕ.

Το νομικό πλαίσιο που σχηματίστηκε στην Ελλάδα, ορίζεται στο άρθρο 27 του ν.4624/2019. Ορίζεται ότι τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβληθούν σε επεξεργασία για τους σκοπούς σχετικούς με τη σύμβαση εργασίας, όταν η επεξεργασία κρίνεται απολύτα απαραίτητη για να αποφασιστεί εάν θα συναφθεί σύμβαση εργασίας, ή για την εκτέλεση σύμβασης εργασίας μετά τη σύναψή της. Ωστόσο, θα πρέπει πάντα να πραγματοποιείται

---

[81] Karyda, Spyridoula, Law No. 4624/2019: Shedding Light on the Greek Adaptation of the GDPR (March 11, 2022). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=4055464 or http://dx.doi.org/10.2139/ssrn.4055464

[82] Άρθρο 88, 2016/679 του ΓΚΠΔ

αξιολόγηση της αναγκαιότητας της επεξεργασίας. Αυτός ο έλεγχος εξισορρόπησης θα πρέπει να διαφυλάσσει στο μέγιστο τόσο τα αντικρουόμενα συμφέροντα, λαμβάνοντας υπόψη το συμφέρον του εργοδότη όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όσο και τα δικαιώματα προσωπικότητας και αξιοπρέπειας του εργαζομένου. [83]

Το άρθρο αυτό αποσκοπεί στην οριοθέτηση μιας άλλης αμφίσημης νομικής βάσης για την επεξεργασία των δεδομένων των εργαζομένων, αυτής της «συγκατάθεσης». Ένα από τα πιο πολυσυζητημένα ζητήματα σε αυτόν τον τομέα πηγάζει από το ερώτημα εάν η «συγκατάθεση» μπορεί να χρησιμοποιηθεί ως νομική βάση για την επεξεργασία προσωπικών δεδομένων των εργαζομένων από τους εργοδότες τους. Ο ΓΚΠΔ ορίζει τη συγκατάθεση ως «ελεύθερη, συγκεκριμένη, ενημερωμένη και σαφή».[84] Η «συγκατάθεση» δεν θα μπορούσε ποτέ να χρησιμεύσει ως νόμιμη νομική βάση στο πλαίσιο της απασχόλησης λόγω της άνισης θέσης μεταξύ εργοδοτών και εργαζομένων. Η προσέγγιση αυτή στηρίζεται στο τεκμήριο ότι, δεδομένης της εξαρτήσεως του εργαζομένου από τον εργοδότη του, η «συγκατάθεση» δεν μπορεί ποτέ να θεωρηθεί ως «ελεύθερη».

Μία άλλη πρόκληση αποτελεί η κρίση για το αν η επεξεργασία είναι απολύτως απαραίτητη και προς το συμφέρον του εργαζομένου. Υπάρχουν περιπτώσεις στις οποίες η «συγκατάθεση» θα μπορούσε να θεωρηθεί ότι παρέχεται ελεύθερα, όταν η επεξεργασία συνδυάζεται με οικονομικά οφέλη για τους εργαζομένους, για παράδειγμα τη δυνατότητα χρήσης των συστημάτων πληροφορικής της εταιρείας για ιδιωτικούς λόγους ή κατά τη δημιουργία ενός εταιρικού προγράμματος διαχείρισης της υγείας ή ασφάλισης, ή σε περιπτώσεις σύγκλισης προς το συμφέρον εργοδότη και εργαζομένου. Εν πάση περιπτώσει, ενδέχεται να υπάρχουν περιπτώσεις στις οποίες ο εργοδότης μπορεί να αποδείξει ότι πράγματι παρέχεται ελεύθερη συγκατάθεση. Δεδομένης της ανισορροπίας εξουσίας μεταξύ ενός εργοδότη και των μελών του προσωπικού του,

---

[83] Άρθρο 27, 4624/2019

[84] Σημείωση 32, 2016/679

οι εργαζόμενοι μπορούν να δώσουν ελεύθερη συγκατάθεση μόνο σε εξαιρετικές περιστάσεις, όταν δεν θα έχει καθόλου δυσμενείς συνέπειες είτε δώσουν τη συγκατάθεσή τους είτε όχι. [85]

Στην ελληνική νομοθεσία γίνεται προσπάθεια να τεθούν όρια στην επεξεργασία όσον αφορά τον έλεγχο στον χώρο εργασίας. Η θεσπισθείσα διάταξη ορίζει ότι όταν έχει εγκατασταθεί κλειστό κύκλωμα τηλεόρασης στους χώρους εργασίας, οπότε και μπορεί χρησιμοποιηθεί για την επεξεργασία προσωπικών δεδομένων, θα πρέπει να έχει κριθεί αναγκαίο για λόγους προστασίας προσώπων ή αγαθών. Επιπρόσθετα, προβλέπται με ακρίβεια ότι η επεξεργασία δεδομένων κατ' αυτό τον τρόπο δεν επιτρέπεται να χρησιμοποιηθεί για λόγους αξιολόγησης των εργαζομένων. Τέλος, οι εργαζόμενοι πρεπει να έχουν ενημερωθεί σχετικά με την ύπαρξη τέτοιου κυκλώματος με έγγραφα ή ηλεκτρονικά μέσα. [86]

4.2.1. Η υπόθεση παραβίασης προσωπικών δεδομένων των εργαζομένων της H&M

Στις 5 Οκτωβρίου 2020, η Αρχή Προστασίας Δεδομένων του Αμβούργου της Γερμανίας επέβαλε πρόστιμο στον λιανοπωλητή ενδυμάτων H&M ύψους 35.2 εκατομμύρια ευρώ. Οι παραβιάσεις του GDPR της H&M αφορούσαν την «παρακολούθηση αρκετών εκατοντάδων εργαζομένων». Αφού οι εργαζόμενοι πήραν άδεια διακοπών ή αναρρωτική άδεια, έπρεπε να παρευρεθούν σε μια συνάντηση επιστροφής στην εργασία. Ορισμένες από αυτές τις συναντήσεις καταγράφηκαν και ήταν προσβάσιμες σε περισσότερους από 50 διευθυντές της H&M. Τα ανώτερα στελέχη της H&M απέκτησαν ευρεία γνώση της ιδιωτικής ζωής των εργαζομένων τους που κυμαίνονται από μάλλον ακίνδυνες λεπτομέρειες έως οικογενειακά ζητήματα και θρησκευτικές πεποιθήσεις. Αυτό το «λεπτομερές προφίλ» χρησιμοποιήθηκε για να βοηθήσει στην αξιολόγηση της απόδοσης των εργαζομένων και στη λήψη αποφάσεων σχετικά με την απασχόλησή τους.[87] Η H&M φαίνεται να

---

[85] Karyda, Spyridoula, Law No. 4624/2019: Shedding Light on the Greek Adaptation of the GDPR (March 11, 2022). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=4055464 or http://dx.doi.org/10.2139/ssrn.4055464

[86] Άρθρο 27, 4624/2019

[87]https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en

έχει παραβιάσει την αρχή ελαχιστοποίησης δεδομένων του GDPR, καθώς επεξεργάστηκε προσωπικές πληροφορίες, ιδιαίτερα ευαίσθητα δεδομένα σχετικά με την υγεία και τις πεποιθήσεις των ανθρώπων, χωρίς να έχει κριθεί απαραίτητος σκοπός. Αντ' αυτού, έπρεπε να έχει θέσει αυστηρούς ελέγχους πρόσβασης στα δεδομένα και η εταιρεία δεν θα έπρεπε να έχει χρησιμοποιήσει αυτά τα δεδομένα για να λάβει αποφάσεις σχετικά με την απασχόληση των ανθρώπων.

4.3. Η προστασία προσωπικών δεδομένων στο χώρο του διαδικτύου

Η ραγδαία τεχνολογική ανάπτυξη αποτελεί αδιαμφισβήτητο χαρακτηριστικό των τελευταίων δεκαετιών και το διαδίκτυο αναπόσπαστο κομμάτι της καθημερινής ζωής των ανθρώπων. Η κυκλοφορία της πληροφορίας είναι πιο εύκολη από ποτέ, διευκολύνοντας σε πολύ μεγάλο βαθμό την εργασία, τη διασκέδαση, την εκπαίδευση και άλλους τομείς της ζωής του ανθρώπου, ωστόσο ενέχει και πολύ σημαντικούς κινδύνους και απειλές. Μέσω του διαδικτύου και της ευρείας διάδοσής του, επιτρέπεται η εύκολη συλλόγη και αποθήκευση προσωπικών δεδομένων. Πολλές φορές, ο χρήστης κατά την χρησιμοποίηση μιας υπηρεσίας αφήνει το ηλεκτρονικό του αποτύπωμα που συμπεριλαμβάνει δεδομένα προσωπικού χαρακτήρα, και χωρίς να έχει ενημερωθεί προηγουμένως είναι εφικτή η συλλογή, η αποθήκευση και η επεξεργασία αυτών.[88] Με οποιαδήποτε επίσκεψη σε μία ιστοσελίδα, τα στοιχεία που συλλέγονται μπορούν να δημιουργήσουν σταδιακά μία βάση δεδομένων που θα υποδεικνύσει, συνήθειες, προτιμήσεις, επιλογές ή/και μοτίβα του χρήστη, έτσι ώστε να χρησιμοποιηθούν για εμπορικούς, πολιτικούς ή άλλους λόγους.

4.3.1. Παράβαση του ΓΚΠΔ από την Amazon

Τον Μάιο του 2018 υποβλήθηκε καταγγελία από δέκα χιλιάδες προς την εταιρία «Amazon.com Inc», η οποία δραστηριοποιείται στον τομέα του ηλεκτρονικού εμπορίου, μέσω μιας γαλλικής ομάδας δικαιωμάτων απορρήτου που προωθεί και υπερασπίζεται τις θεμελιώδεις ελευθερίες στον

---

[88] Leenes R., Van Brakel R., Gutwirth S., De Hert P., (2018), Data Protection and Privacy: The Internet of Bodies (Computers, Privacy and Data Protection), Hart Publishing. Διαθέσιμο στο: https://researchportal.vub.be/en/publications/data-protection-and-privacy-the-internet-of-bodies

ψηφιακό κόσμο- La Quadrature du Net. Σχεδόν τρία χρόνια αργότερα, τον Ιούλιο του 2016, η Εθνική Επιτροπή Προστασίας Δεδομένων του Λουξεμβούργου εξέδωσε το μεγαλύτερο πρόστιμο ποτέ για παραβίαση του ΓΚΠΔ, ύψους 746 εκατομμυρίων ευρώ (888 εκατομμύρια δολάρια) στην Amazon.com Inc. Η εποπτική αρχή στο Λουξεμβούργο, κίνησε έρευνα σχετικά με τον τρόπο με τον οποίο η Amazon επεξεργάζεται τα προσωπικά δεδομένα των πελατών της και διαπίστωσε παραβιάσεις σχετικά με το σύστημα στόχευσης διαφημίσεων της Amazons, οι οποίες πραγματοποιήθηκαν χωρίς την κατάλληλη συγκατάθεση.[89]

4.4. Παραβίαση δεδομένων προσωπικού χαρακτήρα από εταιρίες τηλεπικοινωνίας στην Ιταλία

Η 15η Ιανουαρίου 2020 ήταν μια κρίσιμη ημέρα για τον ιταλικό πάροχο τηλεπικοινωνιών TIM. Η ιταλική DPA Garante εξέδωσε πρόστιμο παραβίασης του ΓΚΠΔ ύψους 27,8 εκατομμυρίων ευρώ για έναν αρκετά εκτεταμένο κατάλογο παραβιάσεων στα πλαίσια της στρατηγικής μάρκετινγκ της εταιρίας. Το εύρος των παράνομων δραστηριοτήτων τους είναι δύσκολο να αγνοηθεί. Η TIM έχει επικοινωνήσει με μη πελάτες πολλές φορές (ορισμένοι αριθμοί πάνω από 150 φορές το μήνα) χωρίς την κατάλληλη συγκατάθεση ή άλλες νομικές βάσεις. Εκατομμύρια άτομα επηρεάστηκαν από την επιθετική στρατηγική μάρκετινγκ.

Οι παραβιάσεις περιελάμβαναν: ακατάλληλη διαχείριση καταλόγων συγκατάθεσης, διατήρηση δεδομένων για υπερβάλον χρονικό διάστημα, παραβιάσεις δεδομένων, ελλειψη κατάλληλης συγκατάθεσης και παραβίαση των δικαιωμάτων που προβλέπονται από τον ΓΚΠΔ, όπως το δικαίωμα στη λήθη και το δικαίωμα εναντίωσης. Οι αναφορές έγιναν σχετικά με προωθητικές κλήσεις χωρίς την κατάλληλη συγκατάθεση και ακόμη και μετά την άσκηση του δικαιώματος εναντίωσης. Περαιτέρω καταγγελίες κατέδειξαν αδυναμία ανταπόκρισης στα αιτήματα των υποκειμένων των δεδομένων όσον αφορά τα δικαιώματά τους βάσει του ΓΚΠΔ, ιδίως όσον αφορά την πρόσβαση στα δεδομένα τους και την εναντίωση στην επεξεργασία για διαφημιστικούς σκοπούς. Εκτός αυτών, η εταιρεία συγκέντρωσε συγκαταθέσεις σε έντυπα με μία μόνο συμμετοχή

[89] https://cnpd.public.lu/en/

για πολλαπλούς σκοπούς. Ως εκ τούτου, καθιστώντας τις συναινέσεις δυσδιάκριτες και ασαφείς. Επίσης, η TIM απέτυχε να διαχειριστεί σωστά τους καταλόγους των υποκειμένων των δεδομένων που ήθελαν να αποκλειστούν από εμπορικές εκστρατείες. Η εταιρεία δεν επικαιροποίησε τους καταλόγους, γεγονός που οδήγησε σε κενά στην ακρίβεια και την ποιότητα των δεδομένων στα εταιρικά συστήματα πληροφοριών. Οι προσωπικές πληροφορίες περιελάμβαναν όνομα, επώνυμο ή όνομα εταιρείας. φορολογικός κωδικός ή αριθμός ΦΠΑ· τηλεφωνική γραμμή, διεύθυνση και στοιχεία επικοινωνίας. [90]

Στις 13 Ιουλίου 2020, η ιταλική εποπτική αρχή προστασίας προσωπικών δεδομένων (DPA-Garante) εξέδωσε πρόστιμο 16.7 εκατομμύρια ευρώ στον τηλεπικοινωνιακό φορέα – Wind Tre S.p.A. Το πρόστιμο εκδόθηκε μετά από πολύπλοκες έρευνες μετά από πολλές καταγγελίες από ιδιώτες. Περισσότεροι από εκατό πελάτες υπέβαλαν καταγγελία για αυτόκλητες δραστηριότητες μάρκετινγκ που πραγματοποιήθηκαν χωρίς την κατάλληλη συγκατάθεση μέσω κλήσεων, φαξ, αυτοματοποιημένων τηλεφωνικών κλήσεων και SMS. Επίσης, αρκετοί πελάτες παραπονέθηκαν ότι δεν μπορούσαν να ανακαλέσουν τη συγκατάθεσή τους ή ακόμη και να αντιταχθούν στην επεξεργασία ενώ τα προσωπικά τους δεδομένα δημοσιεύθηκαν σε δημόσιους καταλόγους. Η έρευνα της εποπτικής αρχής έδειξε ότι οι εφαρμογές που χρησιμοποιήθηκαν είχαν ρυθμιστεί ώστε να απαιτούν από τον χρήστη να συναινεί, σε κάθε πρόσβαση, στην επεξεργασία για διάφορους σκοπούς, συμπεριλαμβανομένου του μάρκετινγκ, της κατάρτισης προφίλ, της κοινοποίησης δεδομένων σε τρίτους, του εμπλουτισμού δεδομένων και της γεωγραφικής τοποθεσίας. Ωστόσο, η ανάκληση αυτής της συγκατάθεσης ήταν δυνατή μόνο μετά από 24 ώρες. [91]

Λίγους μήνες αργότερα, στις 12 Νοεμβρίου 2020, η ιταλική αρχή εξέδωσε πρόστιμο 12,25 εκατομμυρίων ευρώ και σε άλλο τηλεπικοινωνιακό φορέα της χώρας, στη Vodafone Italia, για παράνομη επεξεργασία προσωπικών δεδομένων εκατομμυρίων χρηστών για σκοπούς

---

[90] https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en

[91] https://edpb.europa.eu/news/national-news/2020/telephone-operators-italian-sa-fines-wind-eur-17-million-and-iliad-eur-08_en

τηλεμάρκετινγκ, έπειτα από σχολαστική έρευνα που διεξήχθει από την εποπτική αρχή, που προήλθε από πολυάριθμες καταγγελίες για συνεχείς ανεπιθύμητες τηλεφωνικές κλήσεις που πραγματοποιούνται από τη Vodafone και το δίκτυο πωλήσεών της για την προώθηση των υπηρεσιών της. Η έρευνα αποκάλυψε ένα σύστημα αποθήκευσης πληροφοριών που είχε έως και 4,5 εκατομμύρια επαφές, ενώ η λίστα αγοράστηκε από εξωτερικούς παρόχους χωρίς την κατάλληλη συγκατάθεση. Οι παραβιάσεις επηρέασαν ολόκληρη την ιταλική πελατειακή βάση της Vodafone. Όπως επισημάνθηκε, «η έρευνα έφερε στο φως σημαντικές κρίσιμες πτυχές «διαρθρωτικής» φύσης που έχουν να κάνουν με την παραβίαση όχι μόνο των απαιτήσεων συγκατάθεσης αλλά και βασικών αρχών όπως η λογοδοσία και η προστασία των δεδομένων ήδη από τον σχεδιασμό, όπως ορίζονται στον ΓΚΠΔ της ΕΕ. Αυτές οι κρίσιμες πτυχές θα μπορούσαν να εντοπιστούν στις δραστηριότητες επεξεργασίας που εκτελούνται τόσο σε σχέση με τη βάση δεδομένων πελατών της Vodafone όσο και – ευρύτερα – σε σχέση με τους υποψήφιους χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών». [92]

4.5. Παραβιάση του ΓΚΠΔ και επιβολή προστίμων από την ελληνική εποπτική αρχή

Πέραν των παραβιάσεων στον τομέα των τηλεπικοινωνίων στην Ιταλία, έχει καταγραφεί και στην Ελλάδα παράβαση του ΓΚΠΔ. Στις αρχές του 2022, επιβλήθηκε πρόστιμο συνολικού ποσού 6 εκατομμυρίων ευρώ στην εταιρία Cosmote και στην εταιρία ΟΤΕ πρόστιμο 3,25 εκατομμύρια ευρώ. Η έρευνα ξεκίνησε μετά από γνωστοποίηση διαρροής δεδομένων κλήσεων που αφορούσαν τον Σεπτέμβριο του 2020 (01/09/20-05/09/20) από την COSMOTE Α.Ε. Η εταιρία ενημέρωσε, ως όφειλε, την αρχή σχετικά με το περιστατικό παραβίασης προσωπικών δεδομένων. Λίγες μέρες αργότερα, η αρχή εξέδωσε σχετική ανακοίνωση και ξεκίνησε την έρευνα της περίπτωσης.[93] Η ελληνική εποπτική αρχή, κλήθηκε να διερευνήσει τις συνθήκες κάτω από οποίες έλαβε χώρα η παραβίαση και, στο πλαίσιο αυτό, εξέτασε τη νομιμότητα της τήρησης αρχείων σε σχέση με τα

[92] https://edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en

[93] https://www.dpa.gr/el/enimerwtiko/deltia/deltio-typoy-shetika-me-ti-gnostopoiisi-peristatikoy-parabiasis

δεδομένα που διέρρευσαν, καθώς και τα ισχύοντα μέτρα ασφαλείας εκείνη την περίοδο. Από την έρευνα της υπόθεσης προέκυψε ότι η COSMOTE είχε παραβιάσει τις αρχές της νομιμότητας και της διαφάνειας λόγω της παροχής ασαφών και ανεπαρκών πληροφοριών στους συνδρομητές. Η εταιρεία κρίθηκε επίσης υπεύθυνη για την κακή εκτίμηση επιπτώσεων στην προστασία των δεδομένων, την κακή ανωνυμοποίηση, τα ανεπαρκή μέτρα ασφαλείας που ελήφθησαν και τη μη κατανομή των ρόλων των δύο εταιρειών (COSMOTE / OTE) σε σχέση με την εν λόγω επεξεργασία. [94]

Ωστόσο, δεν είναι η πρώτη φορά που επιβάλλεται πρόστιμο στη συγκεκριμένη εταιρία. Το 2018, η Αρχή Προστασίας Δεδομένων, έπειτα από κατά συρροή παράπονα για τηλεφωνική επικοινωνία με σκοπό προώθηση προϊόντων και υπηρεσιών, διερεύνησε σχετικές κινήσεις των παρόχων κινητής τηλεφωνίας Cosmote, Vodafone, Wind και OTE. Από την έρευνα προέκυψε ότι οι εν λόγω εταιρίες πραγματοποιούσαν κλήσεις οι οποίες δεν στηρίζονταν σε κάποια νομική βάση και δεν λαμβάνουν τα κατάλληλα μέτρα για την πλήρη συμμόρφωσή τους. Επιβλήθηκε πρόστιμο 150 χιλιάδες ευρώ στην κάθε μία, συνολικά 600 χιλιάδες ευρώ, και απαίτησε τη βελτίωση των διαδιακασιών τους για την επίτευξη πλήρους νομιμότητας για να αποφευχθούν μελλοντικές παραβάσεις. [95]

Τέλος, αξίζει να αναφερθεί η υπόθεση παράβασης του ΓΚΠΔ από την εταιρία Clearview AI Inc που εδρεύει στις ΗΠΑ. Κατά της εταιρίας, υποβλήθηκε καταγγελία από τον αστικό μη κερδοσκοπικό οργανισμό "Homo Digitalis" για λογαριασμό ενός καταγγέλλοντος, ο οποίος ισχυρίστηκε ότι δεν ήταν ικανοποιημένος σε σχέση με το δικαίωμα πρόσβασης που άσκησε ενώπιον της προαναφερθείσας εταιρείας. Με την επίμαχη καταγγελία ζητήθηκε επίσης να εξεταστούν στο σύνολό τους οι πρακτικές της εναγομένης εταιρίας υπό το πρίσμα της προστασίας των δεδομένων προσωπικού χαρακτήρα. Η εταιρία μέσω ειδικών τεχνικών συλλέγει φωτογραφίες

---

[94]https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-gia-peristatiko-parabiasis-prosopikon-dedomenon-kai-mi-nomimi

[95] https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimon-se-ypeythynoys-epexergasias-gia-tin-pragmatopoiisi-mi-nomimon

που διατίθενται δημόσια στο διαδίκτυο και εξάγει πληροφορίες από αυτές, όπως η γεωγραφική περιοχή, αντιστοίχηση προσώπων κ.ο.κ., ενώ στη συνέχεια κωδικοποιεί τις πληροφορίες αυτές και δημιουργεί βάσεις δεδομένων. Η Αρχή διαπίστωσε ότι η εταιρεία, η οποία εμπορεύεται υπηρεσίες αναγνώρισης προσώπου, παραβίασε τις αρχές της νομιμότητας και της διαφάνειας του ΓΚΠΔ. Η ελληνική εποπτική αρχή, τον Ιούλιο του 2022, επέβαλε πρόστιμο είκοσι εκατομμυρίων ευρώ (20.000.000) στην Clearview AI Inc. Επιπλέον, η Αρχή διέταξε την εταιρεία να συμμορφωθεί ώστε να ικανοποιήσει το αίτημα του καταγγέλλοντος για πρόσβαση σε προσωπικά δεδομένα, επιβάλλοντας παράλληλα (στην ίδια εταιρεία) απαγόρευση συλλογής και επεξεργασίας προσωπικών δεδομένων υποκειμένων που βρίσκονται στην ελληνική επικράτεια, χρησιμοποιώντας μεθόδους που περιλαμβάνονται στην υπηρεσία αναγνώρισης προσώπου. Με την απόφαση αυτή, η Αρχή διέταξε την Clearview AI Inc. να διαγράψει τα προσωπικά δεδομένα των υποκειμένων που βρίσκονται στην Ελλάδα, τα οποία η εναγομένη συλλέγει και επεξεργάζεται χρησιμοποιώντας τις προαναφερθείσες μεθόδους.[96] Τέλος, να αναφερθεί, ότι στην ίδια εταιρία, για τις ίδιες παραβάσεις είχε επιβληθεί πρόστιμο επίσης 20 εκατομμυρίων ευρώ και από την εποπτική αρχή της Ιταλίας λίγους μήνες νωρίτερα το 2022.[97].

4.6. Προστασία προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης

Η ιδιωτικότητα των χρηστών στα μέσα κοινωνικής δικτύωσης είναι ένας αναδυόμενος ερευνητικός τομέας και έχει προσελκύσει όλο και περισσότερη προσοχή. Έρευνες μελετούν ζητήματα απορρήτου στα μέσα κοινωνικής δικτύωσης από δύο διαφορετικά οπτικές: προσδιορισμός των τρωτών σημείων και μετριασμός των κινδύνων για την προστασία της ιδιωτικής ζωής. Πρόσφατες έρευνες έχουν δείξει την ευπάθεια δεδομένων που δημιουργούνται από χρήστες έναντι των δύο γενικών τύπων επιθέσεων, της αποκάλυψης ταυτότητας και των χαρακτηριστικών αποκάλυψης. Αυτά τα ζητήματα απορρήτου υποχρεώνουν τους εκδότες

---

[96] https://www.dpa.gr/el/enimerwtiko/deltia/anakoinosi-shetika-me-tin-epiboli-prostimoy-stin-etaireia-clearview-ai-inc

[97] https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

δεδομένων κοινωνικών μέσων να προστατεύουν το απόρρητο των χρηστών με την εξυγίανση δεδομένα που δημιουργούνται από χρήστες πριν από τη δημοσίευσή τους. Κατά συνέπεια, έχουν προταθεί διάφορες τεχνικές προστασίας για την ανωνυμοποίηση δεδομένων κοινωνικών μέσων που δημιουργούνται από χρήστες. [98]

Σε μία άλλη έρευνα που διεξήχθει σε μαθητες γυμνασίου σχετικά με το θέμα ιδιωτικής ζωής στο διαδίκτυο, οι μαθητές κλήθηκαν να δώσουν τις απαντήσεις τους σχετικά με το ερώτημα εάν οι μηχανές αναζήτησης και οι ιστότοποι κοινωνικής δικτύωσης θα πρέπει να επιτρέπεται να καταγράφουν, να παρακολουθούν και να μοιράζονται τα προσωπικά δεδομένα των χρηστών τους ή εάν τέτοιες πρακτικές παραβιάζουν το προσωπικό απόρρητο. Από την έρευνα προκύπτουν αρκέτα σημαντικά συμπεράσματα που υποδηλώνουν την άγνοια και την έλλειψη πληροφόρησης. Αρχικά, οι μαθητές φαίνεται να μη θεωρούν σημαντικό το ζήτημα της έκθεσης των δεδομένων τους στο διαδίκτυο. Ως αποτέλεσμα, οι εκπαιδευτικοί βρέθηκαν να παίζουν έναν ρόλο που δεν είχαν προβλέψει: συνεχώς λειτουργούν ως συνήγορος του διαβόλου και κατευθύνοντας επανειλημμένα την προσοχή των μαθητών σε στοιχεία στα πακέτα που υποδηλώνουν τους κινδύνους για προστασία της ιδιωτικής ζωής που δημιουργείται από τα μέσα κοινωνικής δικτύωσης όπως το Facebook και τις μηχανές αναζήτησης στο Διαδίκτυο, όπως το Google. Πολλά άτομα, τόσο έφηβοι όσο και ενήλικες, φαίνονται έτοιμοι να δεχτούν τις ρυθμίσεις ανταλλαγής που χαρακτηρίζουν την Google και το Facebook, δηλαδή, τα δεδομένα τους για τη δωρεάν υπηρεσία σας. Ένα εναλλακτικό μοντέλο υπάρχει ήδη στην Apple, όπου το τέλος για την υπηρεσία (π.χ. iTunes) υπάρχει εδώ και μια δεκαετία και αντιπροσωπεύει έναν άλλο τρόπο αποφυγής της δημιουργίας εσόδων από προσωπικές πληροφορίες για κέρδος. Ερευνητές και δημοσιογράφοι σε όλο τον κόσμο επισημαίνουν στο κοινό τους κινδύνους για ιδιωτικότητα και δημοκρατία που αντιπροσωπεύονται από την εξαιρετική δύναμη των εταιρειών τεχνολογίας. Μελετητές και εκπαιδευτικοί κοινωνικών σπουδών πλαισιώνουν την εξέταση αυτού του θέματος ως οικονομικού,

[98] Ghazaleh Beigi and Huan Liu. 2020. A Survey on Privacy in Social Media: Identification, Mitigation, and Applications. ACM/IMS Trans. Data Sci. 1, 1, Article 7 (January 2020)

πολιτικού και κοινωνικού ζητήματος. Από την έρευνα προκύπτει επίσης ότι οι μαθητές παρουσιάζεται να έχουν μια εκπληκτική εμπιστοσύνη στο Facebook και την Google. [99]

Οι απαιτήσεις ασφάλειας και απορρήτου των κοινωνικών δικτύων εξακολουθούν να μην είναι καλά κατανοητές ή πλήρως καθορισμένες. Παρ 'όλα αυτά, είναι σαφές ότι θα είναι αρκετά διαφορετικά από τις κλασικές απαιτήσεις ασφάλειας και απορρήτου, επειδή τα κοινωνικά δίκτυα περιλαμβάνουν ανησυχίες με επίκεντρο τον χρήστη και επιτρέπουν σε πολλούς χρήστες να καθορίζουν πολιτικές ασφαλείας σε κοινόχρηστα δεδομένα. Έτσι, πρέπει να φέρουμε ένα βάθος εμπειρίας ασφάλειας από πολλούς τομείς και τεχνολογίες ασφάλειας σε αυτόν τον τομέα, καθώς και ένα εύρος γνώσεων σχετικά με τα κοινωνικά δίκτυα.[100]

4.6.1. Δημιουργία προφίλ και χρήση προσωπικών δεδομένων για ταυτοποίηση

Οι περισσότεροι ιστότοποι κοινωνικής δικτύωσης προσφέρουν τις βασικές δυνατότητες διαδικτυακής αλληλεπίδρασης, επικοινωνίας και κοινής χρήσης ενδιαφέροντος, επιτρέποντας στα άτομα να δημιουργούν διαδικτυακά προφίλ που μπορούν να δουν άλλοι χρήστες. Ένα από τα πιο σημαντικά ζητήματα που προκύπτουν σε αυτό το πλαίσιο είναι η ασφάλεια και το απόρρητο των ευαίσθητων πληροφοριών, οι οποίες είναι γενικά οποιαδήποτε δεδομένα θα μπορούσε να χρησιμοποιήσει ένας τρίτος για να προκαλέσει σημαντική βλάβη στους χρήστες. Αυτά τα δεδομένα μπορεί να περιλαμβάνουν οικονομικές πληροφορίες, τις οποίες κάποιος θα μπορούσε να χρησιμοποιήσει για να διαπράξει κλοπή ταυτότητας ή ιατρικές πληροφορίες, όπως καταστάσεις υγείας, διαγνώσεις ή ιστορικό θεραπείας. Η χρήση προσωπικών πληροφοριών στα κοινωνικά δίκτυα εγείρει νέες ανησυχίες και απαιτεί πληροφορίες που προκαλούν ερωτήματα για θέματα ασφαλείας. Τα διαδικτυακά κοινωνικά δίκτυα έχουν πρόσφατα αναδειχθεί ως ερευνητικός τομέας με τεράστια εμβέλεια και χώρο εφαρμογών.

---

[99] Margaret S. Crocco, Avner Segall, Anne-Lise Halvorsen, Alexandra Stamm, Rebecca Jacobsen, “It's not like they're selling your data to dangerous people”: Internet privacy, teens, and (non) controversial public issues, The Journal of Social Studies Research, Volume 44, Issue 1, 2020,

[100] Ahn G. J., Shehab M., and Squicciarini A., "Security and Privacy in Social Networks," in IEEE Internet Computing, vol. 15, no. 3, pp. 10-12, May-June 2011

Αρκετές μελέτες και πρόσφατες ειδήσεις έχουν επισημάνει τον αυξημένο κίνδυνο για τα προσωπικά δεδομένα που επεξεργάζονται οι διαδικτυακές εφαρμογές κοινωνικής δικτύωσης, καθώς και την έλλειψη ευαισθητοποίησης του πληθυσμού των χρηστών. Σε γενικές γραμμές, το ζήτημα της ιδιωτικής ζωής στην κοινωνική δικτύωση συνδυάζεται με την ταυτοποίηση και τη δυνατότητα σύνδεσης των πληροφοριών που είναι διαθέσιμες σε αυτό το κοινωνικό περιβάλλον, τους πιθανούς αποδέκτες του και τις πιθανές χρήσεις του. Η προστασία της ταυτοποίησης και σύνδεσης των πληροφοριών είναι αρκετά δύσκολη, δεδομένου ότι ακόμη και εκείνοι οι ιστότοποι που δεν αποκαλύπτουν τα προσωπικά στοιχεία των χρηστών ενδέχεται να παρέχουν αρκετά δεδομένα για τον εντοπισμό και τη σύνδεση του κατόχου ενός προφίλ. Οι πιθανοί παραλήπτες για τέτοιες προσωπικά αναγνωρίσιμες πληροφορίες περιλαμβάνουν διακομιστές φιλοξενίας για τους ιστότοπους κοινωνικής δικτύωσης, το ίδιο το δίκτυο και τρίτους που ενδέχεται να καταχραστούν ή να κάνουν κακή χρήση τέτοιων κρίσιμων και ευαίσθητων πληροφοριών. [101]

Επιπλέον, ένα νέο πρότυπο για την ασφάλεια περιλαμβάνει την ανάγκη αντιμετώπισης ζητημάτων διαπροσωπικών σχέσεων και ευελιξίας στα διαδικτυακά κοινωνικά δίκτυα. Για παράδειγμα, ένας χρήστης θα μπορούσε να μοιραστεί το προσωπικό του άλμπουμ φωτογραφιών με μέλη της οικογένειας αλλά όχι με συναδέλφους από την εργασία. Οι ιστότοποι κοινωνικής δικτύωσης επιτρέπουν στους χρήστες να δημιουργούν ένα περιορισμένο προφίλ και να επιλέγουν ποιοι άλλοι χρήστες θα αντιστοιχιστούν σε αυτό. Τέτοιοι πρωτόγονοι μηχανισμοί ασφαλείας έχουν περιορισμένη μόνο εκφραστικότητα για τον έλεγχο των αλληλεπιδράσεων χρήστη-χρήστη, ειδικά σε ένα δυναμικό κοινωνικό δίκτυο. Η ανάγκη για νέους μηχανισμούς ασφαλείας που βασίζονται σε μετρήσεις όπως ο κίνδυνος, η εμπιστοσύνη και οι κοινωνικές μετρήσεις γίνεται όλο και πιο επιτακτική.

4.7. Η εμπορευματοποίηση των προσωπικών δεδομένων

Τον Μάρτιο του 2018, μεγάλο μέρος της προσοχής των μέσων ενημέρωσης αφιερώθηκε στον τρόπο με τον οποίο τα δεδομένα συλλέχθηκαν από τους λογαριασμούς στο Facebook

[101] Ahn G. J., Shehab M., and Squicciarini A., "Security and Privacy in Social Networks," in IEEE Internet Computing, vol. 15, no. 3, pp. 10-12, May-June 2011

εκατομμυρίων χρηστών είχαν χρησιμοποιηθεί από τρίτους. Έχει προταθεί ότι οι πληροφορίες που έδωσαν αυτά τα δεδομένα χρησιμοποιήθηκαν ώστε να επηρεάσουν την ψήφο των πολιτών σε πολιτικά ζητήματα όπως το δημοψήφισμα του Ηνωμένου Βασιλείου για το Brexit και η εκλογή του Ντόναλντ Τραμπ στην προεδρία των ΗΠΑ.[102] Αυτή η ιστορία αναδεικνύει ένα πλήθος ζητημάτων που εγείρει το σύγχρονο φαινόμενο των «μαζικών δεδομένων».

Τα «Big Data» είναι ένας ασαφής όρος που ουσιαστικά, χρησιμοποιείται για να δηλώσει την ικανότητα των σημερινών υπολογιστών να συλλαμβάνουν και να αποθηκεύουν τεράστιες ποσότητες δεδομένων. Τα δεδομένα που συλλέγονται μπορούν να αφορούν ακόμη και δεδομένα σχετικά με το πότε οι χρήστες χρησιμοποιούν κάρτες καταστημάτων λιανικής πώλησης ή τα κινητά τους τηλέφωνα (τα οποία μπορούν να καταγράψουν τη γεωγραφική τους θέση και το λογισμικό αναγνώρισης προσώπου που έχει την ικανότητα να αναγνωρίζει άτομα μέσω της καταγραφής τους από κάμερες ασφαλείας ή μέσω της εμφάνισής τους σε φωτογραφίες που δημοσιεύονται στο διαδίκτυο από άλλους, χωρίς τη γνώση ή τη συγκατάθεσή τους. Ο συνδυασμός τέτοιων δεδομένων μπορεί να παρέχει μια πολύ λεπτομερή καταγραφή για την καθημερινή ζωή του ατόμου: τα πρότυπα κατανάλωσης, εργασίας, ταξιδιού, επικοινωνίας, το παιχνίδι, τις αλληλεπιδράσεις με τους άλλους, τις σκέψεις και τα ενδιαφέροντά τους». Όλα αυτά τα δεδομένα μπορούν να αποθηκευτούν και στη συνέχεια να χρησιμοποιηθούν για οικονομικούς σκοπούς, και όχι για την επιδίωξη «καθαρής» έρευνας, τα δεδομένα πλέον συχνά αντιμετωπίζονται «πρωτίστως ως οικονομικό αγαθό, όχι ως ερευνητικό». [103]

Ο κύριος μοχλός πίσω από την άνοδο των μαζικών δεδομένων είναι, φυσικά, οικονομικός. Τα οικονομική οφέλη που θα αποκομιστούν από τη συλλογή και την ανάλυση των δεδομένων που παραδίδουν οι άνθρωποι στις διαδικτυακές πλατφόρμες είναι τεράστια. Για παράδειγμα,

---

[102] C. Cadwalladr and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', Guardian, 17 March 2018, <www.theguardian.com/news/2018/mar/17/cambridgeanalytica-facebook-influence-us-election>

[103] J. Wilbanks, 'Portable approaches to informed consent and open data' in J. Lane et al. (eds), Privacy, Big Data, and the Public Good: frameworks for engagement (New York, NY: Cambridge University Press, 2014)

υπολογίζεται ότι το ένα τρίτο των πωλήσεων της Amazon δημιουργούνται από συστάσεις που βασίζονται στην ανάλυση δεδομένων που υποβάλλουν οι χρήστες στον ιστότοπο. [104] Αυτό έχει ως αποτέλεσμα να δημιουργηθεί μια ολόκληρη βιομηχανία η οποία αναπτύχθηκε γύρω από τη συγκέντρωση και την πώληση δεδομένων, την ενημέρωση των καταναλωτών, την ανάλυση και τη βελτίωση των βάσεων δεδομένων των πελατών, και την ανταλλαγή καταλόγων πελατών. [105]

4.8. Ο Covid-19 και η προστασία προσωπικών δεδομένων

Η έξαρση της νόσου COVID-19 στο τέλος του 2019, ο άγνωστος ιός, τα συμπτώματα, η νόσηση εκατομμυρίων ανθρώπων και η πρωτοφανής κατάσταση που επικράτησε σε παγκόσμιο επίπεδο δημιούργησαν την ανάγκη για νέες έρευνες και μελέτες. Η πανδημία έχει αποβεί ως μια πραγματική δοκιμασία για τον τρόπο με τον οποίο στα πλαίσια προστασίας δεδομένων και απορρήτου, όπως ο ΓΚΠΔ, διεξάγονται έρευνες κατά τη διάρκεια της πανδημίας. Υπάρχουν δύο οπτικές γωνίες. Μια οπτική γωνία είναι μέσω των εξαιρέσεων που χρησιμοποιούνται από τις αντίστοιχες εθνικές υγειονομικές αρχές και τα κυβερνώντα μέρη που προβλέπονται στο άρθρο 9 παράγραφος 2 του GDPR προκειμένου να καταστεί δυνατή η χρήση δεδομένων υγείας για ερευνητικούς σκοπούς και μια άλλη οπτική γωνία είναι μέσω της χρήσης ψηφιακών εφαρμογών σε συσκευές που αποσκοπούν στην παρακολούθηση των κινήσεων και της κατάστασης της υγείας των πολιτών. Αυτό έχει φυσικά προκαλέσει τη δημιουργία επικρίσεων σχετικά με την επάρκεια, την αποτελεσματικότητα και την αποδοτικότητα του ΓΚΠΔ, καθώς και άλλων νομικών και ρυθμιστικών μηχανισμών, οι οποίοι επιτρέπουν τη χρήση και την ανταλλαγή ευρωπαϊκών ψηφιακών δεδομένων υγείας είτε χρησιμοποιούνται για έρευνα είτε για άλλο λόγο. Ορισμένες από αυτές τις επικρίσεις είναι δικαιολογημένες σε κάποιο βαθμό. Ωστόσο, υπάρχουν ρητές αναφορές στις διατάξεις του GDPR (όπως οι αιτιολογικές σκέψεις 46 και 52) που ορίζουν ότι ορισμένοι

---

[104] Mayer-Schonberger, V. and Cukier, K. (2014) Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, New York. p.52

[105]CIPPIC, On the Data Trail: how detailed information about you gets into the hands of organisations with whom you have no relationship. A report on the Canadian data brokerage industry (Ottawa: Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2006), p. 46. Διαθέσιμο στο: www.cippic.ca/sites/default/files/May1-06/DatabrokerReport.pdf

τύποι επεξεργασίας δεδομένων ειδικής κατηγορίας επιτρέπονται για λόγους που εξυπηρετούν τόσο το δημόσιο συμφέρον, όσο και τα συμφέροντα του υποκειμένου των δεδομένων, για τους σκοπούς των ανθρωπιστικών δράσεων, της πρόληψης ασθενειών και της εξάπλωσης επιδημιών. Ως εκ τούτου, τα παραδείγματα αυτά αποδεικνύουν ότι ο κανονισμός αφήνει χώρο και παρέχει περιθώρια στα εθνικά μέσα και οργανισμούς να χειρίζονται δεδομένα σε καταστάσεις συγκρίσιμες με την πανδημία.

Ένα άλλο σημείο που προκαλεί αμφιλεγόμενες σκέψεις είναι η χρήση της «συγκατάθεσης» ως νόμιμης βάσης για την επαναχρησιμοποίηση ευαίσθητων δεδομένων υγείας, διαφορετικά η εκ νέου συγκατάθεση μπορεί αναμφισβήτητα να θεωρηθεί δύσκολη και ακόμη και ανέφικτη.[106] Αυτό οφείλεται στα πολλαπλά βήματα που θα απαιτούνταν, καθώς και στο γεγονός ότι, στην πραγματικότητα, η συγκατάθεση θα εξαρτιόταν εξ ολοκλήρου από την απίθανη πρακτικότητα της εκ νέου επικοινωνίας με όλα τα υποκείμενα των δεδομένων σε περίπτωση που ο αρχικός σκοπός της συλλογής δεδομένων τους δεν είναι ο ίδιος με την περαιτέρω χρήση. Στο πλαίσιο αυτό, σχετικά με το θέμα της «ρητής συγκατάθεσης» για την επεξεργασία δεδομένων υγείας και την επάρκειά της, προβάλλονται επιχειρήματα ότι η συγκατάθεση που παρέχεται στο διαδίκτυο σε περιπτώσεις έκτακτης ανάγκης μπορεί να θεωρηθεί άκυρη.[107] Αν και η «συγκατάθεση» δεν είναι η μόνη νόμιμη βάση που μπορεί να χρησιμοποιηθεί για την επαναχρησιμοποίηση δεδομένων, η βάση του δημόσιου συμφέροντος έχει επίσης επικριθεί λόγω της έλλειψης ομοιόμορφης εφαρμογής και ερμηνείας που υπάρχει σε εθνικό επίπεδο.

Ωστόσο, είναι σημαντικό να σημειωθεί ότι αυτή η έλλειψη ομοιομορφίας οφείλεται, εν μέρει, στο γεγονός ότι κάθε κράτος μέλος έχει περιθώριο εκτίμησης όσον αφορά την πλήρη εφαρμογή της νομοθεσίας της ΕΕ. Αυτό γίνεται προκειμένου να διασφαλιστεί ότι αυτή η έγκριση του ΓΚΠΔ σε εθνικό επίπεδο είναι συμβατή με άλλους κανόνες και μηχανισμούς προστασίας των δεδομένων

---

[106] Becker R, Thorogood A, Ordish J, Beauvais MJS. COVID-19 Research: Navigating the European General Data Protection Regulation. J Med Internet Res 2020

[107] Harris M, Bhatti Y, Buckley J, Sharma D., Fast and frugal innovations in response to the Covid-19 pandemic. Nat Med 2020

για τους οποίους οι σχετικές παρεκκλίσεις παρέχουν ευελιξία κατά την εφαρμογή του νόμου. Στην προκειμένη περίπτωση, αυτό γίνεται προκειμένου να διασφαλιστεί ότι ο ΓΚΠΔ, ο οποίος απλώς ως νομικό πλαίσιο που ευνοεί την καινοτομία και επιτρέπει την εισαγωγή τεχνολογιών που επεξεργάζονται προσωπικά δεδομένα στην αγορά, εφαρμόζεται στο δίκαιο των κρατών μελών και λειτουργεί σε αρμονία με τους εθνικούς κανονισμούς για την προστασία των δεδομένων, καθώς και ότι αφήνει περιθώρια για την εκπόνηση παράγωγου δικαίου σε εθνικό επίπεδο. Ως εκ τούτου, αν και τα πρόσθετα νομοθετικά επίπεδα ή οι εξουσίες που ανατίθενται βάσει του ΓΚΠΔ στα κράτη μέλη να επιβάλλουν πρόσθετους περιορισμούς στην επεξεργασία δεδομένων υγείας και γενετικών δεδομένων μπορεί να φαίνονται πρόσθετα εμπόδια που πρέπει να ξεπεραστούν ή πιθανές αποκλίσεις, η διαδικασία αυτή αφήνει χώρο για διαλειτουργικότητα και για κάθε χώρα να εφαρμόζει σωστά την προστασία των δεδομένων και όπως ταιριάζει καλύτερα στη δικαιοδοσία.[108]

[108]Christofidou M, Lea N, Coorevits P. A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. Yearb Med Inform. 2021 Aug

Κεφάλαιο 5: Συμπεράσματα

Αναμφισβήτητα, το θέμα της προστασίας των δεδομένων προσωπικού χαρακτήρα στη σύγχρονη κοινωνία απότελεί σημαντική πρόκληση, τόσο για την Ευρωπαϊκή Ένωση, απο την πλευρά της μέριμνας, όσο και από τα κράτη μέλη, κάθε ένα ξεχωριστά, και τις εποπτικές αρχές από την πλευρά του ελέγχου της τήρησης της νομοθεσίας. Επίσης, οι επιχειρήσεις, έχουν ήδη αφιερώσει ανθρώπινους και οικονομικούς πόρους για να προσαρμόσουν τις διαδικασίες τους και να συμμορφωθούν με τους κανονισμούς. Τα φυσικά πρόσωπα, πρέπει να είναι πλήρως ενημερωμένα για τα δικαιώματά τους, να σέβονται πρώτα απ' όλα τα ίδια τα προσωπικά τους δεδομένα και να επιδεικνύουν την απαραίτητη προσοχή σε καθημερινή βάση για την έκθεσή τους.

Λαμβάνοντας υπ' όψιν όσα αναφέρθηκαν στα προηγούμενα κεφάλαια, το ευρωπαϊκό δίκαιο, αντιμετωπίζει την προστασία των δεδομένων ως ζήτημα ατομικών δικαιωμάτων. Τα δικαιώματα αυτά οργανώνονται σε δύο επίπεδα. Το ανώτατο επίπεδο περιλαμβάνει τα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και την προστασία των δεδομένων, τα οποία είναι άρρηκτα συνδεδεμένα και με άλλα θεμελιώδη δικαιώματα και αρχές: αξιοπρέπεια, ελευθερία σκέψης, συνείδησης και θρησκείας, ελευθερία επιλογής επαγγέλματος και δικαίωμα προς εργασία, απαγόρευση των διακρίσεων κ.λπ. Το δεύτερο επίπεδο αποτελείται από τα δικαιώματα προστασίας δεδομένων που παρέχονται στα φυσικά πρόσωπα από τον ΓΚΠΔ, όπως η εξουσία συγκατάθεσης και ανάκλησης συγκατάθεσης, το δικαίωμα ενημέρωσης, πρόσβασης, διαγραφής, λήθης και το δικαίωμα εναντίωσης. Το επίκεντρο είναι η προστασία των ατόμων από οποιαδήποτε βλάβη μπορεί να προκληθεί από αθέμιτη χρήση των δεδομένων τους.

Η προσέγγιση βάσει κινδύνου, αντί της χορήγησης ατομικών δικαιωμάτων, επικεντρώνεται στη δημιουργία μιας βιώσιμης οικολογίας πληροφοριών, όπου η ζημία αποτρέπεται με κατάλληλα οργανωτικά και τεχνολογικά μέτρα. Η προστασία των δεδομένων, όταν εξετάζεται από την τελευταία αυτή οπτική γωνία, φαίνεται να είναι μια πειθαρχία ρύθμισης κινδύνου, παρόμοια με την προστασία του περιβάλλοντος, την ασφάλεια των τροφίμων ή ακόμη και τη ρύθμιση των ιατροτεχνολογικών προϊόντων ή των χρηματοπιστωτικών αγορών. Σε αυτούς τους τομείς η έμφαση στα προληπτικά μέτρα, την πιστοποίηση, την ιδιωτική και δημόσια εμπειρογνωμοσύνη και στον τρόπο με τον οποίο επηρεάζονται όχι μόνο τα άτομα από την κοινωνία και τις ομάδες.

Στηριζόμενη στον Γενικό Κανονισμό για την Προστασία Δεδομένων (2016/679), η ελληνική νομοθεσία έθεσε σε ισχύ τον ν. 4624/2019 με προσθήκες και διευκρινήσεις σχετικά με τα μέτρα εφαρμογής του κανονισμού. Στο σύνολο της νομοθεσίας, μεταξύ άλλων, περιλαμβάνονται ορισμοί σχετικά με τις έννοιες που χρησιμοποιούνται, τα δικαιώματα του υποκειμένου, ορίζονται υπεύθυνοι επεξεργασίας και προστασίας, προβλέπονται οδηγίες σχετικά με κυρώσεις και επιβολή προστίμων καθώς και εξαιρέσεις του νόμου.

Προκύπτει ότι, ειδικότερα στους χώρους απασχόλησης, έχει δοθεί ιδιαίτερη προσοχή, καθώς η συλλογή δεδομένων είναι πολλές φορές απαραίτητη ενώ υπάρχουν αντικρουόμενα συμφέροντα. Επιπλέον, ιδιαίτερες προκλήσεις και κίνδυνοι παρουσιάζονται στο διαδίκτυο και στον τομέα των τηλεπικοινωνιών, ενώ εκεί παρατηρούνται και οι περισσότερες παραβάσεις.

Όπως αναφέρθηκε, η έννοια της συγκατάθεσης, ως σαφή και ρητή, έχει δημιουργήσει πολλές προκλήσεις καθώς δεν είναι λίγες οι περιπτώσεις που θεωρείται αμφιλεγόμενη, λόγω της δυσκολίας κατανόησης του εύρους της πιθανής συλλογής και χρήσης των δεδομένων. Παρατηρείται, υπερβολική εμπιστοσύνη και πολλές φορές ακόμη και άγνοια σχετικά με την προστασία των προσωπικών δεδομένων, αφήνοντας περιθώρια εκμετάλλευσης των προσωπικών δεδομένων για εμπορικούς σκοπούς που τελικό σκοπό τη δημιουργία κέρδους.

Η ενημέρωση και η ευαισθητοποίηση των χρηστών σχετικά με την προστασία των προσωπικών δεδομένων αποτελεί πλέον επιτακτική ανάγκη, αν λάβει κανείς υπόψη του την αδιάκοπη ροή πληροφοριών στο διαδίκτυο και τα τόσα παραδείγματα αθέμιτης χρήσης.

Βιβλιογραφία

Αιγυπτιάδου-Αλεξανδροπούλου, Προσωπικά Δεδομένα, Αθήνα Νομική Βιβλιοθήκη, 2016.

Γριβοκωστόπουλος Ι., «Κριτική ανάλυση του Ν. 4624/2019», Επιθεώρηση Δικαίου Πληροφορικής, Τεύχος 1 2021, Διαθεσιμο στο: http://ejournals.lib.auth.gr/infolawj/

Δελούκα-Ιγγλέση Κ. Νομικά Θέματα Ηλεκτρονικού Εμπορίου, Εκδόσεις Σάκκουλα, Αθήνα Θεσσαλονίκη, 2016.

Δούκα Β., Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας, Εκδόσεις Σάκκουλας Αθήνα – Θεσσαλονίκη 2011.

Ιγγλεζάκης Ι., Εισαγωγή στο δίκαιο της Πληροφορικής, Εκδόσεις Σάκκουλα, Αθήνα Θεσσαλονίκη, 2018.

Ιγγλεζάκης Ι., Ο Γενικός κανονισμός Προστασίας προσωπικών Δεδομένων – Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων, Εκδόσεις INTERACTIVE BOOKS 2018.

Ιγγλεζάκης Ι., Η συγκατάθεση στο δίκαιο προστασίας προσωπικών δεδομένων, σε: Κοτσαλή Λεωνίδα, Νομική Βιβλιοθήκη 2016, σελ. 95 επ.

Ιγγλεζάκης, Ι., Ευαίσθητα προσωπικά δεδομένα, Αθήνα-Θεσσαλονίκη, Σάκκουλας, 2004.

Κοτσαλής Λ., (επιμ.), Προσωπικά Δεδομένα- Ανάλυση – Σχόλια – Εφαρμογή, Νομική Βιβλιοθήκη 2016.

Λαζαράκος , Γ., Ο θεσμός του υπεύθυνου προστασίας δεδομένων στο νέο νομοθετικό πλαίσιο των προσωπικών δεδομένων μετά την υιοθέτηση του Κανονισμού (ΕΕ) 679/2016, Εφαρμογές Δημοσίου Δικαίου 2016.

Μήτρου, Λ., Ο γενικός κανονισμός προστασίας δεδομένων, Αθήνα – Θεσσαλονίκη, Σάκκουλας, 2017.

Μήτρου Λ., Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις, ΕπιθΕργΔ 2017, 137 επ.

Μήτρου, Λ., Το δίκαιο στην κοινωνία της πληροφορίας, Αθήνα – Θεσσαλονίκη, Σάκκουλας, 2002.

Νούσκαλης, Γ., Ψηφιακή τεχνολογία και δίκαιο, Η ποινική προστασία της ψηφιακής τεχνολογίας, Αθήνα-Θεσσαλονίκη, Σάκκουλας, 2004

Παπακωνσταντίνου, Ε., Νομικά θέματα πληροφορικής, Αθήνα – Θεσσαλονίκη, Σάκκουλας, 2006.

Παναγοπούλου-Κουτνατζή, Φ., Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, Σάκκουλας, Αθήνα – Θεσσαλονίκη, 2017.

Χριστοδούλου Κ., Δίκαιο Προσωπικών Δεδομένων, Νομική Βιβλιοθήκη 2020.

Ahn G. J., Shehab M., and Squicciarini A., "Security and Privacy in Social Networks," in IEEE Internet Computing, vol. 15, no. 3, pp. 10-12, May-June 2011

Bart Custers, Anne-Sophie Heijne, The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice, Computer Law & Security Review, Volume 46, 2022

Becker R, Thorogood A, Ordish J, Beauvais MJS. COVID-19 Research: Navigating the European General Data Protection Regulation. J Med Internet Res 2020 Aug 27;22(8):e19799.

Christian Kurtz, Florian Wittner, Martin Semmann, Wolfgang Schulz, Tilo Böhmann, Accountability of platform providers for unlawful personal data processing in their ecosystems–A socio-techno-legal analysis of Facebook and Apple's iOS according to GDPR, Journal of Responsible Technology, Volume 9, 2022

Christofidou M, Lea N, Coorevits P. A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. Yearb Med Inform. 2021 Aug

Edwards, L. and Veale, M. (2019). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law and Technology Review, 16-84.

Eugenia Politou, Efthimios Alepis, Constantinos Patsakis, Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy001, https://doi.org/10.1093/cybsec/tyy001

Financial Times: 'One year on, GDPR needs a reality check', available at: https://www.ft.com/

FRA/COE, Handbook on European Data Protection Law, Belgium, 2014, page 56. Also available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

Ghazaleh Beigi and Huan Liu. 2020. A Survey on Privacy in Social Media: Identification, Mitigation, and Applications. ACM/IMS Trans. Data Sci. 1, 1, Article 7 (January 2020)

Ghazaleh Beigi, Kai Shu, Yanchao Zhang, and Huan Liu. 2018. Securing social media user data: An adversarial approach. In Proceedings of the 29th Conference on Hypertext and Social Media. ACM,

Harris M, Bhatti Y, Buckley J, Sharma D., Fast and frugal innovations in response to the Covid-19 pandemic. Nat Med 2020

J. Wilbanks, 'Portable approaches to informed consent and open data' in J. Lane et al. (eds), Privacy, Big Data, and the Public Good: frameworks for engagement (New York, NY: Cambridge University Press, 2014)

Karyda, Spyridoula, Law No. 4624/2019: Shedding Light on the Greek Adaptation of the GDPR (March 11, 2022). Διαθέσιμο στο SSRN: https://ssrn.com/abstract=4055464 or http://dx.doi.org/10.2139/ssrn.4055464

S. E. Koonin and M. J. Holland, 'The value of big data for urban science' in Lane, Privacy, Big Data, and the Public Good, Cambridge University Press (2014)

Leenes R., Van Brakel R., Gutwirth S., De Hert P., (2018), Data Protection and Privacy: The Internet of Bodies (Computers, Privacy and Data Protection), Hart Publishing. Διαθέσιμο στο: https://researchportal.vub.be/en/publications/data-protection-and-privacy-the-internet-of-bodies

Margaret S. Crocco, Avner Segall, Anne-Lise Halvorsen, Alexandra Stamm, Rebecca Jacobsen, "It's not like they're selling your data to dangerous people": Internet privacy, teens, and (non) controversial public issues, The Journal of Social Studies Research, Volume 44, Issue 1, 2020,

Mayer-Schonberger, V. and Cukier, K. (2014) Big Data: A Revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, New York. p.52

Strandburg, Katherine J.. "Privacy, Big Data, and the Public Good: Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context." (2014).

Salami, Emmanuel, An Analysis of the General Data Protection Regulation (EU) 2016/679 (May 10, 2017). Available at SSRN: https://ssrn.com/abstract=2966210

Wachter, S., B. Mittelstadt, and L. Floridi (2016). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law 7,

Zufall, F., & Zingg, R. (2021). Data Portability in a Data-Driven World. In S. Peng, C. Lin, & T. Streinz (Eds.), Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration (pp. 215-234). Cambridge: Cambridge University Press.

Διαδικτυακές Πηγές

B. Quinn and C. Arthur, 'PlayStation Network hackers access data of 77 million users', Guardian, 26 April 2011, www.theguardian.com/technology/2011/apr/26/playstationnetwork-hackers-data Πρόσβαση: 28/10/2022

C. Cadwalladr and E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', Guardian, 17 March 2018, www.theguardian.com/news/2018/mar/17/cambridgeanalytica-facebook-influence-us-election Πρόσβαση: 14/10/2022

J. Espinoza, «EU admits it has been hard to implement GDPR», Financial Times, 23/06/2020 Διαθέσιμο στο: https://www.ft.com/content/66668ba9-706a-483d-b24a-18cfbca142bf Πρόσβαση: 28/08/2022

The History of the General Data Protection Regulation, διαθέσιμο στην ιστοσελίδα: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en Πρόσβαση: 05/09/2022

https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en Πρόσβαση: 05/09/2022

https://edpb.europa.eu/news/national-news/2020/telephone-operators-italian-sa-fines-wind-eur-17-million-and-iliad-eur-08_en Πρόσβαση: 05/09/2022

https://edpb.europa.eu/news/national-news/2020/aggressive-telemarketing-practices-vodafone-fined-over-12-million-euro_en Πρόσβαση: 05/09/2022

https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-gia-peristatiko-parabiasis-prosopikon-dedomenon-kai-mi-nomimi Πρόσβαση: 05/09/2022

https://www.dpa.gr/el/enimerwtiko/deltia/deltio-typoy-shetika-me-ti-gnostopoiisi-peristatikoy-parabiasis Πρόσβαση: 05/09/2022

https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimon-se-ypeythynoys-epexergasias-gia-tin-pragmatopoiisi-mi-nomimon Πρόσβαση: 05/09/2022

https://www.dpa.gr/el/enimerwtiko/deltia/anakoinosi-shetika-me-tin-epiboli-prostimoy-stin-etaireia-clearview-ai-inc Πρόσβαση: 05/09/2022

https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en Πρόσβαση: 05/09/2022

https://www.dpa.gr/ Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Πρόσβαση: 30/08/2022

https://www.lawspot.gr/nomikes-plirofories/nomothesia/nomos-4624-2019
Πρόσβαση:30/08/2022

https://cnpd.public.lu/en/ Πρόσβαση: 05/09/2022