ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της
ΕΛΕΝΗΣ ΚΑΛΠΙΑ (Α.Μ.: ΜΔΙ2016)

ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΧΡΗΣΤΩΝ ΤΩΝ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΣΕ ΟΙΚΟΣΥΣΤΗΜΑΤΑ ΕΞΥΠΝΩΝ ΚΙΝΗΤΩΝ

Επιβλέπουσα Καθηγήτρια:

Λίλιαν Μήτρου

Πειραιάς, Μάιος 2022

Στον Ανδρέα

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας μεταπτυχιακής διπλωματικής εργασίας αποτελεί το ζήτημα της προστασίας της ιδιωτικότητας των χρηστών των μέσων κοινωνικής δικτύωσης σε οικοσυστήματα έξυπνων κινητών τηλεφώνων. Αφορμή για την έρευνα του παρόντος θέματος στάθηκε η αυξανόμενη ανάγκη για τη διασφάλιση των δικαιωμάτων του ανθρώπου – χρήστη έξυπνου κινητού τηλεφώνου, η καθημερινότητα του οποίου πλέον εξαρτάται σχεδόν αποκλειστικά από τις δυνατότητες επικοινωνίας και αλληλεπίδρασης που προσφέρουν τα μέσα κοινωνικής δικτύωσης.

Η εργασία χωρίζεται σε τρία μέρη. Στο πρώτο Κεφάλαιο αναλύεται η έννοια και τα συστατικά στοιχεία ενός οικοσυστήματος έξυπνων κινητών, συμπεριλαμβανομένων των διαφορετικών λειτουργικών συστημάτων και των εφαρμογών που αναπτύσσονται εκεί, καθώς και ο κύκλος ζωής των δεδομένων που συλλέγονται και διακινούνται από τα εμπλεκόμενα μέρη. Επιπλέον, γίνεται αναφορά σε ορισμένα ζητήματα ιδιωτικότητας που παρατηρούνται στα οικοσυστήματα αυτά, με ιδιαίτερη έμφαση στους διαφορετικούς τρόπους συλλογής και επεξεργασίας προσωπικών δεδομένων στο εκάστοτε λειτουργικό σύστημα. Το δεύτερο Κεφάλαιο αφορά τα μέσα κοινωνικής δικτύωσης. Πιο συγκεκριμένα, αναλύονται τα κύρια χαρακτηριστικά τους, τα προσωπικά δεδομένα που δύνανται να συλλέγουν από τους χρήστες, ο τρόπος συλλογής και επεξεργασίας και η ενημέρωση των χρηστών μέσω όρων χρήσης και πολιτικών προστασίας δεδομένων. Παράλληλα, παρατίθεται μία σύντομη ανάλυση των θεωριών σχετικά με τη συμπεριφορά των χρηστών απέναντι στην επεξεργασία των προσωπικών τους δεδομένων. Στο τρίτο Κεφάλαιο επιχειρείται η ανάλυση ειδικότερων νομικών ζητημάτων που αφορούν την προστασία της ιδιωτικότητας των χρηστών των μέσων κοινωνικής δικτύωσης σε οικοσυστήματα έξυπνων κινητών, όπως -ενδεικτικά- η νομιμότητα και η διαφάνεια της επεξεργασίας, οι διαφορετικοί ρόλοι των εμπλεκόμενων μερών, τα ζητήματα συγκατάθεσης και η άσκηση των δικαιωμάτων των χρηστών, ενώ στο τέλος, παρατίθενται κάποια τεχνικά μέτρα σε επίπεδο σχεδιασμού μίας εφαρμογής ή ενός λειτουργικού συστήματος για έξυπνα κινητά τηλέφωνα, με σκοπό τη διασφάλιση ενός υψηλού και αποδεκτού επιπέδου συμμόρφωσης των εμπλεκόμενων μερών με το κανονιστικό πλαίσιο στην Ευρώπη.

ABSTRACT

The subject of this master thesis is the protection of social media users' privacy in smartphone ecosystems. The growing need to safeguard the rights of smartphone users, whose daily life depends almost exclusively on the possibilities of communication and interaction offered by social media, constitutes the reason for researching this topic.

The master thesis is divided into three parts. The first Chapter analyzes the concept and the components of a smartphone ecosystem, including the different operating systems and applications developed there, as well as the life cycle of the data collected and being transferred by the parties involved. In addition, specific privacy issues observed in these ecosystems are presented, with particular emphasis on the different ways of collecting and processing personal data in each operating system. The second Chapter deals with social media, specifically with their characteristics, the personal data that can be collected from users, the data collection and processing methods, the "famous" terms of use and data protection policies. At the same time, this Chapter includes a theoretical analysis regarding the users' behaviour towards the processing of their personal data. The third Chapter analyzes specific legal issues related to the protection of social media users' privacy in smartphone ecosystems, such as - indicatively - the lawfulness and transparency of processing, the different stakeholders' roles, the consent issues and the users' rights. Finally, this Chapter presents some technical measures while designing an application or an operating system for smartphones, in order to ensure a high and acceptable level of compliance with the regulatory framework in Europe.

ΕΙΣΑΓΩΓΗ

Η άνοδος των μέσων κοινωνικής δικτύωσης έχει δημιουργήσει νέες συνήθειες και τρόπους επικοινωνίας των ανθρώπων, οι οποίοι στην εποχή της ραγδαίας τεχνολογικής εξέλιξης έχουν τη δυνατότητα να συνδεθούν με οποιονδήποτε επιθυμούν, όποτε το θελήσουν. Μέσω των έξυπνων κινητών τηλεφώνων, διευκολύνονται από τη μία οι κοινωνικές σχέσεις των ατόμων, πολλαπλασιάζονται από την άλλη οι ανησυχίες για τη νόμιμη και διαφανή επεξεργασία των προσωπικών δεδομένων των χρηστών.

Τα έξυπνα κινητά τηλέφωνα, ως συσκευές "always-on always-carried" αποτελούν συστατικό στοιχείο των οικοσυστημάτων έξυπνων κινητών, τα οποία περιλαμβάνουν εφαρμογές (applications), αλλά και πλήθος δεδομένων που υφίστανται επεξεργασία από διαφορετικά εμπλεκόμενα μέρη. Λόγω της πολυπλοκότητας των σχέσεων που δημιουργούνται σε αυτά τα οικοσυστήματα, ο έλεγχος των δεδομένων από τους ίδιους τους χρήστες είναι δυσχερής, έως και αδύνατος. Οι προκαθορισμένες ρυθμίσεις πρόσβασης των εφαρμογών στα δεδομένα των χρηστών και οι θολές ή δυσνόητες πολιτικές προστασίας δεδομένων, σε συνδυασμό με την έντονη επιθυμία για κοινωνικοποίηση, αποτρέπουν τον χρήστη από την άσκηση ελέγχου στα δεδομένα του. Παράλληλα, τα μέσα κοινωνικής δικτύωσης διαθέτουν την τεχνική ικανότητα να συλλέγουν τεράστιο όγκο δεδομένων του χρήστη, άμεσα ή έμμεσα, ρητά ή σιωπηρά, συγκρίνοντας επιμέρους πληροφορίες ή εξάγοντας συμπεράσματα από τις κινήσεις και τις προτιμήσεις του. Αν και οι χρήστες είναι ενήμεροι για τις παραπάνω επεμβατικές στην ιδιωτικότητά τους πρακτικές, και ίσως, κατ' αρχήν, να ανησυχούν, τείνουν τελικά είτε να αγνοούν τους κινδύνους είτε να τους αποδέχονται, με στόχο να απολαύσουν «ανενόχλητοι» τις ωφέλειες των μέσων κοινωνικής δικτύωσης. Η τυφλή αποδοχή των όρων χρήσης ή το ασυναίσθητο κλικ του κουμπιού δήλωσης συγκατάθεσης αποδεικνύει το παραπάνω γεγονός.

Παρ' όλη την αποδοχή του χρήστη, οι κίνδυνοι για την ιδιωτικότητά παραμένουν εμφανείς και παρόντες, σε μία χρονική στιγμή όπου όλο και περισσότερα μέρη επιθυμούν να εμπλακούν σε οικοσυστήματα έξυπνων κινητών που περιλαμβάνουν εφαρμογές μέσων κοινωνικής δικτύωσης, όπως διαφημιστές και άλλες συνδεδεμένες ιστοσελίδες. Στο σημείο αυτό εμφανίζονται εντονότερα τα ζητήματα νόμιμης διαβίβασης προσωπικών δεδομένων και κατάρτισης λεπτομερούς προφίλ, που αργότερα ενδέχεται να αξιοποιηθεί για προώθηση

προϊόντων ή για την εξαγωγή συμπερασμάτων σχετικά με τη ζωή και τις επιλογές ενός ανθρώπου.

Στην παρούσα εργασία, αφού αποσαφηνιστούν οι έννοιες του οικοσυστήματος έξυπνων κινητών τηλεφώνων και των μέσων κοινωνικής δικτύωσης, θα επιχειρηθεί η αποτύπωση των σημαντικότερων νομικών αλλά και τεχνικών ζητημάτων για την προστασία της ιδιωτικότητας των χρηστών, στοχεύοντας στην καλύτερη κατανόηση της φύσης και της θέσης των τεχνολογιών αυτών στον ψηφιακό αλλά και τον πραγματικό κόσμο.

ΚΕΦΑΛΑΙΟ 1Ο: ΟΙΚΟΣΥΣΤΗΜΑΤΑ ΕΞΥΠΝΩΝ ΚΙΝΗΤΩΝ ΤΗΛΕΦΩΝΩΝ (SMARTPHONE ECOSYSTEMS)

1.1. Τα οικοσυστήματα έξυπνων κινητών τηλεφώνων

1.1.1. Πρώτη προσέγγιση

Τα έξυπνα κινητά τηλέφωνα αποτελούν πλέον την καρδιά της καθημερινότητας του σύγχρονου ανθρώπου. Είναι ο προσωπικός του τηλεφωνικός κατάλογος, το ημερολόγιό του, η κύρια πηγή των πληροφοριών του, το εργαλείο με το οποίο συνδέεται με τους συναδέλφους του, τον προσωπικό του ιατρό ή τον καθηγητή του, καθώς και με τρίτους, φίλους ή αγνώστους, μέσω των δυνατοτήτων κοινωνικής δικτύωσης που παρέχει ένα τέτοιο τηλέφωνο.

Προκειμένου τα έξυπνα κινητά τηλέφωνα να παρέχουν αυτές τις υπηρεσίες, απαιτείται η εγκατάσταση εφαρμογών που θα παρέχουν τις παραπάνω δυνατότητες στον χρήστη. Οι εφαρμογές αυτές ("applications" ή "apps") αποτελούν μεμονωμένα λογισμικά, σχεδιασμένα να «τρέχουν» σε συγκεκριμένα περιβάλλοντα κινητών τηλεφώνων[1].

Επιπροσθέτως, για τη σωστή λειτουργία των έξυπνων κινητών τηλεφώνων είναι απαραίτητη η επεξεργασία δεδομένων. Απλά προσωπικά δεδομένα, προσωπικά δεδομένα ειδικών κατηγοριών (ή «ευαίσθητα» προσωπικά δεδομένα), αλλά και μη προσωπικά δεδομένα, αξιοποιούνται από τις εφαρμογές των κινητών για την παροχή των κατάλληλων υπηρεσιών. Σε αυτά περιλαμβάνονται δεδομένα όπως ονοματεπώνυμα και τηλεφωνικοί αριθμοί επαφών, μηνύματα SMS, δεδομένα θέσης, ακόμα και βιομετρικά δεδομένα όπως καρδιακοί παλμοί, χρόνοι οξυγόνωσης του αίματος, αναγνωριστικά προσώπου και δακτυλικά αποτυπώματα[2].

Το περιβάλλον λειτουργίας έξυπνων κινητών που περιλαμβάνει τα παραπάνω στοιχεία (συσκευή, λειτουργικό σύστημα, εφαρμογές και δεδομένα), χαρακτηρίζεται ως οικοσύστημα έξυπνων κινητών τηλεφώνων[3]. Ένα οικοσύστημα έξυπνων κινητών τηλεφώνων

---

[1] https://www.igi-global.com/dictionary/smartphone-application/47827 , https://www.techopedia.com/definition/2953/mobile-application-mobile-app

[2] Bujari A., Furini M., Mandreoli F., Martoglia R., Montangero M., and Ronzani D. (2018), "Standards, security and business models: Key challenges for the iot scenario", Mobile Networks and Applications, 23(1):147–154

[3] Χαρακτηριστικά οικοσυστ ήματα έξυπνων κινητών τηλεφώνων αποτελούν τα οικοσυστήματα της Apple και της Google.

αποτελείται από ετερογενή και συνεχώς εξελισσόμενα μέρη, που διασυνδέονται μέσω ενός σύνθετου, παγκόσμιου δικτύου σχέσεων[4]. Δεδομένου ότι είναι σχεδόν αδύνατο ένα μόνο τμήμα της αγοράς να προσφέρει όλες τις ζητούμενες υπηρεσίες στους τελικούς χρήστες, τα εν λόγω μέρη συνήθως προέρχονται από διαφορετικές αγορές[5]. Για την ακρίβεια, η δημιουργία και η προσφορά μίας υπηρεσίας στο οικοσύστημα απαιτεί προσεκτική ενορχήστρωση των συμμετεχόντων μερών, καθώς και συνεχή συνδημιουργία. Λόγου χάριν, είναι φανερό πως η αγορά των δικτύων κινητής τηλεφωνίας εξαρτάται από την συνεχή αναβάθμιση των κινητών τηλεφώνων, ενώ ολόκληρη η λειτουργία των έξυπνων κινητών τηλεφώνων βασίζεται στις εφαρμογές που αναπτύσσονται και εγκαθίστανται σε αυτά από τους χρήστες, όπως οι εφαρμογές των μέσων κοινωνικής δικτύωσης. Η αλληλεξάρτηση των μερών αποτελεί επομένως το ουσιαστικό χαρακτηριστικό του οικοσυστήματος, προκειμένου αυτό να αναβαθμίζεται και να ανταποκρίνεται στις μεταβαλλόμενες εσωτερικές και εξωτερικές επιρροές[6].

Σε αυτά τα οικοσυστήματα ωστόσο, όπου η επεξεργασία προσωπικών δεδομένων είναι κρίσιμη, η προστασία της ιδιωτικότητας των χρηστών αμφισβητείται εντόνως. Ενώ είναι εξαιρετικά εύκολο να συλλεγούν, να αποθηκευτούν και να διαβιβαστούν προσωπικά δεδομένα μεταξύ των εμπλεκόμενων μερών του οικοσυστήματος, είναι σχεδόν αδύνατος ο αποτελεσματικός έλεγχος των μερών που δύνανται να έχουν πρόσβαση σε αυτά. Η γνωστή πλέον υπόθεση "Cambridge Analytica[7]" ήταν αυτή που έκρουσε τον κώδωνα του κινδύνου σχετικά με τις πιθανές δυσμενείς συνέπειες της επεξεργασίας προσωπικών δεδομένων των χρηστών στα μέσα κοινωνικής δικτύωσης, υπογραμμίζοντας ότι, στην εποχή της ιλιγγιώδους ανάπτυξης καινοτόμων τεχνολογιών πληροφορικής και επικοινωνιών[8], η ιδιωτικότητα των ατόμων χρήζει αποτελεσματικής και διαρκούς προστασίας.

---

[4] Basole R. C., Russel M. G., Huhtamäki J. and Rubens N. (2012), "Understanding Mobile Ecosystem Dynamics: A Data-Driven Approach", 2012 International Conference on Mobile Business. 15., p.3, http://aisel.aisnet.org/icmb2012/15 (τελευταία πρόσβαση στις 19.12.2021)

[5]«Αγορά»: το σύνολο των επιχειρήσεων ή των δραστηριοτήτων αγοράς και πώλησης ενός συγκεκριμένου προϊόντος ή υπηρεσίας, https://dictionary.cambridge.org/dictionary/english/market (τελευταία πρόσβαση στις 19.12.2021)

[6] Βλ. υποσημείωση 4.

[7] Joris van Hoboken, Fathaigh R Ó (2021), "Smartphone platforms as privacy regulators", Computer Law and Security Review, Volume 41, July 2021, 105557, Elsevier Journal, p.2, https://doi.org/10.1016/j.clsr.2021.105557 (τελευταία πρόσβαση στις 05.01.2022)

[8] Furini M., Mirri S., Montangero M., and Prandi C. (2020), "Privacy Perception when using Smartphone Applications", Mobile Networks and Applications, 25(5):1-7, June 2020, p. 2, DOI: 10.1007/s11036-020-

1.1.2. Ο κύκλος ζωής των δεδομένων στα οικοσυστήματα έξυπνων κινητών τηλεφώνων

Προκειμένου να γίνει κατανοητή η μεγαλειώδης σημασία της προστασίας της ιδιωτικότητας των χρηστών στα οικοσυστήματα έξυπνων κινητών τηλεφώνων, χρειάζεται να εξεταστεί ο κύκλος ζωής των δεδομένων. Με τον τρόπο αυτό θα προσδιοριστεί η ροή των δεδομένων εντός των οικοσυστημάτων και, συνακόλουθα, θα εντοπιστούν οι ευπάθειες που εμφανίζονται για τα δικαιώματα και τις ελευθερίες των χρηστών.

Ο κύκλος ζωής των δεδομένων στα υπό εξέταση οικοσυστήματα ξεκινά από τη στιγμή της λήψης της πρώτης απόφασης σχετικά με τον τρόπο προσπέλασης των δεδομένων, πριν ακόμη αυτά δημιουργηθούν[9]. Στη φάση αυτή δίνεται έμφαση στον σχεδιασμό και την αρχιτεκτονική του οικοσυστήματος, στον τρόπο λειτουργίας του εκάστοτε λειτουργικού συστήματος, αλλά και στις μεθόδους συλλογής δεδομένων, αξιοποίησης και προστασίας τους. Εδώ εμπλέκονται οι κατασκευαστές των συσκευών, οι προγραμματιστές των λειτουργικών συστημάτων και των εφαρμογών, αλλά και οι υπεύθυνοι για την επιλογή του κατάλληλου επιχειρηματικού μοντέλου που θα υιοθετηθεί. Ακολουθεί η φάση της δημιουργίας των δεδομένων, κατά την οποία λαμβάνει χώρα η πρώτη αλληλεπίδραση με τον χρήστη του έξυπνου κινητού τηλεφώνου και συλλέγονται για πρώτη φορά τα δεδομένα του. Η πλειοψηφία εφαρμογών για κινητά τηλέφωνα εμφανίζει στον χρήστη κάποιο αναδυόμενο μήνυμα με το οποίο ζητάει την άδειά του για τη συλλογή των δεδομένων του[10], όπως δεδομένα θέσης ή αποθηκευμένες επαφές, ενώ άλλες εφαρμογές ενημερώνουν απλώς τον χρήστη ότι πρόκειται να συλλέξουν αυτά τα δεδομένα, χωρίς να του παρέχουν κάποια επιλογή ελέγχου[11],[12].

01529-z, (PDF) Privacy Perception when Using Smartphone Applications (researchgate.net) (τελευταία πρόσβαση στις 05.01.2022)

[9] Yerukhimovich A., Balebako R., Boustead A. E., Cunningham R. K., Welser IV W., Housley R., Shay R., Spensky Ch., Stanley K. D., Stewart J., Trachtenberg A., and Winkelman Z. (2016), "Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices", Santa Monica, CA: RAND Corporation, p.4, https://www.rand.org/pubs/research_reports/RR1393.html (τελευταία πρόσβαση στις 05.01.2022)

[10] Βλ. υποκεφάλαιο 1.3. της παρούσης

[11] Ajami R., Al Qirim N., and Ramadan N. (2012), "Privacy Issues in Mobile Social Networks", The 9th International Conference on Mobile Web Information Systems (MobiWIS), Procedia Computer Science, Volume 10, p. 673, https://www.researchgate.net/publication/257719381_Privacy_Issues_in_Mobile_Social_Networks (τελευταία πρόσβαση στις 22.12.2021)

[12] Στη φάση αυτή φαίνεται πως ανακύπτουν τα πρώτα ζητήματα νόμιμης λήψης συγκατάθεσης από τον χρήστη, καθώς και ερωτήματα σχετικά με τη δυνατότητα ελέγχου του χρήστη στα δεδομένα του.

Τα δεδομένα που συλλέγονται από τις εφαρμογές κινητών τηλεφώνων κινούνται συνεχώς και διαβιβάζονται συχνά σε τρίτα μέρη. Έτσι, στην επόμενη φάση της διαβίβασης, τα δεδομένα μεταφέρονται από τη συσκευή σε άλλες φυσικές ή διαδικτυακές τοποθεσίες προς αποθήκευση, ενώ παράλληλα μπορούν να κοινοποιηθούν σε άλλους χρήστες ή μέρη[13]. Η διαδικασία αυτή -η οποία θα έχει ήδη ληφθεί κατά την πρώτη φάση του κύκλου ζωής- πραγματοποιείται συνήθως μέσω ασύρματου δικτύου τηλεπικοινωνιών. Τα εμπλεκόμενα μέρη ενδέχεται να έχουν προβλέψει τεχνικά μέτρα ασφαλείας για την αποφυγή κακόβουλων επιθέσεων κατά τη διαβίβαση[14].

Μία από τις πιο σημαντικές φάσεις του κύκλου αυτού των δεδομένων, είναι η φάση της αποθήκευσης. Στο οικοσύστημα των έξυπνων κινητών τηλεφώνων, τα δεδομένα αποθηκεύονται συχνά απομακρυσμένα σε δίκτυα αποθήκευσης υπολογιστικού νέφους (Cloud-storage networks), τα οποία υποστηρίζουν οι αντίστοιχοι πάροχοι υπηρεσιών υπολογιστικού νέφους. Οι πάροχοι είναι πιθανό να λαμβάνουν αποφάσεις αναφορικά με τον τρόπο ταξινόμησης και διατήρησης των δεδομένων, την τοποθεσία τους εντός του νέφους, τον χρόνο διακράτησής τους και τις εξουσίες πρόσβασης τρίτων σε αυτά τα δεδομένα[15], γεγονός που εγείρει ερωτήματα σχετικά με τη νομιμότητα αλλά και τη διαφάνεια της επεξεργασίας αυτών των δεδομένων. Ταυτόχρονα, ενδέχεται να αποθηκεύονται και στη συσκευή του χρήστη. Ακόμα και σε αυτή την περίπτωση, κάποια στιγμή, τα δεδομένα που έχουν αποθηκευτεί τοπικά, θα μεταδοθούν σε κάποιο μεγαλύτερο δίκτυο ή σύστημα με σκοπό την αναβάθμιση του επιπέδου των υπηρεσιών που παρέχονται από την εκάστοτε εφαρμογή[16].

---

[13] Yerukhimovich A., Balebako R., Boustead A. E., Cunningham R. K., Welser IV W., Housley R., Shay R., Spensky Ch., Stanley K. D., Stewart J., Trachtenberg A., and Winkelman Z. (2016), "Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices", Santa Monica, CA: RAND Corporation, p.4, https://www.rand.org/pubs/research_reports/RR1393.html (τελευταία πρόσβαση στις 05.01.2022)

[14] Όπως η επίθεση γνωστή ως "man-in-the-middle", μέσω της οποίας οι εισβολείς αναμεταδίδουν κρυφά πληροφορίες μεταξύ της συσκευής και του προορισμού διαβίβασης των δεδομένων, υποκλέπτοντας τελικά τα δεδομένα του εκάστοτε χρήστη.

[15] Βλ. υποσημείωση 13.

[16] Ajami R., Al Qirim N., and Ramadan N. (2012), "Privacy Issues in Mobile Social Networks", The 9th International Conference on Mobile Web Information Systems (MobiWIS), Procedia Computer Science, Volume 10, p. 673, https://www.researchgate.net/publication/257719381_Privacy_Issues_in_Mobile_Social_Networks (τελευταία πρόσβαση στις 22.12.2021)

Τα δεδομένα τέλος εισέρχονται στη φάση της αξιοποίησής τους. Ειδικότερα, τα δεδομένα δύναται να αναλυθούν και να χρησιμοποιηθούν, τόσο για τους σκοπούς για τους οποίους συλλέχθηκαν αρχικά όσο και για διαφορετικούς, μετά την σύντηξή τους με άλλα διαθέσιμα δεδομένα. Η αξιοποίηση αυτή περιλαμβάνει την πρόσβαση από προγραμματιστές εφαρμογών που αναλύουν τα δεδομένα για να κατανοήσουν πώς χρησιμοποιούνται ή την πρόσβαση τρίτων διαφημιστών που συλλέγουν μεμονωμένα ή πολλαπλά σύνολα δεδομένων για να καθορίσουν τις διαφημίσεις που θα προβάλλονται σε ένα συγκεκριμένο κινητό τηλέφωνο[17].

Γίνεται επομένως φανερό πως, σε κάθε μία από τις ως άνω φάσεις ροής των δεδομένων, ανακύπτουν ένα ή περισσότερα ερωτήματα που αφορούν την προστασία της ιδιωτικότητας των χρηστών έξυπνων κινητών τηλεφώνων, υπογραμμίζοντας ότι το δικαίωμα στην ιδιωτικότητα μπορεί να παραβιαστεί με ποικίλους τρόπους ανά πάσα στιγμή, ακόμα και πριν από την ουσιαστική συλλογή των δεδομένων του χρήστη.

1.2. Ιδιωτικότητα στα οικοσυστήματα έξυπνων κινητών τηλεφώνων

1.2.1. Συλλογή προσωπικών δεδομένων

Τα τελευταία χρόνια, οι εφαρμογές έξυπνων κινητών τηλεφώνων (εφεξής αναφερόμενες απλά ως «εφαρμογές») έχουν εισέλθει σε μία εντυπωσιακή τροχιά ανάπτυξης. Λειτουργώντας ακατάπαυστα στο έξυπνο κινητό του χρήστη και αναβαθμιζόμενες συνεχώς από τους προγραμματιστές τους, επιτρέπουν τη συλλογή, αποθήκευση και μετάδοση προσωπικών δεδομένων σε πραγματικό χρόνο σε τρίτους, όπως διαφημιστές ή άλλα μέρη του οικοσυστήματος -πολλές φορές εν αγνοία του χρήστη- καταδεικνύοντας την πραγματικά επεμβατική τους φύση.

Στο σημείο αυτό, σκόπιμο είναι να εξειδικευτεί η έννοια του χρήστη ενός έξυπνου κινητού τηλεφώνου. Στην παρούσα εργασία, νοείται ως ο τελικός χρήστης της κινητής συσκευής, ο οποίος δύναται να χρησιμοποιήσει μια εφαρμογή, χωρίς ωστόσο να είναι απαραίτητα και «πελάτης» αυτής[18]. Δεν ενδιαφέρει δηλαδή εάν τελικά θα αποφασίσει να προχωρήσει στην

[17] Yerukhimovich A., Balebako R., Boustead A. E., Cunningham R. K., Welser IV W., Housley R., Shay R., Spensky Ch., Stanley K. D., Stewart J., Trachtenberg A., and Winkelman Z. (2016), "Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices", Santa Monica, CA: RAND Corporation, p.4, https://www.rand.org/pubs/research_reports/RR1393.html (τελευταία πρόσβαση στις 05.01.2022)

[18] GSMA Association (2017), "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications", GSMA Report, p.32 https://aiforimpacttoolkit.gsma.com/resources/GSMA-

πραγματική αξιοποίηση των δυνατοτήτων της εφαρμογής, παρέχοντας παράλληλα τα στοιχεία του, αλλά αρκεί η απλή εγκατάσταση της εφαρμογής στη συσκευή του.

Ακριβώς επειδή τα έξυπνα κινητά τηλέφωνα διαθέτουν από προεπιλογή εγκατεστημένες ποικίλες εφαρμογές, όπως προγράμματα περιήγησης ιστού (web browsers) και προγράμματα ηλεκτρονικού ταχυδρομείου (email), άλμπουμ φωτογραφιών, παιχνίδια, ημερολόγια και λίστες επαφών, υπάρχει πλέον η δυνατότητα συλλογής πολύ περισσότερων προσωπικών δεδομένων από ό,τι ήταν προηγουμένως εφικτό με τη συμβατική χρήση προσωπικών υπολογιστών ή απλών κινητών τηλεφώνων[19]. Για παράδειγμα, προσωπικά δεδομένα όπως η ταυτότητα του χρήστη, το επερχόμενο πρόγραμμά του, η ώρα που ξοδεύει σε διαφορετικές εφαρμογές, καθώς και οι διαφορετικές τοποθεσίες που επισκέπτεται συλλέγονται και καταγράφονται αυτόματα από τις εφαρμογές.

Διακρίνονται έτσι διαφορετικοί τρόποι συλλογής προσωπικών δεδομένων από τα έξυπνα κινητά τηλέφωνα. Αρχικά, τα δεδομένα μπορεί να συλλέγονται άμεσα, εισαγόμενα από τον ίδιο τον χρήστη μέσω της εφαρμογής, περιλαμβάνοντας όνομα, διεύθυνση, αριθμό τηλεφώνου, διεύθυνση email, φύλο, ακόμα και στοιχεία πιστωτικής κάρτας. Έπειτα, δεδομένα όπως η διεύθυνση IP, δεδομένα θέσης, IMEI[20], μοναδικό αναγνωριστικό τηλεφώνου, ενδέχεται να συλλέγονται έμμεσα, χωρίς να τα έχει καταχωρήσει ο χρήστης. Δεδομένα επίσης μπορεί να εξάγονται από την τυποποιημένη ή συνηθισμένη συμπεριφορά του χρήστη του κινητού τηλεφώνου. Για παράδειγμα, μέσω του δέκτη GPS της συσκευής είναι δυνατό να εξαχθούν πληροφορίες σχετικά με τις πρόσφατες τοποθεσίες που επισκέφτηκε ο χρήστης, ενώ εύκολα μπορούν επίσης να καταγραφούν οι επισκέψεις του σε ιστοσελίδες ή άλλες εφαρμογές[21]. Τέλος, συχνά δημιουργούνται νέα δεδομένα από τη χρήση ενός έξυπνου

report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf (τελευταία πρόσβαση στις 22.12.2021)

[19] Xu H., Gupta S., Rosson M. B., and Carroll J. M. (2012), "Measuring Mobile Users' Concerns For Information Privacy", Completed Research Paper, Thirty Third International Conference on Information Systems, Orlando 2012, Published in ICIS, p. 4, https://www.semanticscholar.org/paper/Measuring-Mobile-Users%27-Concerns-for-Information-Xu-Gupta/8ae62044520374dda95952e98204214fb999fcda (τελευταία πρόσβαση στις 20.12.2021)

[20] International Mobile Equipment Identity (IMEI): Πρόκειται για μοναδικό αναγνωριστικό κωδικό αριθμό που είναι ενσωματωμένος στις κινητές συσκευές, ο οποίος αποτελείται από 15 αριθμούς και περιλαμβάνει πληροφορίες για τον κατασκευαστή και το μοντέλο της κινητής συσκευής.

[21] GSMA Association (2017), "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications", GSMA Report, p.32 https://aiforimpacttoolkit.gsma.com/resources/GSMA-report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf (τελευταία πρόσβαση στις 22.12.2021)

κινητού τηλεφώνου, τα οποία τηρούνται είτε τοπικά στη συσκευή του χρήστη είτε σε δίκτυα υπολογιστικού νέφους του κατασκευαστή της συσκευής. Τέτοιου είδους προσωπικά δεδομένα αποτελούν τα αρχεία καταγραφής κλήσεων και τα γραπτά μηνύματα, οι φωτογραφίες που δημιουργούνται από τον χρήστη, οι λίστες επαφών ή τα βιβλία διευθύνσεων, ακόμα και τα διαπιστευτήρια ασφαλείας, όπως οι κωδικοί πρόσβασης σε εφαρμογές και ιστοσελίδες. Γίνεται έτσι σαφές ότι τα έξυπνα κινητά τηλέφωνα είναι πιθανότερο να παραβιάζουν την ιδιωτικότητα των χρηστών τους, σε σχέση με άλλες ψηφιακές συσκευές[22].

1.2.2. Δεδομένα θέσης

Φυσικά, οποιοδήποτε έξυπνο κινητό τηλέφωνο συλλέγει δεδομένα θέσης, αφού πρωτίστως αυτά αξιοποιούνται από τους παρόχους για να ταυτοποιήσουν τους χρήστες και να τους προσφέρουν τις απαραίτητες υπηρεσίες, να διευκολύνουν την κινητικότητα του δικτύου αλλά και τη γρήγορη εύρεση της συσκευής όταν δέχεται μία κλήση ή ένα SMS[23]. Συχνά ωστόσο, η συλλογή των δεδομένων θέσης δεν πραγματοποιείται μόνο για τους παραπάνω σκοπούς, αλλά και για τη σύνδεση του χρήστη με κάποιον κοντινό φίλο του ή την κατάρτιση εξατομικευμένου προφίλ χρήστη αναφορικά με τις τοποθεσίες που έχει επισκεφτεί ή τις προτιμήσεις του σε μία συγκεκριμένη γεωγραφική περιοχή. Οι Michael και Michael επισημαίνουν ότι μια γενική παρακολούθηση τοποθεσίας σε όλο τον χρόνο και τον χώρο έχει ωθήσει τους ανθρώπους να ζούνε σε μία κατάσταση «υπερεπιτήρησης», στην οποία η επιτήρηση είναι συνεχόμενη, ενώ τα φυσικά πρόσωπα και τα αντικείμενα μπορούν να εντοπιστούν και να ταυτοποιηθούν αυτόματα[24].Ένα λοιπόν από τα ακανθώδη θέματα που προκύπτουν από τη χρήση έξυπνων κινητών τηλεφώνων αφορά τη νόμιμη συλλογή των δεδομένων αυτών από τα διαφορετικά μέρη του οικοσυστήματος, την πιθανή διαβίβασή τους σε τρίτα μέρη, αλλά και την άγνοια συλλογής τους από τον χρήστη.

---

[22] Tang J., Zhang B., and Akram U. (2021), "What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management", Information 2021, 12, 311, p. 2, https://doi.org/10.3390/info12080311 (τελευταία πρόσβαση στις 20.12.2021)

[23] Schmitt P., Raghavan B. (2020), "Pretty Good Phone Privacy", p. 3, https://www.researchgate.net/publication/344334346_Pretty_Good_Phone_Privacy (τελευταία πρόσβαση στις 20.12.2021)

[24] Michael M.G. and Michael K. (2010), "Toward a State of Uberveillance", 29(2), IEEE Technology and Society Magazine, p.9, https://www.researchgate.net/publication/224142358_Toward_a_State_of_Uberveillance_Special_Section_Introduction (τελευταία πρόσβαση στις 26.12.2021).

Με τον όρο «δεδομένα θέσης» περιγράφεται οποιοσδήποτε τύπος δεδομένων τοποθετεί ένα φυσικό πρόσωπο είτε σε μία συγκεκριμένη τοποθεσία, μία δεδομένη χρονική στιγμή, είτε σε μία σειρά τοποθεσιών με την πάροδο του χρόνου[25]. Σε αυτά περιλαμβάνεται το γεωγραφικό πλάτος, μήκος και υψόμετρο μίας τοποθεσίας, μέσω της οποίας, σε συνδυασμό με το στοιχείο του χρόνου, μπορεί να εντοπιστεί και στη συνέχεια να ταυτοποιηθεί ένα φυσικό πρόσωπο[26].

Ο εντοπισμός του προσώπου μπορεί να είναι είτε άμεσος είτε έμμεσος[27]. Στην πρώτη περίπτωση, ο εντοπισμός είναι αποτέλεσμα της γεωγραφικής αποκάλυψης της θέσης του έξυπνου κινητού τηλεφώνου, με την αξιοποίηση τεχνολογιών που διαθέτει ήδη το τηλέφωνο, όπως ο δέκτης GPS που χρησιμοποιούν οι διάφορες εγκατεστημένες εφαρμογές στο κινητό τηλέφωνο του χρήστη. Από την άλλη, ο έμμεσος εντοπισμός της τοποθεσίας αναφέρεται στην αποκάλυψη της τοποθεσίας του από το ίδιο το πρόσωπο που χρησιμοποιεί το έξυπνο κινητό του τηλέφωνο, αποκαλύπτοντας -εν γνώσει του- την τοποθεσία του[28].

Δέον επιπλέον να σημειωθεί ότι, συλλέγοντας δεδομένα θέσης, οι προγραμματιστές εφαρμογών ή τα υπόλοιπα μέρη του οικοσυστήματος είναι σε θέση να συνάγουν, εκτός από την τοποθεσία του φυσικού προσώπου, πλήθος άλλων προσωπικών δεδομένων, όπως θρησκευτικές, πολιτικές ή σεξουαλικές πεποιθήσεις. Έτσι, είναι σημαντική η διάκριση των δεδομένων θέσης που συλλέγονται σε ανώνυμα δεδομένα, τα οποία δεν δύνανται σε καμία περίπτωση να ταυτοποιήσουν ένα πρόσωπο, και σε προσωπικά δεδομένα (είτε απλά είτε δεδομένα ειδικών κατηγοριών). Εάν για παράδειγμα ένα άτομο επισκέπτεται κάθε Κυριακή την εκκλησία της γειτονιάς του, μπορούν να συναχθούν εύκολα συμπεράσματα σχετικά με τη θρησκεία του, με αποτέλεσμα μία απλή τοποθεσία να αποτελεί πλέον προσωπικό δεδομένο ειδικής κατηγορίας, αφού αποκαλύπτει εξαιρετικά ευαίσθητες πληροφορίες για

---

[25] Scassa T. (2009) "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", Canadian Journal of Law and Technology, Volume 7, Article 7, p.193, https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1106&context=cjlt (τελευταία πρόσβαση στις 26.12.2021)

[26] Cheung Anne S.Y. (2014), "Location privacy: The challenges of mobile service devices", Computer Law and Security Review, Volume 30, 2014, Elsevier Journal, 41-54, p. 43, https://doi.org/10.1016/j.clsr.2013.11.005 (τελευταία πρόσβαση στις 26.12.2021)

[27] Παράσχης Σπ. (2012), «Κοινωνικά Δίκτυα μέσω φορητών συσκευών: Η προστασία της θέσης», Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς, σελ. 8, διαθέσιμη στο https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4926/Paraschis.pdf?sequence=2&isAllowed=y

[28] Ο έμμεσος εντοπισμός τοποθεσίας αφορά κατά κύριο λόγο τη συλλογή προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης, τα ειδικότερα ζητήματα των οποίων εξετάζονται στο Κεφάλαιο 3ο της παρούσης.

ένα πρόσωπο[29]. Άλλωστε, στο άρθρο 4 περ. 1 του ΓΚΠΔ[30], τα δεδομένα θέσης αναφέρονται ρητά ως στοιχείο βάσει του οποίου ένα πρόσωπο μπορεί να ταυτοποιηθεί άμεσα ή έμμεσα.

Η έννοια ωστόσο της προστασίας των δεδομένων θέσης που συλλέγονται ακατάπαυστα από τα έξυπνα κινητά τηλέφωνα δεν αναφέρεται στην απόκρυψη πληροφοριών ή στην παύση συλλογής τους[31], αλλά στην προστασία των ατόμων από τη χρήση των δεδομένων τους για εμπορικούς ή άλλους σκοπούς, καθώς και στην προστασία από μη εξουσιοδοτημένη συλλογή, διατήρηση ή διαβίβαση σε τρίτα μέρη εντός ή εκτός ενός οικοσυστήματος έξυπνων κινητών τηλεφώνων.

1.2.3. Ενημέρωση του χρήστη

Τα προσωπικά δεδομένα που συλλέγονται από τις εφαρμογές είναι πολύτιμα για τα μέρη του οικοσυστήματος, παρουσιάζοντας ιδιαίτερη οικονομική και εμπορική σημασία[32]. Ωστόσο, οι χρήστες συχνά δεν είναι σε θέση να εκτιμήσουν την αξία ή την ποιότητα των προσωπικών δεδομένων που αποκαλύπτουν μέσω των εφαρμογών[33], ούτε και τους λόγους για τους οποίους παρέχουν τα δεδομένα τους. Καθώς οι πληροφορίες αυτές συνήθως κρύβονται πίσω από ασαφή έγγραφα Πολιτικών Προστασίας Απορρήτου Δεδομένων, αποτελούμενα από κείμενα μακροσκελή και δυσανάγνωστα, με πληθώρα νομικών όρων και ορισμών που τροποποιούνται συνεχώς[34], οι χρήστες καταλήγουν να αγνοούν σε μεγάλο

[29] Bu-Pasha, S., Alen-Savikko, A., Makinen, J., Guinness, R., & Korpisaari, P. (2016), "Eu law perspectives on location data privacy in smartphones and informed consent for transparency", European Data Protection Law Review (EDPL), 2(3), p. 314

[30] Γενικός Κανονισμός για την Προστασία των Δεδομένων [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]

[31] Bu-Pasha, S., Alen-Savikko, A., Makinen, J., Guinness, R., & Korpisaari, P. (2016), "Eu law perspectives on location data privacy in smartphones and informed consent for transparency", European Data Protection Law Review (EDPL), 2(3), p. 312.

[32] Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015) "Privacy and human behavior in the age of information," Science (New York, N.Y.) (347:6221), pp. 509–514.

[33] Buck Ch., Burster S., and Eymann T. (2017) "Priming app information privacy concerns in mobile ecosystems", Working Paper on Information Systems, No. 63, University of Bayreuth, Chair of Information Systems, p.1, http://nbn-resolving.de/urn:nbn:de:bvb:703-epub-3419-8 (τελευταία πρόσβαση στις 27.12.2021)

[34] Chrysakis et al. (2020) "Evaluating the data privacy of mobile applications through crowdsourcing", Legal Knowledge and Information Systems, Project: CAP-A: A Community-driven Approach to Privacy Awareness, p.1, https://www.researchgate.net/publication/347320509_Evaluating_the_Data_Privacy_of_Mobile_Applications_Through_Crowdsourcing (τελευταία πρόσβαση στις 27.12.2021)

βαθμό τις ποικίλες χρήσεις των δεδομένων τους αλλά και τις συνέπειες τυχόν παράνομης ή μη εξουσιοδοτημένης επεξεργασίας των προσωπικών τους δεδομένων.

Επομένως, ένα από τα βήματα για την προστασία της ιδιωτικότητας αποτελεί η γνώση των χρηστών αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων, κάτι που ωστόσο αποτελεί πρόκληση. Κατ' αρχάς, οι χρήστες έχουν διαφορετικές συνήθειες και αντίληψη όσον αφορά την ιδιωτικότητα. Για παράδειγμα, η Αλίκη μπορεί να θεωρεί τη λίστα επαφών της σημαντικότερη σε σύγκριση με την τοποθεσία της, εν αντιθέσει με τον Μπομπ, ο οποίος δίνει μεγαλύτερη σημασία στην προστασία της τοποθεσίας του[35]. Επιπροσθέτως, οι χρήστες έχουν φτάσει στο σημείο να προσπερνούν ασυναίσθητα τα κείμενα των Πολιτικών Προστασίας των εφαρμογών και να πατούν «από συνήθεια» το περίφημο κουμπί «Συμφωνώ/I agree», χωρίς να συνειδητοποιούν τους πιθανούς κινδύνους που λανθάνουν πίσω από την παροχή των προσωπικών τους δεδομένων στις εφαρμογές[36]. Άλλωστε, το πάτημα ενός κουμπιού ή η αποδοχή ενός προσυμπληρωμένου τετραγωνιδίου (pre-ticked box) είναι ιδιαιτέρως ελκυστικά για τον χρήστη, αφού επισπεύδεται η διαδικασία εγκατάστασης και αξιοποίησης της εφαρμογής που επιθυμεί. Ωστόσο, σε αυτές τις περιπτώσεις, η συγκατάθεση που παρέχεται από τους χρήστες αξιολογείται ως θολή και μη ενημερωμένη, κατά παράβαση των απαιτήσεων του ευρωπαϊκού κανονιστικού πλαισίου[37], αφού τοιουτοτρόπως παρέχεται η δυνατότητα στις εταιρείες πίσω από τις εφαρμογές να συμπεριλάβουν στην Πολιτική Προστασίας τους όρους παραβιαστικούς για την ιδιωτικότητα. Έτσι, η εκάστοτε εφαρμογή διαθέτει πλέον την εξουσιοδότηση του χρήστη για τη συλλογή δεδομένων θέσης ή την παρακολούθηση των συνηθειών του, την πρόσβαση στα αρχεία του κινητού του τηλεφώνου, ενδεχομένως και τη διαβίβαση αυτών των δεδομένων

[35] Furini M., Mirri S., Montangero M., and Prandi C. (2020), "Privacy Perception when using Smartphone Applications", Mobile Networks and Applications, 25(5):1-7, June 2020, p. 4, DOI: 10.1007/s11036-020-01529-z, (PDF) Privacy Perception when Using Smartphone Applications (researchgate.net) (τελευταία πρόσβαση στις 05.01.2022)

[36] Lin J., Amini S., Hong J. I., Sadeh N., Lindqvist J., and Zhang J. (2012), "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing", ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 501–510, 10.1145/2370216.2370290 (τελευταία πρόσβαση στις 06.01.2022)

[37] Άρθρο 4 περ. 11' ΓΚΠΔ *«συγκατάθεση του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»*

σε τρίτα μέρη εντός ή εκτός του οικοσυστήματος του έξυπνου κινητού τηλεφώνου που διαθέτει ο χρήστης, συχνά χωρίς ο τελευταίος να το γνωρίζει πραγματικά[38].

1.3. Τεχνικά χαρακτηριστικά για τη συλλογή δεδομένων χρηστών μέσω εφαρμογών έξυπνων κινητών τηλεφώνων

Δύο από τα βασικότερα οικοσυστήματα έξυπνων κινητών τηλεφώνων είναι αυτά των εταιρειών Google και Apple. Δεδομένου ότι στο κάθε οικοσύστημα ο αριθμός των εμπλεκόμενων μερών και των εφαρμογών που λειτουργούν είναι τεράστιος, οι εταιρείες αυτές έχουν αναπτύξει συγκεκριμένους τεχνικούς μηχανισμούς προκειμένου να θέσουν όρους αναφορικά με τα δεδομένα στα οποία μπορούν να έχουν πρόσβαση οι εκάστοτε εφαρμογές[39] και τον τρόπο λήψης της αντίστοιχης εξουσιοδότησης από τον χρήστη.

Η έννοια της εξουσιοδότησης των εφαρμογών στα κινητά τηλέφωνα[40] -η οποία, όπως υπογραμμίστηκε ως άνω, αποτελεί την προϋπόθεση για την εγκατάσταση και την ορθή λειτουργία της εφαρμογής σε ένα έξυπνο κινητό- αναφέρεται στη διαδικασία με την οποία οι χρήστες παρέχουν στις εφαρμογές την άδεια πρόσβασης στα προσωπικά τους δεδομένα, με αντάλλαγμα την παροχή εξειδικευμένων λειτουργιών[41] εντός του οικοσυστήματος έξυπνου κινητού τηλεφώνου που διαθέτουν. Με τον τρόπο αυτό, τα έξυπνα κινητά τηλέφωνα μπορούν να αποκτήσουν πρόσβαση σε πληθώρα προσωπικών δεδομένων του χρήστη τους, είτε μέσω δεκτών GPS, αισθητήρων Bluetooth και μικροφώνων, είτε μέσω απευθείας πρόσβασης στα δεδομένα που ο χρήστης αποθηκεύει τοπικά στο τηλέφωνό του.

---

[38] Όπως στην περίπτωση της εφαρμογής Flashlight, όπου, αν και η κύρια λειτουργία της εφαρμογής ήταν το άνοιγμα του φακού του κινητού τηλεφώνου, μια εις βάθος ανάλυση διαπίστωσε ότι η εφαρμογή είχε πρόσβαση στον αριθμό τηλεφώνου, στο αναγνωριστικό της συσκευής και στην ακριβή τοποθεσία του χρήστη. Επιπλέον, η εφαρμογή είχε τη δυνατότητα να ελέγξει και να διαμορφώσει τα εργαλεία του λογισμικού του κινητού, αλλάζοντας μέχρι και τις ρυθμίσεις οθόνης. Shklovskii. I., Mainwaring S. D., Skúladóttir H. H., and Borgthorsson H. (2014), "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use", ACM Conference on Human Factors in Computing Systems, pages 2347–2356, https://doi.org/10.1145/2556288.2557421 (τελευταία πρόσβαση στις 06.01.2022)

[39] Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T. and Shadbolt N. (2018), "Third Party Tracking in the Mobile Ecosystem", p. 2, https://www.researchgate.net/publication/326138940_Third_Party_Tracking_in_the_Mobile_Ecosystem (τελευταία πρόσβαση στις 05.01.2022)

[40] "Mobile Application Authorization"

[41] Roesner F., Kohno T., Moshchuk, A., Parno B., Wang, H.J., and Cowan C. (2012), "User-driven access control: Rethinking permission granting in modern operating systems", Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012, pp. 224–238, https://www.microsoft.com/en-us/research/publication/user-driven-access-control-rethinking-permission-granting-in-modern-operating-systems-2/ (τελευταία πρόσβαση στις 06.01.2022)

Έτσι, κατά κύριο λόγο, τα λειτουργικά συστήματα για έξυπνα κινητά τηλέφωνα όπως το Android της Google και το iOS της Apple, χρησιμοποιούν ένα τεχνικό μηχανισμό που ονομάζεται «αρχιτεκτονική αδειών» με σκοπό την πρόσβαση των επιμέρους εφαρμογών στις λειτουργίες των συσκευών, αλλά και στα δεδομένα που βρίσκονται εκεί αποθηκευμένα[42].

Το λειτουργικό Android χρησιμοποιεί άδειες που διακρίνονται σε κανονικές και επικίνδυνες[43]. Οι κανονικές άδειες ("normal permissions") περιλαμβάνουν πρόσβαση σε προσωπικά δεδομένα ή λειτουργίες της συσκευής που ενέχουν μικρό κίνδυνο για την ιδιωτικότητα των χρηστών, όπως ο ορισμός της ζώνης ώρας της συσκευής. Το λειτουργικό Android, μάλιστα, εκχωρεί αυτόματα στις εφαρμογές τέτοιες άδειες κατά την εγκατάσταση[44]. Από την άλλη, οι επικίνδυνες άδειες ("dangerous or runtime permissions") είναι εκείνες που ενέχουν υψηλότερο κίνδυνο για την ιδιωτικότητα των χρηστών ή τη λειτουργία άλλων εφαρμογών, αφού όχι μόνο παρέχουν πρόσβαση σε δεδομένα επαφών, δεδομένα θέσης και φωτογραφίες, αλλά μπορούν να ελέγξουν την κάμερα και το μικρόφωνο της συσκευής[45]. Οι εφαρμογές αποκτούν πρόσβαση στα παραπάνω δεδομένα μόνο όταν ο χρήστης το επιτρέπει, μέσω των μηχανισμών που είναι ενσωματωμένοι στην αρχιτεκτονική αδειών[46].

Ομοίως, το λειτουργικό σύστημα της Apple, iOS, έχει αναπτύξει δύο διαφορετικές άδειες. Οι πρώτες, που ονομάζονται «δικαιώματα» ("entitlements"), παρέχουν στις εφαρμογές συγκεκριμένα προνόμια και δυνατότητες, όπως η αποστολή ειδοποιήσεων push[47] στον χρήστη, ενώ οι δεύτερες χαρακτηρίζονται απλώς ως άδειες ("permissions") και επιτρέπουν την πρόσβαση σε ορισμένα προσωπικά δεδομένα του χρήστη, όπως τοποθεσία, ημερολόγιο, στοιχεία επικοινωνίας ή φωτογραφίες[48]. Έτσι, κάθε φορά που εκτελείται μία εφαρμογή και

---

[42] European Union Agency for Network and Information Security "ENISA" (2017) "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", p. 42-46, https://pure.uva.nl/ws/files/42887337/22302384.pdf (τελευταία πρόσβαση στις 06.01.2022)

[43] https://developer.android.com/guide/topics/permissions/overview

[44] Joris van Hoboken, Fathaigh R Ó (2021), "Smartphone platforms as privacy regulators", Computer Law and Security Review, Volume 41, July 2021, 105557, Elsevier Journal, p.9, https://doi.org/10.1016/j.clsr.2021.105557 (τελευταία πρόσβαση στις 05.01.2022)

[45] Βλ. υποσημείωση 41.

[46] Βλ. υποσημείωση 42

[47] Οι ειδοποιήσεις push ("Web Push Notifications") ενημερώνουν τον χρήστη για κάποια εισερχόμενη κλήση βίντεο ή ήχου ή κάποιο άμεσο μήνυμα ή ειδοποίηση, όταν μία εφαρμογή δεν χρησιμοποιείται συχνά από τον χρήστη.

[48] https://developer.apple.com/documentation/bundleresources/entitlements

απαιτείται κάποια άδεια, ζητείται η έγκριση από τον χρήστη, ο οποίος μπορεί είτε να την παράσχει είτε να την αρνηθεί.

Κρίσιμα ζητήματα, ωστόσο, αναφύονται όσον αφορά την αρχιτεκτονική αδειών των παραπάνω λειτουργικών συστημάτων, πιο συγκεκριμένα στις περιπτώσεις όπου οι διάφορες εφαρμογές αιτούνται άδεια πρόσβασης σε προσωπικά δεδομένα που δεν είναι απαραίτητα για την επίτευξη της βασικής τους λειτουργικότητας[49,50]. Το ζήτημα αυτό επιδιώκουν να μετριάσουν οι εταιρείες[51] με την υποχρεωτική ύπαρξη Πολιτικών Προστασίας Δεδομένων σε κάθε εφαρμογή που εισέρχεται στο οικοσύστημά τους, οι οποίες θα περιγράφουν αναλυτικά όλα τα δεδομένα που συλλέγονται -προσωπικού χαρακτήρα ή μη- και θα είναι εύκολα προσβάσιμες από τον χρήστη. Παρ' όλα αυτά, αναπάντητο παραμένει το ερώτημα εάν τα όσα περιγράφονται στις πολιτικές αυτές, απεικονίζουν επακριβώς τα πραγματικά δεδομένα που συλλέγουν οι εφαρμογές.

ΚΕΦΑΛΑΙΟ 2ο: ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

2.1. Εισαγωγικές Έννοιες

Τα μέσα κοινωνικής δικτύωσης αποτελούν μία από τις πιο σημαντικές δραστηριότητες των χρηστών του διαδικτύου, αφού έχουν την «ικανότητα» να επηρεάζουν την καθημερινότητα, τις συνήθειες και τις απόψεις τους. Μέσα κοινωνικής δικτύωσης όπως το Facebook και το Instagram, το YouTube και το Twitter, διαδίδονται και εξελίσσονται με εκρηκτικούς ρυθμούς, προσφέροντας καινοτόμους τρόπους επικοινωνίας, αλληλεπίδρασης και καθημερινής κοινωνικοποίησης.

Το επίπεδο συνδεσιμότητας των χρηστών των μέσων κοινωνικής δικτύωσης έχει αυξηθεί εξαιρετικά τα τελευταία χρόνια, με πάνω από τέσσερα δισεκατομμύρια ανθρώπους να χρησιμοποιούν ένα ή περισσότερα μέσα κοινωνικής δικτύωσης στην καθημερινότητά τους. Σύμφωνα με τα δεδομένα που δημοσίευσε για το 2021 η Εταιρεία Statista, οι ενεργοί χρήστες

---

[49] Ενδεχόμενη παραβίαση της αρχής της ελαχιστοποίησης των δεδομένων, άρθρο 5 περ. γ' ΓΚΠΔ *(«Τα δεδομένα προσωπικού χαρακτήρα είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία»)*

[50] European Union Agency for Network and Information Security "ENISA" (2017) "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", p. 43, https://pure.uva.nl/ws/files/42887337/22302384.pdf (τελευταία πρόσβαση στις 06.01.2022)

[51] https://developer.apple.com/news/?id=08312018a, https://play.google.com/about/developer-content-policy/

του διαδικτύου ανέρχονται στα 4,6 δισεκατομμύρια, ενώ από αυτούς, τα 4,2 δισεκατομμύρια χρησιμοποιούν έστω ένα μέσο κοινωνικής δικτύωσης. Παράλληλα, οι ενεργοί χρήστες των μέσων κοινωνικής δικτύωσης μέσω έξυπνων κινητών τηλεφώνων αγγίζουν τα 4,15 δισεκατομμύρια[52]. Το Facebook -το οποίο πρόσφατα μετονομάστηκε σε "Meta"- σύμφωνα με τα στατιστικά στοιχεία του 2021 αποτελεί το δημοφιλέστερο μέσο κοινωνικής δικτύωσης βάσει του παγκόσμιου μεγέθους κοινού[53]. Λαμβάνοντας υπόψιν ότι το 2021 υπάρχουν περίπου 7,8 δισεκατομμύρια άνθρωποι στον πλανήτη, φαίνεται πως περισσότερο από το 50% του παγκόσμιου πληθυσμού χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης.

Καίριο ρόλο στην εξάπλωση αυτή διαδραματίζει η αδιάκοπη άνοδος των οικοσυστημάτων των έξυπνων κινητών τηλεφώνων. Οι χρήστες φέρουν συνεχώς επάνω τους το έξυπνο κινητό τους και, χωρίς να περιορίζονται από φυσικά όρια, συνδέονται στα μέσα κοινωνικής δικτύωσης οπουδήποτε και οποτεδήποτε. Τότε, αποκαλύπτουν αυτοβούλως δεδομένα σχετικά με τις προτιμήσεις τους, την τοποθεσία τους ή τις κοινωνικές τους σχέσεις, τα οποία καθίστανται διαθέσιμα σε χιλιάδες ή και εκατομμύρια άλλους χρήστες. Η ευρεία αυτή προσβασιμότητα και η ταχύτατη διάδοση περιεχομένου που δημιουργείται μέσω των μέσων κοινωνικής δικτύωσης ενισχύει από τη μία τις διαπροσωπικές επικοινωνίες[54], δημιουργεί από την άλλη προβληματισμούς όσον αφορά την ασφάλεια των δεδομένων των χρηστών.

2.1.1. Προσπάθεια Ορισμού

Σύμφωνα με το λεξικό του Cambridge, ως μέσα κοινωνικής δικτύωσης ορίζονται οι ιστοσελίδες και τα προγράμματα υπολογιστών που επιτρέπουν στους ανθρώπους να επικοινωνούν και να μοιράζονται πληροφορίες στο διαδίκτυο, χρησιμοποιώντας υπολογιστή ή κινητό τηλέφωνο[55].

Από τον παραπάνω ορισμό προκύπτουν τρία βασικά συστατικά στοιχεία των μέσων κοινωνικής δικτύωσης, με πρώτο και κυριότερο το ανθρώπινο στοιχείο. Στα μέσα κοινωνικής δικτύωσης, οι χρήστες δημιουργούν προφίλ με τα προσωπικά τους δεδομένα, όπως όνομα, ηλικία, φωτογραφίες και ενδιαφέροντα, προκειμένου να χτίσουν κοινωνικές σχέσεις ή να

---

[52] https://www.statista.com/statistics/617136/digital-population-worldwide/, https://www.statista.com/topics/1164/social-networks/#dossierKeyfigures

[53] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[54] Zhang N., Wang Ch. And Xu Y. (2011), "Privacy in Online Social Networks", Completed Research Paper, Thirty Second International Conference on Information Systems, Shanghai 2011, p.2, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.8584&rep=rep1&type=pdf (τελευταία πρόσβαση στις 18.02.2022)

[55] https://dictionary.cambridge.org/dictionary/english/social-media

διατηρήσουν τις ήδη υπάρχουσες. Η έννοια του χρήστη μπορεί να αναφέρεται σε διάφορους τύπους οντοτήτων, όπως σε φυσικά πρόσωπα, ομάδες προσώπων, καθώς και σε οργανισμούς, οι οποίοι αλληλοεπιδρούν μεταξύ τους μέσω εργαλείων επικοινωνίας που προσφέρονται από το εκάστοτε μέσο[56].

Το δεύτερο στοιχείο του ως άνω ορισμού είναι ο σκοπός των μέσων κοινωνικής δικτύωσης, εν προκειμένω η επικοινωνία και ο διαμοιρασμός πληροφοριών. Τα μέσα κοινωνικής δικτύωσης αποτελούν εικονικές κοινότητες όπου χρήστες με παρόμοια ενδιαφέροντα επιδιώκουν να ανταλλάξουν απόψεις και να αλληλοεπιδράσουν με τρίτους. Στην πραγματικότητα, κάθε μέσο κοινωνικής δικτύωσης προσφέρει συγκεκριμένες υπηρεσίες με σκοπό τη στόχευση συγκεκριμένου κοινού. Κάποια μέσα έχουν αναπτύξει υπηρεσίες για την προώθηση απόψεων και την κοινή χρήση πληροφοριών, όπως το Twitter, ενώ άλλα λειτουργούν ως εργαλείο κοινωνικοποίησης και γεφύρωσης των διαδικτυακών σχέσεων, όπως το Instagram ή το Facebook[57]. Συχνά, παρέχεται στους χρήστες ένας αποκλειστικός και προεπιλεγμένος τύπος σχέσης που τους συνδέει με κάθε μία από τις επαφές τους σε ένα κοινωνικό δίκτυο. Στο Facebook, για παράδειγμα, αυτές οι επαφές είναι γνωστές ως φίλοι, παρόλο που οι χρήστες κοινωνικών δικτύων συχνά δεν γνωρίζονται μεταξύ τους. Συνεπώς, ανησυχίες εγείρονται όσον αφορά τον τρόπο με τον οποίο τα μέσα κοινωνικής δικτύωσης επεξεργάζονται τα προσωπικά δεδομένα των χρηστών τους για να επιτύχουν τους ως άνω σκοπούς διασύνδεσης ή εξατομικευμένης στόχευσής τους, οι οποίες περιλαμβάνουν ζητήματα διαφάνειας ως προς τη συλλογή και περαιτέρω επεξεργασία των δεδομένων των χρηστών, έως και κατάρτισης προφίλ με βάση στοιχεία που οι ίδιοι οι χρήστες αυτοβούλως παρέχουν στα μέσα κοινωνικής δικτύωσης.

Τέλος, όπως αναλύθηκε στο Κεφάλαιο 1ο της παρούσας, τα μέσα κοινωνικής δικτύωσης αποτελούν εφαρμογές, για τη λειτουργία των οποίων αποτελεί προϋπόθεση η εγκατάστασή τους σε ένα κινητό τηλέφωνο ή έναν υπολογιστή. Επομένως, για την ορθή τους λειτουργία απαιτείται η συλλογή πληθώρας προσωπικών δεδομένων, κάποιες φορές υποχρεωτικών και κάποιες άλλες «σχεδόν» προαιρετικών.

---

[56] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.5, https://hal.archives-ouvertes.fr/hal-00975998 (τελευταία πρόσβαση στις 13.03.2022)

[57] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.7, https://hal.archives-ouvertes.fr/hal-00975998(τελευταία πρόσβαση στις 13.03.2022)

2.1.2. Χαρακτηριστικά μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης διακρίνονται εμφανώς από άλλες διαδικτυακές εφαρμογές λόγω μοναδικών ιδιοτήτων και χαρακτηριστικών. Αρχικά, αποτελούν εφαρμογές με άξονα τον χρήστη ("user-based applications"). Εντός ενός αδόμητου και χωρίς περιορισμούς διαδικτυακού περιβάλλοντος, οι χρήστες είναι ελεύθεροι να δημιουργήσουν από την αρχή το περιεχόμενο που επιθυμούν σύμφωνα με τις σχέσεις που επιδιώκουν να χτίσουν, χωρίς την ύπαρξη εξωτερικού ελέγχου ως προς τη ροή των πληροφοριών εντός του κοινωνικού δικτύου[58,59].

Το γεγονός, επιπλέον, ότι τα μέσα κοινωνικής δικτύωσης δεν αποτελούν πλέον "chat rooms" ή φόρουμ για ανταλλαγή απόψεων μεταξύ αγνώστων, αλλά οι χρήστες διαθέτουν δεκάδες επιλογές αλληλεπίδρασης με τους «φίλους» τους, καταδεικνύει τη διαδραστική τους φύση ("interactivity"). Οι χρήστες μπορούν να σχολιάσουν σε φωτογραφίες και βίντεο τρίτων, να μοιραστούν τις σκέψεις και τις ιδέες τους στο προφίλ τους, ακόμα και να παίξουν διαδικτυακά παιχνίδια εντός του περιβάλλοντος του κοινωνικού δικτύου[60].

Έπειτα, οι εφαρμογές αυτές διατίθενται στον χρήστη με μηδενικό κόστος, αφού το κέρδος τους προέρχεται κυρίως από τον χώρο που παρέχουν σε τρίτες εταιρείες για να διαφημιστούν ("no-cost services"). Τα δημογραφικά στοιχεία των χρηστών, σε συνδυασμό με τα ενδιαφέροντα και τις αλληλεπιδράσεις τους με φίλους ή αγαπημένες σελίδες, οδηγούν στην κατάρτιση ενός εξαιρετικά λεπτομερούς προφίλ, διευκολύνοντας την εμφάνιση στοχευμένων διαφημίσεων. Σε αντίθεση με τις κλασικές τηλεοπτικές διαφημίσεις –όπου οι ενδιαφερόμενοι διαφημίζονται παθητικά, χωρίς να γίνεται γνωστό το πλήθος των τηλεθεατών που είδαν πραγματικά τη διαφήμιση- τα μέσα κοινωνικής δικτύωσης όχι μόνο

---

[58] Al Johani M. (2016) "Personal Information Disclosure and Privacy in Social Networking Sites", Master Thesis, School of Engineering, Computer and Mathematical Sciences, New Zealand, p. 21, http://orapp.aut.ac.nz/bitstream/handle/10292/10320/AlJohaniM.pdf?sequence=3&isAllowed=y (τελευταία πρόσβαση στις 23.01.2022)

[59] Ωστόσο, τα μέσα κοινωνικής δικτύωσης έχουν θεσπίσει μηχανισμούς με τους οποίους ελέγχουν τις αναρτήσεις των χρηστών, έχοντας πολλάκις κατακριθεί για λογοκρισία και περιορισμό της ελευθερίας του λόγου. Μάλιστα, η Ολομέλεια του Ευρωπαϊκού Κοινοβουλίου τον Φεβρουάριο του 2021 έθεσε το ζήτημα της θέσπισης κανόνων δημοκρατικού ελέγχου των μέσων κοινωνικής δικτύωσης για τη διασφάλιση της ελευθερίας της έκφρασης.
https://www.europarl.europa.eu/news/en/press-room/20210204IPR97120/regulate-social-media-platforms-to-defend-democracy-meps-say (τελευταία πρόσβαση στις 16.01.2022)

[60] Πρόκειται κυρίως για εφαρμογές τρίτων μερών, συνδεδεμένες με το εκάστοτε κοινωνικό δίκτυο και εξουσιοδοτημένες από αυτό για να συλλέγουν τα προσωπικά δεδομένα του χρήστη και να τα επεξεργάζονται περαιτέρω, ζήτημα που θα αναπτυχθεί στο Κεφάλαιο 3ο.

επιβεβαιώνουν το κοινό που τις παρακολουθεί, αλλά παρέχουν επιπλέον πληροφορίες για την τοποθεσία των χρηστών, τα ενδιαφέροντά τους, τη συχνότητα προβολής, ακόμα και για τη διάρκεια παρακολούθησης της εκάστοτε διαφήμισης[61].

Επιπρόσθετα, τα μέσα κοινωνικής δικτύωσης περιστρέφονται γύρω από την έννοια της κοινότητας και του αριθμού των φίλων ή ακόλουθων του χρήστη ("community-driven applications"). Εντός ενός τέτοιου περιβάλλοντος, οι χρήστες μέσω των κοινών ενδιαφερόντων τους έχουν τη δυνατότητα να συζητήσουν και να αναδείξουν πλήθος θεμάτων ή να ανταλλάξουν απόψεις με νέους ή παλιούς φίλους ή ακόλουθους[62]. Οι απόψεις αυτές ωστόσο, μαζί με πλήθος άλλων προσωπικών πληροφοριών, διασκορπίζονται συχνά εκτός του προφίλ του χρήστη -σε φίλους του χρήστη, τους φίλους των φίλων του και άλλους άγνωστους χρήστες[63]- λόγω της ταχείας και μη συνειδητής αποδοχής των ρυθμίσεων ασφαλείας κατά την πρώτη είσοδο του χρήστη στο μέσο κοινωνικής δικτύωσης. Οι αρχικές ρυθμίσεις ασφαλείας είναι συνήθως εξ ορισμού κατασκευασμένες έτσι ώστε να επιτρέπουν την ορατότητα των προφίλ σε τρίτους ή την αυτόματη διασύνδεση των χρηστών με τρίτα μέρη, με σκοπό την παραγωγή περισσότερων εκμεταλλεύσιμων πληροφοριών. Ανακύπτει επομένως η ανάγκη καθιέρωσης ρυθμίσεων προφίλ φιλικότερων προς την ιδιωτικότητα των χρηστών, σε συνδυασμό με την σαφή ενημέρωσή τους σχετικά με τα αποτελέσματα της επιλογής της εκάστοτε ρύθμισης. Μέσο επίτευξης του στόχου αυτού αποτελεί ο εξ ορισμού περιορισμός της προσβασιμότητας ενός προφίλ από τρίτους, έτσι ώστε να εμποδίζεται εξ αρχής η προσπέλασή του από αόριστο αριθμό προσώπων[64] και αντίστοιχα να επιτρέπεται μόνο εάν ο χρήστης το επιλέξει μεταγενέστερα.

---

[61] Burns O. (2021), "Social Media and Data Privacy", Chapter 5 in Taal A. (2022) "The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change" CRC Press, p.69

[62] Rewaria S. (2021), "Data Privacy In Social Media Platform: Issues And Challenges", p.3, http://dx.doi.org/10.2139/ssrn.3793386 (τελευταία πρόσβαση στις 20.02.2022)

[63] Το προφίλ του χρήστη μάλιστα εκτίθεται ακόμη περισσότερο όταν επιτρέπεται εξ ορισμού ο σχολιασμός ή η κοινοποίηση του περιεχομένου που δημιουργεί από άγνωστους τρίτους.

[64] Άρθρο 25 παρ. 2 ΓΚΔΠ: «*Ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.*»

Οι συναισθηματικοί τέλος παράγοντες ("emotional factors"), όπως ένας εύκολα προσεγγίσιμος φίλος[65] ή μία ομάδα αυτοβελτίωσης και ανταλλαγής παρόμοιων απόψεων που θα ενισχύσουν ενδεχομένως την αυτοπεποίθηση ή την αυτοεκτίμηση, ωθούν τους χρήστες στην προτίμηση των μέσων κοινωνικής δικτύωσης, δυσχεραίνοντας ακόμη περισσότερο τον έλεγχο στα προσωπικά δεδομένα που αποκαλύπτουν.

2.1.3. Κατηγορίες μέσων κοινωνικής δικτύωσης

Δεκάδες μέσα κοινωνικής δικτύωσης έχουν κάνει την εμφάνισή τους τα τελευταία χρόνια, τα οποία, αν και παρουσιάζουν συνολικά τα χαρακτηριστικά που αναφέρθηκαν μόλις προηγουμένως, χρησιμοποιούνται για διαφορετικούς σκοπούς μία δεδομένη χρονική στιγμή. Έτσι, τα μέσα κοινωνικής δικτύωσης ταξινομούνται συνήθως στις ακόλουθες κατηγορίες: Κοινωνικά δίκτυα (π.χ. Facebook, Twitter), κοινωνικά δίκτυα κοινής χρήσης περιεχομένου (π.χ. Instagram, YouTube, TikTok), φόρουμ συζήτησης (π.χ. Reddit), δίκτυα σελιδοδεικτών και επιμέλειας περιεχομένου (π.χ. Pinterest)[66], δίκτυα κριτικής καταναλωτών (π.χ. TripAdvisor), πλατφόρμες κοινωνικής δικτύωσης με δυνατότητα αγοράς προϊόντων (π.χ. Instagram Shopping και Facebook Marketplace), δίκτυα οικονομίας διαμοιρασμού[67] (π.χ. Airbnb, Beat[68]) και ανώνυμα κοινωνικά δίκτυα με σκοπό την ανώνυμη επικοινωνία.

Οι πιο δημοφιλείς κατηγορίες είναι τα κοινωνικά δίκτυα και τα κοινωνικά δίκτυα κοινής χρήσης περιεχομένου. Τα πρώτα απαιτούν την αποκάλυψη της ταυτότητας του χρήστη με σκοπό τη δημιουργία προφίλ, που τυπικά περιλαμβάνει προσωπικά δεδομένα όπως όνομα, ηλικία, οικογενειακή κατάσταση και άλλα ενδιαφέροντα. Μέσα από αυτό το προφίλ οι χρήστες μοιράζονται τα γεγονότα της ατομικής τους ζωής ή σχολιάζουν και κοινοποιούν το περιεχόμενο τρίτων φίλων τους. Σε γενικές γραμμές, αυτές οι εφαρμογές επιτρέπουν στους χρήστες να προσθέτουν φίλους, να στέλνουν μηνύματα και να μοιράζονται περιεχόμενο. Από την άλλη, τα κοινωνικά δίκτυα κοινής χρήσης περιεχομένου παρέχουν στους χρήστες τη δυνατότητα να μοιράζονται εύκολα βίντεο και φωτογραφίες στο διαδίκτυο, επιτρέποντας

---

[65] "Easy-to-reach friend"

[66] Σύμφωνα με την Εταιρεία Hootsuite https://blog.hootsuite.com/types-of-social-media/ (τελευταία πρόσβαση στις 23.01.2022)

[67] Δίκτυο Οικονομίας Διαμοιρασμού ("Sharing Economy Network"): Ψηφιακή πλατφόρμα με τη μορφή peer-to-peer που επιτρέπει την άμεση και χωρίς μεσάζοντες αλληλεπίδραση μεταξύ δύο ή περισσότερων μερών, συνδέοντας το κάθε μέρος με την πλατφόρμα.
Οικονομία διαμοιρασμού ("Sharing Economy"): Οικονομικό μοντέλο σύμφωνα με το οποίο οι χρήστες δημιουργούν και μοιράζονται αγαθά, υπηρεσίες, χώρο και χρήματα μεταξύ τους. https://www.emerald.com/insight/publication/issn/1757-5818 (τελευταία πρόσβαση στις 23.01.2022)

[68] Εφαρμογή εύρεσης ταξί για έξυπνα τηλέφωνα και κινητές συσκευές.

την κοινόχρηστη ανάρτηση περιεχομένου είτε ιδιωτικά σε επιλεγμένους χρήστες είτε δημόσια[69]. Η δημοφιλέστερη εφαρμογή κοινής χρήσης περιεχομένου είναι αδιαμφισβήτητα το Instagram, το οποίο πλέον ανήκει στο Facebook ή "Meta", και απευθύνεται στους χρήστες έξυπνων κινητών τηλεφώνων που επιθυμούν τη λήψη, τη δημοσίευση και την κοινή χρήση αυτοσχέδιων βίντεο και φωτογραφιών.

Η προφανής επιτυχία των μέσων κοινωνικής δικτύωσης που γίνεται φανερή όχι μόνο από τη δημοφιλία τους, αλλά και από τον εκθετικό πολλαπλασιασμό τους, έχει γεννήσει ερωτήματα ιδιωτικότητας και ασφάλειας των χρηστών. Οι ρυθμίσεις απορρήτου των εν λόγω εφαρμογών -λόγου χάριν ο περιορισμός της πρόσβασης στο προφίλ του χρήστη μόνο σε συγκεκριμένες κατηγορίες φίλων ή επαφών- αποτελούν θεωρητικά ένα πρώτο βήμα για τη διασφάλιση της ασφάλειάς τους, ωστόσο, η πλειοψηφία των χρηστών αρκείται στις προεπιλεγμένες ρυθμίσεις, αφήνοντας τη διαχείριση και τον έλεγχο των δεδομένων τους σχεδόν αποκλειστικά στα χέρια των παρόχων των μέσων κοινωνικής δικτύωσης[70].

2.2. Επεξεργασία Προσωπικών Δεδομένων στα Μέσα Κοινωνικής Δικτύωσης

2.2.1. Κατηγορίες προσωπικών δεδομένων χρηστών

Ο ταχύτατος ρυθμός εξάπλωσης των μέσων κοινωνικής δικτύωσης ωθεί τους χρήστες σε μία αδιάλειπτη προσπάθεια απόκτησης νέων φίλων και ακόλουθων. Με σκοπό τη συνδεσιμότητα ή ακόμα και την απόκτηση αναγνωρισιμότητας, είναι πρόθυμοι να αποκαλύψουν πλήθος προσωπικών δεδομένων και πληροφοριών, που πολλές φορές μπορεί να φτάνουν μέχρι τη δημοσίευση ιδιαίτερα προσωπικών πτυχών της ζωής τους. Το προφίλ του εκάστοτε χρήστη προκειμένου να γίνει προσιτό στους φίλους του, εμπλουτίζεται με δημογραφικά στοιχεία, επαγγελματικές διευθύνσεις, ενδιαφέροντα και προτιμήσεις, όπως και με εξατομικευμένο περιεχόμενο, φωτογραφίες και βίντεο. Έτσι, τα μέσα κοινωνικής δικτύωσης δύνανται να εξάγουν εμμέσως ένα τεράστιο όγκο προσωπικών δεδομένων για τον χρήστη -συνήθως εν αγνοία του- είτε μέσω σύγκρισης και ανάλυσης των προτιμήσεων,

---

[69] Rewaria S. (2021), "Data Privacy In Social Media Platform: Issues And Challenges", p.4, http://dx.doi.org/10.2139/ssrn.3793386 (τελευταία πρόσβαση στις 20.02.2022)

[70] Kosta E., Kalloniatis Ch., Mitrou L. and Gritzalis S. (2010) "Data protection issues pertaining to social networking under EU law", Research Paper, Transforming Government: People, Process and Policy Vol. 4 No. 2, p. 194, Emerald Group Publishing Limited, Transforming Government: People, Process and Policy | Emerald Insight (τελευταία πρόσβαση στις 13.02.2022)

των αλληλεπιδράσεων και των καθημερινών δραστηριοτήτων του, είτε μέσω διαφόρων συνδεδεμένων πηγών στο διαδίκτυο[71].

Σε αυτό επομένως το πλαίσιο, τα προσωπικά δεδομένα που συλλέγονται από τα μέσα κοινωνικής δικτύωσης θα μπορούσαν να ταξινομηθούν στις ακόλουθες δύο γενικές κατηγορίες: στα προσωπικά δεδομένα που παρέχονται ρητά από τον χρήστη ("explicit personal data") και στα προσωπικά δεδομένα που συλλέγονται σιωπηρά ("implicit personal data")[72].

Τα προσωπικά δεδομένα που παρέχονται ρητά αφορούν οποιαδήποτε πληροφορία παρέχει ο χρήστης ενεργώντας αυτοβούλως, συμπεριλαμβανομένων των γραπτών μηνυμάτων που αποστέλλονται μέσω των μέσων κοινωνικής δικτύωσης, καθώς και των δεδομένων που εξάγονται από τις παρεχόμενες πληροφορίες, όπως μεταδεδομένα ενσωματωμένα σε φωτογραφίες[73]. Σε αυτή την κατηγορία, ανήκουν τα δεδομένα εξυπηρέτησης, τα δεδομένα γνωστοποίησης, τα «εμπιστευμένα» δεδομένα και τα τυχαία ή συμπτωματικά δεδομένα[74].

Τα δεδομένα εξυπηρέτησης ("service data") αποτελούν το σύνολο των υποχρεωτικών δεδομένων που παρέχει ένας χρήστης στο εκάστοτε μέσο κοινωνικής δικτύωσης με σκοπό τη δημιουργία του προσωπικού του λογαριασμού, όπως όνομα χρήστη, ημερομηνία γέννησης, χώρα κ.λπ. Από την άλλη, τα δεδομένα γνωστοποίησης ("disclosed data") καταχωρούνται στο κοινωνικό δίκτυο προαιρετικά και αφορούν το περιεχόμενο που αναρτά ο χρήστης στο προσωπικό του προφίλ, όπως για παράδειγμα φωτογραφίες και βίντεο, ενημερώσεις κατάστασης, σχόλια και κοινόχρηστοι σύνδεσμοι. Το επίπεδο ορατότητας των πληροφοριών από τρίτους καθορίζεται από τις προεπιλεγμένες ρυθμίσεις του μέσου κοινωνικής δικτύωσης, εκτός εάν ο χρήστης, ως δημιουργός του περιεχομένου, επιλέξει να

---

[71] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.16, https://hal.archives-ouvertes.fr/hal-00975998 (τελευταία πρόσβαση στις 13.03.2022)

[72] Βλ. υποσημείωση 71.

[73] Όπως για παράδειγμα η ώρα και η ημερομηνία που λήφθηκε η φωτογραφία, πληροφορίες σχετικά με το είδος της κάμερας, ακόμη και πληροφορίες πνευματικών δικαιωμάτων που επιβεβαιώνουν τη νόμιμη ιδιοκτησία της φωτογραφίας.

[74] Σύμφωνα με την κατηγοριοποίηση του Bruce Schneier, Schneier B. (2010) "A taxonomy of social networking data", IEEE Security and Privacy 8(4) (2010) 88, https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html (τελευταία πρόσβαση στις 25.01.2022)

τις τροποποιήσει, ορίζοντας στενότερο εύρος ορατότητας[75]. Έπειτα, τα εμπιστευμένα δεδομένα ("entrusted data") αφορούν το σύνολο των πληροφοριών που ένας χρήστης κοινοποιεί στο προφίλ κάποιου τρίτου, όπως σχόλια κάτω από φωτογραφίες ή δημοσιεύσεις περιεχομένου εκτός του δικού του προφίλ. Οι ανησυχίες για την προστασία των προσωπικών δεδομένων ανακύπτουν κυρίως από την στιγμή απώλειας ελέγχου των δεδομένων του χρήστη. Για παράδειγμα, αφού ένας χρήστης αναρτήσει ένα σχόλιο στο προφίλ κάποιου φίλου του, ο έλεγχος του σχολίου και των δεδομένων που εμπεριέχονται εκεί μεταβιβάζεται στον τελευταίο, ο οποίος πλέον μπορεί να ορίσει αυτοβούλως το επίπεδο ορατότητάς του σε άλλους χρήστες. Συνεπώς, το σχόλιο ενδέχεται να μείνει αναρτημένο στο εν λόγω προφίλ για όσο χρονικό διάστημα επιλέξει ο τρίτος, ακόμη κι εάν ο χρήστης επιθυμεί τη διαγραφή του[76]. Αντιθέτως, τα τυχαία ή συμπτωματικά δεδομένα ("incidental data") αποτελούν δεδομένα που δημοσιοποιούν τρίτοι χρήστες μέσων κοινωνικής δικτύωσης σχετικά με έναν χρήστη στο προφίλ του τελευταίου.

Τα προσωπικά δεδομένα που συλλέγονται σιωπηρά ή -με άλλα λόγια- που δεν παρέχονται ρητά από τον χρήστη, αποτελούν τη δεύτερη γενική κατηγορία δεδομένων στα μέσα κοινωνικής δικτύωσης. Η εξαγωγή των «σιωπηρών» αυτών δεδομένων βασίζεται κατά κύριο λόγο στην ανάλυση των συμπεριφορών των χρηστών ή προέρχεται από τη σύγκριση πλήθους πληροφοριών που παρέχονται ρητά από τους χρήστες. Είναι για παράδειγμα δυνατό να προβλεφθούν τα χαρακτηριστικά των σχέσεων μεταξύ μίας ομάδας χρηστών, απλώς και μόνο αναλύοντας τα διαφορετικά πρότυπα επικοινωνίας που έχουν αναπτύξει με το πέρασμα του χρόνου, όπως τα μηνύματα κειμένου και οι ώρες επικοινωνίας τους, οι δημοσιευμένες φωτογραφίες και ο αριθμός των κοινών τους φίλων[77]. Πρόκειται για μια «παρασκηνιακή» προσέγγιση[78] κατά την οποία τα δεδομένα συλλέγονται χωρίς την άμεση ανάμειξη ή τη ρητή και σαφή συγκατάθεση του χρήστη[79]. Έτσι, τα σιωπηρά δεδομένα

[75] Richthammer et al. (2014) "Taxonomy of social network data types", EURASIP Journal on Information Security, 2014:11 http://jis.eurasipjournals.com/content/2014/1/11 (τελευταία πρόσβαση στις 25.01.2022)

[76] Bruce Schneier, Schneier B. (2010) "A taxonomy of social networking data", IEEE Security and Privacy 8(4) (2010) 88, https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html (τελευταία πρόσβαση στις 25.01.2022)

[77] Raad E., Chbeir R., Dipanda A. (2013) "Discovering relationship types between users using profiles and shared photos in a social network", Multimedia Tools and Applications, 64(1) (2013) 141–170, https://hal.archives-ouvertes.fr/hal-00665036 (τελευταία πρόσβαση στις 25.01.2022)

[78] Huang E.,Y., and Lin C.,Y., (2005) "Customer-oriented financial service personalization" Industrial Management & Data Systems Vol. 105 (1), pp. 26-44

[79] Themistocleous Ch., Smith A. and Wagner Ch. (2014) "The ethical dilemma of implicit vs explicit data collection: Examining the factors that influence the voluntary disclosure of information by consumers to

ταξινομούνται σε δύο υποκατηγορίες, ήτοι στα δεδομένα συμπεριφοράς και στα συναγόμενα δεδομένα.

Τα δεδομένα συμπεριφοράς ("behavioral data") συνάγονται από τις ενέργειες του χρήστη στα μέσα κοινωνικής δικτύωσης, παρακολουθώντας τα ποικίλα μοτίβα των δραστηριοτήτων του[80]. Κατά συνέπεια, αναλύοντας τη συμπεριφορά του, όπως για παράδειγμα τα άρθρα που επιλέγει να διαβάσει, τις δημοσιεύσεις τις οποίες σχολιάζει ή τις ομάδες που ακολουθεί, τα μέσα κοινωνικής δικτύωσης αποκτούν εύκολα πληροφορίες σχετικά με το τι ενδιαφέρει τον χρήστη, τους φίλους με τους οποίους αλληλοεπιδρά συχνότερα, ποιες ειδήσεις προσελκύουν περισσότερο το ενδιαφέρον του, ακόμα και τις πολιτικές του πεποιθήσεις. Ένα από τα ζητήματα ιδιωτικότητας που θα μπορούσαν να σημειωθούν εν προκειμένω αφορά τη δυνατότητα λήψης αποφάσεων για τον χρήστη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας από τα μέσα κοινωνικής δικτύωσης, αλλά και από τα έξυπνα τηλέφωνα τα οποία χρησιμοποιεί για να συνδέεται σε αυτά, πρακτική που ενδεχομένως να αντιβαίνει στα δικαιώματα και τις ελευθερίες του εκάστοτε υποκειμένου των δεδομένων. Ιδιαιτέρως από τη στιγμή που η αυτοματοποιημένη λήψη αποφάσεων συνήθως λαμβάνει χώρα εν αγνοία των χρηστών που επηρεάζονται, είναι πιθανόν οι τελευταίοι ως υποκείμενα δεδομένων να μην είναι καν σε θέση να ασκήσουν αποτελεσματικά τα δικαιώματά τους για εναντίωση στην επεξεργασία αυτή[81].

Τελευταία κατηγορία αλλά εξίσου σημαντική, είναι τα συναγόμενα δεδομένα ("derived data"), όσα δηλαδή μπορούν να συναχθούν από όλα τα άλλα δεδομένα του χρήστη και δεν σχετίζονται με τις συνήθειές του. Για παράδειγμα, συναγόμενο δεδομένο αποτελεί η τοποθεσία του χρήστη η οποία αποκαλύπτεται από την IP του κινητού του τηλεφώνου[82]. Τέτοιου είδους δεδομένα συνάγονται από τον συνδυασμό δύο ή περισσότερων πληροφοριών. Εάν λόγου χάριν ένας σημαντικός αριθμός φίλων του χρήστη φοιτούσε στο ίδιο σχολείο της ίδιας πόλης, είναι πιθανό να συναχθεί ότι και ο χρήστης φοιτούσε στο σχολείο αυτό και

commercial organizations", Conference Paper, IEEE International Symposium on Ethics in Science, Technology and Engineering, p.1., https://dl.acm.org/doi/pdf/10.5555/2960587.2960632 (τελευταία πρόσβαση στις 25.01.2022)

[80] Schneier B. (2010) "A taxonomy of social networking data", IEEE Security and Privacy 8(4) (2010) 88, https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html (τελευταία πρόσβαση στις 25.01.2022)

[81] Βλ. υποκεφάλαιο 3.4. της παρούσης

[82] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.17, https://hal.archives-ouvertes.fr/hal-00975998 (τελευταία πρόσβαση στις 13.03.2022)

επιπλέον ότι εκείνη την περίοδο της ζωής του κατοικούσε στη συγκεκριμένη πόλη. Στο παράδειγμα αυτό, τα μέσα κοινωνικής δικτύωσης ή τρίτα μέρη χρειάζονται πρόσβαση σε τρεις πληροφορίες προκειμένου να εξάγουν τα συναγόμενα δεδομένα, ήτοι στους φίλους του χρήστη, το σχολείο και την αντίστοιχη πόλη.

Αδιαμφισβήτητα είναι τελικά φανερό ότι σε οποιαδήποτε ενέργεια προχωρήσει ο χρήστης ή εκδηλώσει οποιοδήποτε ενδιαφέρον, αυτό θα καταγραφεί και θα αναλυθεί ταχύτατα από τα μέσα κοινωνικής δικτύωσης, με κάποια από τα δεδομένα μάλιστα να ταξινομηθούν και να πωληθούν σε δευτερόλεπτα σε τρίτους[83]. Παρ' όλους τους γνωστούς αυτούς κινδύνους ωστόσο, τα μέσα κοινωνικής δικτύωσης αναπτύσσονται ραγδαία, δημιουργώντας προβληματισμούς σχετικά με την ανοχή και τον συμβιβασμό των χρηστών σε αντάλλαγμα της συνδεσιμότητάς τους.

2.2.2. Η συμπεριφορά των χρηστών απέναντι στην επεξεργασία των προσωπικών τους δεδομένων: Οι δύο βασικές θεωρίες

Η συμμετοχή στα μέσα κοινωνικής δικτύωσης συνδέεται με τρεις κύριες ανάγκες της σύγχρονης ανθρώπινης φύσης: (α) την ανάγκη για διασκέδαση και απόδραση από την έντονη καθημερινότητα, (β) την ανάγκη για κοινωνικοποίηση και (γ) την ανάγκη για διαμόρφωση ταυτότητας[84]. Όπως αναλύθηκε παραπάνω, αυτή η συμμετοχή περιλαμβάνει την αυτόβουλη και ιδιαίτερα πρόθυμη αποκάλυψη προσωπικών δεδομένων από τους χρήστες για σχετικά μικρές ανταμοιβές, οι οποίες θα ικανοποιήσουν μία ή περισσότερες από τις ως άνω ανάγκες. Η συγκεκριμένη ωστόσο συμπεριφορά γεννάει ποικίλες ανησυχίες για το απόρρητό των προσωπικών δεδομένων τους, αφού οι περισσότεροι χρήστες, αν και φαίνεται να ανησυχούν για το απόρρητό τους και θα ήταν πρόθυμοι να το προστατεύσουν, στην πραγματικότητα ενεργούν εκ διαμέτρου αντίθετα.

Ποικίλες έρευνες έχουν δημοσιευτεί αναφορικά με την αδυναμία των χρηστών να ισορροπήσουν ανάμεσα στις ανησυχίες για την ιδιωτικότητά τους και την ανάγκη για

[83] Zuboff S. (2019) "The Age of Surveillance Capitalism", London: Profile Books

[84] Debatin et al. (2009) "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", Journal of Computer-Mediated Communication, Volume 15, Issue 1, 1 Pages 83–108, https://doi.org/10.1111/j.1083-6101.2009.01494.x

αποκάλυψη των προσωπικών τους δεδομένων[85], έχοντας έτσι αναδειχθεί δύο βασικές θεωρίες.

Η πρώτη θεωρία περιγράφει το φαινόμενο του «παράδοξου της ιδιωτικότητας» ("the privacy paradox"), σύμφωνα με το οποίο οι χρήστες των μέσων κοινωνικής δικτύωσης επισημαίνουν μεν τις ανησυχίες τους για την ιδιωτικότητα, πράττουν δε ελάχιστα για την προστατεύσουν[86]. Με τον τρόπο αυτό δημιουργείται μία παράδοξη «διχοτόμηση» μεταξύ της στάσης και της συμπεριφοράς των χρηστών προς την ιδιωτικότητά τους[87], μία έντονη ασυμφωνία παρατηρούμενη εντόνως στα διαδικτυακά συστήματα κατάρτισης προφίλ[88].

Συγκεκριμένα, στο πλαίσιο των δραστηριοτήτων των μέσων κοινωνικής δικτύωσης μέσω έξυπνων κινητών τηλεφώνων παρατηρείται το ακόλουθο μοτίβο. Παρ' όλο που έχουν σχεδιαστεί ποικίλες στρατηγικές προστασίας της ιδιωτικότητας του χρήστη, όπως ο περιορισμός της πρόσβασης τρίτων στο προφίλ του ή η απαγόρευση αναδημοσίευσης περιεχομένου από τρίτους, με σκοπό τον έλεγχο της ροής των πληροφοριών μεταξύ του στενού κύκλου των φίλων[89], ο χρήστης, υποκινούμενος από την ένταση της επιθυμίας του για κοινωνικοποίηση, αμελεί τις προστατευτικές αυτές δικλείδες και προβαίνει στην αποκάλυψη προσωπικών του δεδομένων, υποτιμώντας τους κινδύνους που προκύπτουν από την πράξη του αυτή[90].

---

[85] Σιδέρη Μ., Κίτσιου Αγ., Τζωρτζάκη Ελ., Καλλονιάτης Χ. και Γκρίτζαλης Στ. (2017), «Προστασία της Ιδιωτικότητας σε Ψηφιακά Κοινωνικά Δίκτυα. Μια αναγκαία συνθήκη για τη διατήρηση της κοινωνικής συνοχής στην Κοινωνία της Πληροφορίας», Κεφάλαιο στο «Κοινωνική και Πολιτισμική Βιωσιμότητα», ΠΜΣ Περιβαλλοντική Εκπαίδευση, ΤΕΠΑΕΣ, Πανεπιστήμιο Αιγαίου, Ρόδος 2017, σελ. 134-174

[86] Dwyer C, Hiltz SR and Passerini K (2007) "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace", Conference Paper, Thirteenth Americas Conference on Information Systems, Keystone, CO. http://csis.pace.edu/dwyer/research/DwyerAMCIS2007.pdf (τελευταία πρόσβαση στις 29.01.2022)

[87] *"Paradoxical dichotomy between privacy attitudes and privacy behaviour":* Kokolakis Sp. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Volume 64, Elsevier Journal, p. 125, https://www.sciencedirect.com/science/article/pii/S0167404815001017 (τελευταία πρόσβαση στις 29.01.2022)

[88] Barth S. and De Jong M DT (2017), "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review", Telematics and Informatics, Volume 34(7), Elsevier Journal, pp. 1038–1058, https://www.sciencedirect.com/science/article/pii/S0736585317302022(τελευταία πρόσβαση στις 29.01.2022)

[89] Βλ. υποσημείωση 88.

[90] Buschel et al. (2014), "Protecting Human Health and Security in Digital Europe: How to Deal With The Privacy Paradox?", Science and Engineering Ethics, Volume 20, pp. 639-658

Πλήθος ερευνών έχουν διεξαχθεί για την κατανόηση του παράδοξου. Ωστόσο, δεν υπάρχει ακόμη κάποια αποδεκτή θεωρία που να αξιοποιείται για την εξήγηση της διαδικτυακής συμπεριφοράς των χρηστών όσον αφορά την εθελούσια αποκάλυψη πληροφοριών, ούτε υπάρχει ομοφωνία σχετικά με τις νοητικές διαδικασίες στις οποίες βασίζονται οι χρήστες όταν αποφασίζουν εάν θα προβούν ή όχι στην αποκάλυψη.

Οι Acquisti και Grossklags (2005) υποστήριξαν ότι η απόφαση των χρηστών για την αποκάλυψη των δεδομένων τους μπορεί να επηρεαστεί από ελλιπείς πληροφορίες που δέχονται, ακόμα και από οριοθετημένη ορθολογικότητα[91]. Οι ίδιοι επιπλέον, επιχειρώντας να εξηγήσουν το παράδοξο σε μία έρευνά τους που δημοσιεύτηκε το 2006, ερμηνεύουν πως ο παράγοντας που οδηγεί στην ασυνέπεια της συμπεριφοράς των χρηστών θα μπορούσε να είναι η εμπιστοσύνη που αναπτύσσουν τόσο προς τους παρόχους υπηρεσιών που θεωρούν τίμιους στις μεταξύ τους συναλλαγές, όσο και προς τους τρίτους χρήστες με τους οποίους εμφανίζουν ομοιότητες και κοινά ενδιαφέροντα[92]. Για παράδειγμα, όταν οι πολιτικές προστασίας δεδομένων εμφανίζονται ευδιάκριτα και κατανοητά, οι χρήστες τείνουν να επιλέγουν διαδικτυακές εφαρμογές που προστατεύουν καλύτερα την ιδιωτικότητά τους[93,94]. Τέλος, σύμφωνα με την Sandra Petronio, οι επιλογές του χρήστη για την ιδιωτικότητά του

[91] Ενώ τα περισσότερα από τα άτομα που συμμετείχαν στην έρευνα (περίπου 89%) ανέφεραν ότι ανησυχούν μέτρια ή πολύ για την ιδιωτικότητά τους, περισσότερο από το 21% του δείγματος παραδέχτηκε ότι έχει αποκαλύψει τον αριθμό κοινωνικής ασφάλισής του για εκπτώσεις ή καλύτερες υπηρεσίες, ενώ περισσότεροι από το 28% είχαν δώσει τους αριθμούς τηλεφώνου τους σε εμπόρους ή διοργανωτές κληρώσεων. Acquisti A. and Grossklags J. (2005) "Privacy and rationality in individual decision making", IEEE, Security and Privacy Magazine, Volume 3 (1), pp.26-33, DOI:10.1109/MSP.2005.22 (τελευταία πρόσβαση στις 29.01.2022)

[92] Acquisti A. and Grossklags J. (2006), "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", In: Danezis G., Golle P. (eds) Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, Volume 4258, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11957454_3 (τελευταία πρόσβαση στις 29.01.2022)

[93] Kokolakis Sp. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Volume 64, Elsevier Journal, p. 125, https://www.sciencedirect.com/science/article/pii/S0167404815001017 (τελευταία πρόσβαση στις 29.01.2022)

[94] Οι Tsai κ.α. διεξήγαγαν μελέτη σχετικά με τις ανησυχίες των χρηστών κατά τις ηλεκτρονικές τους αγορές, διενεργώντας παράλληλα εμπειρικό πείραμα με την αξιοποίηση μίας μηχανής αναζήτησης αγορών που εμφάνιζε στους χρήστες αναλυτικές πληροφορίες για τις πολιτικές απορρήτου των καταστημάτων. Διαπιστώθηκε από το πείραμα ότι οι χρήστες πραγματικά ανέτρεχαν στις επιμέρους πολιτικές και τελικά επέλεγαν να αγοράσουν από διαδικτυακά καταστήματα με μεσαίο ή υψηλό επίπεδο προστασίας της ιδιωτικότητας, με βάση την εκάστοτε πολιτική απορρήτου. Tsai et al. (2011) "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", Information Systems Research, Volume 22 No 2, pp. 254-268, https://www.jstor.org/stable/23015560 (τελευταία πρόσβαση στις 29.01.2022)

διαφοροποιούνται σύμφωνα με τις εκάστοτε επιθυμίες του, τους κοινωνικούς ή προσωπικούς του στόχους, το περιβάλλον, αλλά και το κοινωνικοπολιτικό πλαίσιο[95,96].

Από την άλλη, η λεγόμενη θεωρία του υπολογισμού ή λογισμού της ιδιωτικότητας ("privacy calculus theory") εξηγεί ότι οι άνθρωποι αποκαλύπτουν προσωπικές πληροφορίες τους σε καταστάσεις όπου τα οφέλη είναι μεγαλύτερα από τις αρνητικές συνέπειες[97,98], ενώ η τελική συμπεριφορά τους καθορίζεται από το αποτέλεσμα αυτού του υπολογισμού[99].

Εν προκειμένω, οι χρήστες, πριν παράσχουν τα προσωπικά τους δεδομένα, «εκτελούν» μια ανάλυση μεταξύ της αντιληπτής απώλειας της ιδιωτικής ζωής και του πιθανού κέρδους που θα λάβουν από την αποκάλυψη αυτή. Εάν τα κέρδη υπερβαίνουν τις αναμενόμενες ζημίες, τότε οι χρήστες αποφασίζουν να αποκαλύψουν τα προσωπικά τους δεδομένα[100]. Στις κοινωνικές ωστόσο αλληλεπιδράσεις, οι ανταμοιβές είναι ως επί το πλείστον άυλες και

---

[95] Petronio S. (2002), "Boundaries of Privacy: Dialectics of Disclosure", Albany, NY: State University of New York Press

[96] Σιδέρη Μ., Κίτσιου Αγ., Τζωρτζάκη Ελ., Καλλονιάτης Χ. και Γκρίτζαλης Στ. (2017), «Προστασία της Ιδιωτικότητας σε Ψηφιακά Κοινωνικά Δίκτυα. Μια αναγκαία συνθήκη για τη διατήρηση της κοινωνικής συνοχής στην Κοινωνία της Πληροφορίας», Κεφάλαιο στο «Κοινωνική και Πολιτισμική Βιωσιμότητα», ΠΜΣ Περιβαλλοντική Εκπαίδευση, ΤΕΠΑΕΣ, Πανεπιστήμιο Αιγαίου, Ρόδος 2017, σελ. 145

[97] Culnan M.J. and Armstrong P.K. (1999) "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", Organ. Sci. Volume 10, pp. 104–115, https://doi.org/10.1287/orsc.10.1.104 (τελευταία πρόσβαση στις 29.01.2022)

[98] Cain J. A. and Imre I. (2021), "Everybody wants some: Collection and control of personal information, privacy concerns, and social media use", Article in New media & Society, Sage Journals, 1–20, p. 2, DOI: 10.1177/14614448211000327 https://journals.sagepub.com/home/nms (τελευταία πρόσβαση στις 04.02.2022)

[99] Xu H., Dinev T., Smith J. and Hart P. (2011), "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", J. Assoc. Inf. Syst. Volume 12, 1, "Information Privacy Concerns: Linking Individual Perceptions with Inst" by Heng Xu, Tamara Dinev et al. (aisnet.org) (τελευταία πρόσβαση στις 29.01.2022)

[100] Οι Beresford κ.α. διεξήγαγαν εμπειρικό πείραμα, στο οποίο ζητήθηκε από τους συμμετέχοντες να αγοράσουν ένα DVD από ένα από τα δύο ανταγωνιστικά καταστήματα. Ως προϋπόθεση αγοράς, το πρώτο κατάστημα ζήτησε εισόδημα και ημερομηνία γέννησης, ενώ το δεύτερο ζήτησε αγαπημένο χρώμα και έτος γέννησης. Προφανώς, οι πληροφορίες που ζητήθηκαν από το πρώτο κατάστημα είναι πιο ευαίσθητες και σε καμία περίπτωση ανάλογες του σκοπού της αγοράς του DVD. Παρ 'όλα αυτά, όσο η τιμή πώλησης ήταν η ίδια, οι συμμετέχοντες αγόραζαν εξ' ίσου από τα δύο καταστήματα. Όταν όμως η τιμή ορίστηκε 1 ευρώ λιγότερο στο πρώτο κατάστημα, σχεδόν όλοι οι συμμετέχοντες επέλεξαν το φθηνότερο κατάστημα, αν και ζητούσε πιο ευαίσθητες πληροφορίες. Beresford A.R., Kübler D. and Preibusch S. (2012) "Unwillingness to pay for privacy: A field experiment", Economics Letters, Elsevier Journal, Volume 117, Issue 1, pp. 25-27, https://doi.org/10.1016/j.econlet.2012.04.077 (τελευταία πρόσβαση στις 29.01.2022)

επομένως δύσκολο να παρατηρηθούν[101]. Λόγου χάριν, στα μέσα κοινωνικής δικτύωσης επιθυμητό κέρδος αποτελεί μία εξατομικευμένη εμπειρία πλοήγησης ή η προβολή διαφημίσεων σχετιζόμενων με τα ενδιαφέροντα του χρήστη. Πιθανός δε κίνδυνος είναι σίγουρα η αποκλειστικά αυτοματοποιημένη λήψη αποφάσεων για αυτόν. Παρ' όλα αυτά, οι περισσότεροι χρήστες δεν είναι γνωστικά ικανοί να υπολογίσουν με σιγουριά τους κινδύνους, αφού διαθέτουν πρόσβαση σε ελάχιστες και μη τεκμηριωμένες πληροφορίες σχετικά με τους συμβιβασμούς στους οποίους προβαίνουν αποκαλύπτοντας τα δεδομένα τους, λαμβάνοντας τελικά αποφάσεις σε περιορισμένο χρόνο και βασιζόμενοι σε ελλιπή στοιχεία[102].

Συμπερασματικά, οι δύο θεωρίες που αναπτύχθηκαν επιδιώκουν να ερμηνεύσουν τις ασυμφωνίες των εσωτερικών διεργασιών των χρηστών πριν τη χορήγηση των δεδομένων τους και των εν τέλει παράλογων συμπεριφορών τους στον πραγματικό κόσμο[103]. Το ερώτημα που παραμένει είναι εάν το μακροπρόθεσμο κόστος της αλόγιστης αποκάλυψης προσωπικών δεδομένων υπέρ βραχυπρόθεσμων κερδών, μπορεί να γίνει κατανοητό με τη διαφανέστερη ενημέρωση και λήψη συγκατάθεσης των χρηστών σχετικά με τις πρακτικές επεξεργασίας προσωπικών δεδομένων.

2.3. Οι όροι χρήσης των μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης συλλέγουν αδιαλείπτως προσωπικά δεδομένα και άλλες πληροφορίες από τους χρήστες τους με προφανή σκοπό την καλύτερη παροχή υπηρεσιών επικοινωνίας ή ψυχαγωγίας σε αυτούς. Παρασκηνιακά, ωστόσο, υφίσταται πλήθος διαφορετικών σκοπών που οδηγούν στη συλλογή αυτών των δεδομένων, ακόμα και στη διαβίβασή τους σε τρίτα μέρη, όπως διαφημιστές ή συνδεδεμένες ιστοσελίδες και άλλες εφαρμογές. Σε ένα πρώτο επίπεδο, όλες οι οντότητες που εμπλέκονται στην επεξεργασία προσωπικών δεδομένων επιδιώκουν τη συμμόρφωσή τους με τις θεμελιώδεις αρχές που εισάγει ο ΓΚΠΔ, καθώς και τους κανόνες περί νόμιμης και ενημερωμένης επεξεργασίας προσωπικών δεδομένων από τους χρήστες, συνήθως με τη μορφή Πολιτικών Προστασίας

[101] Kokolakis Sp. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Volume 64, Elsevier Journal, p. 128, https://www.sciencedirect.com/science/article/pii/S0167404815001017 (τελευταία πρόσβαση στις 29.01.2022)

[102] Βλ. υποσημείωση 101.

[103] Betzing J.H., Tietz M., vom Brocke J. et al. (2020) "The impact of transparency on mobile privacy decision making", Electron Markets, Volume 30, pp. 607–625, https://doi.org/10.1007/s12525-019-00332-3 (τελευταία πρόσβαση στις 29.01.2022)

Δεδομένων ή Όρων και Προϋποθέσεων Χρήσης. Τα κείμενα αυτά είτε εμφανίζονται στις εφαρμογές των μέσων κοινωνικής δικτύωσης κατά την εγγραφή του χρήστη, πριν την ρητή παροχή των πρώτων προσωπικών δεδομένων στην εφαρμογή[104], είτε αποστέλλονται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου κάθε φορά που αλλάζουν κάποιοι από τους όρους τους.

Συμφωνώντας με τους όρους χρήσης των μέσων κοινωνικής δικτύωσης, από νομική σκοπιά οι χρήστες υπογράφουν μια ηλεκτρονική σύμβαση, που επιτρέπει στα μέσα κοινωνικής δικτύωσης να συλλέγουν και να μοιράζονται ορισμένα ή και όλα τα προσωπικά δεδομένα του χρήστη[105]. Σε αντίθεση όμως με τις παραδοσιακές συμβάσεις, δεν λαμβάνει χώρα οποιαδήποτε διαπραγμάτευση μεταξύ του χρήστη και της εταιρείας πίσω από το μέσο κοινωνικής δικτύωσης. Οι όροι χρήσης είναι μια πρόταση προς κατάρτιση διμερούς σύμβασης που μπορεί να χαρακτηριστεί ως πρόταση «πάρε τη ή άφησέ τη» ("take it or leave it proposal"), αφού οι χρήστες δεν χρειάζεται καν να την αποδεχθούν ρητά για να ξεκινήσει η ισχύς της[106]. Επακολούθως, εάν ο χρήστης δεν αποδεχτεί του όρους χρήσης -είτε ρητά, «τικάροντας» το αντίστοιχο κουτάκι πριν την ολοκλήρωση της εγγραφής, είτε σιωπηρά, απλώς διαβάζοντας το σχετικό μήνυμα προτού προχωρήσει στο επόμενο στάδιο- η εμπειρία του στο μέσο κοινωνικής δικτύωσης που έχει επιλέξει θα σταματήσει εκεί[107]. Μέσω των ως άνω συμφωνιών, παρέχεται στα μέσα κοινωνικής δικτύωσης υπέρμετρη εξουσία συλλογής προσωπικών δεδομένων, οδηγώντας στο συμπέρασμα ότι στην πραγματικότητα οι

[104] "Explicit Personal Data", βλ. Κεφάλαιο 2.2.1. της παρούσης

[105] Άρθρο 1 Όρων Χρήσης του Twitter *«Μπορείτε να χρησιμοποιήσετε τις Υπηρεσίες μόνο εάν συμφωνείτε να συνάψετε μια δεσμευτική σύμβαση με το Twitter και δεν είστε άτομο που απαγορεύεται να λαμβάνει υπηρεσίες σύμφωνα με τους νόμους της ισχύουσας δικαιοδοσίας»*, https://twitter.com/en/tos (τελευταία πρόσβαση στις 04.02.2022)

[106] Fiesler C., Beard N. and Keegan B. C. (2020) "No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service", Conference Paper, Proceedings of the Fourteenth International AAAI Conference on Web and Social Media (ICWSM 2020), Volume 14, p. 188, https://ojs.aaai.org/index.php/ICWSM/article/view/7290 (τελευταία πρόσβαση στις 04.02.2022)

[107] Προοίμιο Όρων Χρήσης του Instagram *"Οι παρόντες Όροι χρήσης (ή "Όροι χρήσης") διέπουν την από μέρους σας χρήση του Instagram, με την εξαίρεση των περιπτώσεων όπου αναφέρουμε ρητά ότι ισχύουν ξεχωριστοί (και όχι αυτοί) όροι, και παρέχουν πληροφορίες για την Υπηρεσία του Instagram ("Υπηρεσία"). Όταν δημιουργείτε έναν λογαριασμό στο Instagram ή χρησιμοποιείτε το Instagram, αποδέχεστε τους παρόντες Όρους χρήσης."* (τελευταία πρόσβαση στις 04.02.2022)

συμφωνίες αυτές αποτελούν περισσότερο δεσποτικούς κανόνες για την προστασία συγκεκριμένων επιχειρηματικών μοντέλων[108].

Με την πάροδο του χρόνου επιβεβαιώνεται διαρκώς η σημαντικότερη ανησυχία όσον αφορά τους όρους χρήσης και τις πολιτικές προστασίας δεδομένων - η έκδηλη δηλαδή περιπλοκότητά τους που καταστεί τα κείμενα αυτά δυσανάγνωστα και σε πολλές περιπτώσεις πρακτικώς ακατανόητα. Συχνά μάλιστα, ακόμη και νομικοί, εξειδικευμένοι σε ζητήματα προστασίας της ιδιωτικότητας, ερμηνεύουν διαφορετικά τις έννοιες και τις ρήτρες των κειμένων αυτών. Επιπλέον, πέρα από τη δυσκολία αναγνωσιμότητας, ζητήματα σχεδίασης και παρουσίασης στον χρήστη, όπως οι μακροσκελείς προτάσεις και η μικρή γραμματοσειρά, καθιστούν τις πολιτικές λιγότερο προσιτές στους χρήστες[109]. Για παράδειγμα, στο πλαίσιο μίας ερευνητικής μελέτης, εξετάστηκαν οι όροι χρήσης και οι πολιτικές προστασίας δεδομένων δέκα διαφορετικών μέσων κοινωνικής δικτύωσης. Εκεί διαπιστώθηκε ότι ένα κείμενο όρων χρήσης απαρτίζεται κατά μέσο όρο από 26.320 λέξεις, ενώ μία μέση πολιτική προστασίας δεδομένων από 7.984 λέξεις[110].

Λίγοι έτσι είναι οι χρήστες που διαβάζουν πραγματικά και εξαντλητικά τους όρους χρήσης των μέσων κοινωνικής δικτύωσης· εκείνοι που ανησυχούν περισσότερο για την προστασία της ιδιωτικότητάς τους και ασχολούνται με τα κείμενα αυτά ως μέρος της στρατηγικής τους για τον έλεγχο των προσωπικών τους δεδομένων[111]. Στον αντίποδα, το μεγαλύτερο ποσοστό των χρηστών συχνά αγνοεί τους όρους και τις πολιτικές προστασίας, καθώς αυτά τα έγγραφα παραμένουν μεγάλα, περίπλοκα και απογοητευτικά για τους περισσότερους. Αυτή η συμπεριφορά φαίνεται να είναι κοινή τόσο κατά την εγγραφή σε νέες εφαρμογές όσο και κατά την αλλαγή των πολιτικών των εφαρμογών που χρησιμοποιούν ήδη οι χρήστες. Όταν

---

[108] Rustad M. L. and Koenig T. H. (2014) "Wolves of the world wide web: reforming social networks' contracting practices", Wake Forest Law Review, Volume 49, p. 1431, Suffolk University Law School Research Paper No. 14-25, https://ssrn.com/abstract=2479918 (τελευταία πρόσβαση στις 04.02.2022)

[109] Fiesler C., Beard N. and Keegan B. C. (2020) "No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service", Conference Paper, Proceedings of the Fourteenth International AAAI Conference on Web and Social Media (ICWSM 2020), Volume 14, p. 189, https://ojs.aaai.org/index.php/ICWSM/article/view/7290 (τελευταία πρόσβαση στις 04.02.2022)

[110] Obar J.A. and Hatelt A. (2019) "TL; DR and TC; DU: an assessment of the length and complexity of social media policies", Conference Paper, Association for education in journalism and mass communication Conference, Toronto, ON, Canada

[111] Cain J. A. and Imre I. (2021) "Everybody wants some: Collection and control of personal information, privacy concerns, and social media use", Article in New media & Society, Sage Journals, 1–20, p. 5, DOI: 10.1177/14614448211000327 https://journals.sagepub.com/home/nms (τελευταία πρόσβαση στις 04.02.2022)

διαβάζουν τα κείμενα αυτά, μπορεί να παραμείνουν στις σχετικές σελίδες μόνο για όση ώρα χρειάζεται για να φτάσουν στο κουμπί «αποδοχή», ή απλώς να τα αναγνώσουν διαγωνίως σε πολύ λιγότερο από τον απαιτούμενο χρόνο ανάγνωσης[112,113].

Είναι επομένως πρόδηλη η τάση των χρηστών να αγνοούν τις πολιτικές προστασίας δεδομένων και τους όρους χρήσης όταν δραστηριοποιούνται στα μέσα κοινωνικής δικτύωσης, αφού τα κείμενα αυτά αντιμετωπίζονται ως ανεπιθύμητα εμπόδια για την επίτευξη του σκοπού τους, την απόλαυση δηλαδή των ωφελειών της διαδικτυακής τους παρουσίας[114]. Για πολλούς χρήστες φαντάζει «ταλαιπωρία» η αντιμετώπιση ενός τεράστιου όγκου δυσανάγνωστων κειμένων σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών τους, ιδιαίτερα όταν το μέσο κοινωνικής δικτύωσης βρίσκεται εκεί για να προσφέρει κάτι πολύ πιο ενδιαφέρον[115]. Αυτός, παρ' όλα αυτά, είναι ο σκοπός που λανθάνει πίσω από τις φανταχτερές εφαρμογές κοινωνικής δικτύωσης, οι οποίες έχουν εξ αρχής σχεδιαστεί για να ενθαρρύνουν τους χρήστες να μοιράζονται όσο το δυνατόν περισσότερα προσωπικά τους δεδομένα, παρ' όλο που οι κίνδυνοι είναι εμφανείς· και με την αλματώδη άνθισή τους, εντείνονται συνεχώς οι κοινωνικές και οικονομικές ανησυχίες σχετικά με τον ρόλο που παίζουν στη διευκόλυνση ή την παράκαμψη των διαδικασιών νόμιμης λήψης συγκατάθεσης του χρήστη με σκοπό την προστασία της ιδιωτικής του ζωής.

[112] Obar J.A. and Oeldorf-Hirsch A. (2020) "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services", Information, Communication & Society, Volume 23, No. 1, p. 140, https://doi.org/10.1080/1369118X.2018.1486870 (τελευταία πρόσβαση στις 04.02.2022)

[113] *«Συμφωνώ με αυτούς τους όρους και τις προϋποθέσεις»*, φράση που συχνά χαρακτηρίζεται χιουμοριστικά ως «το μεγαλύτερο ψέμα στο Διαδίκτυο». Βλ. υποσημείωση 112.

[114] Επιβεβαιώνοντας την εφαρμογή της θεωρίας του «παράδοξου της ιδιωτικότητας».

[115] Obar J.A. and Oeldorf-Hirsch A. (2020) "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services", Information, Communication & Society, Volume 23, No. 1, p. 142, https://doi.org/10.1080/1369118X.2018.1486870 (τελευταία πρόσβαση στις 04.02.2022)

ΚΕΦΑΛΑΙΟ 3ο: ΖΗΤΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΥΠΟ ΤΟ ΠΡΙΣΜΑ ΤΟΥ ΚΑΝΟΝΙΣΤΙΚΟΥ ΠΛΑΙΣΙΟΥ ΣΤΗΝ ΕΥΡΩΠΗ

3.1. Οι ρόλοι των εμπλεκόμενων μερών

Η αδιάκοπη εξέλιξη των λειτουργικών συστημάτων των έξυπνων κινητών τηλεφώνων, η συνεχής ανάπτυξη πολλαπλών και πρωτότυπων εφαρμογών, καθώς και ο ιλιγγιώδης πολλαπλασιασμός των μέσων κοινωνικής δικτύωσης, έχουν οδηγήσει σε ολοένα και μεγαλύτερη αύξηση της ανταλλαγής προσωπικών δεδομένων μεταξύ των εφαρμογών, μονοπωλώντας αισθητά το ενδιαφέρον των συμμετεχόντων μερών. Ενώ οι εφαρμογές αυτές καθιστούν εφικτή την κοινή χρήση προσωπικών δεδομένων και την επικοινωνία μεταξύ χρηστών, οι ανησυχίες που σχετίζονται με την προστασία της ιδιωτικότητας των τελευταίων φαίνεται να εντείνονται μέρα με την ημέρα. Δεδομένου ότι υπάρχουν συνεχώς δημοσίως διαθέσιμα στο διαδίκτυο τόσα πολλά προσωπικά δεδομένα, η έννοια της ιδιωτικότητας εξετάζεται από διαφορετικές οπτικές γωνίες ανάλογα με τα συμφέροντα των εμπλεκόμενων μερών, με τη νομιμότητα και τη διαφάνεια της επεξεργασίας των προσωπικών δεδομένων να αποτελεί πλέον μία επίκαιρη πρόκληση[116].

Με σκοπό να διερευνηθούν τα ζητήματα της προστασίας της ιδιωτικότητας που αφορούν τις δραστηριότητες των ατόμων στα μέσα κοινωνικής δικτύωσης μέσω έξυπνων κινητών συσκευών, χρειάζεται να αποσαφηνιστούν οι ρόλοι των εμπλεκομένων μερών στο πλαίσιο του ΓΚΠΔ, ξεκινώντας από τους ίδιους τους χρήστες των εφαρμογών. Οι χρήστες είναι τα άτομα που διαθέτουν ένα λογαριασμό -ή αλλιώς «προφίλ»- σε ένα μέσο κοινωνικής δικτύωσης και εισέρχονται σε αυτό μέσω της συσκευής έξυπνου τηλεφώνου που διαθέτουν. Δεν ενδιαφέρει ιδιαίτερα εάν οι χρήστες εισάγουν το πραγματικό τους όνομα στο προφίλ τους, καθώς η ταυτοποίησή τους βασίζεται κυρίως σε άλλα αναγνωριστικά στοιχεία, όπως συμπεριφορές, αλληλεπιδράσεις και ενδιαφέροντα. Εφόσον είναι φυσικά πρόσωπα που μπορούν να ταυτοποιηθούν, άμεσα ή έμμεσα, οι χρήστες αποτελούν υποκείμενα των δεδομένων, σύμφωνα με το άρθρο 4 περ. 1 του ΓΚΠΔ[117], των οποίων τα προσωπικά δεδομένα χρήζουν προστασίας.

---

[116] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.1, https://hal.archives-ouvertes.fr/hal-00975998 (τελευταία πρόσβαση στις 13.03.2022)

[117] Άρθρο 4 περ. 1 ΓΚΠΔ: "*«δεδομένα προσωπικού χαρακτήρα»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο*

Όσον αφορά τα έξυπνα κινητά τηλέφωνα και τα μέσα κοινωνικής δικτύωσης, ο ΓΚΠΔ δεν περιέχει κάποια συγκεκριμένη διάταξη, αλλά επιβάλλει ένα σύνολο υποχρεώσεων στους υπεύθυνους επεξεργασίας, στις οντότητες δηλαδή που καθορίζουν τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών δεδομένων[118,119]. Λαμβάνοντας υπόψη ότι τα εμπλεκόμενα μέρη διαφοροποιούνται ανάλογα με τις δραστηριότητες του χρήστη, στα υπό εξέταση οικοσυστήματα δεν αναγνωρίζεται μόνο ένας, μοναδικός υπεύθυνος επεξεργασίας, αλλά πολλαπλοί υπεύθυνοι επεξεργασίας συνυπάρχουν, ενεργώντας μόνοι ή από κοινού με τους υπόλοιπους.

Αρχικά, ως υπεύθυνοι επεξεργασίας ενδέχεται να λειτουργούν οι εταιρείες ανάπτυξης και συντήρησης των λειτουργικών συστημάτων που έχουν ενσωματωμένα τα έξυπνα κινητά τηλέφωνα, καθώς και τα εκάστοτε καταστήματα εφαρμογών ("app stores"). Σε πρώτο χρόνο, οι χρήστες παρέχουν τα προσωπικά τους δεδομένα στο λειτουργικό σύστημα για να δημιουργηθεί ένας προσωπικός λογαριασμός, τα οποία δεδομένα έπειτα θα διαβιβαστούν από το σύστημα στο κατάστημα εφαρμογών, με σκοπό να επιτρέψει στον χρήστη την εγκατάσταση μίας εφαρμογής στο κινητό του τηλέφωνο. Εάν οποιοδήποτε λειτουργικό σύστημα χρησιμοποιεί αυτά τα δεδομένα για να βελτιώσει τις δικές του υπηρεσίες, τότε το τελευταίο θα λογίζεται και πάλι ως υπεύθυνος επεξεργασίας, σύμφωνα με τον ορισμό του άρθρου 4 περ. 7 του ΓΚΠΔ. Ομοίως, ένα κατάστημα εφαρμογών θα θεωρείται υπεύθυνος επεξεργασίας προσωπικών δεδομένων όταν διατηρεί σε αρχείο τις εφαρμογές που

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"

[118] Mahieu R., V. Hoboken J., and Asghari H. (2019), "Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe", Journal of Intellectual Property, Information Technology and Electronic Commerce Law, par. 8-9, https://www.jipitec.eu/issues/jipitec-10-1-2019/4879 (τελευταία πρόσβαση στις 13.02.2022)

[119] Άρθρο 4 περ. 7 ΓΚΠΔ: "*«υπεύθυνος επεξεργασίας»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα·…*"

εγκαταστάθηκαν ή αγοράστηκαν στο παρελθόν από τον χρήστη μέσω των διαπιστευτηρίων σύνδεσης ή των αριθμών πιστωτικών καρτών που καταχωρήθηκαν στο κατάστημα[120,121].

Τα μέσα κοινωνικής δικτύωσης, στη συνέχεια, δύναται να έχουν πολλαπλούς ρόλους όσον αφορά την επεξεργασία των προσωπικών δεδομένων των χρηστών. Τις περισσότερες φορές έχουν τον ρόλο του υπεύθυνου επεξεργασίας. Οι πάροχοι των μέσων κοινωνικής δικτύωσης καθορίζουν τις διαφορετικές λειτουργικότητες της εκάστοτε εφαρμογής, συμπεριλαμβανομένου του καθορισμού των δεδομένων που υφίστανται επεξεργασία, του σκοπού και των όρων της επεξεργασίας, καθώς και όλων των βασικών εργαλείων σχετικά με τη διαχείριση των χρηστών, όπως η εγγραφή και η διαγραφή των λογαριασμών τους[122].

Μέσα από τις λειτουργίες αυτές, παρέχονται υπηρεσίες όχι μόνο προς τους χρήστες, αλλά και προς τρίτους, όπως διαφημιστές και άλλους στοχεύοντες φορείς[123], οι οποίοι

---

[120] Bu-Pasha, S., Alen-Savikko, A., Makinen, J., Guinness, R., & Korpisaari, P. (2016), "Eu law perspectives on location data privacy in smartphones and informed consent for transparency", European Data Protection Law Review (EDPL), 2(3), p. 317

[121] Για παράδειγμα, η εταιρεία Google αναπτύσσει ένα από τα δύο πιο διαδεδομένα λειτουργικά συστήματα στον κόσμο, το Λειτουργικό Σύστημα "Android". Για τις υπηρεσίες που προσφέρει στα έξυπνα κινητά τηλέφωνα που διαθέτουν το Android, όπως το κατάστημα εφαρμογών "Google Play Services" και οι εφαρμογές που αναπτύσσονται από την Google, η τελευταία αποτελεί συνήθως τον υπεύθυνο επεξεργασίας των δεδομένων των χρηστών. Αν και στις πολιτικές προστασίας δεδομένων που διαθέτει, η Google αναγράφει ότι ως κατασκευαστής του λειτουργικού συστήματος Android δεν συλλέγει κανένα προσωπικό δεδομένο από τους χρήστες -στο βαθμό που το λειτουργικό εκτελείται αποκλειστικά εντός της φορητής συσκευής (βλ. https://www.android.com/enterprise/data-protection/)- σημειώνεται πως και μόνο το γεγονός της συλλογής δεδομένων σχετικά με τον τύπο του έξυπνου κινητού τηλεφώνου, τη ζώνη ώρας και την τοποθεσία του κατόχου του ανά πάσα στιγμή, προσδίδει στην Google τον ρόλο του υπεύθυνου επεξεργασίας, σύμφωνα με τις διατάξεις του ΓΚΠΔ.

[122] Kosta E., Kalloniatis Ch., Mitrou L. and Gritzalis S. (2010) "Data protection issues pertaining to social networking under EU law", Research Paper, Transforming Government: People, Process and Policy Vol. 4 No. 2, p. 196, Emerald Group Publishing Limited, Transforming Government: People, Process and Policy | Emerald Insight (τελευταία πρόσβαση στις 13.02.2022)

[123] Σύμφωνα με τις Κατευθυντήριες Γραμμές 8/2020 σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης που εξέδωσε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, ως στοχεύων φορέας χαρακτηρίζεται το φυσικό ή το νομικό πρόσωπο που χρησιμοποιεί υπηρεσίες κοινωνικής δικτύωσης με σκοπό να κατευθύνει συγκεκριμένο περιεχόμενο προς συγκεκριμένο κοινό χρηστών, βάσει προσδιορισμένων παραμέτρων και κριτηρίων. Αυτή η επιλογή του σκοπούμενου κοινού σύμφωνα με ορισμένα ενδιαφέροντα ή χαρακτηριστικά είναι που διακρίνει τους στοχεύοντες φορείς από τους υπόλοιπους χρήστες των μέσων κοινωνικής δικτύωσης. Σκοπός της στόχευσης συνήθως είναι η προβολή των φορέων σε μεγαλύτερο κοινό και η αύξηση της αναγνωρισιμότητάς τους, Κατευθυντήριες γραμμές 8/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης Έκδοση 2.0, παρ. 25, διαθέσιμες στο https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_el (τελευταία πρόσβαση στις 01.03.2022)

δραστηριοποιούνται ή συνεργάζονται με το εκάστοτε μέσο κοινωνικής δικτύωσης[124]. Στις τελευταίες αυτές περιπτώσεις, οι πάροχοι αποτελούν εκτελούντες την επεξεργασία για λογαριασμό των τρίτων, σύμφωνα με το άρθρο 4 περ. 8 του ΓΚΠΔ[125]. Πιο συγκεκριμένα, όταν ο εκάστοτε στοχεύων φορέας ορίζει τα κριτήρια της διαφήμισης ή παρέχει ο ίδιος στον πάροχο μία συγκεκριμένη λίστα με στοιχεία πελατών που επιθυμεί να προσεγγίσει, τότε ο πάροχος του μέσου κοινωνικής δικτύωσης λειτουργεί ως εκτελών την επεξεργασία των δεδομένων[126,127].

Ωστόσο, σε κάποιες περιπτώσεις οι ρόλοι των εμπλεκόμενων μερών ενδέχεται να περιπλέκονται περαιτέρω. Η πρόσφατη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) σχετικά με την από κοινού ευθύνη βάσει του ΓΚΠΔ επεκτείνει τη νομική ανάλυση της ευθύνης για την προστασία των προσωπικών δεδομένων από τις εφαρμογές μέσων κοινωνικής δικτύωσης. Καθοδηγούμενο από την ανάγκη για αποτελεσματική και πλήρη προστασία, το ΔΕΕ υιοθετεί μια διασταλτική ερμηνεία της έννοιας της «από κοινού ευθύνης» μεταξύ των μέσων κοινωνικής δικτύωσης και των στοχευόντων φορέων με τους οποίους συνεργάζεται[128]. Συγκεκριμένα, το ΔΕΕ καταλήγει στο συμπέρασμα ότι ο χειριστής μιας σελίδας στο Facebook είναι από κοινού υπεύθυνος επεξεργασίας των προσωπικών δεδομένων των επισκεπτών της σελίδας με το Facebook, παρόλο που η σελίδα αυτή δεν διαθέτει πρόσβαση στα προσωπικά δεδομένα που υφίστανται επεξεργασία[129]. Εφόσον ο

---

[124] Κατευθυντήριες γραμμές 8/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης Έκδοση 2.0, παρ. 21, διαθέσιμες στο https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_el (τελευταία πρόσβαση στις 01.03.2022)

[125] Άρθρο 4 περ. 8 ΓΚΠΔ: "*«εκτελών την επεξεργασία» αποτελεί το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας*"

[126] Επίσης, ως εκτελών την επεξεργασία των δεδομένων λειτουργεί ένα μέσο κοινωνικής δικτύωσης όταν επεξεργάζεται προσωπικά δεδομένα για λογαριασμό ενός στοχεύοντος φορέα με σκοπό τη μέτρηση της απόδοσης ή της απήχησης μίας διαφημιστικής καμπάνιας, ή την παροχή στατιστικών στοιχείων για τους χρήστες που αλληλοεπίδρασαν με τη συγκεκριμένη διαφήμιση.

[127] Η απλή ωστόσο παρουσίαση πληροφοριών σε μία σελίδα μέσου κοινωνικής δικτύωσης, προοριζόμενη σε ευρύτερο κοινό (όπως για παράδειγμα πληροφορίες για το ωράριο λειτουργίας ή την τοποθεσία του καταστήματος), χωρίς προηγούμενη επιλογή του κοινού χρηστών, δεν μπορεί να θεωρηθεί στόχευση.

[128] Υπόθεση C-210/16 Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, Απόφαση της 5ης Ιουνίου 2018, https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=2151335 (τελευταία πρόσβαση στις 13.02.2022)

[129] Κατευθυντήριες γραμμές 8/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης Έκδοση 2.0, παρ. 32-35, διαθέσιμες στο

χειριστής της σελίδας μπορεί να χρησιμοποιήσει τα φίλτρα που παρέχει το Facebook για τον καθορισμό των κριτηρίων βάσει των οποίων θα συλλέγονται τα προσωπικά δεδομένα από το Facebook για την εξαγωγή στατιστικών, συμμετέχει και αυτός ενεργά στον καθορισμό των σκοπών επεξεργασίας των προσωπικών δεδομένων[130]. Το ΔΕΕ διευκρινίζει επιπροσθέτως ότι τα εν λόγω μέρη ενδέχεται να εμπλέκονται σε διαφορετικά στάδια της επεξεργασίας και σε διαφορετικό βαθμό, με αποτέλεσμα το επίπεδο της ευθύνης του καθένα να εκτιμάται λαμβάνοντας υπόψιν όλα τα επιμέρους κρίσιμα περιστατικά[131]. Ομοίως, στη σχετική υπόθεση Fashion ID[132], το ΔΕΕ έκρινε ότι μία ιστοσελίδα που ενσωματώνει ένα "plugin" («πρόσθετο»), εν προκειμένω το κουμπί «Μου αρέσει» του Facebook, για την επεξεργασία προσωπικών δεδομένων από ένα τρίτο μέρος[133], βάσει του ΓΚΠΔ θεωρείται από κοινού υπεύθυνος επεξεργασίας με το τρίτο μέρος, δηλαδή με το Facebook[134].

Συνεπώς, η υποχρέωση της αποτελεσματικής εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων ήδη από το σχεδιασμό και εξ ορισμού που επιβάλλει το άρθρο 25 του ΓΚΠΔ εφαρμόζεται σε όλα τα εμπλεκόμενα μέρη που αναλαμβάνουν τον ρόλο του υπεύθυνου επεξεργασίας στα μέσα κοινωνικής δικτύωσης εντός των οικοσυστημάτων έξυπνων κινητών τηλεφώνων[135]. Παράλληλα, μετά την πρόσφατη νομολογία του ΔΕΕ περί

---

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_el (τελευταία πρόσβαση στις 01.03.2022)

[130] Υπόθεση C-210/16 Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, Απόφαση της 5ης Ιουνίου 2018, σκέψη 39.

[131] Υπόθεση C-210/16 Wirtschaftsakademie Schleswig-Holstein, EU:C:2018:388, Απόφαση της 5ης Ιουνίου 2018, σκέψη 43.

[132] Υπόθεση C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629, Απόφαση της 29ης Ιουλίου 2019, https://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&doclang=EL (τελευταία πρόσβαση στις 13.02.2022)

[133] Συγκεκριμένα, όταν ένας χρήστης επισκεπτόταν την ιστοσελίδα της Fashion ID διαβιβάζονταν στο Facebook πληροφορίες αναφορικά με τη διεύθυνση πρωτοκόλλου διαδικτύου (IP address) και τη συμβολοσειρά φυλλομετρητή (browser string) αυτού του χρήστη.

[134] Βάσει του άρθρου 26 παρ. 1 ΓΚΠΔ, στην περίπτωση αυτή, οι από κοινού υπεύθυνοι επεξεργασίας υποχρεούνται να καταρτίσουν συμφωνία, όπου θα καθορίζονται ρητά και διαφανώς οι αντίστοιχες ευθύνες των μερών για τη συμμόρφωσή τους με τις απαιτήσεις του ΓΚΠΔ «*ιδίως όσον αφορά την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και τα αντίστοιχα καθήκοντά τους για να παρέχουν τις πληροφορίες που αναφέρονται στα άρθρα 13 και 14*».

[135] Βλ. και Αιτιολογική Σκέψη 78 του ΓΚΠΔ: «*Κατά την ανάπτυξη, τον σχεδιασμό, την επιλογή και τη χρήση εφαρμογών, υπηρεσιών και προϊόντων που βασίζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για την εκπλήρωση του έργου τους, οι παραγωγοί προϊόντων, υπηρεσιών και εφαρμογών θα πρέπει να ενθαρρύνονται να λαμβάνουν υπόψη τους το δικαίωμα προστασίας των δεδομένων, κατά την ανάπτυξη και τον σχεδιασμό τέτοιων προϊόντων, υπηρεσιών και εφαρμογών, ώστε, λαμβανομένων υπόψη των τελευταίων εξελίξεων, να διασφαλίζεται*

από κοινού ευθύνης για την επεξεργασία των προσωπικών δεδομένων των χρηστών, τα μέσα κοινωνικής δικτύωσης αλλά και οι στοχεύοντες φορείς βαρύνονται με περισσότερες υποχρεώσεις, με στόχο τη διασφάλιση της νόμιμης, δίκαιης και διαφανούς επεξεργασίας των προσωπικών δεδομένων.

3.2. Διαφάνεια κατά την επεξεργασία των προσωπικών δεδομένων των χρηστών

Ο διαδραστικός χαρακτήρας και η αμεσότητα της επικοινωνίας που προσφέρουν τα μέσα κοινωνικής δικτύωσης, σε συνδυασμό με την ευκολία πρόσβασης που παρέχουν τα έξυπνα κινητά τηλέφωνα, έχει καταστήσει τη ζωή των χρηστών πιο διαφανή από ποτέ[136]. Όσο περισσότερο οι χρήστες απολαμβάνουν τη δυνατότητα να μοιράζονται τις ιδέες και τα ενδιαφέροντά τους στο διαδίκτυο ή να κάνουν νέες γνωριμίες, παρέχοντας με ποικίλους τρόπους τα προσωπικά τους δεδομένα στις εκάστοτε εφαρμογές, τόσο πιο διαφανής χρειάζεται να καταστεί ο τρόπος με τον οποίο τα εμπλεκόμενα μέρη επεξεργάζονται αυτά τα δεδομένα.

Η έννοια της διαφάνειας θα μπορούσε να χαρακτηριστεί ως μία εύλογη προσδοκία του χρήστη σχετικά με την ύπαρξη μέτρων που στοχεύον στη διασφάλιση της ιδιωτικότητάς του. Εν προκειμένω όμως, η έννοια αυτή αναφέρεται στη σαφή και ανοιχτή αποκάλυψη των πρακτικών συλλογής προσωπικών δεδομένων του χρήστη, της εν γένει επεξεργασίας τους, της ποιότητας και των ορίων αυτής[137].

Έτσι, σύμφωνα με το άρθρο 5 παρ.1 στ. α' του ΓΚΠΔ, τα προσωπικά δεδομένα «*υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων*», ενώ σύμφωνα με το στ. β' του ίδιου άρθρου, τα προσωπικά δεδομένα συλλέγονται μόνο για «*καθορισμένους, ρητούς και νόμιμους σκοπούς*». Επιπρόσθετα, με βάση την αρχή της διαφάνειας, η οποία καθιερώνεται στα άρθρα 12-14 του ΓΚΠΔ, τα φυσικά πρόσωπα χρειάζεται να ενημερώνονται αναφορικά με την επεξεργασία των προσωπικών τους δεδομένων με σαφήνεια και ακρίβεια, ενώ η ενημέρωση αυτή πρέπει να είναι συνοπτική, διαφανής και κατανοητή, εύκολα προσβάσιμη και σε απλή γλώσσα

ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων.»

[136] Zhang N., Wang Ch. And Xu Y. (2011), "Privacy in Online Social Networks", Completed Research Paper, Thirty Second International Conference on Information Systems, Shanghai 2011, p.2, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.8584&rep=rep1&type=pdf (τελευταία πρόσβαση στις 18.02.2022)

[137] Gkoulalas - Divanis A., and Bettini Cl. (2018) "Handbook of Mobile Data Privacy", Springer Nature Switzerland AG 2018, p. 201

διατυπωμένη και, κατά περιπτώσεις, απεικονισμένη[138,139]. Σκοπός της είναι να διασφαλίζει ότι η επεξεργασία προσωπικών δεδομένων που λαμβάνει χώρα ανά περίπτωση, μπορεί να γίνει κατανοητή ανά πάσα στιγμή, καθώς και ότι οι πληροφορίες για την επεξεργασία πρέπει να είναι διαθέσιμες πριν, κατά τη διάρκεια και μετά την πραγματοποίηση της επεξεργασίας. Επομένως, η διαφάνεια χρειάζεται να καλύπτει όχι μόνο την επεξεργασία σε πραγματικό χρόνο, αλλά και την προγραμματισμένη επεξεργασία (εκ των προτέρων διαφάνεια ή "ex-ante transparency") και τον χρόνο μετά την πραγματοποίηση της επεξεργασίας (εκ των υστέρων διαφάνεια ή "ex-post transparency")[140]. Πιθανοί μηχανισμοί για την επίτευξη της διαφάνειας αποτελούν η καταγραφή και η αναφορά των παραπάνω πληροφοριών σε κάποιο εσωτερικό σύστημα του υπεύθυνου επεξεργασίας, οι πολιτικές προστασίας δεδομένων, καθώς και απευθείας ειδοποιήσεις προς τα υποκείμενα των δεδομένων[141].

Όσον αφορά ιδιαίτερα τα έξυπνα κινητά τηλέφωνα και τις εφαρμογές που έχουν αναπτυχθεί για να λειτουργούν σε αυτά, οι παραπάνω πληροφορίες αντανακλώνται κυρίως μέσω των πολιτικών «απορρήτου» ή «προστασίας προσωπικών δεδομένων» που παρέχονται από τους κατασκευαστές των λειτουργικών συστημάτων και τους παρόχους εφαρμογών[142]. Η παρουσία μιας τέτοιας πολιτικής που περιγράφει την έκταση και τους σκοπούς της επεξεργασίας των προσωπικών δεδομένων του χρήστη συμβάλλει στην απαραίτητη διαφάνεια[143], αφού παρατηρείται πως οι χρήστες τείνουν να έχουν ισχυρότερη αίσθηση

---

[138] Βλ. και Αιτιολογική Σκέψη 58 του ΓΚΠΔ

[139] Σε κάθε περίπτωση, ο υπεύθυνος επεξεργασίας χρειάζεται να ενημερώνει τον χρήστη σχετικά με την ταυτότητά του και τα στοιχεία επικοινωνίας του, τον σκοπό επεξεργασίας, τους αποδέκτες των δεδομένων, το χρονικό διάστημα αποθήκευσής τους, τα δικαιώματά του, τη νομική βάση επεξεργασίας των δεδομένων του και την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, σύμφωνα με τις διατάξεις του άρθρου 13 ΓΚΠΔ.

[140] Castelluccia C., Guerses S., Hansen M., Hoepman J. H., van Hoboken J., and Vieira B. (2017), "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", ENISA, the European Union Agency for Network and Information Security, p. 48, https://doi.org/10.2824/114584 (τελευταία πρόσβαση στις 18.02.2022)

[141] Βλ. υποσημείωση 140.

[142] Σύμφωνα με τις οδηγίες της Ομάδας Εργασίας του άρθρου 29 μάλιστα, οι πολιτικές προστασίας δεδομένων των εκάστοτε εφαρμογών που συμπεριλαμβάνονται στα καταστήματα εφαρμογών θα πρέπει να είναι διαθέσιμες στον χρήστη πριν από τη λήψη και εγκατάσταση της εφαρμογής, προκειμένου να είναι έγκαιρα ενημερωμένος. Art 29 WP, 'Guidelines on Transparency under Regulation 2016/679' (2018) WP260, rev.01, https://ec.europa.eu/newsroom/article29/items/622227 (τελευταία πρόσβαση στις 18.02.2022)

[143] Tang J., Zhang B., and Akram U. (2021), "What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management", Information 2021, 12, 311, p. 4, https://doi.org/10.3390/info12080311 (τελευταία πρόσβαση στις 20.12.2021)

ελέγχου του απορρήτου τους όταν αντιλαμβάνονται ότι η πολιτική απορρήτου των εφαρμογών είναι συνοπτική, σαφής και κατανοητή[144]. Επιπλέον, εάν η εν λόγω πολιτική καθορίζει επακριβώς τα προσωπικά δεδομένα που συλλέγονται, τον τρόπο με τον οποίο αξιοποιούνται ή σε ποιους ενδεχομένως διαβιβάζονται, οι αντιληπτοί κίνδυνοι των χρηστών μειώνονται, ενισχύοντας την πεποίθησή τους για ασφάλεια της ιδιωτικότητάς τους[145].

Παρ' όλη την ύπαρξη τέτοιων πολιτικών από κατασκευαστές λειτουργικών και παρόχους μέσων κοινωνικής δικτύωσης, εξακολουθεί να υφίσταται ασάφεια ως προς τη φύση, τον χρόνο, τον σκοπό ή τα μέσα της επεξεργασίας δεδομένων. Είναι γεγονός ότι οι περισσότεροι χρήστες μέσων κοινωνικής δικτύωσης μέσω έξυπνων κινητών τηλεφώνων δεν είναι επαρκώς ενημερωμένοι σχετικά με την ταυτότητα του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία, τους αποδέκτες των δεδομένων τους, καθώς και την έκταση και τον σκοπό της επεξεργασίας των δεδομένων. Λίγοι είναι οι χρήστες που διαβάζουν διεξοδικά τις πολιτικές προστασίας των εφαρμογών και των κινητών τους, ενώ ακόμη λιγότεροι αυτοί που κατανοούν πραγματικά τα περίπλοκα έγγραφα πριν εγκαταστήσουν τις εκάστοτε εφαρμογές στις συσκευές τους[146]. Επιπλέον, δεν είναι σπάνιο οι εταιρείες να τροποποιούν συχνά τα κείμενα των πολιτικών προστασίας προσωπικών δεδομένων που διαθέτουν, προκειμένου να προσθέσουν άλλους σκοπούς επεξεργασίας, όπως η διαβίβαση δεδομένων για άλλους -όχι απαραίτητα συναφείς- σκοπούς. Ακόμη κι αν κοινοποιηθεί η αλλαγή της πολιτικής στον χρήστη, είναι σχεδόν βέβαιο ότι δεν θα δοθεί η απαραίτητη προσοχή, αφού ο πρωταρχικός στόχος του χρήστη είναι να συνεχίσει να χρησιμοποιεί απρόσκοπτα την εφαρμογή που έχει επιλέξει. Η πρακτική του "clickwrap" αποδεικνύει την παραπάνω συμπεριφορά. Η συμφωνία clickwrap (ή αλλιώς "click accept") αποτελεί μια ψηφιακή προτροπή προς τους χρήστες να συμφωνήσουν ή να αποδεχτούν εύκολα και γρήγορα τις πολιτικές ή τους όρους χρήσης μίας εφαρμογής, όπως ένα μέσο κοινωνικής δικτύωσης, χωρίς την υποχρέωση ανάγνωσης του περιεχομένου αυτών των εγγράφων[147].

---

[144] Li H.,Sarathy R., and Xu H. (2011), "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors", Decision Support Systems, Volume 51, Issue 3, Pages 434-445, https://doi.org/10.1016/j.dss.2011.01.017 (τελευταία πρόσβαση στις 18.02.2022)

[145] Libaque-Sáenz C.F.; Wong, S.F., Chang, Y., and Bravo, E.R. (2020) "The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps", Information and Management, Volume 58, 103284, https://doi.org/10.1016/j.im.2020.103284 (τελευταία πρόσβαση στις 18.02.2022)

[146] «Το παράδοξο της ιδιωτικότητας», Βλ. Κεφ. 2.2.2. της παρούσης.

[147] Συνήθης φράση clickwrap που χρησιμοποιείται: «*Δημιουργώντας τον λογαριασμό σας, συμφωνείτε με την Πολιτική Προστασίας Προσωπικών Δεδομένων και τους Όρους Χρήσης της Εφαρμογής*». Εν

Επειδή απαιτείται μία απλή, θετική ενέργεια από τον χρήστη, ένα δηλαδή και μόνο κλικ, το clickwrap είναι η πιο συχνά χρησιμοποιούμενη πρακτική από τις εταιρείες λειτουργικών συστημάτων ή τους παρόχους των μέσων κοινωνικής δικτύωσης. Ο ρόλος των clickwraps είναι να τροφοδοτούν την επιθυμία του χρήστη για την ψηφιακή του αλληλεπίδρασή και τη δημιουργία περιεχομένου όσο το δυνατόν πιο γρήγορα, διευκολύνοντας παράλληλα τις διαδικασίες συλλογής και αποθήκευσης των προσωπικών δεδομένων του χρήστη[148].

Είναι έτσι φανερό ότι, στα οικοσυστήματα έξυπνων κινητών τηλεφώνων, όπου λειτουργούν εφαρμογές μέσων κοινωνικής δικτύωσης, η ανάγκη για διαφάνεια και λογοδοσία των εταιρειών και των παρόχων είναι πλέον απαράμιλλης σημασίας.

3.3. Η συγκατάθεση των χρηστών

Ο ΓΚΠΔ στοχεύει στην καθιέρωση εντονότερου ελέγχου των πολιτών της Ε.Ε. στα προσωπικά τους δεδομένα, μεταξύ άλλων και στις διαδικασίες συγκατάθεσης. Στο άρθρο 4 περ. 11 του ΓΚΠΔ ως συγκατάθεση ορίζεται *«κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη*[149]*, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν».* Επιπλέον, στην αιτιολογική σκέψη του ΓΚΠΔ αναφέρεται ρητά πως η συγκατάθεση θα πρέπει να παρέχεται με σαφή και θετική ενέργεια, η οποία μπορεί να περιλαμβάνει τη συμπλήρωση τετραγωνιδίου κατά την επίσκεψη σε μία διαδικτυακή ιστοσελίδα (τα λεγόμενα "tickboxes"), την ελεύθερη επιλογή τεχνικών ρυθμίσεων από τον χρήστη, ακόμη και τη σαφή δήλωση του τελευταίου ότι αποδέχεται την επεξεργασία των προσωπικών του δεδομένων[150]. Σε κάθε περίπτωση, ο μηχανισμός λήψης συγκατάθεσης δεν θα πρέπει *«να διαταράσσει αδικαιολόγητα τη χρήση της υπηρεσίας για την οποία παρέχεται*[151]*»*. Επιπλέον, η συγκατάθεση, αφού δοθεί, δεν θα πρέπει να θεωρείται δεδομένη επ' αόριστον. Τα

προκειμένω ο χρήστης αποδέχεται την πολιτική και τους όρους χρήσης ταυτόχρονα με την ολοκλήρωση μίας άλλης ενέργειας.

[148] https://ironcladapp.com/journal/contract-management/what-is-a-clickwrap-agreement/ (τελευταία πρόσβαση στις 19.02.2022)

[149] Διορθωτικό στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης L 119 της 4ης Μαΐου 2016)

[150] Γίνεται αντιληπτό έτσι ότι πρακτικές όπως το "clickwrap" είναι αποδεκτές υπό προϋποθέσεις.

[151] Βλ. και Αιτιολογική Σκέψη 32 του ΓΚΠΔ

υποκείμενα των δεδομένων χρειάζεται να μπορούν να ανακαλέσουν τη συγκατάθεσή τους με εύκολο και γρήγορο τρόπο ανά πάσα στιγμή (Άρθρο 7 παρ. 3 ΓΚΠΔ) και να ζητήσουν την οριστική διαγραφή τω προηγούμενων δεδομένων που είχαν συλλεγεί στη βάση της συγκατάθεσής τους.

Όπως αναφέρθηκε παραπάνω[152], τα προσωπικά δεδομένα των χρηστών συλλέγονται από τους εκάστοτε υπεύθυνους επεξεργασίας στη νομική βάση της εκτέλεσης της διμερούς σύμβασης μεταξύ του χρήστη και της εταιρείας που παρέχει το λειτουργικό σύστημα στο έξυπνο κινητό του ή του μέσου κοινωνικής δικτύωσης που έχει επιλέξει, αλλά και της εκπλήρωσης των σκοπών των εννόμων συμφερόντων που επιδιώκει ο εκάστοτε υπεύθυνος επεξεργασίας. Οι πληροφορίες αυτές περιγράφονται στις πολιτικές προστασίας προσωπικών δεδομένων που έχουν καταρτιστεί, με τις οποίες όμως ο χρήστης συμφωνεί συνήθως χωρίς να έχει κατανοήσει ή έστω αναγνώσει. Στις πολιτικές προστασίας αναγράφεται ότι ο χρήστης με την αποδοχή του, παρέχει τη συγκατάθεσή του σε μια εφαρμογή να έχει πρόσβαση σε ορισμένα από τα αρχεία ή τα προσωπικά του δεδομένα, παρ' όλο που αυτή δεν παρέχεται ρητά. Η συγκεκριμένη πρακτική δίνει ώθηση στις εταιρείες και τους παρόχους να εκμεταλλεύονται τα προσωπικά δεδομένα του χρήστη απεριορίστως υπό τον μανδύα της γενικής συγκατάθεσης.

Στις υπό εξέταση περιστάσεις, η συγκατάθεση για τη συλλογή των προσωπικών δεδομένων του χρήστη θα έπρεπε να αφορά μόνο μία συγκεκριμένη ενέργεια, χωρίς να αποτελεί το γενικό «πράσινο σήμα»[153] για την μετέπειτα απεριόριστη εκμετάλλευση δεδομένων[154]. Ωστόσο, οι εκάστοτε υπεύθυνοι επεξεργασίας χρησιμοποιούν την άδεια αυτή για την εκπλήρωση σκοπών, διαφορετικών από τους σκοπούς της αρχικής συλλογής των δεδομένων του χρήστη. Για αυτό, αξίζει να εξεταστούν αναλυτικότερα ορισμένα είδη επεξεργασιών προσωπικών δεδομένων που απαιτούν τη ρητή συγκατάθεση του χρήστη των μέσων κοινωνικής δικτύωσης, εντός των οικοσυστημάτων έξυπνων κινητών τηλεφώνων.

---

[152] Βλ. Κεφάλαιο 2.3. της παρούσης.

[153] Rewaria S. (2021), "Data Privacy In Social Media Platform: Issues And Challenges", p.26, http://dx.doi.org/10.2139/ssrn.3793386 (τελευταία πρόσβαση στις 20.02.2022)

[154] Για παράδειγμα, οι χρήστες συχνά επιτρέπουν στο λειτουργικό σύστημα του τηλεφώνου τους να αποκτήσει πρόσβαση στην τρέχουσα τοποθεσία τους για την παροχή μίας υπηρεσίας GPS σε πραγματικό χρόνο. Η εν λόγω συγκατάθεση θα πρέπει να αφορά μόνο τη συγκεκριμένη ενέργεια και όχι την περαιτέρω αποθήκευση της τοποθεσίας στους διακομιστές του λειτουργικού για μελλοντική χρήση.

3.3.1. Συγκατάθεση για τη συλλογή δεδομένων θέσης

Η αξιοποίηση των δεδομένων θέσης έχει λάβει σπουδαίες διαστάσεις λόγω της δημοτικότητας των υπηρεσιών που προσφέρουν τα μέσα κοινωνικής δικτύωσης, βασιζόμενα στη συλλογή δεδομένων θέσης των χρηστών. Για παράδειγμα, η γεωγραφική σήμανση ("geotagging") αποτελεί ένα διαδεδομένο τρόπο επισύναψης πληροφοριών τοποθεσίας των χρηστών στο περιεχόμενο που μοιράζονται στα μέσα κοινωνικής δικτύωσης, όπως σε φωτογραφίες ή αναρτήσεις κειμένου[155]. Η σήμανση αυτή μπορεί να πραγματοποιηθεί είτε από την ίδια την συσκευή έξυπνου κινητού τηλεφώνου κατά τη στιγμή της ανάρτησης (αυτόματα και χωρίς την παρέμβαση του χρήστη), είτε να προστεθεί χειροκίνητα σε μεταγενέστερο χρόνο, μέσω εργαλείων που προσφέρονται[156].

Παρέχοντας διαφορετικές δυνατότητες στον χρήστη, όπως η προσθήκη γεωγραφικής σήμανσης στις φωτογραφίες του ή η κοινοποίηση της τοποθεσίας του σε πραγματικό χρόνο με τη χρήση GPS, τα μέσα κοινωνικής δικτύωσης μπορούν να συγκεντρώσουν πλήθος προσωπικών δεδομένων σχετικών με την ιδιωτική ζωή του χρήστη, φτάνοντας ακόμη και στην κατάρτιση προφίλ είτε από τα ίδια τα μέσα, είτε από τρίτα μέσα στα οποία η τοποθεσία θα διαβιβαστεί. Μάλιστα, πολλές φορές, οι εφαρμογές αυτές ζητούν τη συγκατάθεση του χρήστη για τη συλλογή της τοποθεσίας του ακόμη κι αν αυτή δεν σχετίζεται με την κύρια υπηρεσία που η εφαρμογή παρέχει, ενημερώνοντάς τον μάλιστα ότι αυτή ενδέχεται να αξιοποιηθεί και για σκοπούς διαφήμισης[157]. Ωστόσο, η συγκατάθεση αυτή δεν μπορεί να θεωρηθεί νόμιμη, αφού δεν παρέχονται οι απαραίτητες πληροφορίες στον χρήστη και δημιουργείται η εντύπωση πως η χρήση της υπηρεσίας χωρίς την αποκάλυψη της τοποθεσίας είναι αδύνατη.

Για τη διασφάλιση της ελευθερίας της συγκατάθεσης του χρήστη, οι αρχικές ρυθμίσεις της εφαρμογής στο λειτουργικό σύστημα του έξυπνου κινητού τηλεφώνου χρειάζεται εξ

---

[155] Bilogrevic Ig. (2018), "Privacy in Geospatial Applications and Location-Based Social Networks", Chapter 8, in Gkoulalas-Divanis A., and Bettini Cl. (2018) "Handbook of Mobile Data Privacy", Springer Nature Switzerland AG 2018, p. 240

[156] Παράσχης Σπ. (2012), «Κοινωνικά Δίκτυα μέσω φορητών συσκευών: Η προστασία της θέσης», Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς, σελ. 18, διαθέσιμη στο https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4926/Paraschis.pdf?sequence=2&isAllowed=y (τελευταία πρόσβαση στις 20.02.2022)

[157] Κατευθυντήριες γραμμές 5/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, σελ. 8, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_el.pdf (τελευταία πρόσβαση στις 20.02.2022)

ορισμού και από τον σχεδιασμό να παρέχουν στον χρήση την επιλογή να αποδεχτεί ή να απορρίψει τη συλλογή της τοποθεσίας του[158]. Η μη παροχή οποιασδήποτε άλλης επιλογής εκτός της αποδοχής των όρων για την αυτόματη συλλογή δεδομένων θέσης κρίνεται απολύτως ασύμβατη με τις διατάξεις του ΓΚΠΔ. Λόγω της ιδιαίτερης φύσης των δεδομένων θέσης, είναι αναγκαίο να ζητείται ξεχωριστή συγκατάθεση από τον χρήστη, διακριτή από την εν γένει αποδοχή των όρων χρήσης και της πολιτικής απορρήτου της εφαρμογής, ενώ στα κείμενα αυτά κρίνεται απαραίτητη η σαφής αναφορά των δεδομένων θέσης που ενδέχεται να συλλεγούν με ευδιάκριτο και σαφή τρόπο[159]. Επιπλέον, κρίσιμη κρίνεται η ξεχωριστή λήψη συγκατάθεσης για την αποκάλυψη της τοποθεσίας των χρηστών σε τρίτους χρήστες, καθώς και η περιοδική αίτηση για ανανέωσή της.

3.3.2. Συγκατάθεση για την εγκατάσταση cookies

Όταν ένας χρήστης κατεβάζει και εγκαθιστά για πρώτη φορά μια εφαρμογή στο έξυπνο κινητό του τηλέφωνο, ένα αναδυόμενο παράθυρο εμφανίζεται, το οποίο ζητάει τη συγκατάθεση του χρήστη για την εγκατάσταση cookies στη συσκευή του. Ανάλογα με τις προτιμήσεις του, ο χρήστης μπορεί είτε να τα αποδεχτεί είτε να τα απορρίψει, εκτός από ορισμένες φορές που η επιλογή αυτή δεν παρέχεται λόγω της αναγκαιότητας των cookies για τη λειτουργία της εφαρμογής.

Τα cookies είναι μικρά αρχεία κειμένου που αποστέλλονται και αποθηκεύονται στην εκάστοτε συσκευή κάθε φορά που ο χρήστης χρησιμοποιεί μία εφαρμογή. Από μόνα τους, τα cookies είναι αβλαβή, παρέχουν διευκολύνσεις και εξυπηρετούν κρίσιμες λειτουργίες για τις εφαρμογές. Ωστόσο, έχουν τη δυνατότητα να αποθηκεύσουν πλήθος προσωπικών δεδομένων, αρκετά για να ταυτοποιήσουν τον χρήστη της εφαρμογής χωρίς τη συγκατάθεσή του. Λόγω αυτού του χαρακτηριστικού, τα cookies αποτελούν ένα από τα βασικότερα εργαλεία των διαφημιστών και άλλων στοχευόντων φορέων για την παρακολούθηση της διαδικτυακής δραστηριότητας του εκάστοτε χρήση, ώστε να μπορούν να προτείνουν συγκεκριμένες και ελκυστικές διαφημίσεις. Δεδομένου του όγκου των προσωπικών δεδομένων που ενδεχομένως περιέχονται στα cookies και αρκούν για να ταυτοποιήσουν ένα

[158] Άρθρο 25 παρ.2 ΓΚΠΔ.

[159] Bu-Pasha, S., Alen-Savikko, A., Makinen, J., Guinness, R., & Korpisaari, P. (2016), "Eu law perspectives on location data privacy in smartphones and informed consent for transparency", European Data Protection Law Review (EDPL), 2(3), p. 320-321

φυσικό πρόσωπο, θεωρούνται προσωπικά δεδομένα και, επομένως, υπόκεινται στις απαιτήσεις του ΓΚΠΔ[160,161].

Οι υπεύθυνοι επεξεργασίας βασίζουν την επεξεργασία των προσωπικών δεδομένων των χρηστών είτε στη συγκατάθεση που λαμβάνουν είτε στα έννομα συμφέροντά τους[162]. Ωστόσο, στις 2 Φεβρουαρίου του 2022 η Βελγική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με την απόφαση 21/2022[163] «τάραξε τα νερά» όσον αφορά τα έννομα συμφέροντα των εταιρειών που χρησιμοποιούν cookies, διαπιστώνοντας ότι το «Πλαίσιο Διαφάνειας και Συναίνεσης» ("Transparency and Consent Framework" - "TCF") -ένα εργαλείο ανοιχτού κώδικα του Interactive Advertising Bureau Europe ("IAB")[164],που επιτρέπει στις ιστοσελίδες, τις εφαρμογές και τους στοχεύοντες φορείς να συλλέγουν και να καταγράφουν τις προτιμήσεις των χρηστών για διαφημιστικούς σκοπούς[165]- παραβιάζει πλήθος απαιτήσεων του ΓΚΠΔ. Στην πράξη, το TCF αποθηκεύει τις προτιμήσεις του χρήστη δημιουργώντας σειρές χαρακτήρων ("coded character strings") που λειτουργούν ως ψηφιακό σήμα, το οποίο αποστέλλεται μαζί με άλλα δεδομένα του χρήστη στους διαφημιστές για να προβάλουν εξειδικευμένο περιεχόμενο[166]. Οι χρήστες των ιστοσελίδων που χρησιμοποιούσαν το εργαλείο TCF δεν διέθεταν το δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων τους, δεν είχαν την επιλογή να απορρίψουν τα cookies, ούτε και ενημερώνονταν για την εγκατάστασή τους στη συσκευή τους. Η Βελγική Αρχή Προστασίας συμπέρανε ότι το έννομο συμφέρον δεν μπορεί να αξιοποιηθεί ως νομική βάση για τη συμμετοχή στο TCF με την

---

[160] https://gdpr.eu/cookies/, https://cookies.insites.com/ (τελευταία πρόσβαση στις 20.02.2022)

[161] Αιτιολογική Σκέψη 30 του ΓΚΠΔ.

[162] Για παράδειγμα, τα λειτουργικά cookies δεν δύναται να απορριφθούν, καθώς είναι απαραίτητα για τη σωστή λειτουργία μίας εφαρμογής. Επομένως, νομική βάση αποτελεί το έννομο συμφέρον του υπεύθυνου επεξεργασίας και δεν απαιτείται η λήψη της συγκατάθεσης από τον χρήστη.

[163] Decision on the merits 21/2022 of 2 February 2022, Case number: DOS-2019-01377 https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf#page111 (τελευταία πρόσβαση στις 20.02.2022)

[164] Το IAB Ευρώπης είναι μία ομοσπονδία που εκπροσωπεί σε ευρωπαϊκό επίπεδο τον κλάδο του μάρκετινγκ και της ψηφιακής διαφήμισης. https://iabeurope.eu/about-us/ (τελευταία πρόσβαση στις 20.02.2022)

[165] https://support.google.com/analytics/answer/10022331?hl=el (τελευταία πρόσβαση στις 20.02.2022)

[166] Ως προς του ρόλους των εμπλεκόμενων μερών, η Βελγική Αρχή διαπίστωσε ότι το IAB, μαζί με τους διαφημιστές, τις πλατφόρμες διαχείρισης συγκατάθεσης και τους παρόχους ιστοσελίδων, αποτελούν από κοινού υπεύθυνους επεξεργασίας των δεδομένων των χρηστών, αναφορικά με τη συλλογή και τη διάδοση των προτιμήσεων, των εναντιώσεων, καθώς και τη συγκατάθεση των χρηστών για την επεξεργασία των δεδομένων τους, καθώς όχι μόνο οι αποφάσεις τους είναι συμπληρωματικές με αυτές του IAB, ασκούν επίσης επιρροή στον καθορισμό του σκοπού και των μέσων επεξεργασίας των δεδομένων. https://www.lawspot.gr/nomika-blogs/stergios_konstantinoy/velgiki-apdph-horis-nomimi-vasi-oi-diadiktyakes-diafimiseis?lspt_destination=upgrade#_ftn6 (τελευταία πρόσβαση στις 20.02.2022)

τρέχουσα μορφή του, καθώς τα έννομα συμφέροντα των οργανισμών που συμμετέχουν στο TCF αντισταθμίζονται από τα συμφέροντα των υποκειμένων των δεδομένων[167]. Η απόφαση επομένως θέτει την έγκυρη συγκατάθεση ως τη μόνη λειτουργική νομική βάση για την επεξεργασία προσωπικών δεδομένων στο πλαίσιο του άμεσου μάρκετινγκ και της συμπεριφορικής διαφήμισης, αναγκάζοντας πλέον όλα τα εμπλεκόμενα μέρη να επανεξετάσουν τις πρακτικές συλλογής δεδομένων μέσω της εγκατάστασης cookies.

Εκτός από τις ρυθμιστικές διατάξεις του ΓΚΠΔ αναφορικά με τη συγκατάθεση των χρηστών των μέσων κοινωνικής δικτύωσης σε οικοσυστήματα έξυπνων κινητών τηλεφώνων, έπειτα από πολλά χρόνια διαπραγματεύσεων[168], τα κράτη-μέλη της Ε.Ε. έφτασαν σε συμφωνία επί της διαπραγματευτικής εντολής για αναθεωρημένους κανόνες σχετικά με την προστασία της ιδιωτικής ζωής και του απορρήτου κατά τη χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών· στο γνωστό ως «σχέδιο Κανονισμού ePrivacy»[169], το οποίο πρόκειται να εξειδικεύει και να συμπληρώνει τον ΓΚΠΔ.

Ο προτεινόμενος Κανονισμός ePrivacy περιέχει διατάξεις που απαιτούν από τις εφαρμογές και τους παρόχους μέσων κοινωνικής δικτύωσης ως μέσα ηλεκτρονικής επικοινωνίας να διασφαλίζουν κατάλληλες ρυθμίσεις ιδιωτικότητας όσον αφορά την παρακολούθηση των χρηστών, αλλά και τη συλλογή δεδομένων από ιστοσελίδες και εφαρμογές για έξυπνα κινητά τηλέφωνα. Μεταξύ άλλων, το σχέδιο Κανονισμού περιλαμβάνει απλούστερες και πιο σαφείς ρυθμίσεις σχετικά με την χρήστη των cookies, η οποία πρόκειται να εξορθολογιστεί, αφού, όπως αναλύθηκε ως άνω, έχει οδηγήσει σε σύγχυση τους χρήστες αλλά και τους παρόχους των εφαρμογών. Προτείνονται έτσι φιλικότερες προς τον χρήστη ρυθμίσεις αναφορικά με τον τρόπο αποδοχής ή άρνησης των cookies παρακολούθησης και άλλων

---

[167] Decision on the merits 21/2022 of 2 February 2022, Case number: DOS-2019-01377 https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf#page111 (τελευταία πρόσβαση στις 20.02.2022)

[168] Η Επιτροπή υιοθέτησε την πρόταση Κανονισμού ePrivacy το 2017, ο οποίος πρόκειται να αντικαταστήσει την υπάρχουσα Οδηγία ePrivacy [Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)].

[169] Σχέδιο κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες) — Εντολή του Συμβουλίου, https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf, https://www.consilium.europa.eu/el/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/ (τελευταία πρόσβαση στις 20.02.2022)

αναγνωριστικών και διευκρινίζεται ότι δεν θα απαιτείται συγκατάθεση για τα cookies που δεν επεμβαίνουν στην ιδιωτικότητα του χρήστη, αλλά βελτιώνουν απλώς την εμπειρία του[170]. Προβλέπεται επίσης η εξάρτηση της πρόσβασης σε μία εφαρμογή ή μία ιστοσελίδα από τη συγκατάθεση για τη χρήση cookies για πρόσθετους σκοπούς ως εναλλακτική λύση αντί της επί πληρωμή πρόσβασης στην εφαρμογή, υπό την προϋπόθεση ότι ο χρήστης έχει πραγματική επιλογή μεταξύ των δύο προσφορών. Τέλος, το σχέδιο περιλαμβάνει ρυθμίσεις για την αποφυγή της παροχής επαναλαμβανόμενης συγκατάθεσης σχετικά με τα cookies, με τη δημιουργία εξατομικευμένου για κάθε χρήστη καταλόγου εγκεκριμένων παρόχων[171].

3.4. Κατάρτιση Προφίλ

Τα μέσα κοινωνικής δικτύωσης αποτελούν εφαρμογές που παρέχονται δωρεάν[172] και βασίζονται στη λογική της κοινής χρήσης των προσωπικών δεδομένων των χρηστών. Οι επαφές και οι φίλοι των χρηστών, οι φωτογραφίες και οι γεωγραφικές σημάνσεις, τα σχόλια, οι απόψεις και οι προτιμήσεις που εκφράζονται μέσω των "likes" ή των "retweets", έχουν πλέον μετατραπεί σε ορατό και μετρήσιμο περιεχόμενο. Όσο αυξάνεται το περιεχόμενο που δημιουργείται αυτοβούλως από τους χρήστες, τόσο περισσότερο ανεβαίνει η αξία του για τους διαφημιστές και τα εμπλεκόμενα μέρη του οικοσυστήματος, τα οποία, επιδιώκοντας υψηλότερο κέρδος, αξιοποιούν τα δεδομένα για σκοπούς είτε στοχευμένης διαφήμισης, είτε για την πρόβλεψη της συμπεριφοράς των χρηστών μέσω της κατάρτισης προφίλ[173].

Ο ΓΚΠΔ χρησιμοποιεί τον όρο «κατάρτιση προφίλ» για να περιγράψει οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας προσωπικών δεδομένων που *«συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου» (Άρθρο 4 περ. 4).* Αυτή η επεξεργασία δεδομένων αποτελεί τη δημοφιλέστερη πρακτική των μέσων κοινωνικής δικτύωσης, κατά την οποία οι δραστηριότητες των χρηστών αναλύονται μέσω τεχνικών μηχανικής μάθησης, επιτρέποντας την αναγνώριση του κάθε χρήστη σύμφωνα με τη συμπεριφορά περιήγησής

---

[170] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (τελευταία πρόσβαση στις 20.02.2022)

[171] https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation (τελευταία πρόσβαση στις 20.02.2022)

[172] "No-cost services", βλ. υποκεφάλαιο 2.1.2. της παρούσης

[173] Mitrou L., Kandias M., Stavrou V., and Gritzalis D. (2014), "Social media profiling: A Panopticon or Omniopticon tool?", in Proc. of the 6th Conference of the Surveillance Studies Network, Spain, April 2014, p.12, https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf (τελευταία πρόσβαση στις 22.02.2022)

του, τις καθημερινές του συνήθειες και τα κλικ, ακόμα και τα δεδομένα θέσης που κοινοποιεί εθελοντικά στον λογαριασμό του[174].

Μολονότι η ανάλυση αυτή των ενεργειών των χρηστών μπορεί να αποδειχθεί χρήσιμη για την εξατομίκευση, τη διαχείριση του προφίλ ενός χρήστη ή τον εντοπισμό κακόβουλης ή καταχρηστικής συμπεριφοράς[175], ενδέχεται να οδηγήσει σε παραβίαση των δικαιωμάτων και των ελευθεριών του. Όταν μάλιστα συνδυάζεται με την αυξανόμενη επικράτηση των έξυπνων κινητών τηλεφώνων και των μέσων κοινωνικής δικτύωσης στην αγορά των νέων τεχνολογιών, η κατάρτιση προφίλ εμφανίζει εξαιρετικά σημαντικά ρίσκα για την ιδιωτικότητα των χρηστών.

Η κατάρτιση προφίλ αποτελεί συνήθως μία αδιαφανή διαδικασία, η οποία βασίζεται σε πληροφορίες που εξάγονται από τα προσωπικά δεδομένα που έχουν αποκαλύψει οι χρήστες για διαφορετικούς όμως σκοπούς[176], υπερβαίνοντας τις εύλογες προσδοκίες και τις προβλέψεις τους για την ασφάλεια των προσωπικών τους δεδομένων. Υπονομεύεται έτσι η ικανότητα των χρηστών να ασκήσουν επαρκή έλεγχο στα προσωπικά τους δεδομένα[177], κι ως εκ τούτου η ικανότητά τους για αποτελεσματική λήψη αποφάσεων. Η στόχευση επιπλέον των χρηστών μέσω καταρτισμένων προφίλ ενδέχεται να συνεπάγεται διακρίσεις και κοινωνικό αποκλεισμό. Η κατάρτιση προφίλ από τα μέσα κοινωνικής δικτύωσης μπορεί να περιλαμβάνει άμεση ή έμμεση ταξινόμηση των χρηστών, με βάση κριτήρια σχετικά με τη φυλετική ή εθνική καταγωγή, την κατάσταση υγείας ή τον σεξουαλικό προσανατολισμό του χρήστη. Η χρήση τέτοιων κριτηρίων στο πλαίσιο στοχευμένης διαφήμισης, που σχετίζεται για παράδειγμα με προσφορές εύρεσης εργασίας, μπορεί να μειώσει την ορατότητα των ευκαιριών σε άτομα που το προφίλ τους εντάσσεται σε συγκεκριμένες κοινωνικές ομάδες, προτρέποντας τους χρήστες σε μορφοποίηση ή προσαρμογή της ατομικής τους

---

[174] Cheung Anne S.Y. (2014), "Location privacy: The challenges of mobile service devices", Computer Law and Security Review, Volume 30, 2014, Elsevier Journal, 41-54, p. 50, https://doi.org/10.1016/j.clsr.2013.11.005 (τελευταία πρόσβαση στις 26.12.2021)

[175] Mitrou L., Kandias M., Stavrou V., and Gritzalis D. (2014), "Social media profiling: A Panopticon or Omniopticon tool?", in Proc. of the 6th Conference of the Surveillance Studies Network, Spain, April 2014, p.12, https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf (τελευταία πρόσβαση στις 22.02.2022)

[176] Πρόκειται για τα δεδομένα συμπεριφοράς ή αλλιώς "behavioral data", βλ. υποκεφάλαιο 2.2.1. της παρούσης

[177] Ward O. (2021), "Stop scrolling: EDPB adopts guidelines on targeting of social media users", Article posted on Lexology, https://www.lexology.com/library/detail.aspx?g=37c91855-2562-4c4b-bc62-a8cb8908202a (τελευταία πρόσβαση στις 23.02.2022)

συμπεριφοράς, ώστε να καταφέρουν να ενταχθούν στο κοινό προβολής της διαφήμισης. Ο φόβος της διάκρισης ή του κοινωνικού αποκλεισμού που δημιουργείται στους χρήστες μπορεί να οδηγήσει ακόμη και σε αυτολογοκρισία ή αυτοκαταπίεση[178,179]. Τέλος, η ανάλυση του περιεχομένου που μοιράζεται ένας χρήστης μέσω των μέσων κοινωνικής δικτύωσης μπορεί να αποκαλύψει πληροφορίες σχετικά με τη συναισθηματική του κατάσταση, αλλά και πότε αναμένεται να είναι πιο δεκτικός σε διαφημίσεις ή άλλες προσφορές. Με βάση το συναισθηματικό αυτό προφίλ που καταρτίζεται για τον χρήστη, καθίσταται ευκολότερη η έμμεση επιρροή της συμπεριφοράς του, γεγονός που αποδεδειγμένα[180] μπορεί να οδηγήσει σε χειραγώγηση των επιλογών του.

Για τους παραπάνω λόγους, οι χρήστες, ως υποκείμενα των δεδομένων, έχουν το δικαίωμα να αντιταχθούν στην κατάρτιση προφίλ από τους υπεύθυνους επεξεργασίας, εάν αυτή η επεξεργασία παράγει έννομα αποτελέσματα για το υποκείμενο, ή το επηρεάζει σημαντικά[181,182]. Για την εξειδίκευση της έννοιας της «σημαντικής επιρροής» που ο ΓΚΠΔ θέτει ως κριτήριο για την εναντίωση στην εν λόγω επεξεργασία, η Ομάδα Εργασίας του άρθρου 29 επισημαίνει ότι ακόμη και η κατάρτιση προφίλ για προωθητικούς σκοπούς θα μπορούσε ενδεχομένως να επηρεάσει τα υποκείμενα σημαντικά, μεταξύ άλλων εάν η κατάρτιση προφίλ είναι παρεμβατική και στοχεύει ευάλωτες ή μειονοτικές ομάδες, ή στερεί ευκαιρίες από ορισμένες ομάδες[183]. Τα cookies, που αναφέρθηκαν ως άνω, επιτρέπουν

---

[178] Mitrou L., Kandias M., Stavrou V., and Gritzalis D. (2014), "Social media profiling: A Panopticon or Omniopticon tool?", in Proc. of the 6th Conference of the Surveillance Studies Network, Spain, April 2014, p.13, https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf (τελευταία πρόσβαση στις 22.02.2022)

[179] «*Η αποκάλυψη προσωπικών πληροφοριών και η κακή χρήση τους μπορεί να βλάψει τα συναισθήματα των ανθρώπων και να προκαλέσει σημαντική ζημιά στις ζωές των ανθρώπων*», Warren S.D. and Brandeis L.D. (1890), "The Right to Privacy", Harvard Law Review, Vol. IV, No. 5, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (τελευταία πρόσβαση στις 22.02.2022)

[180] Υπόθεση "Cambridge Analytica"

[181] Άρθρο 22 παρ. 1 ΓΚΠΔ «*Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο*»

[182] Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T. and Shadbolt N. (2018), "Third Party Tracking in the Mobile Ecosystem", p. 7, https://www.researchgate.net/publication/326138940_Third_Party_Tracking_in_the_Mobile_Ecosystem (τελευταία πρόσβαση στις 05.01.2022)

[183] Ομάδα Εργασίας για την Προστασία Δεδομένων του Άρθρου 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού 2016/679, 17/EL, WP251αναθ.01, σελ. 15, Data protection | European Commission (europa.eu) (τελευταία πρόσβαση στις 23.02.2021)

τέτοιες δραστηριότητες χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων και ενδέχεται να παραβιάζουν το άρθρο 22 του ΓΚΠΔ[184]. Επομένως, οι υπεύθυνοι επεξεργασίας που επιδιώκουν να βασίζονται στην συγκατάθεση ως βάση για την κατάρτιση προφίλ θα πρέπει να αποδεικνύουν ότι τα υποκείμενα των δεδομένων κατανοούν τον σκοπό τον οποίο αφορά η συγκατάθεσή τους και κατά συνέπεια, ότι γνωρίζουν ακριβώς τους λόγους για τους οποίους θα χρησιμοποιήσουν τα δεδομένα τους[185].

3.5. Διασυνοριακές διαβιβάσεις προσωπικών δεδομένων

Η λειτουργία ενός καταστήματος εφαρμογών για έξυπνα κινητά τηλέφωνα παράγει μεγάλο όγκο δεδομένων σε καθημερινή βάση. Όλα τα δεδομένα, όπως προσωπικές πληροφορίες των χρηστών, οι πληρωμές τους και το ιστορικό λήψεων των εφαρμογών τους, καταγράφονται στα συστήματα των κατασκευαστών των λειτουργικών συστημάτων, ώστε να παρέχονται ομαλά οι απαραίτητες υπηρεσίες. Έχουν έτσι δημιουργηθεί παγκόσμια κέντρα αποθήκευσης δεδομένων, στα οποία διαβιβάζονται κάθε δευτερόλεπτο δισεκατομμύρια προσωπικών δεδομένων από όλα τα μέρη του κόσμου, όπου λειτουργεί η εκάστοτε εφαρμογή[186]. Με παρόμοιο τρόπο, τα μέσα κοινωνικής δικτύωσης συλλέγουν και αποθηκεύουν συνεχώς προσωπικά δεδομένα των χρηστών σε τοποθεσίες που έχουν επιλεγεί από τις εκάστοτε εταιρείες, εντός ή εκτός Ε.Ε., προκειμένου να είναι δυνατή η διαχείριση του όγκου των δεδομένων των χρηστών. Εκτός από τις παραπάνω διαβιβάσεις δεδομένων, παρατηρείται επιπλέον η διαβίβαση προσωπικών δεδομένων χρηστών σε τρίτα μέρη, όπως διαφημιστές και εταιρείες παροχής εργαλείων μέτρησης της δημοτικότητας ή της επισκεψιμότητας μίας εφαρμογής. Γίνεται έτσι φανερή η ανάγκη διασφάλισης ενός επαρκούς επιπέδου ασφαλείας ως προς τη διασυνοριακή διαβίβαση των προσωπικών δεδομένων, γεγονός που καταδεικνύεται από την πρόσφατη νομολογία της Ευρωπαϊκής Ένωσης αναφορικά με την προσπάθεια καθιέρωσης σαφών κανόνων για τις διασυνοριακές διαβιβάσεις, με γνώμονα τη νόμιμη και διαφανή επεξεργασία των προσωπικών δεδομένων των χρηστών των εφαρμογών, συμπεριλαμβανομένων των μέσων κοινωνικής δικτύωσης.

---

[184] Βλ. υποκεφάλαιο 3.3.

[185] Βλ. υποσημείωση 184.

[186] GSMA Association (2017), "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications", GSMA Report, p.38 https://aiforimpacttoolkit.gsma.com/resources/GSMA-report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf (τελευταία πρόσβαση στις 22.12.2021)

Ο ΓΚΠΔ θέτει ρητά κανόνες σχετικούς με τις διασυνοριακές διαβιβάσεις δεδομένων, τα οποία διαβιβάζονται είτε σε ένα άλλο κράτος εκτός Ε.Ε. μεταξύ επιχειρήσεων που ανήκουν στον ίδιο όμιλο ή επιδιώκουν κοινό οικονομικό σκοπό είτε σε κάποιον τρίτο, διεθνή φορέα εκτός Ε.Ε. Σύμφωνα με τα άρθρα του 5ου Κεφαλαίου του ΓΚΠΔ, οι διασυνοριακές διαβιβάσεις δεδομένων χρειάζεται να στηρίζονται σε μία από τις εξής βάσεις νομιμότητας, κατά σειρά προτεραιότητας. Συγκεκριμένα, οι διαβιβάσεις δύνανται να λαμβάνουν χώρα βασιζόμενες σε αποφάσεις επάρκειας που έχει εκδώσει η Ευρωπαϊκή Επιτροπή[187]. Σε περίπτωση που δεν υπάρχει απόφαση επάρκειας, η διαβίβαση μπορεί να πραγματοποιείται υπό την προϋπόθεση ότι παρέχονται κατάλληλες εγγυήσεις[188], ή μπορεί να διέπεται από δεσμευτικούς εταιρικούς κανόνες[189,190].

Τον Φεβρουάριο του 2022 η Γαλλική Αρχή Προστασίας Δεδομένων (CNIL) εξέδωσε απόφαση σχετικά με τη νομιμότητα της διαβίβασης προσωπικών δεδομένων σε τρίτες χώρες, κρίνοντας ότι ένας ιστότοπος δεν μπορούσε να χρησιμοποιήσει τα cookies "Google Analytics" της Google, διότι κάτι τέτοιο συνεπάγεται διαβίβαση προσωπικών δεδομένων από την Ευρώπη στις ΗΠΑ κατά παράβαση της απόφασης Schrems II του 2020[191]. Στη μνημειώδη αυτή απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης (εφεξής ως «ΔΕΕ») στο πλαίσιο εξέτασης της υπόθεσης C-311/18 "Data Protection Commissioner of Ireland v. Facebook & Max Schrems" κρίθηκε ως ανίσχυρη η απόφαση της Ευρωπαϊκής Επιτροπής αναφορικά με την επάρκεια της προστασίας που παρέχεται από τον μηχανισμό της ασπίδας προστασίας της ιδιωτικής ζωής (Privacy Shield) για τη διαβίβαση προσωπικών δεδομένων από την Ευρώπη

[187] Άρθρο 45 παρ.1 ΓΚΠΔ *«Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί εφόσον η Επιτροπή έχει αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό. Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια.»*

[188] Άρθρο 46 ΓΚΠΔ. Στην παράγραφο 3 αναφέρονται και οι τυποποιημένες συμβατικές ρήτρες ως νομική βάση για τη διασυνοριακή διαβίβαση δεδομένων.

[189] Άρθρο 47 ΓΚΠΔ.

[190] Παρεκκλίσεις για ειδικές καταστάσεις προβλέπει το άρθρο 49 του ΓΚΠΔ.

[191] https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply (τελευταία πρόσβαση στις 25.02.2022)

στις ΗΠΑ[192,193]. Κινούμενη στο πλαίσιο της Schrems II, η CNIL κατέληξε στο συμπέρασμα ότι οι διαβιβάσεις προς τις ΗΠΑ επί του παρόντος δεν ρυθμίζονται επαρκώς, ελλείψει απόφασης επάρκειας, κι ως εκ τούτου η διαβίβαση δεδομένων μπορεί να πραγματοποιηθεί μόνο εάν παρέχονται κατάλληλες εγγυήσεις ειδικότερα για την υπό εξέταση ροή προσωπικών δεδομένων[194]. Παρ' όλο που η Google είχε λάβει μέτρα για να ρυθμίσει τις διαβιβάσεις δεδομένων, αυτά δεν ήταν αρκετά για να διασφαλιστεί η αποτροπή μη εξουσιοδοτημένης πρόσβασης σε αυτά από τις αμερικανικές υπηρεσίες, γεγονός που δημιουργεί κίνδυνο παραβίασης δεδομένων ευρωπαίων πολιτών και συνεπάγεται παραβίαση του Κεφαλαίου 5ου του ΓΚΠΔ. Η CNIL με την απόφασή της, επιπλέον, διατύπωσε γενική σύσταση προς τους υπεύθυνους επεξεργασίας να χρησιμοποιούν cookies μόνο για την παραγωγή ανώνυμων στατιστικών δεδομένων στις περιπτώσεις που δεν διασφαλίζεται κατάλληλα η διαβίβαση εκτός Ε.Ε., έτσι ώστε να εξαιρούνται από την υποχρέωση λήψης συγκατάθεσης από τους χρήστες.

Όπως ήταν αναμενόμενο, οι ανωτέρω αποφάσεις είχαν ισχυρό αντίκτυπο στην αγορά των μέσων κοινωνικής δικτύωσης, συμπέρασμα που συνήχθη και από την ετήσια έκθεση της εταιρείας Meta, σύμφωνα με την οποία, το Facebook και οι λοιπές πλατφόρμες της Meta, αδυνατούν να συνεχίσουν να παρέχουν υπηρεσίες στην Ευρώπη, εάν δεν υιοθετηθεί ένα νομικό πλαίσιο που να επιτρέπει τη διαβίβαση δεδομένων στις ΗΠΑ[195]. Μπορεί η δήλωση αυτή να διαψεύστηκε άμεσα από τους εκπροσώπους της Εταιρείας, δεν παύει ωστόσο να

---

[192] Ο προσφεύγων, Max Schrems, είχε αμφισβητήσει τη νομιμότητα της διαβίβασης προσωπικών δεδομένων του από το Facebook της Ιρλανδίας στην έδρα του Facebook στις ΗΠΑ. Υποστήριξε ότι οι τυποποιημένες συμβατικές ρήτρες διαβίβασης δεδομένων μεταξύ των δύο χωρών δεν ήταν σύμφωνες με την απόφαση επάρκειας 2010/87, καθώς η αμερικανική νομοθεσία επιτρέπει την πρόσβαση στα προσωπικά δεδομένα ευρωπαίων πολιτών που βρίσκονται αποθηκευμένα στις υποδομές εταιρειών όπως το Facebook στις ΗΠΑ. Επιπλέον, τα άτομα δεν γνώριζαν ότι παρακολουθούνται, μέσω των προσωπικών δεδομένων που διαβιβάζονται στις ΗΠΑ., Κανέλλος Λ. (2020), The GDPR Handbook, Εκδόσεις Νομική Βιβλιοθήκη, σελ. 163-165

[193] https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en, https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II (τελευταία πρόσβαση στις 25.02.2022)

[194] https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply (τελευταία πρόσβαση στις 25.02.2022)

[195] *"If a new transatlantic data transfer framework is not adopted and we are unable to continue to rely on SCCs or rely upon other alternative means of data transfers from Europe to the United States, we will likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe, which would materially and adversely affect our business, financial condition, and results of operations"*, Meta Platforms Annual Report, p. 9, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf (τελευταία πρόσβαση στις 25.02.2022)

αποτελεί ένδειξη πως τα προσωπικά δεδομένα των χρηστών των μέσων κοινωνικής δικτύωσης είναι κρίσιμο να διασφαλίζονται και να προστατεύονται με σαφώς καθορισμένους ρυθμιστικούς, νομικούς μηχανισμούς.

3.6. Τα δικαιώματα των χρηστών

Η παρουσία των ατόμων σε οικοσυστήματα έξυπνων κινητών τηλεφώνων μέσω εφαρμογών όπως τα μέσα κοινωνικής δικτύωσης και η συνακόλουθη παροχή τεράστιου όγκου προσωπικών δεδομένων, άμεσα ή έμμεσα, είναι ανάγκη να συνοδεύεται από διασφαλίσεις διαφάνειας και προστασίας των δικαιωμάτων και των ελευθεριών τους. Οι χρήστες, ως υποκείμενα δεδομένων, χρειάζεται να έχουν τουλάχιστον τη δυνατότητα να γνωρίζουν τον βαθμό επεξεργασίας των προσωπικών τους δεδομένων, και φυσικά, να μπορούν να λάβουν αυτά τα δεδομένα, να τα διορθώσουν, ακόμη και να τα διαγράψουν σε συγκεκριμένες περιπτώσεις. Ο ΓΚΠΔ επικεντρώνεται στην προστασία των υποκειμένων των δεδομένων ως αυτόνομων και ελεύθερων ατόμων, παρέχοντάς τους ρητά τη δυνατότητα άσκησης των δικαιωμάτων τους, γεγονός που αποδεικνύει τον «επαναστατικό» τους χαρακτήρα. Στο ΚΕΦΑΛΑΙΟ ΙΙΙ του ΓΚΠΔ «Δικαιώματά του υποκειμένου των δεδομένων» (Άρθρα 13-23) αναγράφονται αναλυτικά τα δικαιώματα των υποκειμένων.

Αρχικά, σύμφωνα με το άρθρο 15 του ΓΚΠΔ, ο χρήστης ως υποκείμενο των δεδομένων *«έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες»*, όπως ο σκοπός και ο χρόνος επεξεργασίας, οι κατηγορίες προσωπικών δεδομένων, οι αποδέκτες, καθώς και η πιθανή ύπαρξη αυτοματοποιημένης επεξεργασίας. Το αίτημα χρειάζεται να γίνει εγγράφως στον υπεύθυνο επεξεργασίας και ο τελευταίος είναι υποχρεωμένος να παράσχει αντίγραφο των δεδομένων στο υποκείμενο εντός χρονικού διαστήματος 30 ημερών. Επιπλέον, σύμφωνα με την Αιτιολογική Σκέψη 63 του ΓΚΠΔ, μπορεί να παρέχεται πρόσβαση στο υποκείμενο των δεδομένων εξ αποστάσεως, μέσω αφαλούς μηχανισμού[196]. Επιπρόσθετα, όσον αφορά τους από κοινού υπεύθυνους επεξεργασίας, αν και δεν αναφέρεται ρητά στο άρθρο 26 του ΓΚΠΔ, απαιτείται μεν να

[196] Αιτιολογική Σκέψη 63 του ΓΚΠΔ: *«…Ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να παρέχει πρόσβαση εξ αποστάσεως σε ασφαλές σύστημα μέσω του οποίου το υποκείμενο των δεδομένων αποκτά άμεση πρόσβαση στα δεδομένα που το αφορούν. Το δικαίωμα αυτό δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό…»*

ορίζεται ένα ενιαίο σημείο επικοινωνίας στο οποίο τα υποκείμενα των δεδομένων να μπορούν να υποβάλλουν τα αιτήματα πρόσβασής τους, χωρίς όμως να είναι εφικτός ο αποκλεισμός υποβολής ενός αιτήματος πρόσβασης στον καθένα από τους υπεύθυνους επεξεργασίας[197].

Το διαδικτυακό περιβάλλον, η αμεσότητα και η ευκολία σύνδεσης και αλληλεπίδρασης, καθώς και η ύπαρξη σχετικού λογαριασμού χρήστη αποτελούν τα χαρακτηριστικά που καθιστούν την παραπάνω πρόταση για ευχερέστερη πρόσβαση στα προσωπικά δεδομένα του χρήστη εφικτή και σε ένα βαθμό απαραίτητη, σύμφωνα με το άρθρο 15 παρ. 1 και 2 του ΓΚΠΔ[198]. Επομένως, όσον αφορά τα καταστήματα εφαρμογών, τα λειτουργικά συστήματα των έξυπνων τηλεφώνων αλλά και τα μέσα κοινωνικής δικτύωσης, κρίνεται προσφορότερη η καθιέρωση ενός εύχρηστου, αυτόματου μηχανισμού ελέγχου του προφίλ του χρήστη από τον ίδιο, στον οποίο θα συμπεριλαμβάνονται όλες οι απαραίτητες πληροφορίες, όπως οι πηγές συλλογής των δεδομένων που εμπεριέχονται στο προφίλ του, οι κατηγορίες των δεδομένων που τηρούνται, η ταυτότητα του υπεύθυνου επεξεργασίας αλλά και τυχόν τρίτων αποδεκτών των δεδομένων, όπως στοχεύοντες φορείς και διαφημιστές ή εκτελούντες την επεξεργασία, καθώς και όλες οι υπόλοιπες πληροφορίες του άρθρου 15 ΓΚΔΠ[199]. Φυσικά, είναι αναμενόμενο πως, αφού ο χρήστης έχει παραχωρήσει σε εφαρμογές όπως τα μέσα κοινωνικής δικτύωσης τεράστια πρόσβαση σε προσωπικά του δεδομένα, σε περίπτωση που ασκήσει το εν λόγω δικαίωμά του, θα λάβει ένα αντίγραφο ιλιγγιώδους ίσως μεγέθους, αφού σε αυτό θα περιέχονται όλα όσα έχει ποτέ δημοσιεύσει στο προφίλ του, όσα μηνύματα έχει αποστείλει μέσω της εφαρμογής, ακόμα και όσα «Μου αρέσει» έχει πατήσει σε οποιαδήποτε δημοσίευση εντός της εφαρμογής[200].

---

[197] Άρθρο 26 παρ. 3 ΓΚΠΔ: «Ανεξάρτητα από τους όρους της συμφωνίας που αναφέρεται στην παράγραφο 1, το υποκείμενο των δεδομένων μπορεί να ασκήσει τα δικαιώματά του δυνάμει του παρόντος κανονισμού έναντι και κατά καθενός από τους υπευθύνους επεξεργασίας».

[198] Κατευθυντήριες γραμμές 8/2020 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τη στόχευση χρηστών μέσων κοινωνικής δικτύωσης Έκδοση 2.0, παρ. 101, διαθέσιμες στο https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_el (τελευταία πρόσβαση στις 01.03.2022)

[199] Ομάδα Εργασίας για την Προστασία Δεδομένων του Άρθρου 29, Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του Κανονισμού 2016/679, 17/EL, WP251αναθ.01, σελ. 20, Data protection | European Commission (europa.eu) (τελευταία πρόσβαση στις 23.02.2021)

[200] https://www.legalcheek.com/lc-journal-posts/gdpr-social-media-and-the-right-to-be-forgotten/ (τελευταία πρόσβαση στις 02.03.2022)

Ένα ακόμη δικαίωμα με το οποίο εξοπλίζει ο ΓΚΠΔ τους χρήστες των μέσων κοινωνικής δικτύωσης αλλά και των έξυπνων κινητών τηλεφώνων αποτελεί το δικαίωμα διαγραφής ή αλλιώς «δικαίωμα στη λήθη»[201]. Σύμφωνα με αυτό, το υποκείμενο των δεδομένων μπορεί να αιτηθεί τη διαγραφή των προσωπικών του δεδομένων, εφόσον δεν επιθυμεί πια αυτά να αποτελούν αντικείμενο επεξεργασίας ή δεν υφίσταται κάποιος νόμιμος λόγος να τα διατηρήσει ο υπεύθυνος επεξεργασίας[202], ή εάν αντιτάσσεται στην εν λόγω επεξεργασία.

Η άσκηση του δικαιώματος διαγραφής παρουσιάζει ιδιαίτερο ενδιαφέρον στην περίπτωση που οι χρήστες επιθυμούν τη διαγραφή των δεδομένων τους από τα μέσα κοινωνικής δικτύωσης, ακόμη και τη διαγραφή ολόκληρου του προφίλ τους, με επακόλουθο την διαγραφή της ίδιας της εφαρμογής από τα έξυπνα κινητά τους τηλέφωνα. Συγκεκριμένα, η δεύτερη παράγραφος του άρθρου 17 αναφέρει ότι ο υπεύθυνος επεξεργασίας, όχι μόνο υποχρεούται να διαγράψει τα δεδομένα από τα μέσα που διαθέτει -όπως εφαρμογές ή λειτουργικά συστήματα έξυπνων κινητών- αλλά και να λάβει εύλογα μέτρα *«για να ενημερώσει τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς τους υπευθύνους επεξεργασίας τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα»*[203]. Αυτοί οι υπεύθυνοι επεξεργασίας μπορεί να είναι τρίτα μέρη όπως μία μηχανή αναζήτησης ή μία εταιρεία κατασκευής λειτουργικών συστημάτων, ένα άλλο μέσο κοινωνικής δικτύωσης ή μία εφαρμογή που συνδέεται με το μέσο κοινωνικής δικτύωσης που χρησιμοποιεί ο χρήστης, περιλαμβάνοντας επίσης και άλλους μεμονωμένους χρήστες, για παράδειγμα φίλους ή ακόλουθους του χρήστη. Αναδημοσιεύσεις και κοινοποιήσεις περιεχομένου, σχόλια, εκ νέου αναρτήσεις ή φωτογραφίες που δημοσιεύονται από τρίτους συνιστούν επεξεργασία

---

[201] Η εξέταση του δικαιώματος στη λήθη ξεκίνησε στην Ισπανία, όταν το 2009 ο Mario González ανακάλυψε μέσω μιας αναζήτησης στο Google ότι το όνομά του εμφανιζόταν ακόμη σε δύο δημοσιεύματα ισπανικής εφημερίδας που είχαν αναρτηθεί στο διαδίκτυο, σχετικά με μία διαταγή εκπλειστηριασμού του σπιτιού του το 1998. Ο González τότε ζήτησε να αφαιρεθούν τα άρθρα αλλά η εφημερίδα αρνήθηκε. Με την εμβληματική έτσι απόφαση "Google Spain κατά Costeja Gonzalez", το ΔΕΕ έκρινε ότι ο Mario Costeja Gonzalez είχε δικαίωμα να ζητήσει τη διαγραφή των δεδομένων του από την Google, ενώ η τελευταία ήταν υποχρεωμένη να ικανοποιήσει το αίτημα διαγραφής. https://curia.europa.eu/juris/liste.jsf?language=el&num=c-131/12. Σε συνέχεια αυτής της απόφασης, η Google μάλιστα ανέπτυξε ένα σύστημα για την άμεση και εύκολη υποβολή του δικαιώματος των χρηστών της στη λήθη. (https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636596607835233538-3993345926&hl=el&rd=1)

[202] Άρθρο 17 και Αιτιολογικές Σκέψεις 65 και 66 του ΓΚΠΔ

[203] Άρθρο 17 παρ. 2 ΓΚΠΔ

δεδομένων από τρίτα μέρη, τα οποία και θα πρέπει να διαγραφούν από κάθε σημείο όπου βρίσκονται αποθηκευμένα. Έτσι, τα μέσα κοινωνικής δικτύωσης, καθώς και τα λειτουργικά συστήματα -όταν πρόκειται για διαγραφή ολόκληρων εφαρμογών-, ως υπεύθυνοι επεξεργασίας, υποχρεούνται να ενημερώνουν όλα τα συνδεδεμένα μέρη για τη διαγραφή συγκεκριμένων δεδομένων που αιτείται ο χρήστης[204]. Τα αιτήματα διαγραφής θα μπορούσαν να περιλαμβάνουν την αφαίρεση μίας φωτογραφίας, μίας ανάρτησης ή ενός σχολίου, ακόμη και μίας γεωγραφικής σήμανσης που δεν επιθυμεί πλέον ο χρήστης να εμφανίζεται δημόσια. Όσον αφορά τη διαγραφή του προφίλ του χρήστη από το μέσο κοινωνικής δικτύωσης, αυτή θα πρέπει να συνεπάγεται την οριστική απομάκρυνση όλων των προσωπικών δεδομένων που ο χρήστης έχει καταχωρήσει σε αυτή, αφού μόνο έτσι διασφαλίζεται ότι τα δεδομένα του παύουν πλέον να είναι διαθέσιμα στον υπεύθυνο επεξεργασίας και σε τρίτα, συνεργαζόμενα μέρη[205]. Προβληματισμούς ωστόσο εγείρουν τα «παραθυράκια» που παραμένουν ανοιχτά και αφορούν τους όρους χρήσης των μέσων κοινωνικής δικτύωσης, σύμφωνα με τους οποίους παρέχεται μία περίοδος χάριτος, που μπορεί να αγγίζει μέχρι και τις 30 ημέρες, προκειμένου ο χρήστης εάν θέλει να ανακτήσει τον λογαριασμό του[206]. Με τον τρόπο αυτό κάμπτεται σε ένα βαθμό ο απόλυτος χαρακτήρας και η υποχρεωτικότητα ικανοποίησης του δικαιώματος διαγραφής, καθώς φαίνεται πως οι εφαρμογές τηρούν τα δεδομένα του χρήστη σε ξεχωριστά σημεία αποθήκευσης, για να είναι δυνατή η αξιοποίηση της ως άνω δυνατότητας επαναφοράς του λογαριασμού του.

Συμπερασματικά, είναι φανερό πως τα προσωπικά δεδομένα των φυσικών προσώπων που παρέχονται στα μέσα κοινωνικής δικτύωσης μέσω λειτουργικών συστημάτων για έξυπνα κινητά τηλέφωνα σπάνια παύουν να υπάρχουν. Χωρίς να διαθέτουν εξ αρχής μία προκαθορισμένη διάρκεια ζωής και από τη στιγμή που υφίστανται σε διάφορες μορφές[207],

---

[204] Myers C. (2014), "Digital Immortality vs. "The Right to be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy", p.54, DOI:10.21018/rjcpr.2014.3.175 (τελευταία πρόσβαση στις 03.03.2022)

[205] Το πάτημα του κουμπιού «Οριστική Διαγραφή Λογαριασμού» χαρακτηρίζεται ως «ψηφιακός θάνατος» ενός προσώπου.

[206] Βλ. Όρους Χρήσης του Instagram https://help.instagram.com/370452623149242/?helpref=hc_fnav (τελευταία πρόσβαση στις 03.03.2022)

[207] Yerukhimovich A., Balebako R., Boustead A. E., Cunningham R. K., Welser IV W., Housley R., Shay R., Spensky Ch., Stanley K. D., Stewart J., Trachtenberg A., and Winkelman Z. (2016), "Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices", Santa Monica, CA: RAND Corporation, pp. 4-5, https://www.rand.org/pubs/research_reports/RR1393.html (τελευταία πρόσβαση στις 05.01.2022)

για απροσδιόριστες χρονικές περιόδους, ενδέχεται να συνεχίζουν απρόσκοπτα να αντιγράφονται, να αναμεταδίδονται και να αξιοποιούνται από τρίτους.

3 7. Τεχνικά μέτρα προστασίας των χρηστών

Με την αλματώδη αύξηση του αριθμού των μέσων κοινωνικής δικτύωσης, η οριοθέτηση της έννοιας της ιδιωτικότητας και της ασφάλειας των χρηστών έχει καταστεί μία πολύπλοκη διαδικασία. Όσο τα έξυπνα κινητά τηλέφωνα και οι εφαρμογές που βρίσκονται εκεί εγκατεστημένες συλλέγουν συνεχώς προσωπικά δεδομένα χρηστών μέσω αισθητήρων και μηχανισμών αυτόματης αποθήκευσης δεδομένων στις συσκευές τους, τα τεχνικά μέτρα προστασίας που λαμβάνονται από τους κατασκευαστές των εφαρμογών χρειάζεται να γίνονται αυστηρότερα, με σκοπό τη διασφάλιση ενός ασφαλούς περιβάλλοντος κοινωνικής δραστηριοποίησης.

Τα πρότυπα προστασίας των προσωπικών δεδομένων των χρηστών θα πρέπει να σχεδιάζονται και να εφαρμόζονται τόσο στις υπάρχουσες όσο και στις νέες εφαρμογές έξυπνων κινητών τηλεφώνων, προκειμένου να πληρούνται οι βασικές προϋποθέσεις διαφάνειας και ασφαλείας, που θα οδηγήσουν εν τέλει στη δημιουργία εμπιστοσύνης από τους χρήστες. Πρακτικές για την ενσωμάτωση ρυθμίσεων απορρήτου στην ανάπτυξη του λογισμικού, όπως η απαίτηση μόνο ενός ελάχιστου αριθμού προσωπικών δεδομένων για την παροχή υπηρεσιών, αλλά και η αξιοποίηση κατάλληλων τεχνικών για την προστασία των δεδομένων, αποτελούν μέτρα ήδη από τον σχεδιασμό των εφαρμογών, τα οποία προβλέπονται ρητά από το άρθρο 25 παρ. 1 του ΓΚΠΔ[208] (*«Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού»*). Σύμφωνα με το άρθρο αυτό, οι κατασκευαστές λειτουργικών συστημάτων και οι πάροχοι των μέσων κοινωνικής δικτύωσης, ως υπεύθυνοι επεξεργασίας, χρειάζεται να λαμβάνουν αποτελεσματικά τα προσήκοντα τεχνικά μέτρα κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας, καθώς και κατά τη στιγμή της επεξεργασίας των προσωπικών δεδομένων. Συγκεκριμένα, η προστασία ήδη από τον σχεδιασμό σε ένα

[208] Άρθρο 25 παρ. 1 ΓΚΠΔ: «*Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, ο υπεύθυνος επεξεργασίας εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του παρόντος κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων.*»

λειτουργικό σύστημα ή μια εφαρμογή πρέπει να λαμβάνεται υπόψη από τον σχεδιασμό μίας εφαρμογής, την ανάπτυξη, την υλοποίηση και τη χρήση της, ακόμη και μέχρι την κατάργησή της από το έξυπνο κινητό του χρήστη, αφού αποτελεί καθοριστικό κριτήριο για την ποιότητα[209] του επιπέδου προστασίας του τελευταίου. Έτσι, κατάλληλες εσωτερικές πολιτικές και τεχνικές ασφαλείας πρέπει να θεσπιστούν, ανταποκρινόμενες στις υψηλές απαιτήσεις του ΓΚΠΔ, με σκοπό την απόδειξη της συμμόρφωσης με το κανονιστικό πλαίσιο για την προστασία των δεδομένων των χρηστών τους[210].

Αναφορικά με την ασφάλεια στις τεχνολογίες πληροφορικής και επικοινωνιών – «ΤΠΕ»[211], όπως είναι οι εφαρμογές έξυπνων κινητών τηλεφώνων και τα λογισμικά γενικότερα, η κλασική τριάδα για την προστασία των δεδομένων, πιο συγκεκριμένα η τριάδα «εμπιστευτικότητα-ακεραιότητα-διαθεσιμότητα»[212], είναι ευρέως γνωστή και αποδεκτή, καθώς αποτελεί μια σταθερή βάση για την αξιολόγηση των χαρακτηριστικών ασφάλειας των ΤΠΕ, τον εντοπισμό των κινδύνων και την επιλογή των κατάλληλων μέτρων για την αντιμετώπισή τους[213]. Επιπρόσθετα, τα ακόλουθα χαρακτηριστικά προστασίας δεδομένων έχουν προταθεί για να συμπληρώσουν την παραπάνω τριάδα και να επεκτείνουν τους στόχους ασφάλειας δεδομένων, ειδικότερα όταν πρόκειται για επεξεργασία προσωπικών δεδομένων από τα μέσα κοινωνικής δικτύωσης: ανωνυμία, αποσύνδεση και παρεμβασιμότητα[214].

Η ανωνυμία διασφαλίζει ότι ένας μη εξουσιοδοτημένος τρίτος δεν μπορεί να αναγνωρίσει επαρκώς έναν χρήστη μέσα σε ένα σύνολο χρηστών του μέσου κοινωνικής δικτύωσης. Η δυνατότητα αποσύνδεσης ("unlinkability") στη συνέχεια αναφέρεται στην αδυναμία ενός μη εξουσιοδοτημένου τρίτου να διακρίνει εάν δύο ή περισσότερες πληροφορίες που αποτελούν

---

[209] Hansen M., Hoepman J.H., and Jensen M. (2016), "Towards Measuring Maturity of PrivacyEnhancing Technologies," in Annual Privacy Forum (APF 2015), DOI: 10.1007/978-3-319-31456-3_1 (τελευταία πρόσβαση στις 13.03.2022)

[210] Αιτιολογική Σκέψη 78 ΓΚΠΔ.

[211] "Information and Communication Technologies – ICT"

[212] "Confidentiality – Integrity – Availability", "The CIA Triad"

[213] European Union Agency for Network and Information Security "ENISA" (2017) "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", p. 47, https://pure.uva.nl/ws/files/42887337/22302384.pdf (τελευταία πρόσβαση στις 13.03.2022)

[214] Hansen M., Jensen M. and Rost M. (2015) "Protection Goals for Privacy Engineering," in International Workshop on Privacy Engineering (IWPE), IEEE CS Security and Privacy Workshops (SPW), p. 160 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163220 (τελευταία πρόσβαση στις 13.03.2022)

προσωπικά δεδομένα κάποιου χρήστη σχετίζονται ή όχι μεταξύ τους[215]. Η έννοια της αποσύνδεσης συνδέεται με τις αρχές της αναγκαιότητας, της ελαχιστοποίησης δεδομένων, και του περιορισμού της περιόδου αποθήκευσης, καθώς οι μηχανισμοί για την επίτευξη μίας τέτοιας μορφής αποσύνδεσης δεδομένων περιλαμβάνουν την εκ των προτέρων αποφυγή συλλογής περιττών δεδομένων, τον διαχωρισμό των πλαισίων εντός των οποίων κινούνται τα δεδομένα[216], την ψευδωνυμοποίηση αλλά και την έγκαιρη διαγραφή τους από το εκάστοτε λειτουργικό σύστημα, όταν παρέλθει η απαραίτητη περίοδος διακράτησής τους[217,218,219]. Η παρεμβασιμότητα τέλος, αφορά τη δυνατότητα παρέμβασης στην τρέχουσα ή σε μία προγραμματισμένη επεξεργασία προσωπικών δεδομένων, ιδίως από τα άτομα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία[220], με στόχο την εφαρμογή διορθωτικών μέτρων

---

[215] Raad E., Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, p.3, https://hal.archives-ouvertes.fr/hal-00975998 (τελευταία πρόσβαση στις 13.03.2022)

[216] GSMA Association (2017), "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications", GSMA Report, p.31, https://aiforimpacttoolkit.gsma.com/resources/GSMA-report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf (τελευταία πρόσβαση στις 22.12.2021)

[217] European Union Agency for Network and Information Security "ENISA" (2014), «Privacy and Data Protection by Design – from policy to engineering», p.6, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (τελευταία πρόσβαση στις 19.03.2022)

[218] Παραδείγματα εφαρμογής της αποσύνδεσης σε οικοσυστήματα έξυπνων κινητών τηλεφώνων:

- Οι διαφορετικές εφαρμογές μέσων κοινωνικής δικτύωσης θα πρέπει να απομονώνονται από προεπιλογή, εφόσον επεξεργάζονται προσωπικά δεδομένα για διαφορετικούς σκοπούς. Οποιαδήποτε ανταλλαγή δεδομένων θα πρέπει να αποτρέπεται, εκτός εάν ο σκοπός της ορίζεται ρητά ή επιλέγεται από τον χρήστη.
- Τα μοναδικά αναγνωριστικά για τη σύνδεση του χρήστη στην εφαρμογή δεν θα πρέπει να χρησιμοποιούνται για διαφορετικούς σκοπούς, ενώ αυτά δεν θα πρέπει να συνδέονται ή να διαβιβάζονται μεταξύ των εφαρμογών.
- Τα προσωπικά δεδομένα θα πρέπει να διαγράφονται το συντομότερο δυνατό από την εφαρμογή, ενώ εάν αυτό δεν είναι εφικτό, θα πρέπει να ανωνυμοποιούνται άμεσα,

European Union Agency for Network and Information Security "ENISA" (2017) "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", p. 51, https://pure.uva.nl/ws/files/42887337/22302384.pdf (τελευταία πρόσβαση στις 13.03.2022)

[219] Αιτιολογική Σκέψη 78 του ΓΚΔΠ: «*Τέτοια μέτρα θα μπορούσαν να περιλαμβάνουν, μεταξύ άλλων, την ελαχιστοποίηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, την ψευδωνυμοποίηση δεδομένων προσωπικού χαρακτήρα το συντομότερο δυνατόν, τη διαφάνεια όσον αφορά τις λειτουργίες και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία δεδομένων και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφάλειας*».

[220] Hansen M., Jensen M. and Rost M. (2015) "Protection Goals for Privacy Engineering," in International Workshop on Privacy Engineering (IWPE), IEEE CS Security and Privacy Workshops (SPW), p. 160 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163220 (τελευταία πρόσβαση στις 13.03.2022)

και αντισταθμίσεων όπου χρειάζεται. Σχετίζεται με τις αρχές που αφορούν τα δικαιώματα των υποκειμένων των δεδομένων, όπως τα δικαιώματα διόρθωσης και διαγραφής δεδομένων, το δικαίωμα ανάκλησης της συγκατάθεσης ή το δικαίωμα εναντίωσης στην επεξεργασία, επηρεάζοντας όλα τα ενδιαφερόμενα μέρη που σχετίζονται με αυτή την παρέμβαση. Τα μέτρα για την υποστήριξη της απαίτησης παρεμβασιμότητας περιλαμβάνουν καθιερωμένες διαδικασίες για τον επηρεασμό ή την πλήρη ή μερική διακοπή της επεξεργασίας δεδομένων, τη χειροκίνητη ανάκληση μιας αυτοματοποιημένης απόφασης ή μίας ρύθμισης, την ύπαρξη ενιαίων σημείων επαφής για τα αιτήματα παρέμβασης των υποκειμένων των δεδομένων, ακόμα και κουμπιά για την εύκολη αλλαγή μιας ρύθμισης από τους χρήστες[221].

Με βάση τα εν λόγω χαρακτηριστικά, οι κατασκευαστές λογισμικού των εφαρμογών θα πρέπει να ακολουθούν συγκεκριμένα βήματα προκειμένου να συμμορφώνονται με τις απαιτήσεις προστασίας της ιδιωτικότητας. Επιπλέον, οι σχεδιαστικές λύσεις των εφαρμογών για έξυπνα κινητά τηλέφωνα χρειάζεται να προσαρμόζονται στα διαφορετικά γνωστικά επίπεδα χρηστών, ενώ οι ίδιες οι εφαρμογές απαιτείται να διαθέτουν φιλικές προς τον χρήστη διεπαφές, προσιτές και κατανοητές ρυθμίσεις ασφαλείας, καθώς και κέντρα υποστήριξής των χρηστών, με επίκεντρο την ανάγκη για μεγαλύτερη προστασία των προσωπικών δεδομένων που υφίστανται επεξεργασία. Όλα τα παραπάνω, σε συνδυασμό με την παροχή αποδείξεων από τον εκάστοτε υπεύθυνο επεξεργασίας ότι η επεξεργασία προσωπικών δεδομένων των χρηστών διενεργείται με σκοπό την προάσπιση των δικαιωμάτων και των ελευθεριών τους, οδηγούν στη συμμόρφωση των κατασκευαστών των εφαρμογών με τη θεμελιώδη αρχή της λογοδοσίας του ΓΚΠΔ[222].

Αξίζει στη συνέχεια να αναφερθούν σημαντικές τεχνικές για την αύξηση του επιπέδου ιδιωτικότητας των χρηστών στις εφαρμογές των οικοσυστημάτων έξυπνων κινητών τηλεφώνων, οι οποίες ενσωματώνουν τα χαρακτηριστικά που αναπτύχθηκαν αμέσως παραπάνω. Σε αυτές περιλαμβάνεται η κρυπτογράφηση, η τεχνική "application sandboxing",

[221] European Union Agency for Network and Information Security "ENISA" (2014), "Privacy and Data Protection by Design – from policy to engineering", p.7, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (τελευταία πρόσβαση στις 19.03.2022)

[222] Άρθρο 5 παρ. 2, σε συνδυασμό με τα άρθρα 24 και 32 ΓΚΠΔ.

καθώς και η κρυπτογράφηση δίσκου[223], οι οποίες στοχεύουν στον έλεγχο και την προστασία των προσωπικών δεδομένων που συλλέγονται και αποθηκεύονται στη συσκευή του χρήστη.

Η κρυπτογράφηση δεδομένων είναι μία διαδικασία κωδικοποίησης πληροφοριών, μέσω της οποίας η αρχική αναπαράσταση της πληροφορίας μετατρέπεται από αναγνώσιμο «απλό κείμενο» σε μη αναγνώσιμη από τον άνθρωπο μορφή (γνωστή ως κρυπτόγραμμα ή "ciphertext"). Μόνο εξουσιοδοτημένα μέρη, που διαθέτουν το κατάλληλο κλειδί αποκρυπτογράφησης, μπορούν να αποκρυπτογραφήσουν το κρυπτόγραμμα, με σκοπό να το διαβάσουν ή να αποκτήσουν πρόσβαση στις αρχικές πληροφορίες[224]. Ο κύριος στόχος της κρυπτογράφησης είναι να αποτρέψει τη μη εξουσιοδοτημένη πρόσβαση και ανάγνωση δεδομένων[225] - προστατεύοντας για παράδειγμα τα δεδομένα του χρήστη μίας εφαρμογής πριν από την κοινοποίησή τους σε κάποιο άλλο μέρος κάθε φορά που αποστέλλεται ένα μήνυμα κειμένου ή εικόνας- και για αυτό αποτελεί έναν από τους πιο σημαντικούς τρόπους προστασίας των δεδομένων που αποθηκεύονται ή χρησιμοποιούνται στις εφαρμογές των έξυπνων κινητών τηλεφώνων.

Η τεχνική του "application sandboxing" ή αλλιώς "application containerization"[226] αποτελεί επίσης μέτρο για την προστασία των δεδομένων του χρήστη, ειδικότερα όταν αυτά βρίσκονται σε κατάσταση ηρεμίας ("data at rest"). Πρόκειται για μία προσέγγιση ανάπτυξης και διαχείρισης των εφαρμογών για έξυπνα κινητά τηλέφωνα, βάσει της οποίας περιορίζονται εξαιρετικά τα περιβάλλοντα στα οποία μπορεί να εκτελεστεί συγκεκριμένος κώδικας και κατ' επέκταση να αποθηκευτούν τα δεδομένα του χρήστη[227], αφού η εκάστοτε εφαρμογή απομονώνεται μέσα σε ένα «ψηφιακό κοντέινερ» το οποίο περιέχει μόνο δεδομένα που δημιουργεί η ίδια[228]. Σημειώνεται ότι τόσο η Apple όσο και η Google

---

[223] Τα λειτουργικά συστήματα iOS και το Android παρέχουν κρυπτογράφηση δίσκου για την προστασία των δεδομένων που συλλέγονται από εφαρμογές και αποθηκεύονται στη συσκευή του χρήστη.

[224] Sun G., Xie Y., Liao D., Yu H., and Chang V. (2017) "User-defined privacy location-sharing system in mobile online social networks", Journal of Network and Computer Applications, Volume 86, Pages 34-45, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.11.024 (τελευταία πρόσβαση στις 19.03.2022)

[225] Άρθρο 32 παρ. 1 ΓΚΠΔ και Αιτιολογική Σκέψη 83 ΓΚΠΔ.

[226] https://www.appdome.com/how-to/mobile-app-security/no-code-data-encryption/prevent-mobile-data-exploits-data-at-rest-encryption/ (τελευταία πρόσβαση στις 19.03.2022)

[227] https://www.techtarget.com/searchmobilecomputing/definition/application-sandboxing (τελευταία πρόσβαση στις 19.03.2022)

[228] Joris van Hoboken, Fathaigh R Ó (2021), "Smartphone platforms as privacy regulators", Computer Law and Security Review, Volume 41, July 2021, 105557, Elsevier Journal, p.9, https://doi.org/10.1016/j.clsr.2021.105557 (τελευταία πρόσβαση στις 19.03.2022)

εφαρμόζουν αυτή την τεχνική δυνατότητα. Η Apple περιγράφει αυτό το τεχνικό χαρακτηριστικό ως απομόνωση των δεδομένων χρήστη σε μια εφαρμογή από άλλες εφαρμογές, καθώς και προστασία τους από ανεπιθύμητη πρόσβαση από άλλες εφαρμογές. Ομοίως, η Google εφαρμόζει την τεχνική αυτή για να διασφαλίσει ότι οι εφαρμογές δεν μπορούν να αλληλοεπιδράσουν μεταξύ τους και ότι έχουν περιορισμένη πρόσβαση στο λειτουργικό σύστημα που αυτή παρέχει στον τελικό χρήστη του έξυπνου κινητού τηλεφώνου[229].

Όσον αφορά ακολούθως την προστασία των δεδομένων θέσης, τα οποία είτε δηλώνονται από τον ίδιο τον χρήστη, είτε συλλέγονται αυτόματα από τα μέσα κοινωνικής δικτύωσης μέσω μίας έξυπνης συσκευής, έχει αναπτυχθεί η τεχνική "k-anonymity"[230], προκειμένου να καταστεί εφικτός ο διαχωρισμός τοποθεσίας-χρήστη[231]. Συνδυάζοντας σύνολα δεδομένων με παρόμοια χαρακτηριστικά, ο εντοπισμός πληροφοριών που αφορούν ένα από τα υποκείμενα των δεδομένων που περιέχονται στο σύνολο, μπορεί να καθίσταται δύσκολος έως αδύνατος. Τα δεδομένα των μελών συγκεντρώνονται σε μια μεγαλύτερη ομάδα δεδομένων, πράγμα που σημαίνει ότι οι πληροφορίες που βρίσκονται εκεί θα μπορούσαν να αντιστοιχούν σε οποιοδήποτε μεμονωμένο μέλος, αποκρύπτοντας ή καλύπτοντας έτσι την ταυτότητα αυτού που αναζητείται[232]. Σημειώνεται, επιπλέον, ότι το "k" στην τεχνική "k-anonymity" αναφέρεται σε μια μεταβλητή τιμή, η οποία αφορά τον αριθμό των φορών που κάθε συνδυασμός τιμών εμφανίζεται σε ένα σύνολο δεδομένων[233].

Η ενσωμάτωση των παραπάνω τεχνικών για την επέκταση της ιδιωτικότητας του χρήστη στο επίπεδο του αρχικού σχεδιασμού μίας εφαρμογής για έξυπνα κινητά τηλέφωνα μπορεί

---

[229] Joris van Hoboken, Fathaigh R Ó (2021), "Smartphone platforms as privacy regulators", Computer Law and Security Review, Volume 41, July 2021, 105557, Elsevier Journal, p.9, https://doi.org/10.1016/j.clsr.2021.105557 (τελευταία πρόσβαση στις 19.03.2022)

[230] Αναφέρεται και ως η τεχνική "Hiding in the Crowd".

[231] Sun G., Xie Y., Liao D., Yu H., and Chang V. (2017) "User-defined privacy location-sharing system in mobile online social networks", Journal of Network and Computer Applications, Volume 86, Pages 34-45, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.11.024 (τελευταία πρόσβαση στις 19.03.2022)

[232] Kang J., Steiert D., Lin D., and Fu Y. (2020), "Move With Me: Location Privacy Preservation for Smartphone Users", IEEE Transactions On Information Forensics And Security, Volume 15, p. 711-724, https://dl.acm.org/doi/abs/10.1109/TIFS.2019.2928205 (τελευταία πρόσβαση στις 19.03.2022)

[233] Αν για παράδειγμα k=2, τα σημεία δεδομένων έχουν γενικευθεί αρκετά ώστε να υπάρχουν τουλάχιστον δύο συνδυασμοί δεδομένων στην ομάδα. Ειδικότερα στην περίπτωση των μέσων κοινωνικής δικτύωσης, εάν ένα σύνολο δεδομένων περιλαμβάνει τοποθεσίες και ηλικίες για μια ομάδα χρηστών, τα δεδομένα θα πρέπει να γενικευθούν τόσο ώστε κάθε ζευγάρι τοποθεσιών-ηλικιών να εμφανίζεται τουλάχιστον δύο φορές, https://www.immuta.com/articles/k-anonymity-everything-you-need-to-know-2021-guide/ (τελευταία πρόσβαση στις 19.03.2022)

να οδηγήσει σε μείωση των πιθανοτήτων της παράνομης ή μη εξουσιοδοτημένης αποκάλυψης, συλλογής, διατήρησης και διαβίβασης προσωπικών δεδομένων, με την παράλληλη διατήρηση υψηλής λειτουργικότητας αυτών των εφαρμογών[234].

[234] Islam M. B., and Iannella R. (2011), "Privacy by Design: Does it matter for Social Networks?", Conference Paper, Conference: IFIP Summer School 2011, p. 3, https://dl.ifip.org/db/conf/primelife/primelife2011/IslamI11.pdf (τελευταία πρόσβαση στις 19.03.2022)

ΕΠΙΛΟΓΟΣ

Τα τελευταία χρόνια, τα οικοσυστήματα έξυπνων κινητών τηλεφώνων επεκτείνονται ραγδαία, προσπαθώντας αδιάλειπτα να αυξήσουν τη δημοτικότητά τους και να ικανοποιήσουν τους χρήστες τους. Παράλληλα, τα μέσα κοινωνικής δικτύωσης γίνονται ολοένα και ισχυρότερα, επεκτείνοντας τις δυνατότητές τους, με την ανάπτυξη καινοτόμων υπηρεσιών όπως το Metaverse, το οποίο θα αποτελέσει σίγουρα τα επόμενα χρόνια την μετεξέλιξή τους, προσθέτοντας νέες παραμέτρους στην πρόκληση της προστασίας της ιδιωτικότητας.

Από τις προκλήσεις των κοινωνικών δικτύων στα οικοσυστήματα των έξυπνων κινητών τηλεφώνων, η προστασία των δικαιωμάτων και των ελευθεριών των χρηστών από την έναρξη κατασκευής μίας εφαρμογής έως την οριστική κατάργησή της από ένα λειτουργικό σύστημα είναι ζωτικής σημασίας και αποτελεί κανονιστική απαίτηση για όλα τα εμπλεκόμενα μέρη. Εναπόκειται επομένως, σε όλα τα μέρη ενός οικοσυστήματος έξυπνων κινητών τηλεφώνων να παρέχουν στους χρήστες τους μια ποικιλία εργαλείων υποστήριξης, ευθυγραμμιζόμενων με το κανονιστικό πλαίσιο για την προστασία της ιδιωτικότητας, όπως βελτιωμένες δυνατότητες διαχείρισης δεδομένων, εύχρηστες διεπαφές, λεπτομερή έλεγχο πρόσβασης και ασφαλή αποθήκευση και διαβίβαση προσωπικών δεδομένων στο διαδίκτυο. Στόχο αποτελεί η χορήγηση στον χρήστη μεγαλύτερου ελέγχου των δεδομένων του και η ευαισθητοποίησή του σχετικά με τους κινδύνους κατά τη χρήστη των εκάστοτε εφαρμογών.

Είναι βέβαιο πως, οπουδήποτε κι αν βρίσκεται ο άνθρωπος των σημερινών και των επόμενων γενεών, θα έχει πάντοτε τη δυνατότητα να συνδεθεί στα μέσα κοινωνικής δικτύωσής του μέσω του έξυπνου κινητού του τηλεφώνου ή μίας έξυπνης συσκευής και να απολαύσει την ελευθερία της «δωρεάν» επικοινωνίας οποτεδήποτε το επιθυμεί. Η ιλιγγιώδης ωστόσο επεξεργασία προσωπικών δεδομένων των χρηστών αποτελεί στην πραγματικότητα το αντάλλαγμα για την απόλαυση των υπηρεσιών αυτών, τίμημα το οποίο συχνά κρίνεται δυσανάλογο σε σχέση με τον σκοπό της χρήσης των μέσων αυτών. Οι ανησυχίες έτσι για το επίπεδο προστασίας της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης είναι συνεχείς, ενώ κρίσιμες παραμένουν ακόμη οι επιπτώσεις της αποτυχίας των εμπλεκόμενων μερών να ανταποκριθούν στις υποχρεώσεις τους για την προστασία των προσωπικών δεδομένων των χρηστών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Κανέλλος Λ. (2020), The GDPR Handbook, Εκδόσεις Νομική Βιβλιοθήκη

2. ΞΕΝΟΓΛΩΣΣΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Gkoulalas - Divanis A., and Bettini Cl. (2018), "Handbook of Mobile Data Privacy", Springer Nature Switzerland AG 2018

Petronio S. (2002), "Boundaries of Privacy: Dialectics of Disclosure", Albany, NY: State University of New York Press

Taal A. (2022), "The GDPR Challenge: Privacy, Technology, and Compliance in an Age of Accelerating Change", CRC Press

Zuboff S. (2019), "The Age of Surveillance Capitalism", London: Profile Books

3. ΞΕΝΟΓΛΩΣΣΗ ΑΡΘΡΟΓΡΑΦΙΑ

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015) "Privacy and human behavior in the age of information," Science (New York, N.Y.) (347:6221), pp. 509–514.

Acquisti A. and Grossklags J. (2005) "Privacy and rationality in individual decision making", IEEE, Security and Privacy Magazine, Volume 3 (1), DOI:10.1109/MSP.2005.22

Acquisti A. and Grossklags J. (2006), "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", In: Danezis G., Golle P. (eds) Privacy Enhancing Technologies. PET 2006. Lecture Notes in Computer Science, Volume 4258, Springer, Berlin, Heidelberg. **https://doi.org/10.1007/11957454_3**

Ajami R., Al Qirim N., and Ramadan N. (2012), "Privacy Issues in Mobile Social Networks", The 9th International Conference on Mobile Web Information Systems (MobiWIS), Procedia Computer Science, Volume 10, https://www.researchgate.net/publication/257719381_Privacy_Issues_in_Mobile_Social_Networks

Al Johani M. (2016) "Personal Information Disclosure and Privacy in Social Networking Sites", Master Thesis, School of Engineering, Computer and Mathematical Sciences, New Zealand, http://orapp.aut.ac.nz/bitstream/handle/10292/10320/AlJohaniM.pdf?sequence=3&isAllowed=y

Barth S. and De Jong M DT (2017), "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online behavior–a systematic literature review", Telematics and Informatics, Volume 34(7), Elsevier Journal, pp. 1038–1058, https://www.sciencedirect.com/science/article/pii/S0736585317302022

Basole R. C., Russel M. G., Huhtamäki J. and Rubens N. (2012), "Understanding Mobile Ecosystem Dynamics: A Data-Driven Approach", 2012 International Conference on Mobile Business. 15., http://aisel.aisnet.org/icmb2012/15

Beresford A.R., Kübler D. and Preibusch S. (2012) "Unwillingness to pay for privacy: A field experiment", Economics Letters, Elsevier Journal, Volume 117, Issue 1, https://doi.org/10.1016/j.econlet.2012.04.077

Betzing J.H., Tietz M., vom Brocke J. et al. (2020) "The impact of transparency on mobile privacy decision making", Electron Markets, Volume 30, pp. 607–625, https://doi.org/10.1007/s12525-019-00332-3

Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T. and Shadbolt N. (2018), "Third Party Tracking in the Mobile Ecosystem", https://www.researchgate.net/publication/326138940_Third_Party_Tracking_in_the_Mobile_Ecosystem

Bruce Schneier, Schneier B. (2010) "A taxonomy of social networking data", IEEE Security and Privacy 8(4) (2010) 88, https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html

Buck Ch., Burster S., and Eymann T. (2017) "Priming app information privacy concerns in mobile ecosystems", Working Paper on Information Systems, No. 63, University of Bayreuth, Chair of Information Systems, http://nbn-resolving.de/urn:nbn:de:bvb:703-epub-3419-8

Bujari A., Furini M., Mandreoli F., Martoglia R., Montangero M., and Ronzani D. (2018), "Standards, security and business models: Key challenges for the iot scenario", Mobile Networks and Applications, 23(1):147–154

Bu-Pasha, S., Alen-Savikko, A., Makinen, J., Guinness, R., & Korpisaari, P. (2016), "Eu law perspectives on location data privacy in smartphones and informed consent for transparency", European Data Protection Law Review (EDPL), 2(3)

Buschel et al. (2014), "Protecting Human Health and Security in Digital Europe: How to Deal With The Privacy Paradox?", Science and Engineering Ethics, Volume 20, pp. 639-658

Cain J. A. and Imre I. (2021) "Everybody wants some: Collection and control of personal information, privacy concerns, and social media use", Article in New media & Society, Sage Journals, 1–20, DOI: 10.1177/14614448211000327 https://journals.sagepub.com/home/nms

Castelluccia C., Guerses S., Hansen M., Hoepman J. H., van Hoboken J., and Vieira B. (2017), "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", ENISA, the European Union Agency for Network and Information Security, https://doi.org/10.2824/114584

Cheung Anne S.Y. (2014), "Location privacy: The challenges of mobile service devices", Computer Law and Security Review, Volume 30, 2014, Elsevier Journal, 41-54, https://doi.org/10.1016/j.clsr.2013.11.005

Chrysakis et al. (2020) "Evaluating the data privacy of mobile applications through crowdsourcing", Legal Knowledge and Information Systems, Project: CAP-A: A Community-

driven Approach to Privacy Awareness, https://www.researchgate.net/publication/347320509_Evaluating_the_Data_Privacy_of_Mobile_Applications_Through_Crowdsourcing

Culnan M.J. and Armstrong P.K. (1999) "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", Organ. Sci. Volume 10, pp. 104–115, https://doi.org/10.1287/orsc.10.1.104

Debatin et al. (2009) "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", Journal of Computer-Mediated Communication, Volume 15, Issue 1, 1 Pages 83–108, https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dwyer C, Hiltz SR and Passerini K (2007) "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and Myspace", Conference Paper, Thirteenth Americas Conference on Information Systems, Keystone, CO. http://csis.pace.edu/dwyer/research/DwyerAMCIS2007.pdf

Fiesler C., Beard N. and Keegan B. C. (2020) "No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service", Conference Paper, Proceedings of the Fourteenth International AAAI Conference on Web and Social Media (ICWSM 2020), Volume 14, https://ojs.aaai.org/index.php/ICWSM/article/view/7290

Furini M., Mirri S., Montangero M., and Prandi C. (2020), "Privacy Perception when using Smartphone Applications", Mobile Networks and Applications, 25(5):1-7, June 2020, DOI: 10.1007/s11036-020-01529-z, (PDF) Privacy Perception when Using Smartphone Applications (researchgate.net)

Hansen M., Hoepman J.H., and Jensen M. (2016), "Towards Measuring Maturity of Privacy Enhancing Technologies," in Annual Privacy Forum (APF 2015), DOI: 10.1007/978-3-319-31456-3_1

Hansen M., Jensen M. and Rost M. (2015) "Protection Goals for Privacy Engineering," in International Workshop on Privacy Engineering (IWPE), IEEE CS Security and Privacy Workshops (SPW), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163220

Huang E.,Y., and Lin C.,Y., (2005) "Customer-oriented financial service personalization" Industrial Management & Data Systems Vol. 105 (1), pp. 26-44

Islam M. B., and Iannella R. (2011), "Privacy by Design: Does it matter for Social Networks?", Conference Paper, Conference: IFIP Summer School 2011, https://dl.ifip.org/db/conf/primelife/primelife2011/IslamI11.pdf

Joris van Hoboken, Fathaigh R Ó (2021), "Smartphone platforms as privacy regulators", Computer Law and Security Review, Volume 41, July 2021, 105557, Elsevier Journal, https://doi.org/10.1016/j.clsr.2021.105557

Kang J., Steiert D., Lin D., and Fu Y. (2020), "Move With Me: Location Privacy Preservation for Smartphone Users", IEEE Transactions On Information Forensics And Security, Volume 15, p. 711-724, https://dl.acm.org/doi/10.1109/TIFS.2019.2928205

Kokolakis Sp. (2017) "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon", Computers & Security, Volume 64, Elsevier Journal, https://www.sciencedirect.com/science/article/pii/S0167404815001017

Kosta E., Kalloniatis Ch., Mitrou L. and Gritzalis S. (2010) "Data protection issues pertaining to social networking under EU law", Research Paper, Transforming Government: People, Process and Policy Vol. 4 No. 2, Emerald Group Publishing Limited, Transforming Government: People, Process and Policy | Emerald Insight

Li H.,Sarathy R., and Xu H. (2011), "The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors", Decision Support Systems, Volume 51, Issue 3, Pages 434-445, https://doi.org/10.1016/j.dss.2011.01.017

Libaque-Sáenz C.F.; Wong, S.F., Chang, Y., and Bravo, E.R. (2020) "The effect of Fair information practices and data collection methods on privacy-related behaviors: A study of Mobile apps", Information and Management, Volume 58, 103284, https://doi.org/10.1016/j.im.2020.103284

Lin J., Amini S., Hong J. I., Sadeh N., Lindqvist J., and Zhang J. (2012), "Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing", ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 501–510, 10.1145/2370216.2370290

Mahieu R., V. Hoboken J., and Asghari H. (2019), "Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe", Journal of Intellectual Property, Information Technology and Electronic Commerce Law, https://www.jipitec.eu/issues/jipitec-10-1-2019/4879

Michael M.G. and Michael K. (2010), "Toward a State of Uberveillance", 29(2), IEEE Technology and Society Magazine, https://www.researchgate.net/publication/224142358_Toward_a_State_of_Uberveillance_Special_Section_Introduction

Mitrou L., Kandias M., Stavrou V., and Gritzalis D. (2014), "Social media profiling: A Panopticon or Omniopticon tool?", in Proc. of the 6th Conference of the Surveillance Studies Network, Spain, April 2014, https://www.infosec.aueb.gr/Publications/2014-SSN-Privacy%20Social%20Media.pdf

Myers C. (2014), "Digital Immortality vs. "The Right to be Forgotten": A Comparison of U.S. and E.U. Laws Concerning Social Media Privacy", DOI:10.21018/rjcpr.2014.3.175

Obar J.A. and Hatelt A. (2019) "TL; DR and TC; DU: an assessment of the length and complexity of social media policies", Conference Paper, Association for education in journalism and mass communication Conference, Toronto, ON, Canada

Obar J.A. and Oeldorf-Hirsch A. (2020) "The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services", Information, Communication & Society, Volume 23, No. 1, https://doi.org/10.1080/1369118X.2018.1486870

Raad E., and Chbier R. (2013), "Privacy in Online Social Networks", Security and Privacy Preserving in Social Networks, Springer-Verlag Wien, https://hal.archives-ouvertes.fr/hal-00975998

Raad E., Chbeir R., Dipanda A. (2013) "Discovering relationship types between users using profiles and shared photos in a social network", Multimedia Tools and Applications, 64(1) (2013) 141–170, https://hal.archives-ouvertes.fr/hal-00665036

Rewaria S. (2021), "Data Privacy In Social Media Platform: Issues And Challenges", http://dx.doi.org/10.2139/ssrn.3793386

Richthammer et al. (2014) "Taxonomy of social network data types", EURASIP Journal on Information Security, 2014:11 http://jis.eurasipjournals.com/content/2014/1/11

Roesner F., Kohno T., Moshchuk, A., Parno B., Wang, H.J., and Cowan C. (2012), "User-driven access control: Rethinking permission granting in modern operating systems", Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012, pp. 224–238, https://www.microsoft.com/en-us/research/publication/user-driven-access-control-rethinking-permission-granting-in-modern-operating-systems-2/

Rustad M. L. and Koenig T. H. (2014) "Wolves of the world wide web: reforming social networks' contracting practices", Wake Forest Law Review, Volume 49, p. 1431, Suffolk University Law School Research Paper No. 14-25, https://ssrn.com/abstract=2479918

Tsai et al. (2011) "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", Information Systems Research, Volume 22 No 2, pp. 254-268, https://www.jstor.org/stable/23015560

Scassa T. (2009) "Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy", Canadian Journal of Law and Technology, Volume 7, Article 7, https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1106&context=cjlt

Shklovskii. I., Mainwaring S. D., Skúladóttir H. H., and Borgthorsson H. (2014), "Leakiness and creepiness in app space: Perceptions of privacy and mobile app use", ACM Conference on Human Factors in Computing Systems, pages 2347–2356, https://doi.org/10.1145/2556288.2557421

Schmitt P., Raghavan B. (2020), "Pretty Good Phone Privacy", https://www.researchgate.net/publication/344334346_Pretty_Good_Phone_Privacy

Schneier B. (2010) "A taxonomy of social networking data", IEEE Security and Privacy 8(4) (2010) 88, https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html

Sun G., Xie Y., Liao D., Yu H., and Chang V. (2017) "User-defined privacy location-sharing system in mobile online social networks", Journal of Network and Computer Applications, Volume 86, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2016.11.024

Tang J., Zhang B., and Akram U. (2021), "What Drives Authorization in Mobile Applications? A Perspective of Privacy Boundary Management", Information 2021, 12, 311, https://doi.org/10.3390/info12080311

Themistocleous Ch., Smith A. and Wagner Ch. (2014) "The ethical dilemma of implicit vs explicit data collection: Examining the factors that influence the voluntary disclosure of information by consumers to commercial organizations", Conference Paper, IEEE International Symposium on Ethics in Science, Technology and Engineering, p.1., https://dl.acm.org/doi/pdf/10.5555/2960587.2960632

Ward O. (2021), "Stop scrolling: EDPB adopts guidelines on targeting of social media users", Article posted on Lexology, https://www.lexology.com/library/detail.aspx?g=37c91855-2562-4c4b-bc62-a8cb8908202a

Xu H., Dinev T., Smith J. and Hart P. (2011), "Information privacy concerns: Linking individual perceptions with institutional privacy assurances", J. Assoc. Inf. Syst. Volume 12, 1, "Information Privacy Concerns: Linking Individual Perceptions with Inst" by Heng Xu, Tamara Dinev et al. (aisnet.org)

Xu H., Gupta S., Rosson M. B., and Carroll J. M. (2012), "Measuring Mobile Users' Concerns For Information Privacy", Completed Research Paper, Thirty Third International Conference on Information Systems, Orlando 2012, Published in ICIS, https://www.semanticscholar.org/paper/Measuring-Mobile-Users%27-Concerns-for-Information-Xu-Gupta/8ae62044520374dda95952e98204214fb999fcda

Yerukhimovich A., Balebako R., Boustead A. E., Cunningham R. K., Welser IV W., Housley R., Shay R., Spensky Ch., Stanley K. D., Stewart J., Trachtenberg A., and Winkelman Z. (2016), "Can Smartphones and Privacy Coexist? Assessing Technologies and Regulations Protecting Personal Data on Android and iOS Devices", Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/research_reports/RR1393.html

Zhang N., Wang Ch. And Xu Y. (2011), "Privacy in Online Social Networks", Completed Research Paper, Thirty Second International Conference on Information Systems, Shanghai 2011, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.8584&rep=rep1&type=pdf

4. ΛΟΙΠΕΣ ΠΗΓΕΣ

European Union Agency for Network and Information Security "ENISA" (2014), «Privacy and Data Protection by Design – from policy to engineering», https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

European Union Agency for Network and Information Security "ENISA" (2017) "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR", https://pure.uva.nl/ws/files/42887337/22302384.pdf

GSMA Association (2017), "Safety, privacy and security across the mobile ecosystem: Key issues and policy implications", GSMA Report, https://aiforimpacttoolkit.gsma.com/resources/GSMA-report_Safety-Privacy-and-Security-across-the-mobile-ecosystem.pdf

Παπαβασιλείου Β., Φωκιάλη Π., Νικολάου Ε., Μαντζάνος Δ. και Καΐλα Μ. (2017), «Κοινωνική και Πολιτισμική Βιωσιμότητα», ΠΜΣ Περιβαλλοντική Εκπαίδευση, ΤΕΠΑΕΣ, Πανεπιστήμιο Αιγαίου, Ρόδος 2017

Παράσχης Σπ. (2012), «Κοινωνικά Δίκτυα μέσω φορητών συσκευών: Η προστασία της θέσης», Μεταπτυχιακή Διατριβή, Πανεπιστήμιο Πειραιώς, διαθέσιμη στο https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4926/Paraschis.pdf?sequence=2&isAllowed=y

5. ΒΑΣΙΚΕΣ ΙΣΤΟΣΕΛΙΔΕΣ

https://android.com/enterprise/data-protection/

https://www.appdome.com/how-to/mobile-app-security/no-code-data-encryption/prevent-mobile-data-exploits-data-at-rest-encryption/

https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf#page111

https://blog.hootsuite.com/types-of-social-media/

https://cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

https://cookies.insites.com/

https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=2151335

https://curia.europa.eu/juris/document/document.jsf?text=&docid=209357&doclang=EL

https://curia.europa.eu/juris/liste.jsf?language=el&num=c-131/12

https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/14039b47-2e2f-4054-9dc5-71bcc7cf01ce.pdf

https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

https://developer.android.com

https://developer.apple.com

https://dictionary.cambridge.org

https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

https://dl.acm.org/doi/abs/10.1109/TIFS.2019.2928205

https://ec.europa.eu/newsroom/article29/items/622227

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_el

https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en,

https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_el.pdf

https://www.emerald.com/insight/publication/issn/1757-5818

https://europarl.europa.eu/news/en/press-room/20210204IPR97120/regulate-social-media-platforms-to-defend-democracy-meps-say

https://gdpr.eu/cookies/

https://google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636596607835233538-3993345926&hl=el&rd=1

https://help.instagram.com/370452623149242/?helpref=hc_fnav

https://iabeurope.eu/about-us/

https://www.igi-global.com/dictionary/smartphone-application/47827

https://www.immuta.com/articles/k-anonymity-everything-you-need-to-know-2021-guide/

https://ironcladapp.com/journal/contract-management/what-is-a-clickwrap-agreement/

https://lawspot.gr/nomika-blogs/stergios_konstantinoy/velgiki-apdph-horis-nomimi-vasi-oi-diadiktyakes-diafimiseis?lspt_destination=upgrade#_ftn6

https://www.legalcheek.com/lc-journal-posts/gdpr-social-media-and-the-right-to-be-forgotten/

https://statista.com

https://support.google.com/analytics/answer/10022331?hl=el

https://www.techtarget.com/searchmobilecomputing/definition/application-sandboxing

https://techopedia.com/definition/2953/mobile-application-mobile-app

https://twitter.com/en/tos