ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΔΙΚΤΥΑΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εξέταση Απειλών Ιδιωτικότητας και Δεδομένων Προσωπικού Χαρακτήρα σε Εφαρμογές Ηλεκτρονικών Αγορών του Περιβάλλοντος Android

Νικόλαος Δ. Μπαλάμπος

Επιβλέπων: **Κωνσταντίνος Λιμνιώτης,** Διδάσκων εκτός Τμήματος

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2024

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Εξέταση Απειλών Ιδιωτικότητας και Δεδομένων Προσωπικού Χαρακτήρα σε Εφαρμογές Ηλεκτρονικών Αγορών του Περιβάλλοντος Android

Νικόλαος Δ. Μπαλάμπος

Α.Μ.: Μ1571

ΕΠΙΒΛΕΠΩΝ: **Κωνσταντίνος Λιμνιώτης,** Διδάσκων εκτός Τμήματος

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: **Νικόλαος Πασσάς,** Εργαστηριακό Διδακτικό Προσωπικό
Δημήτριος Κατσιάνης, Διδάσκων εκτός Τμήματος

Οκτώβριος 2024

ΠΕΡΙΛΗΨΗ

Αντικείμενο της εργασίας αυτής είναι η μελέτη του τρόπου εκτέλεσης των εφαρμογών στο λειτουργικό σύστημα Android και η πιθανή απειλή, που προκύπτει ως αποτέλεσμα του τρόπου εκτέλεσης, για την ιδιωτικότητα και τα δεδομένα προσωπικού χαρακτήρα του χρήστη. Εξετάζονται διάφορες δημοφιλείς εφαρμογές οι οποίες προσφέρουν δυνατότητα ηλεκτρονικών αγορών, καθώς και η συμμόρφωσή τους με το Γενικό Κανονισμό για την Προστασία των Δεδομένων.

Αρχικά, γίνεται αναφορά στον Γενικό Κανονισμό για την Προστασία των Δεδομένων, ο οποίος εφαρμόζεταιστα κράτη-μέλη της Ευρωπαϊκής Ένωσης. Ο κανονισμός αυτός θεσπίζει κανόνες, οι οποίοι αφορούν την επεξεργασία και κυκλοφορία δεδομένων προσωπικού χαρακτήρα των πολιτών της Ευρωπαϊκής Ένωσης. Περιγράφονται τα κυριότερα άρθρα του, όπως αυτά τα οποία διέπουν την επεξεργασία των δεδομένων, καθώς και τη νομική της βάση. Επίσης, γίνεται αναφορά στις αρχές Προστασίας Εξ' Ορισμού και Προστασίας Ήδη από το Σχεδιασμό.

Στη συνέχεια, παρατίθεται βιβλιογραφική έρευνα για τον τρόπο εκτέλεσης των εφαρμογών στο λειτουργικό σύστημα Android. Εξετάζονται τα βασικά σημεία της αρχιτεκτονικής του, ενώ στη συνέχεια περιγράφεται ο τρόπος εκχώρησης πόρων και εκτέλεσης μιας εφαρμογής, εντός του δικού της ελεγχόμενου περιβάλλοντος. Στις δύο τελευταίες ενότητες, εξετάζονται τα permissions, η έγκριση των οποίων δίνει σημαντικά περισσότερες λειτουργικότητες στην εφαρμογή, καθώς και διάφορα αναγνωριστικά, τα οποία μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του χρήστη.

Η βιβλιογραφική έρευνα συνεχίζεται, με την εξέταση του τρόπου λειτουργίας του οικοσυστήματος προβολής διαφημίσεων. Εξετάζονται περιπτώσεις κατά τις οποίες η συλλογή δεδομένων ενδέχεται να επηρεάσει δυσμενώς τον χρήστη, καθώς και ο τρόπος με τον οποίο πραγματοποιείται αυτή η συλλογή. Γίνεται ξεχωριστή αναφορά σε δημοφιλείς τρόπους ιχνηλάτησης, όπως και στην τεχνική intra-library collusion.

Τέλος, μέσω προσομοιώσεων, εξετάζεται η εκτέλεση ενός συνόλου δημοφιλών εφαρμογών ηλεκτρονικών αγορών. Με χρήση στατικής ανάλυσης, εξάγονται τα permissions τα οποία αιτούνται οι εφαρμογές αυτές. Στη συνέχεια, με χρήση στατικής αλλά και δυναμικής ανάλυσης, εντοπίζονται οι ιχνηλάτες οι οποίοι συσχετίζονται με την εκάστοτε εφαρμογή. Ακολουθεί η εξέταση των πολιτικών απορρήτου των εφαρμογών αυτών και συγκεκριμένα του βαθμού ταύτισής τους με τα αποτελέσματα των προσομοιώσεων και του βαθμού υιοθέτησης των αρχών και πρακτικών που περιγράφονται στον Γενικό Κανονισμό για την Προστασία των Δεδομένων.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Προστασία Ιδιωτικότητας και Δεδομένων Προσωπικού Χαρακτήρα

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: ιδιωτικότητα, δεδομένα προσωπικού χαρακτήρα, Γενικός Κανονισμός Προστασίας για την Προστασία των Δεδομένων, εφαρμογές ηλεκτρονικών αγορών, Android

ABSTRACT

This study deals with the execution of applications within Android operating system, along with the privacy and personal data risks, stemming from the way of execution. A set of popular e-shopping applications are being examined, along with their compliance with General Data Protection Regulation (GDPR).

Firstly, GDPR is being examined. GDPR prescribes principles for processing and free movement of European Union residents' personal data. GDPR's main articles are being referred, especially those regulating data processing and its legal basis. Also, Data Protection by Default and Data Protection by Design principles are being examined.

Bibliographic research follows, describing the way of execution of an application running on Android operating system. Android architecture is being described, along with resource allocation and the application's execution within their own controlled environment. The chapter concludes, with the notion of permissions and the various Android identifiers.

The next chapter focuses on the way mobile advertising ecosystem works. Some cases of data collection, used to adversely influence user are being reported, along with the way this collection is being performed. Attention is drawn to popular tracking methods, along with intra-library collusion technique.

Finally, using simulations, a static and dynamic analysis is being performed on some popular e-shopping applications. Their permissions and trackers are being examined. The study concludes by reviewing the applications' privacy policies; specifically their degree of consonance with the simulation results and the adoption of GDPR's principles.

SUBJECT AREA: Privacy and Personal Data Protection

KEYWORDS: privacy, personal data, General Data Protection Regulation, e-shopping applications, Android

Στην οικογένειά μου

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον Διδάκτορα Κωνσταντίνο Λιμνιώτη για τη δυνατότητα που μου προσέφερε, ώστε να επιλέξω μεταξύ διαφόρων θεμάτων της συγκεκριμένης θεματικής περιοχής (προστασία δεδομένων προσωπικού χαρακτήρα), το θέμα που ταίριαζε περισσότερο στα ενδιαφέροντά μου.

Επίσης θα ήθελα να εκφράσω τις ευχαριστίες μου, για την πολύτιμη βοήθειά του στην επίλυση απορριών, την υπομονή του, καθώς και τον εμπλουτισμό της βιβλιογραφίας μου.

Αναγνωρίζω τη στήριξη της οικογένειάς μου, τόσο κατά τη διάρκεια εκπόνησης της εργασίας αυτής, όσο και κατά τη συνολική διάρκεια της εκπαιδευτικής μου σταδιοδρομίας. Εκτιμώ ιδιαίτερα τη συμβολή της στη διεύρυνση των οριζόντων μου. Θα ήθελα να ευχαριστήσω τους γονείς μου, Τάκη και Ελένη, για την καθοδήγηση που μου προσέφεραν, καθώς και τον αδελφό μου, Θανάση, για την αμέριστη και ειλικρινή στήριξή του.

Ευχαριστώ τον αληθινό μου φίλο, Βαγγέλη, για την ηθική συμπαράστασή του κατά τη διάρκεια των φοιτητικών μου χρόνων. Παρότι μόλις δώδεκα μήνες στα ίδια έδρανα, αρκούν για μια πραγματική και διαχρονική φιλία.

Επίσης, ευχαριστώ τον εξαιρετικό φίλο και συνάδελφο, Γιώργο, για την καθοδήγηση και υποστήριξη, σχεδόν από τα πρώτα βήματα της επαγγελματικής μου σταδιοδρομίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα εργασία εκπονήθηκε στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, στο πλαίσιο του Μεταπτυχιακού Προγράμματος Σπουδών "Πληροφορική και Τηλεπικοινωνίες" στην ειδίκευση "Τηλεπικοινωνιακά Συστήματα και Δικτυακές Τεχνολογίες", υπό την επίβλεψη του διδάκτορα Κωνσταντίνου Λιμνιώτη. Το αντικείμενο της εργασίας, εξετάζεται τόσο θεωρητικά, μέσω βιβλιογραφικής έρευνας, όσο και πειραματικά, μέσω προσομοιώσεων με χρήση του λογισμικού GenyMotion. Κατά τη διάρκεια της ενασχόλησης μου με την εργασία αυτή, στάθηκε πολύτιμη η συνεργασία με τον διδάκτορα Κωνσταντίνο Λιμνιώτη, τον οποίο ευχαριστώ θερμά.

1. ΕΙΣΑΓΩΓΗ

Οι κινητές επικοινωνίες έχουν γνωρίσει ιδιαίτερα μεγάλη ανάπτυξη τα τελευταία 25 χρόνια. Η ανάπτυξη υποδομών 3G, καθώς και η έλευση των πρώτων smartphones στα μέσα της δεκαετίας του 2000, αποτέλεσε το έναυσμα για την ευρεία εξάπλωση της πρόσβασης στο internet μέσω των κινητών συσκευών.

Το λειτουργικό σύστημα Android, ανεπτυγμένο κυρίως από τη Google, από τα τέλη της δεκαετίας του 2000, αποτελεί το ευρύτερα χρησιμοποιούμενο λειτουργικό σύστημα για χρήση σε smartphones. Οι δυνατότητες των σημερινών κινητών μπορούν να αξιοποιηθούν σε μεγάλο βαθμό από τις εφαρμογές οι οποίες είναι διαθέσιμες, είτε δωρεάν είτε επί πληρωμή, από το Google Play Store ή από τρίτες υπηρεσίες διανομής περιεχομένου.

Μια εφαρμογή, ανεπτυγμένη για το λειτουργικό σύστημα Android, εκτελείται εντός ενός εικονικού περιβάλλοντος, παρόμοια με μια εφαρμογή Java. Με αυτόν τον τρόπο εκτέλεσης, προστατεύεται το ίδιο το λειτουργικό σύστημα, καθώς και οι υπόλοιπες εφαρμογές και οι αποθηκευμένες πληροφορίες του χρήστη. Επίσης, ελέγχεται αυστηρά η πρόσβαση στους διάφορους πόρους της συσκευής, όπως η κάμερα και ο δέκτης GPS.

Κατ' εξαίρεση, μια εφαρμογή μπορεί να ζητήσει πρόσβαση σε πόρους εκτός του ελεγχόμενου περιβάλλοντος στο οποίο εκτελείται. Από τη στιγμή που το ίδιο το Android, ή για κάποια κρίσιμα είδη προσβάσεων ο ίδιος ο χρήστης, της εκχωρήσει τη ζητούμενη πρόσβαση, ο τρόπος που θα χρησιμοποιηθούν οι πόροι αυτοί επαφίεται στην ίδια την εφαρμογή.

Καθώς οι προγραμματιστές και οι εκδότες των εφαρμογών ενδέχεται να έχουν σημαντικό οικονομικό όφελος μέσω της συλλογής δεδομένων προσωπικού χαρακτήρα κατά την πρόσβαση σε συγκεκριμένους πόρους, έχουν θεσπιστεί κανονισμοί, οι οποίοι καθορίζουν τα πλαίσια στα οποία πραγματοποιείται η συλλογή και η μετέπειτα επεξεργασία των δεδομένων. Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων αποτελεί την Ευρωπαϊκή πρωτοβουλία για την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών της Ευρωπαϊκής Ένωσης. Μεταξύ άλλων, θεσπίζονται κανόνες για τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα, η τήρηση των οποίων είναι υποχρεωτική για οποιονδήποτε διαχειρίζεται τέτοια δεδομένα πολιτών της Ευρωπαϊκής Ένωσης.

Στα πλαίσια της εργασίας, εξετάζονται 8 δημοφιλείς εφαρμογές οι οποίες υποστηρίζουν ηλεκτρονικές αγορές, αναφορικά με τις προσβάσεις τις οποίες αιτούνται, καθώς και με τα τρίτα μέρη με τα οποία ανταλλάσσουν δεδομένα κατά την εκτέλεσή τους. Καθώς η ανταλλαγή αυτών των δεδομένων ενδέχεται να περιλαμβάνει και δεδομένα προσωπικού χαρακτήρα των χρηστών, εξετάζεται επίσης η συμμόρφωσή τους με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων.

Ως εκ τούτου, τα βασικά ερευνητικά ερωτήματα της εν λόγω εργασίας έγκεινται στον έλεγχο συμμόρφωσης γνωστών εφαρμογών ηλεκτρονικών καταστημάτων ως προς τη νομοθεσία με τα προσωπικά δεδομένα, με έμφαση ιδίως στο αν η συντελούμενη επεξεργασία δεδομένων είναι διαφανής και αν είναι υπέρμετρη ή όχι.

2. ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ (GDPR)

2.1 Γενικά

Το δικαίωμα στην ιδιωτικότητα έχει κατοχυρωθεί από τον ΟΗΕ, μέσω της Οικουμενικής Διακήρυξης των Ανθρωπίνων Δικαιωμάτων (Άρθρο 12), ήδη από το 1948. [1]

Άρθρο 12

Κανείς δεν επιτρέπεται να υποστεί αυθαίρετες επεμβάσεις στην ιδιωτική του ζωή, την οικογένεια, την κατοικία ή την αλληλογραφία του, ούτε προσβολές της τιμής και της υπόληψης του. Καθένας έχει το δικαίωμα να τον προστατεύουν οι νόμοι από επεμβάσεις και προσβολές αυτού του είδους.

Ειδικά στην Ευρωπαϊκή Ένωση, η προστασία της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα, αποτελεί αντικείμενο των Άρθρων 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων. [2]

Άρθρο 7

Κάθε πρόσωπο έχει δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του.

Άρθρο 8

Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από τον νόμο. Κάθε πρόσωπο έχει δικαίωμα να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.

Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

Επίσης, όσον αφορά το Ευρωπαϊκό νομικό πλαίσιο, ο Ευρωπαϊκός Κανονισμός 2016/679 [Γενικός Κανονισμός για την Προστασία των Δεδομένων – General Data Protection Regulation – (GDPR)] αποτελεί τον κύριο Κανονισμό που διέπει τη συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα πολιτών των κρατών – μελών της Ευρωπαϊκής Ένωσης. [3]

Με έναρξη ισχύος την 25η Μαΐου 2018, ο GDPR αντικατέστησε την Data Protection Directive 95/46/EC.

2.2 Αντικείμενο, Στόχοι και Εδαφικό Πεδίο Εφαρμογής

Με βάση το Άρθρο 1, αντικείμενο του Κανονισμού, είναι η *θέσπιση κανόνων που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων*

προσωπικού χαρακτήρα και κανόνων που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα.

Ως στόχος του Κανονισμού, περιγράφεται η *προστασία θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα*.

Ένα ιδιαίτερο χαρακτηριστικό του Κανονισμού, όπως περιγράφεται στο Άρθρο 3, είναι το εδαφικό πεδίο εφαρμογής του. Συγκεκριμένα, παρότι αποτελεί κανονισμό της Ευρωπαϊκής Ένωσης, αποτελεί δεσμευτικό πλαίσιο λειτουργίας ακόμη και για εταιρείες με έδρα σε τρίτες χώρες, εφόσον αυτές δραστηριοποιούνται στη συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα πολιτών της Ευρωπαϊκής Ένωσης.

Άρθρο 3

Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

Ο παρών κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων των δεδομένων που βρίσκονται στην Ένωση από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με:

α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή

β) την παρακολούθηση της συμπεριφοράς τους, στον βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ένωσης.

Ειδικά για την περίπτωση της εξαγωγής δεδομένων προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης, υπάρχουν ιδιαίτερα δεσμευτικοί κανόνες, κάτω από τους οποίους κάτι τέτοιο μπορεί να πραγματοποιηθεί, όπως περιγράφεται στο Κεφάλαιο V του κανονισμού.

Όπως έχει προκύψει και στην πράξη, το Άρθρο 3 του GDPR, σε συνδυασμό με τα υψηλά πρόστιμα στην περίπτωση που δεν υπάρξει σωστή διαχείριση των δεδομένων προσωπικού χαρακτήρα, έχει οδηγήσει πολλές εταιρείες, ακόμα και εκτός Ευρωπαϊκής Ένωσης, στην τροποποίηση του τρόπου που διαχειρίζονται τα δεδομένα αυτά. Τέλος, ακόμη και άλλες χώρες, έχουν εκσυγχρονίσει τους αντίστοιχους νόμους τους. [4]

2.3 Ορισμοί

Στα Άρθρα 4 και 9, καθώς και στη Σκέψη 26, καταγράφονται διάφορες ορολογίες – κλειδιά, που αφορούν τα είδη των δεδομένων προσωπικού χαρακτήρα, τους εμπλεκομένους στην επεξεργασία τους, καθώς και τις διαδικασίες που αφορούν την ίδια την επεξεργασία.

Άρθρο 4

- **Δεδομένα Προσωπικού Χαρακτήρα (Personal Data):** *Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο [«υποκείμενο των δεδομένων (data subject)»]· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.*
- **Επεξεργασία (Processing):** *Κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.*
- **Κατάρτιση Προφίλ (Profiling):** *Οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.*
- **Ψευδωνυμοποίηση (Pseudonymisation):** *Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.*
- **Υπεύθυνος Επεξεργασίας (Controller):** *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.*
- **Εκτελών την Επεξεργασία (Processor):** *Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.*
- **Τρίτος (Third Party):** *Οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.*

Με βάση τον ορισμό των “δεδομένων προσωπικού χαρακτήρα”, όπως έχει διατυπωθεί στο Άρθρο 4, υπάρχουν διάφορες παράμετροι του Android οι οποίες μπορούν να

ενταχθούν στη συγκεκριμένη κατηγορία. Όπως περιγράφονται και στην Ενότητα 3.6, παραδείγματα τέτοιων παραμέτρων είναι ο Android ID, ο Google Advertising ID (GAID), καθώς και οι διευθύνσεις MAC και IP. Αυτό αιτιολογείται, διότι συνδυαζόμενες και με άλλες πληροφορίες μπορούν να οδηγήσουν στην ταυτοποίηση του χρήστη.

Μια ειδική κατηγορία δεδομένων προσωπικού χαρακτήρα ορίζεται στο Άρθρο 9. Τα ευαίσθητα δεδομένα προσωπικού χαρακτήρα (sensitive personal data) περιλαμβάνουν δεδομένα που σχετίζονται με *τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.*

Στη Σκέψη 26, καταγράφονται διάφορες λεπτές διαφορές μεταξύ δεδομένων προσωπικού χαρακτήρα, δεδομένων προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση (pseudonymous data), καθώς και ανώνυμων δεδομένων (Anonymous Data).

Τα δεδομένα που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζουν να θεωρούνται πληροφορίες σχετικές με ταυτοποιήσιμο φυσικό πρόσωπο. Έτσι, λαμβάνοντας υπόψη την δυνατότητα συσχέτισής τους με άλλες, συμπληρωματικές, πληροφορίες και λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία, είναι πιθανή η ταυτοποίηση του υποκειμένου. Συνεπώς, και για τα δεδομένα προσωπικού χαρακτήρα που έχουν υποστεί ψευδωνυμοποίηση, συνεχίζει να ισχύει ο GDPR.

Ως ανώνυμα, χαρακτηρίζονται τα δεδομένα που δεν σχετίζονται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Ο GDPR δεν ισχύει στην περίπτωση των ανώνυμων δεδομένων. Όμως, για τον χαρακτηρισμό τους ως τέτοια, θα πρέπει να ληφθεί υπόψη και η ύπαρξη άλλων συμπληρωματικών πληροφοριών και τεχνολογιών, που θα μπορούσαν να τα εντάξουν στα ψευδωνυμοποιημένα.

2.4 Αρχές που Διέπουν την Επεξεργασία

Στα Άρθρα 5 και 17 καταγράφονται οι αρχές που διέπουν την επεξεργασία και τη διαγραφή, αντίστοιχα, των δεδομένων προσωπικού χαρακτήρα.

Άρθρο 5

1. Τα δεδομένα προσωπικού χαρακτήρα:

α) Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων [«νομιμότητα, αντικειμενικότητα και διαφάνεια (lawfulness, fairness and transparency)»].

β) Συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς· η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς δεν θεωρείται ασύμβατη με τους αρχικούς σκοπούς [...] [«περιορισμός του σκοπού (purpose limitation)»].

γ) Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία [«ελαχιστοποίηση των δεδομένων (data minimisation)»].

δ) Είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας [«ακρίβεια (accuracy)»].

ε) Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα· τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον τα δεδομένα προσωπικού χαρακτήρα θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς [...] και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων [«περιορισμός της περιόδου αποθήκευσης (storage limitation)»].

στ) Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων [«ακεραιότητα και εμπιστευτικότητα (integrity and confidentiality)»].

2. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με την παράγραφο 1 [«λογοδοσία (accountability)»].

Άρθρο 17

Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση, εάν ισχύει ένας από τους ακόλουθους λόγους:

α) Τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

β) Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία [...] και δεν υπάρχει άλλη νομική βάση για την επεξεργασία.

γ) Το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία [...] και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία [...].

[...]

Ειδικά το Άρθρο 5, κωδικοποιεί τις αρχές που πρέπει να τηρούνται κατά την συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα, όσον αφορά τη “διαφάνεια”, ο χρήστης μιας εφαρμογής πρέπει να έχει πληροφορηθεί πλήρως και εξ’αρχής για την επεξεργασία των προσωπικών του δεδομένων και η πληροφόρηση αυτή πρέπει να έχει γίνει με κατανοητό τρόπο. Η πληροφόρηση αυτό πρέπει να

περιλαμβάνει τα δεδομένα που θα συλλεχθούν, τους εμπλεκομένους στην επεξεργασία, καθώς και τους λόγους για τους οποίους αυτή πραγματοποιείται. [5]

Οι αναφορές στον “περιορισμό του σκοπού”, στην “ελαχιστοποίηση των δεδομένων” , καθώς και στον “περιορισμό της περιόδου αποθήκευσης” υπάρχουν, ώστε να περιοριστεί η καταχρηστική συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

Η ρητή αναφορά για τη “λογοδοσία” του υπευθύνου επεξεργασίας αποτελεί σημείο – κλειδί της μετάβασης από την Data Protection Directive 95/46/EC στον GDPR. [6]

2.5 Νομιμότητα Επεξεργασίας (Νομική Βάση) & Συγκατάθεση Χρήστη

Προκειμένου η συλλογή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα να είναι έννομες, είναι απαραίτητο να στηρίζονται σε μια έγκυρη νομική βάση. Στον GDPR, η νομιμότητα της επεξεργασίας, περιγράφεται στα Άρθρα 4, 6 και 7.

Ειδικότερα, το Άρθρο 6 αναφέρεται στις προϋποθέσεις που πρέπει να πληρούνται, προκειμένου η επεξεργασία να θεωρείται νόμιμη.

Άρθρο 6

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) Το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς.

β) Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης.

γ) Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.

δ) Η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.

ε) Η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

στ) Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Η προϋπόθεση (α), δηλαδή η απλή συγκατάθεση του χρήστη, είναι αυτή που επικαλείται συνήθως για τη συλλογή και μετέπειτα επεξεργασία των δεδομένων προσωπικού χαρακτήρα, από τους προγραμματιστές των εφαρμογών.

Παρ'όλ'αυτά, ακόμα και η απλή συγκατάθεση του χρήστη, εφόσον αυτή δοθεί, πρέπει να πληροί διάφορα κριτήρια προκειμένου να θεωρηθεί νόμιμη. Αυτά περιγράφονται στα Άρθρα 4 και 7.

Άρθρο 4

- **Συγκατάθεση του Υποκειμένου των Δεδομένων (Data Subject Consent):** *Κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.*

Άρθρο 7

Εάν η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, το αίτημα για συγκατάθεση υποβάλλεται κατά τρόπο ώστε να είναι σαφώς διακριτό από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση. Κάθε τμήμα της δήλωσης αυτής το οποίο συνιστά παράβαση του παρόντος κανονισμού δεν είναι δεσμευτικό.

Το υποκείμενο των δεδομένων έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση προ της ανάκλησής της. Πριν την παροχή της συγκατάθεσης, το υποκείμενο των δεδομένων ενημερώνεται σχετικά. Η ανάκληση της συγκατάθεσης είναι εξίσου εύκολη με την παροχή της.

Κατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαιτέρως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης.

Με βάση τη διατύπωση της "συγκατάθεσης", υπάρχουν συγκεκριμένες προϋποθέσεις ώστε αυτή να θεωρηθεί έγκυρη. Πολλές φορές οι εφαρμογές αναγκάζουν τον χρήστη να αποδεχθεί την επεξεργασία των προσωπικών του δεδομένων από πρώτα ή τρίτα μέρη, ώστε να μπορέσει να εγκαταστήσει και να χρησιμοποιήσει την εφαρμογή. Επίσης, το σημείο της "πλήρους επίγνωσης" είναι άξιο αναφοράς, καθώς ενδέχεται η σχετική πληροφόρηση του χρήστη να είναι ελλιπής ή τουλάχιστον δυσνόητη. Τέλος, η αναφορά σε "σαφή θετική ενέργεια" σχετίζεται με την πρακτική "προστασίας εξ'ορισμού", όπως αυτή περιγράφεται στην Ενότητα 2.6.

2.6 Προστασία Εξ' Ορισμού & Ήδη από τον Σχεδιασμό

Ο ίδιος ο GDPR, μέσω της Σκέψης 32 και του επακόλουθου Άρθρου 25, μεριμνεί για την εφαρμογή των μεθόδων Προστασίας Δεδομένων Εξ' Ορισμού (Data Protection by Default) και Προστασίας Δεδομένων Ήδη από το Σχεδιασμό (Data Protection by

Design). Μέσω του πρώτου, ο προγραμματιστής δεσμεύεται ώστε να μην προσπαθήσει να “ξεγελάσει” τον χρήστη, μέσω κατάλληλων προεπιλεγμένων ρυθμίσεων που θα έχουν ως αποτέλεσμα την κοινοποίηση δεδομένων προσωπικού χαρακτήρα προς πρώτα ή τρίτα μέρη. Η δεύτερη αρχή, επίσης δεσμεύει τον προγραμματιστή μιας εφαρμογής ώστε να έχει ενσωματώσει εξ’αρχής και να συνεχίσει να υποστηρίζει κατά τον κύκλο ζωής της, πρακτικές, ώστε να προστατεύονται τα δεδομένα προσωπικού χαρακτήρα στα οποία έχει πρόσβαση η εφαρμογή.

Σκέψη 32

Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας των δεδομένων που το αφορούν, για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων με ηλεκτρονικά μέσα, ή με προφορική δήλωση. Αυτό θα μπορούσε να περιλαμβάνει τη συμπλήρωση ενός τετραγωνιδίου κατά την επίσκεψη σε διαδικτυακή ιστοσελίδα, την επιλογή των επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, στο συγκεκριμένο πλαίσιο, ότι το υποκείμενο των δεδομένων αποδέχεται την πρόταση επεξεργασίας των οικείων δεδομένων προσωπικού χαρακτήρα. Επομένως, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς. [...]

Άρθρο 25

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.

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 υποχρεώση 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 αρχές προστασίας των δεδομένων εξ' ορισμού και ήδη από τον σχεδιασμό, αποτελούν μια επιπλέον δικλείδα ασφαλείας, εμπλέκοντας άμεσα και τον ίδιο τον προγραμματιστή της εφαρμογής, στην ευθύνη που απορρέει από την πρόσβαση σε δεδομένα προσωπικού χαρακτήρα του χρήστη της εφαρμογής.

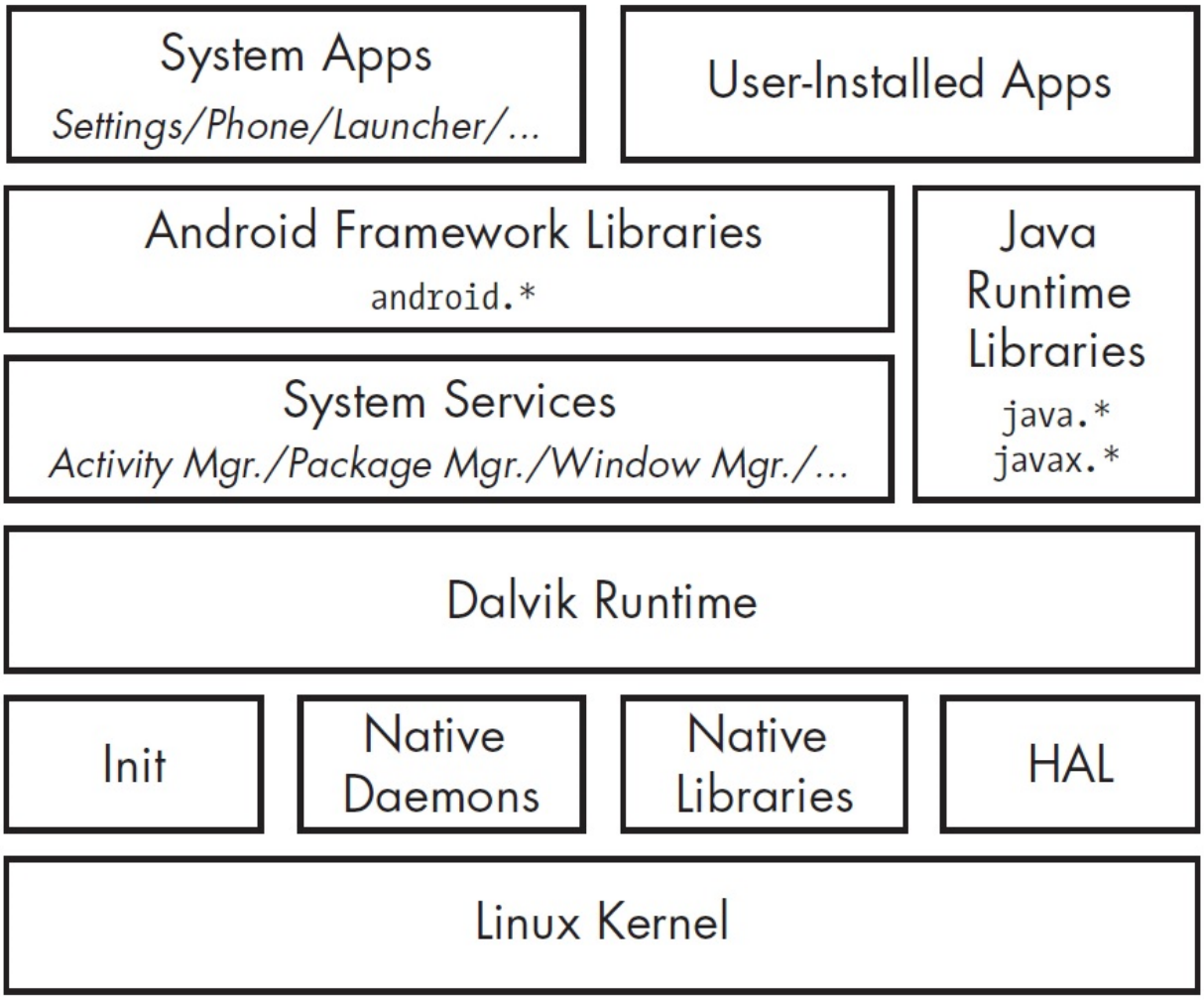
3. ΕΚΤΕΛΕΣΗ ΕΦΑΡΜΟΓΩΝ ΣΕ ANDROID

3.1 Γενικά

Στο Κεφάλαιο 2 περιγράφηκε το κύριο νομοθετικό πλαίσιο που ισχύει στην Ευρωπαϊκή Ένωση, έχοντας ως σκοπό την προστασία των δεδομένων προσωπικού χαρακτήρα των πολιτών της Ένωσης. Στο Κεφάλαιο 3 περιγράφεται ο τρόπος εκτέλεσης μιας εφαρμογής στο λειτουργικό σύστημα Android. Γνωρίζοντας τις λεπτομέρειες αυτές, στο Κεφάλαιο 4 μπορούν να διερευνηθούν οι απειλές που μπορεί να προκύψουν, σχετικά με την εξασφάλιση της ιδιωτικότητας.

3.2 Η Αρχιτεκτονική του Android

Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική του Android, η οποία έχει κληρονομήσει πολλά χαρακτηριστικά της από την αντίστοιχη του Linux.



Σχήμα 1: Διάγραμμα της Αρχιτεκτονικής του Android [7]

Τα βασικά στοιχεία αυτής της αρχιτεκτονικής, είναι τα εξής: [7] [8] [9]

- **Linux Kernel:** Ο πυρήνας του Android, ο οποίος βασίζεται στον αντίστοιχο του Linux. Διαχειρίζεται τους drivers του υλικού, όπως αυτών της οθόνης, της κάμερας και των διεπαφών δικτύου. Επίσης, αναλαμβάνει τον χρονοπρογραμματισμό των διεργασιών, τη διαχείριση της μνήμης και την εκχώρηση πόρων, συμπεριλαμβανομένης της πρόσβασης στο σύστημα αρχείων.
- **Init:** Η αρχική διεργασία, που εκκινεί όλες τις υπόλοιπες.
- **Hardware Abstraction Layer (HAL):** Αποτελεί ένα ενδιάμεσο layer, το οποίο συνδέει μέσω πολλαπλών libraries το υλικό με τις Java API Frameworks. Όποτε ένα API πραγματοποιήσει ένα call για πρόσβαση σε κάποια συσκευή (π.χ. κάμερα), καλείται το αντίστοιχο library για να την υλοποιήσει.
- **Android Runtime (ART):** Αποτελεί μια έκδοση της Java Virtual Machine (JVM), βελτιστοποιημένη για εκτέλεση σε κινητά. Αυτή αναλαμβάνει την εκτέλεση των εφαρμογών του Android, οι οποίες κατά κανόνα είναι γραμμένες σε Java. Λόγω της προαναφερθείσας βελτιστοποίησης, δεν μπορεί να τρέξει άμεσα τα αρχεία .class της παραδοσιακής Java. Αντίθετα, αναλαμβάνει την εκτέλεση αρχείων .dex ή .odex. Αυτά τα αρχεία περιλαμβάνονται στις βιβλιοθήκες συστήματος (αρχεία JAR) ή σε ξεχωριστές εφαρμογές (αρχεία APK). Μέχρι την έκδοση Android 5.0, η αντίστοιχη VM ονομαζόταν Dalvik.
- **Libraries:** Περιλαμβάνονται βιβλιοθήκες, τόσο σε C/C++ όσο και σε Java, για την υποστήριξη των προγραμματιστών εφαρμογών. Σε αυτές συμπεριλαμβάνονται κατάλληλες βιβλιοθήκες για την υποστήριξη πολυμέσων, βιβλιοθήκες OpenGL για προβολή γραφικών, βιβλιοθήκες SQLite για υποστήριξη βάσεων δεδομένων, Web-Kits για την απλοποίηση του φορτώματος ιστοσελίδων και βιβλιοθήκες SSL για την υποστήριξη κρυπτογράφησης.
- **System Services:** Τα services αυτά αναλαμβάνουν την υλοποίηση θεμελιωδών δυνατοτήτων του Android, όπως την προβολή περιεχομένου στην οθόνη, την πλοήγηση μέσω αφής, την επικοινωνία μέσω μίας δικτυακής διεπαφής κλπ. Η πλειοψηφία τους χρησιμοποιεί την object-oriented λογική: ορίζει τον εκάστοτε πόρο ως ένα remote interface, το οποίο και χειρίζεται μέσω κατάλληλων κλήσεων συστήματος.
- **System Apps:** Πρόκειται για εφαρμογές ενσωματωμένες στο Android, οι οποίες δεν μπορούν να απεγκατασταθούν από τον χρήστη. Εξ'ορισμού θεωρούνται ασφαλείς και τυπικά βρίσκονται στο path /system.
- **User-Installed Apps:** Περιλαμβάνει τις εφαρμογές που εγκαθιστά ο χρήστης, τις οποίες και μπορεί να απεγκαταστήσει κατά βούληση. Τυπικά βρίσκονται στο path /data. Όπως περιγράφεται στην Ενότητα 3.4, οι εφαρμογές αυτές εκτελούνται απομονωμένες η μια από την άλλη. Συνεπώς, κατά κανόνα, μια τέτοια εφαρμογή δεν μπορεί να επηρεάσει την εκτέλεση ή τα δεδομένα μιας άλλης. Οι εφαρμογές αυτές, προκειμένου να αποκτήσουν πρόσβαση σε ένα πόρο (π.χ. κάμερα), πρέπει να το ζητήσουν ρητά και να τους δοθεί η σχετική άδεια.

3.3 Η Δομή μιας Εφαρμογής Android

Μια εφαρμογή Android, περιλαμβάνει τα εξής συστατικά στοιχεία (components): [7]

- **Activities:** Ουσιαστικά πρόκειται για τις μεμονωμένες εικόνες που συνθέτουν τη γραφική διεπαφή χρήστη (GUI) της εφαρμογής.
- **Services:** Πρόκειται για components τα οποία εκτελούνται στο παρασκήνιο και πραγματοποιούν διάφορες εργασίες (π.χ. επικοινωνία με ένα απομακρυσμένο server). Δεν επηρεάζουν το GUI, με αποτέλεσμα ο χρήστης να μην αντιλαμβάνεται άμεσα την λειτουργία τους.
- **Content Providers:** Αποτελούν ένα είδος interface για τα ίδια τα δεδομένα της εφαρμογής. Παρέχουν έτσι τη δυνατότητα δια-δεργασιακής επικοινωνίας (inter-process communication), δίνοντας έτσι στην εφαρμογή τη δυνατότητα να διαμοιράζει, με ελεγχόμενο τρόπο, μέρος των δεδομένων της.
- **Broadcast Receivers:** Τα components αυτά αναλαμβάνουν να χειριστούν system-wide events, όπως την αλλαγή της κατάστασης μιας δικτυακής διεπαφής.

Τα components αυτά, δηλώνονται στο αρχείο AndroidManifest.xml, το οποίο αποτελεί αρχείο-κλειδί για κάθε εφαρμογή.

Επιπλέον της δήλωσης των components, το αρχείο AndroidManifest.xml, περιλαμβάνει και διάφορα άλλα metadata της εφαρμογής, συμπεριλαμβανομένου του ονόματος του package και των permissions που απαιτούνται για την εκτέλεσή της. [7]

Το AndroidManifest.xml, μαζί με το αρχείο classes.dex (που περιλαμβάνει τον εκτελέσιμο κώδικα της εφαρμογής), καθώς και διάφορα άλλα αρχεία, τοποθετούνται σε ένα container με κατάληξη .apk. Αυτό το είδος αρχείου αποτελεί επέκταση του γνωστού .jar, το οποίο έχει προκύψει από το .zip format. Το .apk αποτελεί το εκτελέσιμο της εφαρμογής.

3.4 Η Εκτέλεση μιας Εφαρμογής Android

Ο τρόπος εκτέλεσης μιας εφαρμογής στο Android, παρουσιάζει κοινά σημεία με τον αντίστοιχο τρόπο εκτέλεσης στο Linux.

Στο Linux, μια διεργασία εκτελείται με ID, το οποίο είναι χαρακτηριστικό του χρήστη ή του daemon που την εκκίνησε. Η παράμετρος αυτή, που ονομάζεται user ID (UID) χρησιμοποιείται επίσης και για τον διαχωρισμό των προσβάσεων στους διάφορους κοινόχρηστους πόρους του συστήματος. Η υποστήριξη μιας τέτοιας δυνατότητας είναι απαραίτητη για το λειτουργικό, καθώς πρέπει να υποστηρίζει πολλαπλούς χρήστες, με διαφορετικά εκχωρημένα δικαιώματα στον καθένα. Με αυτό τον τρόπο, ο πυρήνας (kernel) επιτυγχάνει διαχωρισμό των πόρων που χρησιμοποιεί η κάθε διεργασία, ενώ ταυτόχρονα προστατεύει το ίδιο το λειτουργικό από “κακόβουλες” διεργασίες. Τέλος, υπάρχουν συγκεκριμένες δεσμευμένες τιμές για την παράμετρο UID, όπως η τιμή 0 που αντιστοιχεί στον χρήστη root.

Το Android, έχει υιοθετήσει αυτή τη λογική από το Linux, έχοντάς την προσαρμόσει στις ιδιαιτερότητες των κινητών συσκευών. Καθώς στις συσκευές αυτές η υποστήριξη πολλαπλών χρηστών είναι περιττή δυνατότητα, η παράμετρος UID χρησιμοποιείται για

να ορίσει τις διάφορες διεργασίες που εκτελούνται από τον ένα και μοναδικό φυσικό χρήστη της συσκευής. [7]

Αυτός ο διαχωρισμός των διεργασιών, με βάση το μοναδικό UID της καθεμίας, το οποίο ονομάζεται και app ID, αποτελεί σημείο-κλειδί της εκτέλεσής τους στο λειτουργικό σύστημα Android.

Κατά την εγκατάσταση κάθε εφαρμογής, πραγματοποιείται εκχώρηση σε αυτή ενός μοναδικού app ID από το Android. Επίσης, της εκχωρείται ένας κατάλογος, εντός του /data/data, στον οποίο η συγκεκριμένη εφαρμογή έχει τη δυνατότητα ανάγνωσης και εγγραφής. Όποτε ο χρήστης θελήσει να τρέξει την εφαρμογή, το Android δημιουργεί μια διεργασία με UID ίδιο με το app ID της εφαρμογής και ξεκινά την εκτέλεση του κώδικα. Τα system services (AID_SYSTEM) ξεκινούν με UID 1000 και πάνω, ενώ στις εφαρμογές (AID_APP) εκχωρούνται τιμές UID 10000 και πάνω. [7]

Με αυτό τον τρόπο, το Android επιτυγχάνει την απομόνωση των διαφόρων εφαρμογών, αναγκάζοντας την καθεμία να εκτελεστεί από μια αποκλειστική διεργασία και η πρόσβασή της να περιορίζεται σε ένα συγκεκριμένο κατάλογο του συστήματος αρχείων. Αυτός ο περιορισμός, όπου η κάθε εφαρμογή εκτελείται σε ένα περιορισμένο περιβάλλον, περιγράφεται με τον όρο sandboxing.

3.5 Permissions

Η λογική του αυστηρού sandboxing, αν και εξασφαλίζει υψηλά επίπεδα ασφάλειας, θέτει ιδιαίτερους περιορισμούς στη λειτουργικότητα των εφαρμογών. Αυτό, διότι κάθε εφαρμογή, από προεπιλογή, μπορεί να έχει πρόσβαση μόνο στα αρχεία της και σε λίγους ακόμα πόρους του συστήματος. Προκειμένου το Android να χαλαρώσει αυτά τα αυστηρά πλαίσια λειτουργίας, δίνει στις εφαρμογές τη δυνατότητα να αιτούνται και να αποκτούν δικαιώματα πρόσβασης σε διάφορους επιπλέον πόρους. Αυτά τα δικαιώματα, ονομάζονται permissions. Επιπρόσθετα αυτών των permissions, τα οποία ορίζονται από το ίδιο το Android, κάθε εφαρμογή έχει τη δυνατότητα να ορίσει και δικά της, custom-made.

Παραδείγματα διαμοιραζόμενων πόρων, οι οποίοι προστατεύονται από permissions, είναι τόσο φυσικές οντότητες (διεπαφή δικτύου, δέκτης GPS, κάμερα, κάρτα SD), όσο και δεδομένα που βρίσκονται αποθηκευμένα στο κινητό (λίστα επαφών, μηνύματα). Επίσης, μέσω κατάλληλων permissions, μπορεί να επιτραπεί η πρόσβαση σε τρίτες εφαρμογές. [7]

Μία εφαρμογή δηλώνει ρητά τα permissions που προτίθεται να χρησιμοποιήσει στο αρχείο AndroidManifest.xml, όπως αυτό έχει περιγραφεί στην Ενότητα 3.3, μέσω του tag <uses-permission>. Τα permissions που καταγράφονται στο AndroidManifest.xml εξετάζονται από το system service “package manager”. [7]

Η αρμοδιότητα του package manager είναι να διατηρεί μια βάση δεδομένων που περιλαμβάνει όλα τα εγκατεστημένα packages, μαζί με τα permissions που έχουν εκχωρηθεί στο καθένα. Αυτή η βάση δεδομένων βρίσκεται στο /data/system/packages.xml.

Τα permissions που προτίθεται να χρησιμοποιήσει μια εφαρμογή, ελέγχονται και ενδεχομένως εγκρίνονται κατά την αρχική φάση της εγκατάστασής της. Επίσης, υπάρχει

η δυνατότητα να εγκριθούν ή να απορριφθούν επιλεκτικά από τον χρήστη, κατά τη φάση της εκτέλεσης. Εφόσον τα ζητούμενα permissions εγκριθούν, η εφαρμογή αποκτά την πρόσβαση που ζητάει στον αντίστοιχο πόρο, χωρίς άλλη ειδοποίηση του χρήστη.

Τα permissions εντάσσονται σε 5 κατηγορίες, ανάλογα με το ρίσκο που προκαλεί η έγκρισή τους για την ασφάλεια του συστήματος και των άλλων εφαρμογών. [10]

Η αυτόματη έγκριση ή απόρριψη ενός αιτήματος για ένα permission από τον package manager, καθορίζεται σε μεγάλο βαθμό από την κατηγορία στην οποία αυτό ανήκει. Οι 3 σημαντικότερες κατηγορίες είναι οι εξής: [10]

- **Normal:** Περιλαμβάνει permissions τα οποία αφορούν απομονωμένες λειτουργίες της εφαρμογής και είναι χαμηλού ρίσκου για την ασφάλεια του συστήματος, των άλλων εφαρμογών και του χρήστη. Permissions αυτής της κατηγορίας, εγκρίνονται αυτόματα, χωρίς να απαιτείται η αποδοχή τους από τον χρήστη, παρότι ο αυτός έχει τη δυνατότητα να ενημερωθεί για τα permissions αυτά. Παράδειγμα permission αυτής της κατηγορίας είναι το ACCESS_NETWORK_STATE, το οποίο δίνει τη δυνατότητα στην εφαρμογή να λάβει πληροφορίες για το δίκτυο κινητής επικοινωνίας στο οποίο είναι συνδεδεμένο το κινητό.
- **Dangerous:** Πρόκειται για permissions, τα οποία δίνουν πρόσβαση σε ιδιωτικά δεδομένα χρήστη εκτός του sandbox της εφαρμογής. Επίσης, μπορεί να δίνουν κάποιου είδους έλεγχο πάνω στη συσκευή, με τρόπο που να μπορεί να επηρεάσει αρνητικά τον χρήστη. Ένα παράδειγμα της πρώτης κατηγορίας είναι το READ_CONTACTS, όπου δίνει τη δυνατότητα στην εφαρμογή να διαβάσει τη λίστα επαφών του χρήστη, θέτοντας ενδεχομένως σε κίνδυνο την ιδιωτικότητά του. Αντίστοιχο παράδειγμα της δεύτερης κατηγορίας είναι το CAMERA, που δίνει τη δυνατότητα στην εφαρμογή να αποκτήσει πρόσβαση στην κάμερα του κινητού. Το Android δεν εγκρίνει αυτόματα την αίτηση για permissions αυτής της κατηγορίας. Αντίθετα, ενημερώνει τον χρήστη για το permission και ζητά την δική του, ρητή, έγκριση πριν το εκχωρήσει στην εφαρμογή.
- **Signature:** Πρόκειται για το αυστηρότερο permission. Εγκρίνεται αυτόματα μόνο αν η εφαρμογή που ζητά το permission έχει το ίδιο πιστοποιητικό (certificate) με την εφαρμογή που όρισε το συγκεκριμένο permission. Σε αυτή την περίπτωση, η έγκριση δίνεται αυτόματα, χωρίς να μεσολαβήσει ενημέρωση του χρήστη. Το level αυτό χρησιμοποιείται για να προστατέψει permissions του Android που για λόγους ασφαλείας δεν πρέπει να χρησιμοποιούνται από εφαρμογές τρίτων, ή permissions που έχει ορίσει στο AndroidManifest.xml μια εφαρμογή και για διάφορους λόγους ο developer δεν επιθυμεί να χρησιμοποιούνται από εφαρμογές τρίτων developers.

Στον παρακάτω πίνακα καταγράφονται τα permissions που ζητούνται πιο συχνά, από τις δημοφιλέστερες εφαρμογές του Google Play Store. [5] [11] [12] [13]

Πίνακας 1: Συχνότερα Αιτούμενα Permissions

ACCESS_COARSE_LOCATION	Πρόσβαση στην τοποθεσία της συσκευής (μέσω πληροφοριών δικτύου κινητής ή Wi-Fi)

ACCESS_FINE_LOCATION	Πρόσβαση στην τοποθεσία της συσκευής (μέσω GPS)
ACCESS_MEDIA_LOCATION	Πρόσβαση στην τοποθεσία που έχει καταγραφεί στα EXIF metadata φωτογραφιών και βίντεο
ANSWER_PHONE_CALLS	Απάντηση σε εισερχόμενες κλήσεις
BLUETOOTH	Πρόσβαση σε δέκτη Bluetooth (έως Android 12)
BLUETOOTH_ADVERTISE	Διαφήμιση της συσκευής μέσω Bluetooth
BLUETOOTH_CONNECT	Επικοινωνία με paired συσκευές μέσω Bluetooth
BLUETOOTH_SCAN	Σάρωση μέσω Bluetooth για άλλες συσκευές
BODY_SENSORS	Πρόσβαση σε αισθητήρες σώματος (π.χ. μέτρηση παλμών)
CALL_PHONE	Εκκίνηση εξερχομένων κλήσεων
CAMERA	Πρόσβαση σε κάμερα
GET_ACCOUNTS	Πρόσβαση σε λίστα λογαριασμών της συσκευής
INTERNET	Δυνατότητα δημιουργίας network sockets
MEDIA_CONTENT_CONTROL	Πρόσβαση στο πολυμέσο που αναπαράγεται
READ_CALENDAR	Διάβασμα του ημερολογίου
READ_CALL_LOG	Διάβασμα του ιστορικού κλήσεων
READ_CONTACTS	Διάβασμα της λίστας επαφών
READ_EXTERNAL_STORAGE	Διάβασμα του εξωτερικού χώρου αποθήκευσης
READ_PHONE_NUMBERS	Διάβασμα του αριθμού τηλεφώνου (μέσω SIM)
READ_PHONE_STATE	Διάβασμα της κατάστασης τηλεφώνου (π.χ. πληροφορίες δικτύου, κλήσεις σε εξέλιξη)
READ_SMS	Διάβασμα των μηνυμάτων SMS
RECEIVE_SMS	Λήψη μηνυμάτων SMS
RECEIVE_MMS	Λήψη μηνυμάτων MMS
RECORD_AUDIO	Εγγραφή ήχου από μικρόφωνο
SEND_SMS	Αποστολή μηνυμάτων SMS

SYSTEM_ALERT_WINDOW	Δημιουργία παραθύρου “ALERT” πάνω από υπόλοιπα παράθυρα
VIBRATE	Πρόσβαση στη συσκευή δόνησης
WRITE_CALENDAR	Εγγραφή σε ημερολόγιο
WRITE_CONTACTS	Εγγραφή σε λίστα των επαφών
WRITE_EXTERNAL_STORAGE	Εγγραφή σε εξωτερικό χώρο αποθήκευσης
WRITE_SETTINGS	Διάβασμα / Εγγραφή των ρυθμίσεων συστήματος του τηλεφώνου

Στον παραπάνω πίνακα, με πράσινο έχουν καταγραφεί τα normal permissions, ενώ με κόκκινο σημειώνονται όσα ανήκουν στην κατηγορία dangerous. [13]

Η ορθή χρήση των permissions ώστε να προστατεύεται η ιδιωτικότητα του χρήστη, καθώς και τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν, δεν είναι εύκολη. Αφενός, οι χρήστες γενικά έχουν περιορισμένη γνώση των κινδύνων που πηγάζουν από την έγκριση των permissions τα οποία αιτούνται οι διάφορες εφαρμογές. Αφετέρου, οι προγραμματιστές δυσκολεύονται να κατανοήσουν και να χειριστούν κατάλληλα τα permissions. Πολλές φορές, αναγκάζονται να ζητήσουν περισσότερα permissions από αυτά τα οποία χρειάζεται η εφαρμογή τους ώστε να είναι λειτουργική, διότι απαιτούνται από τις libraries τις οποίες ενσωματώνουν. Με αυτό τον τρόπο, οι libraries μπορούν να δημιουργήσουν ένα πληρέστερο προφίλ χρήστη, μέσω των επιπρόσθετων permissions που αποκτούν, χωρίς ταυτόχρονα να έχουν την απαιτούμενη νομική βάση για αυτό. Αυτό καθίσταται εφικτό, λόγω και του τρόπου που το Android κληροδοτεί αδιάκριτα τα permissions από την εφαρμογή στις ενσωματωμένες libraries, χωρίς να δίνει στον χρήστη τη δυνατότητα να παρέμβει στην κληροδότηση αυτή. [14] [15] [16]

3.6 Αναγνωριστικά στο Android

Υπάρχουν διάφορες παράμετροι, οι οποίοι μπορούν να χρησιμοποιηθούν για την ταυτοποίηση μιας κινητής συσκευής, η οποία χρησιμοποιεί το λειτουργικό σύστημα Android. [14] [5] [17] [18]

Κάποιες από αυτές τις παραμέτρους είναι χαρακτηριστικές του υλικού της συσκευής, μερικές χαρακτηρίζουν το ίδιο το λειτουργικό σύστημα Android, ενώ άλλες προκύπτουν από τον πάροχο του δικτύου κινητής επικοινωνίας. Οι περισσότερες από αυτές είναι μόνιμες, ενώ λίγες μπορούν να αλλαχθούν κατά βούληση από τον χρήστη.

- **Android ID:** Πρόκειται για ψευδοτυχαία αριθμητική παράμετρο, μεγέθους 64-bit. Η παράμετρος αυτή είναι ημι-μόνιμη, με την έννοια ότι μπορεί να τροποποιηθεί μέσω της επαναφοράς της κινητής συσκευής στις εργοστασιακές της ρυθμίσεις. Δεν απαιτείται η έγκριση κάποιου permission για την πρόσβαση στην τιμή της παραμέτρου. Ο σκοπός αυτής της παραμέτρου είναι να προσδιορίζει την συσκευή κυρίως για τεχνικούς λόγους, παρά για λόγους tracking. Από την

έκδοση Android 8, δεν επιτρέπεται η πρόσβαση των εφαρμογών στην παράμετρο Android ID. [14]

- **Google Advertising ID (GAID):** Η παράμετρος αυτή είναι επίσης ψευδοτυχαία, με μέγεθος 32 ψηφία. Σε αντίθεση με την Android ID, μπορεί να γίνει reset από τον χρήστη, χωρίς την ανάγκη της επαναφοράς του κινητού στις εργοστασιακές του ρυθμίσεις. Πλέον, η Google ενθαρρύνει την χρήση του GAID για την ταυτοποίηση του χρήστη για διαφημιστικούς λόγους. [18] [19]
- **IMEI:** Η τιμή του IMEI (International Mobile Equipment Identity) έχει μέγεθος 15 ή 16 ψηφία και όπως υποδηλώνει το όνομά του χρησιμοποιείται για την ταυτοποίηση της συσκευής. Μέσω του IMEI, είναι δυνατή η εξαγωγή πληροφοριών για την κινητή συσκευή, όπως τον κατασκευαστή, την χώρα κατασκευής, και τον μοναδικό σειριακό αριθμό. Η παράμετρος αυτή είναι χαρακτηριστική της συσκευής και δεν μπορεί να αλλάξει από τον χρήστη. [20]
- **IMSI:** Η παράμετρος αυτή, που αποτελεί ακρωνύμιο του International Mobile Subscriber Identity, χαρακτηρίζει μοναδικά τη SIM του χρήστη. Έχει μέγεθος 15 ψηφίων. Από τον IMSI μπορούν να εξαχθούν πληροφορίες για τη χώρα και τον τηλεπικοινωνιακό πάροχο. Τα τελευταία 10 ψηφία μπορούν να χρησιμοποιηθούν για να ταυτοποιήσουν τον χρήστη. Όπως και ο IMEI, δεν μπορεί να τροποποιηθεί από τον χρήστη. [21]
- **MAC Addresses:** Πρόκειται για διευθύνσεις 48-bit, που προσδιορίζουν μοναδικά τις δικτυακές διεπαφές Wi-Fi και Bluetooth. Και στις 2 περιπτώσεις, τα πρώτα 24-bits προσδιορίζουν τον κατασκευαστή, ενώ τα τελευταία 24-bits αποτελούν ένα είδος μοναδικού ID της διεπαφής. Οι διευθύνσεις MAC δεν μπορούν να τροποποιηθούν εύκολα από τον χρήστη.

Όλες οι παραπάνω παράμετροι εντάσσονται στα δεδομένα προσωπικού χαρακτήρα, όπως αυτά ορίστηκαν στην Ενότητα 2.3, καθώς συνδυαζόμενα και με άλλες πληροφορίες, μπορούν να ταυτοποιήσουν τον χρήστη.

4. ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

4.1 Γενικά

Στο Κεφάλαιο 3 πραγματοποιήθηκε μια περιγραφή του τρόπου εκτέλεσης των εφαρμογών στο λειτουργικό σύστημα Android. Το Κεφάλαιο 4 επικεντρώνεται στη δημιουργία προφίλ του χρήστη, καθώς και στους τρόπους με τους οποίους αυτό καθίσταται εφικτό. Καθώς η επιτυχημένη δημιουργία προφίλ απαιτεί ιχνηλάτηση (tracking) του χρήστη, το Κεφάλαιο 4 ολοκληρώνεται με μερικές από τις γνωστότερες τεχνικές ιχνηλάτησης.

4.2 Οικοσύστημα Προβολής Διαφημίσεων

Η συλλογή δεδομένων προσωπικού χαρακτήρα, μέσω των online δραστηριοτήτων του χρήστη, λαμβάνει χώρα σε πολλές περιπτώσεις web services. Μεταξύ των δεδομένων που συλλέγονται, είναι: οι αναζητήσεις που κάνει, τα sites που επισκέπτεται ή τα προϊόντα που αγοράζει.

Η καταγραφή αυτών των δεδομένων, καθώς και η μετέπειτα επεξεργασία τους, βρίσκει πολλές εφαρμογές: [22] [23]

- **Διακύμανση Τιμών:** Όπως έχει παρατηρηθεί, η αναγραφόμενη τιμή ενός προϊόντος μπορεί να διαφοροποιηθεί, ανάλογα με την εκτιμούμενη οικονομική κατάσταση του υποψήφιου πελάτη. [24] Τέτοια συμπεράσματα για την οικονομική του κατάσταση, μπορούν να εξαχθούν από την τοποθεσία του.
- **Προσωποποιημένα Αποτελέσματα Αναζητήσεων:** Μια μηχανή αναζήτησης μπορεί να επιστρέφει αποτελέσματα συναφή με τους όρους αναζήτησης, τα οποία όμως βασίζονται επιπλέον και στις πληροφορίες που έχουν συλλεχθεί για τον χρήστη. Αυτό έχει σαν αποτέλεσμα, ο χρήστης να μην λαμβάνει αποτελέσματα τα οποία ενδεχομένως τον ενδιαφέρουν, αν αυτά δεν “ταιριάζουν” με τις προηγούμενες, καταγεγραμμένες, δραστηριότητές του.
- **Οικονομική Αξιοπιστία:** Έχουν υπάρξει καταγραφές οικονομικών ιδρυμάτων, τα οποία κρίνουν την οικονομική αξιοπιστία ενός πελάτη, με βάση τις online δραστηριότητές του. Ένα παράδειγμα καταγράφεται στο [25], όπου παρατηρήθηκε μείωση του πιστωτικού ορίου, επειδή ο πελάτης πραγματοποίησε online αγορά από διαδικτυακό κατάστημα, οι πελάτες του οποίου συνήθως καθυστερούσαν τις πληρωμές προς την τράπεζα.
- **Ασφαλιστική Κάλυψη:** Οι ασφαλιστικές εταιρείες μπορούν να χρησιμοποιήσουν τις πληροφορίες από τις online δραστηριότητες ενός χρήστη, ώστε να αξιολογήσουν τα ασφαλιστικά πακέτα που θα του προσφέρουν. Αυτό, διότι οι online δραστηριότητες ενός χρήστη εμπεριέχουν πολλές πληροφορίες για τον τρόπο ζωής και τα ενδιαφέροντά του.
- **Αγορά Εργασίας:** Ένας εργοδότης ενδέχεται να αναζητήσει πληροφορίες για τους υποψήφιους εργαζομένους, μέσω του internet. Παρότι οι πληροφορίες αυτές ενδέχεται να είναι ελλιπείς ή ανενημέρωτες, ενδέχεται να καθορίσουν την έκβαση μιας πρόσληψης. Ήδη, στη Φινλανδία, έχει απαγορευτεί η διαδικτυακή αναζήτηση των υποψηφίων εργαζομένων από τους εργοδότες τους. [26]

Προκειμένου να γίνει κατανοητός ο τρόπος λειτουργίας των web services που συλλέγουν και επεξεργάζονται τα δεδομένα αυτά, εξετάζεται η περίπτωση των παρόχων διαφημιστικού περιεχομένου (ad providers). Οι ad providers χρησιμοποιούνται από πληθώρα δωρεάν εφαρμογών, οι οποίες βασίζονται σε αυτούς για την εξασφάλιση μέρους των κερδών τους, χωρίς να χρεώνουν άμεσα τον χρήστη.

Ο σκοπός του ad provider είναι να επιλέξει ποια διαφήμιση θα προβληθεί στο κινητό του χρήστη. Όσο πιο εξατομικευμένες στα ενδιαφέροντα του χρήστη είναι οι διαφημίσεις, τόσο πιο κερδοφόρες θα είναι αυτές. Προκειμένου να επιτευχθεί η ζητούμενη εξατομίκευση, είναι απαραίτητη η συλλογή από τον ad provider όσο περισσότερων πληροφοριών για το συγκεκριμένο χρήστη.

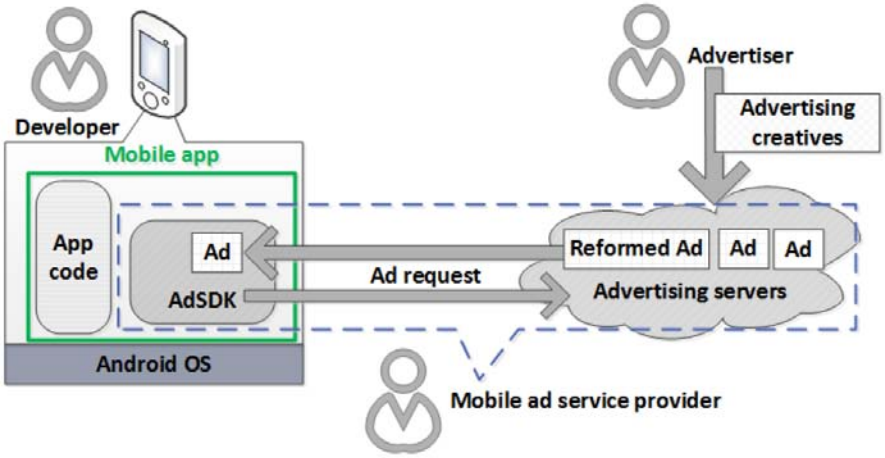
4.2.1 Οντότητες Οικοσυστήματος

Προκειμένου να μελετηθεί ο τρόπος λειτουργίας του οικοσυστήματος, αρχικά εξετάζεται ο ρόλος της καθεμίας οντότητας που το απαρτίζει. [18]

- **Mobile Ad Developer:** Πρόκειται για τον προγραμματιστή της εφαρμογής, ο οποίος έχει ενσωματώσει στον κώδικά της τη δυνατότητα προβολής διαφημίσεων.
- **AdSDK Provider:** Αυτή είναι η οντότητα που αναλαμβάνει την προβολή της κατάλληλης διαφήμισης στη συσκευή του χρήστη, μέσω της αντίστοιχης βιβλιοθήκης η οποία έχει ενσωματωθεί στη χρησιμοποιούμενη εφαρμογή. Επίσης, διαχειρίζονται τα advertising networks, στα οποία ο διαφημιζόμενος ανεβάζει το διαφημιστικό περιεχόμενο.
- **Advertiser:** Ο διαφημιζόμενος παρέχει τη διαφήμιση στο advertising network, ώστε, μέσω του AdSDK, αυτή να προβληθεί στο κινητό του χρήστη.

4.2.2 Τρόπος Λειτουργίας Οικοσυστήματος

Η δομή που χρησιμοποιείται για την λήψη και προβολή των διαφημίσεων, εντός μιας εφαρμογής, φαίνεται στο παρακάτω σχήμα.



Σχήμα 2: Δομή του Οικοσυστήματος Προβολής Διαφημίσεων [18]

Ο τρόπος λειτουργίας της συγκεκριμένης δομής παραμένει απλός. Τυπικά, μια εφαρμογή που χρησιμοποιεί διαφημίσεις, ενσωματώνει πολλαπλές βιβλιοθήκες με σκοπό την προβολή διαφημίσεων (ad libraries). Όποτε εκτελείται η εφαρμογή, η κάθε ενσωματωμένη ad library επικοινωνεί με τους ad servers του δικού της advertising network. Στο μήνυμα ad request, που στέλνεται μέσω HTTP(S), περιλαμβάνονται διάφορα χαρακτηριστικά του χρήστη, τα οποία έχει συλλέξει η ad library. Χρησιμοποιώντας τα δεδομένα αυτά, ο ad server επιλέγει την κατάλληλη διαθέσιμη διαφήμιση και την επιστρέφει στην ad library, προκειμένου αυτή να προβληθεί στο κινητό του χρήστη. [18]

Όπως γίνεται φανερό, προκειμένου ο AdSDK Provider να μπορέσει να προσφέρει εξατομικευμένη διαφήμιση στον χρήστη, απαιτείται συλλογή και αποστολή πληροφοριών σε αυτόν, μέσω της ad library που έχει ενσωματωθεί στην εφαρμογή. Η αποστολή αυτών των πληροφοριών, μέσω του μηνύματος ad request που θα στείλει η βιβλιοθήκη, εγείρει θέματα ιδιωτικότητας και προστασίας των δεδομένων προσωπικού χαρακτήρα για τον χρήστη.

4.2.3 Λειτουργία της Ad-Library

Προκειμένου να διερευνηθούν περεταίρω οι απειλές στην ιδιωτικότητα του χρήστη που προκύπτουν από την εκτέλεση των ad libraries, απαιτείται εξέταση του τρόπου που λειτουργεί μια τέτοια βιβλιοθήκη, όντας ενσωματωμένη σε μια εγκατεστημένη εφαρμογή.

Ένα χαρακτηριστικό του τρόπου με τον οποίο το Android διαχειρίζεται τα permissions, όπως αυτά περιγράφηκαν στην Ενότητα 3.5, είναι ότι αυτά κληροδοτούνται αυτούσια από την εκτελούμενη εφαρμογή σε όλες τις βιβλιοθήκες οι οποίες έχουν ενσωματωθεί στον κώδικά της. Εάν μια ενσωματωμένη βιβλιοθήκη χρειάζεται ένα permission για να τρέξει, αυτό θα ζητηθεί μέσω της εφαρμογής από τον χρήστη, ακόμη και στην περίπτωση που η εφαρμογή δεν το χρειάζεται για την ουσιαστική λειτουργία της ίδιας.

Αυτά τα permissions μπορούν να χρησιμοποιηθούν καταχρηστικά από μια ad library, προκειμένου αυτή να αποκτήσει πρόσβαση σε identifiers που ταυτοποιούν τη συγκεκριμένη συσκευή. Παραδείγματα τέτοιων παραμέτρων παρουσιάστηκαν στην Ενότητα 3.6. Επιπρόσθετα, μια ad library μπορεί να αποκτήσει πρόσβαση μέσω των κατάλληλων permissions σε ευαίσθητες πληροφορίες του χρήστη. Για παράδειγμα, μέσω του WRITE_EXTERNAL_STORAGE, ενός permission που ζητείται κατά κόρον από τις εφαρμογές, αυτές αποκτούν πρόσβαση σε όλη την εξωτερική μνήμη της συσκευής, ακόμα και στα δεδομένα των άλλων εφαρμογών. Το αίτημα αυτό παραβιάζει την αρχή της data minimization, καθώς την απαιτούμενη πρόσβαση της εφαρμογής στα δικά της δεδομένα, την παρέχει αυτόματα το ίδιο το Android.

Τυπικά, αυτές οι πληροφορίες που συλλέγονται από μια ad library, αποστέλλονται μέσω του μηνύματος ad request στον ad server, προκειμένου ο τελευταίος να επιλέξει την κατάλληλη διαφήμιση προς προβολή στον συγκεκριμένο χρήστη. Επιπροσθέτως, μέσω των identifiers, ο ad server πλέον είναι σε θέση να συσχετίζει τα αιτήματα που προέρχονται από την ίδια συσκευή.

Τέλος, εκτός από τη διαρροή δεδομένων προσωπικού χαρακτήρα, προκύπτουν και θέματα που εντάσσονται καθαρά στην ασφάλεια της επικοινωνίας. Για παράδειγμα, στην περίπτωση που τα μηνύματα μεταξύ της ad library και του ad server ανταλλαχθούν μέσω HTTP, αντί του ασφαλέστερου HTTPS, η επικοινωνία αυτή μπορεί να υπονομευθεί μέσω επίθεσης man-in-the-middle, αφού δεν είναι κρυπτογραφημένη αλλά ούτε και αυθεντικοποιημένη.

4.3 Ιχνηλάτηση

Η σοβαρότητα της διαρροής δεδομένων προσωπικού χαρακτήρα εντείνεται ακόμη περισσότερο στην περίπτωση των ιχνηλατών (trackers). Ένας 3rd party tracker αποτελεί ένα service, διαφορετικό από αυτό το οποίο ρητά χρησιμοποιεί ο χρήστης. Η ύπαρξη tracker είναι ιδιαίτερα διαδεδομένη πρακτική: μόνο στο web, πάνω από το 45% των 10.000 δημοφιλέστερων sites συνδέονται με τουλάχιστον έναν tracker. [27]

Οι trackers αποτελούν μεγάλη απειλή για την ιδιωτικότητα του χρήστη, καθώς, όντας ενσωματωμένοι σε πολύ μεγάλο αριθμό sites, συλλέγουν τεράστια ποσότητα πληροφοριών σχετικές με την online δραστηριότητα των χρηστών.

Εν συντομία, ένας 3rd party tracker ο οποίος είναι ενσωματωμένος σε κάποια διαδικτυακή υπηρεσία “1st party” (π.χ. web site), ενημερώνεται κατά τη χρήση της υπηρεσίας αυτής από τους χρήστες. Μέσω διαφόρων τεχνικών, οι οποίες θα αναλυθούν στη συνέχεια, ο tracker είναι σε θέση να διακρίνει τους χρήστες αυτούς. Όμως η μεγαλύτερη απειλή για την ιδιωτικότητα έγκειται στο γεγονός ότι επιπλέον είναι σε θέση να συσχετίσει τη χρήση μιας υπηρεσίας από ένα χρήστη με τη χρήση μιας άλλης υπηρεσίας από τον ίδιο χρήστη, υπό την προϋπόθεση ότι ο tracker είναι ενσωματωμένος και στις δύο αυτές υπηρεσίες.

4.3.1 HTTP Cookies

Παραδοσιακά, το tracking γινόταν με χρήση HTTP Cookies. Η λογική των cookies ήταν η δυνατότητα αποθήκευσης μιας μικρής ποσότητας δεδομένων (έως 4 KB) σε ένα αποκλειστικό χώρο αποθήκευσης του browser, όποτε ο χρήστης επισκεπτόταν ένα web site για πρώτη φορά. Τη δυνατότητα αυτή, για αποθήκευση δεδομένων όπως ενός αναγνωριστικού, την έχει κάθε server ο οποίος έχει ενσωματωμένο τουλάχιστον ένα δικό του element στην ιστοσελίδα που επισκέπτεται ο χρήστης. Σε κάθε επόμενη επίσκεψη του χρήστη, τα περιεχόμενα του cookie αποστέλλονται αυτόματα στον αντίστοιχο server. Η όλη διαδικασία είναι γρήγορη και γίνεται χωρίς την εμπλοκή του χρήστη. Εφόσον ο τελευταίος επιτρέψει τη χρήση cookies, η ιχνηλάτηση σταματάει είτε με τη λήξη του cookie είτε με τη χειροκίνητη διαγραφή του από τον χρήστη. Ένας 3rd party tracker μπορεί να εκμεταλλευθεί την αποδοχή των cookies από τον χρήστη, ενσωματώνοντας elements σε διάφορα 1st party web sites. Με αυτό τον τρόπο και μέσω των μοναδικών αναγνωριστικών που έχει συμπεριλάβει στα cookies, μπορεί να καταγράφει τις επισκέψεις του συγκεκριμένου χρήστη στα sites αυτά.

4.3.2 Fingerprinting

Η ευαισθητοποίηση των χρηστών για τους κινδύνους των HTTP Cookies, καθώς και ο περιορισμός της εφαρμογής τους στην περίπτωση της πλοήγησης στο web, έχει

οδηγήσει στην ανάπτυξη εναλλακτικών μηχανισμών tracking. Ο πιο αποδοτικός, ενώ ταυτόχρονα και δυσκολότερος στην αντιμετώπιση, είναι το fingerprinting. [14]

Η λογική του fingerprinting είναι η χρήση ενός μοναδικού αναγνωριστικού για την ίδια τη συσκευή του χρήστη, ώστε ο χρήστης να μπορεί να ταυτοποιηθεί. Με αυτό τον τρόπο, παρακάμπτεται η ανάγκη εγκατάστασης cookie, ενώ η όλη διαδικασία συνεχίζει να παραμένει διάφανη για το χρήστη. Με αυτόν τον τρόπο, ο μέσος χρήστης δεν αντιλαμβάνεται το tracking που πραγματοποιείται, ενώ και τα αντίμετρα που μπορούν να εφαρμοστούν είναι εν μέρει μόνο αποδοτικά και θα πρέπει να περιλαμβάνουν προσεκτική υλοποίηση με βάση την αρχή “προστασία ήδη από τον σχεδιασμό”. [22] [14]

Πέρα από την χρήση κάποιων από τα αναγνωριστικά που παρουσιάστηκαν στην Ενότητα 3.6, το fingerprinting μπορεί να χρησιμοποιήσει πολλούς άλλους λιγότερο ή περισσότερο εξεζητημένους τρόπους για να ταυτοποιήσει το χρήστη. [22]

- **Fingerprinting βάσει του Δικτύου:** Στην περίπτωση αυτή, για την ταυτοποίηση του χρήστη χρησιμοποιούνται παράμετροι όπως η διεύθυνση IP. Με βάση αυτή, μπορεί να προσδιοριστεί επιπλέον ο ISP και κατά προσέγγιση η τοποθεσία. Επίσης, είναι δυνατός ο προσδιορισμός της χρήσης proxy ή firewall. [28] [29] Τέλος, είναι εύκολος και ο προσδιορισμός δικτυακών παραμέτρων, όπως οι ταχύτητες ανεβάσματος και κατεβάσματος, οι καθυστερήσεις και το jitter. [30] [31]
- **Fingerprinting βάσει της Συσκευής:** Στην κατηγορία αυτή εντάσσεται το fingerprinting που χρησιμοποιεί το GAID. Άλλοι παράμετροι που μπορούν να χρησιμοποιηθούν είναι η έκδοση του Android, η ζώνη ώρας και η απόκλιση του ρολογιού. Στην περίπτωση των υπολογιστών, επιπλέον παράμετροι που εντάσσονται στην κατηγορία αυτή, είναι η ανάλυση της οθόνης και οι εγκατεστημένες γραμματοσειρές, καθώς και τα plugins. Η ακραία περίπτωση είναι η χρήση παραμέτρων που εξάγονται από την ίδια τη registry (ID εξαρτημάτων, όνομα υπολογιστή, product ID του λειτουργικού συστήματος, εγκατεστημένοι drivers). Αναλυτική περιγραφή του τρόπου με τον οποίο καθίσταται δυνατή η πρόσβαση στις παραμέτρους αυτές, παρουσιάζεται στο [28].
- **Fingerprinting με χρήση Canvas:** Η τεχνική αυτή, χρησιμοποιεί τη δημιουργία αόρατων στον χρήστη γραφικών, εκμεταλλευόμενη μικρές διαφορές στην απεικόνισή τους ανάλογα με εξοπλισμό του χρήστη, προκειμένου να εξάγει ένα μοναδικό προσδιοριστικό. Συγκεκριμένα, δημιουργείται ένα κείμενο το οποίο απεικονίζεται σε ένα αόρατο, στον χρήστη, παράθυρο. Στη συνέχεια, το περιεχόμενο το παραθύρου, μαζί με το απεικονισμένο κείμενο, περνά από μια συνάρτηση κατακερματισμού (hash function), η έξοδος της οποίας αποτελεί το fingerprint. [22] Η χρήση canvas αποτελεί την πιο συχνά χρησιμοποιούμενη μέθοδο fingerprinting, κυρίως στο web. Η μέθοδος αυτή βρίσκει εφαρμογή σε άνω του 5% των 100.000 διασημότερων sites. [32]

4.4 Intra-Library Collusion

Μια βιβλιοθήκη, εκτός από την προβολή διαφημίσεων, εξυπηρετεί και άλλες θεμιτές λειτουργίες. Οι βιβλιοθήκες χρησιμοποιούνται εκτενώς για την εύκολη υλοποίηση πολύπλοκων λειτουργιών, όπως είναι η πρόσβαση στο υλικό της συσκευής, ενώ η χρήση τους τα τελευταία χρόνια έχει επεκταθεί και στην υποστήριξη λειτουργιών των

κοινωνικών δικτύων. Οι λόγοι αυτοί, έχουν οδηγήσει στην ενσωμάτωσή τους σχεδόν σε κάθε διαθέσιμη εφαρμογή.

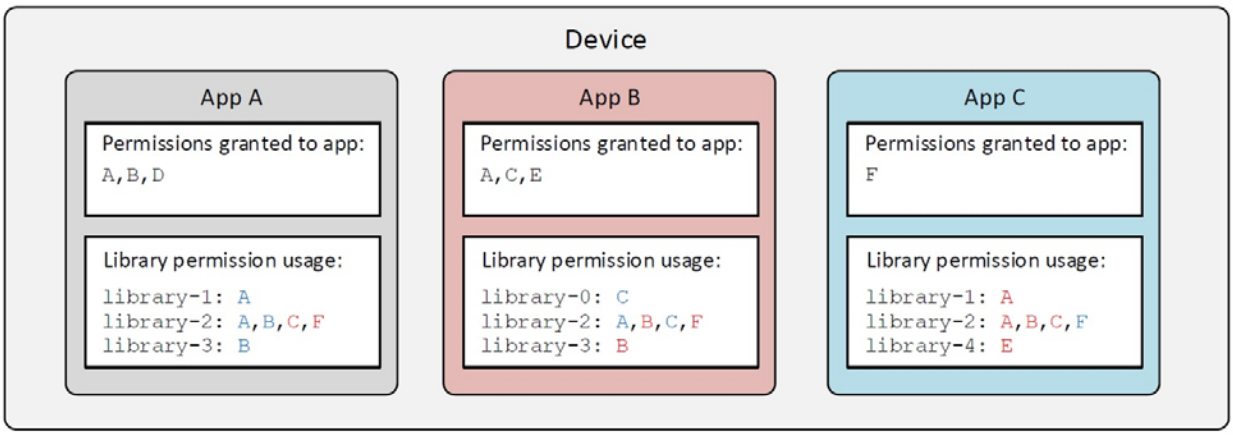
Όπως έχει περιγραφεί στην Ενότητα 4.2.3, μια βιβλιοθήκη η οποία έχει ενσωματωθεί σε μία εφαρμογή, εκτελείται με τα ίδια permissions τα οποία έχουν εκχωρηθεί στην εφαρμογή.

Με βάση την παραπάνω παρατήρηση, το τωρινό μοντέλο ασφαλείας (security model) του Android, δίνει σε μια μεμονωμένη βιβλιοθήκη τις εξής δυνατότητες: [33] [5]

- Κατάχρηση των permissions που έχουν εκχωρηθεί στην εφαρμογή, τα οποία εκχωρούνται αυτούσια και στη library.
- Tracking του χρήστη, χωρίς τη συγκατάθεσή του.
- Εκτενή συλλογή πληροφοριών για τον χρήστη, με αποτέλεσμα τη δυνατότητα δημιουργίας λεπτομερούς profile.

Η τελευταία παρατήρηση αποτελεί μεγάλη απειλή στην ιδιωτικότητα του χρήστη, καθώς και στην προστασία των δεδομένων προσωπικού χαρακτήρα, λόγω του φαινομένου της intra-library collusion. [33]

Ως intra-library collusion περιγράφεται το φαινόμενο κατά το οποίο μια μεμονωμένη βιβλιοθήκη αποκτά συνδυασμένα περισσότερα δικαιώματα πρόσβασης, μέσω της ενσωμάτωσής της σε πολλαπλές εφαρμογές. Στην περίπτωση αυτή, η καθεμία από αυτές της δίνει πρόσβαση σε ένα διακριτό υποσύνολο των permissions. Μέσω των πολλαπλών ενσωματώσεων, η ίδια βιβλιοθήκη αποκτά προσβάσεις σε ένα σύνολο πόρων, στους οποίους δεν θα είχε πρόσβαση μέσω καμίας από τις επιμέρους, μεμονωμένες, εφαρμογές στις οποίες έχει ενσωματωθεί.



Σχήμα 3: Αναπαράσταση Intra-Library Collusion [33]

Στο παραπάνω σχήμα παρουσιάζεται ένα παράδειγμα εμφάνισης της intra-library collusion. Στην κινητή συσκευή, υπάρχουν εγκατεστημένες τρεις εφαρμογές, με κάποια permissions να έχουν εκχωρηθεί στην καθεμία. Επίσης, η κάθε εφαρμογή έχει ενσωματωμένες από τρεις βιβλιοθήκες. Δίπλα από κάθε βιβλιοθήκη, καταγράφονται τα permissions τα οποία επιθυμεί να έχει εκχωρημένα η εκάστοτε βιβλιοθήκη. Όπως έχει περιγραφεί, τα permissions της κάθε εφαρμογής εκχωρούνται αυτόματα και στην καθεμία από τις ενσωματωμένες βιβλιοθήκες της. Συνεπώς, για την κάθε βιβλιοθήκη, τα

ζητούμενα permissions τα οποία της έχουν εκχωρηθεί εμφανίζονται με μπλε, ενώ με κόκκινο εμφανίζονται τα ζητούμενα permissions τα οποία δεν έχει αποκτήσει μέσω της αντίστοιχης εφαρμογής.

Η παραπάνω σχηματική αναπαράσταση περιγράφεται και στον παρακάτω πίνακα.

Πίνακας 2: Permissions και Βιβλιοθήκες σε Intra-Library Collusion

Εφαρμογή	Εκχωρημένα Permissions Εφαρμογή	Ενσωματωμένες Βιβλιοθήκες	Ζητούμενα Permissions Βιβλιοθήκης	Εκχωρημένα Permissions Βιβλιοθήκης
App A	A / B / D	library-1	A	A / B / D
		library-2	A / B / C / F	A / B / D
		library-3	B	A / B / D
App B	A / C / E	library-0	C	A / C / E
		library-2	A / B / C / F	A / C / E
		library-3	B	A / C / E
App C	F	library-1	A	F
		library-2	A / B / C / F	F
		library-4	E	F

Όπως γίνεται φανερό, λόγω της intra-library collusion, η library-2 επιτυγχάνει να αποκτήσει όλα τα permissions που θέλει, χωρίς να τα παίρνει ρητά από μια και μόνο εφαρμογή, αλλά τμηματικά, εκμεταλλευόμενη την ενσωμάτωσή της και στις 3 εφαρμογές.

Η ομαδοποίηση των συλλεγμένων δεδομένων, στα οποία θα αποκτά πρόσβαση η βιβλιοθήκη, δεν είναι απαραίτητο ότι θα γίνει στη συσκευή του χρήστη. Η βιβλιοθήκη μπορεί να συλλέγει τα μεμονωμένα δεδομένα στα οποία αποκτά πρόσβαση κάθε φορά και να τα στέλνει στον απομακρυσμένο server. Η συσχέτισή τους μπορεί να πραγματοποιηθεί εσωτερικά στον server, χωρίς το υποκείμενο των δεδομένων να μπορέσει να το αντιληφθεί.

Δεδομένα του χρήστη, η γνώση των οποίων θα ήταν προς όφελος τρίτων, είναι μεταξύ άλλων: [33]

- Η τοποθεσία του χρήστη, μέσω της οποίας μπορούν να εξαχθούν συμπεράσματα για τον τόπο διαμονής του, καθώς και για τις περιοχές στις οποίες κυκλοφορεί.
- Η χρήση που κάνει στις εφαρμογές του, καθώς και πληροφορίες για τα αρχεία στον χώρο αποθήκευσης, οδηγώντας έτσι έμμεσα σε ασφαλή συμπεράσματα για τα ενδιαφέροντά του.
- Οι πληροφορίες για τη συσκευή, διευκολύνοντας έτσι κατά πολύ το fingerprinting, ενώ ταυτόχρονα μπορεί να εκτιμηθεί το εισόδημά του.

- Μετα-δεδομένα τα οποία αφορούν τις επικοινωνίες, καθώς και αντίστοιχα logs, η ανάλυση των οποίων μπορεί να οδηγήσει σε συμπεράσματα για τον κοινωνικό του κύκλο, αλλά και γενικότερα για την προσωπικότητά του.

Επίσης, οι library-0, library-1, library-3, επιπρόσθετα από τα permissions τα οποία ζητά η καθεμία, αποκτούν όλα τα permissions τα οποία έχουν εκχωρηθεί στις τρεις εφαρμογές. Αυτό ενδεχομένως αποτελεί πρόβλημα, στην περίπτωση που οι βιβλιοθήκες αυτές περιλαμβάνουν κενά ασφαλείας, τα οποία θα μπορούσαν να εκμεταλλευθούν από κάποιο κακόβουλο τρίτο.

Το πρόβλημα της intra-library collusion επιδεινώνεται, καθώς πολλές βιβλιοθήκες παρέχουν κατάλληλη νομική βάση για τα δεδομένα που ζητούν να στείλουν στον εξωτερικό server. Όμως, ο χρήστης συνήθως δεν έχει καμία πληροφόρηση για την περεταίρω επεξεργασία που αυτά υφίστανται, από τη στιγμή που σταλθούν στον server.

5. ΣΤΑΤΙΚΗ ΚΑΙ ΔΥΝΑΜΙΚΗ ΑΝΑΛΥΣΗ ΕΦΑΡΜΟΓΩΝ

5.1 Γενικά

Με βάση τα ανωτέρω, στη συνέχεια εστιάζουμε στη μελέτη συγκεκριμένης κατηγορίας εφαρμογών, προκειμένου να διερευνήσουμε και να αξιολογήσουμε πτυχές της επεξεργασίας προσωπικών δεδομένων που συντελούν, μέσω δοκιμών σε κατάλληλο περιβάλλον, Ως εκ τούτου, στο Κεφάλαιο 5, αρχικά, παρουσιάζεται το περιβάλλον της προσομοίωσης. Στη συνέχεια παρατίθενται και σχολιάζονται τα αποτελέσματα που έχουν προκύψει από τη στατική και δυναμική ανάλυση της εκτέλεσης ενός δείγματος 8 δημοφιλών εφαρμογών από το Google Play Store, οι οποίες προσφέρουν τη δυνατότητα online αγορών. Τέλος, εξετάζονται οι αντίστοιχες πολιτικές απορρήτου και ελέγχεται ο βαθμός ταύτισης με τα ευρήματα των προσομοιώσεων καθώς και ο βαθμός στον οποίο έχει υιοθετηθεί η αρχή “προστασίας δεδομένων εξ’ ορισμού”.

5.2 Δομή Περιβάλλοντος Προσομοίωσης

Για τις ανάγκες της προσομοίωσης, χρησιμοποιήθηκε το περιβάλλον Genymotion 3.7.1, σε συνεργασία με το VirtualBox 7.0.10. [35] [36]

Μέσω του Genymotion, δημιουργήθηκε μια εικονική συσκευή Samsung Galaxy S10, στην οποία εκτελείται το λειτουργικό Android 12.0. Ύστερα από την εγκατάσταση του GApps module, μέσω της επίσημης πλατφόρμας Google Play Store εγκαταστάθηκαν οι παρακάτω εφαρμογές για δοκιμή:

- AB (έκδοση 2.49)
- Booking (έκδοση 50.1.1)
- e-Food (έκδοση 8.13.2)
- Germanos (έκδοση 2.1.2)
- Nike (έκδοση 24.45.1)
- Pull & Bear (έκδοση 11.7.2)
- Wolt (έκδοση 24.36.1)
- Zara (έκδοση 15.7.1)

Η επιλοή των ως άνω εφαρμογών έγινε με βάση τη δημοφιλία τους.

Όλες οι παραπάνω εφαρμογές, εγκαταστάθηκαν με τις προεπιλεγμένες ρυθμίσεις, προκειμένου να εξετασθεί η ικανοποιητική υιοθέτηση της αρχής “προστασίας δεδομένων εξ’ ορισμού”.

Για τις ανάγκες της στατικής και δυναμικής ανάλυσης, χρησιμοποιήθηκαν οι παρακάτω εφαρμογές:

- **Exodus (έκδοση 3.3.2):** Η εφαρμογή Exodus πραγματοποιεί στατική ανάλυση στην προς εξέταση εφαρμογή, για τον εντοπισμό ενσωματωμένων ιχνηλατών, καθώς και για την εξαγωγή των ζητούμενων permissions. Μέσω της επίσημης

καταγραφής της Google [13], τα permissions αυτά μπορούν να ενταχθούν σε μια από τις 3 κατηγορίες που έχουν περιγραφεί στην Ενότητα 3.5.

- **TC Slim (έκδοση 2024.01.03):** Η εφαρμογή TC Slim, γνωστή και ως Tracker Control, πραγματοποιεί δυναμική ανάλυση για τον εντοπισμό ιχνηλατών, με τους οποίους επιχειρεί να επικοινωνήσει η προς εξέταση εφαρμογή κατά την εκτέλεσή της. Επίσης, κατηγοριοποιεί τους εκάστοτε ιχνηλάτες, με βάση το σκοπό για τον οποίο πραγματοποιείται η ιχνηλάτηση. Έτσι, αυτοί μπορούν να κατηγοριοποιηθούν ως “analytics”, “advertising” κλπ.

5.3 Αποτελέσματα Προσομοίωσης

Στην ενότητα αυτή παρουσιάζονται τα αποτελέσματα των προσομοιώσεων, που εκτελέστηκαν στο περιβάλλον που έχει περιγραφεί στην Ενότητα 5.2. Αρχικά παρουσιάζονται τα αποτελέσματα της στατικής ανάλυσης και των permissions, ενώ στη συνέχεια τα αποτελέσματα που αφορούν τον εντοπισμό ιχνηλατών, μέσω στατικής και δυναμικής ανάλυσης.

5.3.1 Εξέταση Permissions

Στον παρακάτω πίνακα παρουσιάζονται τα permissions της κάθε μίας προς εξέταση εφαρμογής, τα οποία εντοπίστηκαν από το Exodus. Το χρώμα της πρώτης στήλης υποδηλώνει το είδος του permission. Με πράσινο χαρακτηρίζονται τα normal permissions, με κόκκινο τα dangerous, ενώ με χρυσαφί τα signature. Το σύμβολο “X” σε ένα κελί, υποδηλώνει ότι η εφαρμογή της εκάστοτε στήλης χρησιμοποιεί το permission της αντίστοιχης γραμμής. Στην τελευταία σειρά αναγράφεται το πλήθος των permissions που ζητά η εφαρμογή της κάθε στήλης, ενώ σε παρένθεση καταγράφεται πόσα από αυτά ανήκουν στην κατηγορία “dangerous”.

Πίνακας 3: Χρησιμοποιούμενα Permissions (android.permission.*) ανά εφαρμογή, με βάση τη στατική ανάλυση του Exodus

	ONOMA PERMISSION	AB	Booking	e-Food	Germanos	Nike	Pull & Bear	Wolt	Zara
	ACCESS_COARSE_LOCATION	X	X	X	X	X	X	X	X
	ACCESS_FINE_LOCATION	X	X	X	X	X	X	X	X
	ACCESS_MEDIA_LOCATION						X		
	ACCESS_NETWORK_STATE	X	X	X	X	X	X	X	X
	ACCESS_WIFI_STATE	X	X		X	X	X	X	X
	BIND_NOTIFICATIONS_ LISTENER_SERVICE								X
	BLUETOOTH				X				
	BLUETOOTH_ADMIN				X				
	BLUETOOTH_CONNECT					X			
	BLUETOOTH_SCAN					X			
	CHANGE_WIFI_STATE	X			X	X	X		X
	FOREGROUND_SERVICE		X	X	X	X	X	X	X
	GET_ACCOUNTS		X		X				
	HIGH_SAMPLING_RATE_		X			X			

	SENSORS								
	INSTALL_SHORTCUT		X						
	INTERNET	X	X	X	X	X	X	X	X
	MODIFY_AUDIO_SETTINGS							X	
	NFC		X				X		X
	POST_NOTIFICATIONS	X	X	X	X	X	X	X	X
	READ_CALENDAR		X						
	READ_EXTERNAL_STORAGE	X	X		X	X	X		X
	READ_MEDIA_AUDIO						X		
	READ_MEDIA_IMAGES		X		X	X	X	X	X
	READ_MEDIA_VIDEO		X				X	X	X
	READ_PHONE_STATE		X					X	
	READ_SYNC_SETTINGS		X			X			
	READ_SYNC_STATS					X			
	RECEIVE_BOOT_COMPLETED		X	X	X	X	X	X	X
	RECORD_AUDIO						X		X
	REORDER_TASKS				X				
	SCHEDULE_EXACT_ALARM					X			
	SET_ALARM		X						
	SET_TIME_ZONE						X		X
	USE_BIOMETRIC				X	X			
	USE_FINGERPRINT				X	X			
	VIBRATE	X		X		X	X		X
	WAKE_LOCK	X	X	X	X	X	X	X	X
	WRITE_CALENDAR		X						
	WRITE_EXTERNAL_STORAGE		X		X		X		X
	WRITE_SETTINGS						X		X
	WRITE_SYNC_SETTINGS		X			X			
ΖΗΤΟΥΜΕΝΑ PERMISSIONS (DANGEROUS PERMISSIONS)		10 (4)	23 (11)	9 (3)	19 (7)	22 (7)	21 (10)	13 (6)	20 (8)

Από τον παραπάνω πίνακα γίνεται φανερό το μεγάλο πλήθος των permissions τα οποία ζητούν οι εφαρμογές. Με εξαίρεση τις εφαρμογές AB, e-Food και Wolt, όλες οι υπόλοιπες αιτούνται την έγκριση 19-23 permissions για τη λειτουργία τους.

Η εφαρμογή e-Food είναι η μόνη η οποία ζητάει μονοψήφιο αριθμό permissions, μόλις 9. Επίσης, με μόλις 3 να ανήκουν στην κατηγορία dangerous, απαιτεί το μικρότερο ποσοστό από dangerous permissions (33.3%). Με τη διαφορά ενός επιπλέον dangerous permission, λειτουργεί η εφαρμογή AB, με 10 permissions, από τα οποία 4 ανήκουν στην κατηγορία των dangerous.

Οι εφαρμογή της Booking αιτείται τα περισσότερα permissions, συνολικά 23, από τα οποία 11 εντάσσονται στα dangerous. Το ποσοστό αυτό, 47,8%, είναι το υψηλότερο από τις εφαρμογές που εξετάστηκαν.

Ιδιαίτερο ενδιαφέρον παρουσιάζει το ζευγάρι Pull & Bear και Zara. Και οι δύο εταιρείες ανήκουν στον ίδιο όμιλο, Inditex. Εξετάζοντας τα permissions, παρατηρούμε ότι ζητούν σχεδόν τα ίδια permissions, με εξαίρεση τα ACCESS_MEDIA_LOCATION και READ_MEDIA_AUDIO (dangerous permissions, η έγκριση των οποίων απαιτείται από την εφαρμογή Pull & Bear) και BIND_NOTIFICATIONS_LISTENER_SERVICE (signature permission, το οποίο αιτείται από την εφαρμογή Zara). Και οι δύο εφαρμογές αιτούνται πρόσβαση σε μεγάλο αριθμό permissions. Η εφαρμογή Pull & Bear χρησιμοποιεί 21 permissions, από τα οποία 10 ανήκουν στην κατηγορία dangerous, τα

οποία αντιστοιχούν σε ποσοστό 47.6%. Τα αντίστοιχα πλήθη permissions για την εφαρμογή Zara είναι 20 και 8, με το ποσοστό των dangerous να είναι 40%.

Όσον αφορά τα dangerous permissions, όλες οι εφαρμογές ζητούν πρόσβαση στην τοποθεσία, μέσω των permissions ACCESS_COARSE_LOCATION και ACCESS_FINE_LOCATION. Αυτό εν μέρει είναι αναμενόμενο, καθώς οι εφαρμογές αυτές ανήκουν στην κατηγορία των αγορών και μέρος της λειτουργικότητάς τους βασίζεται στη γνώση της ακριβούς τοποθεσίας του χρήστη (είτε για την καθοδήγησή του σε ένα κατάστημα είτε για την αποστολή της παραγγελίας του). Επίσης, είναι αναμενόμενη η αίτηση για το dangerous permission POST_NOTIFICATIONS, προκειμένου ο χρήστης να μπορεί να ενημερωθεί σε πραγματικό χρόνο για ζητήματα που αφορούν την παραγγελία του.

Παρό'όλ'αυτά, υπάρχουν dangerous permissions, των οποίων η αναγκαιότητα δεν είναι προφανής για την ομαλή λειτουργία τέτοιων εφαρμογών. Τέτοιο παράδειγμα είναι το ACCESS_MEDIA_LOCATION, το οποίο εντοπίστηκε σε μια εφαρμογή. Ύστερα από την εκχώρησή του, η εφαρμογή αποκτά πρόσβαση στην τοποθεσία στην οποία έχει ληφθεί ένα αρχείο πολυμέσων (π.χ. φωτογραφία), μέσω των μετα-δεδομένων EXIF. Ένα άλλο παράδειγμα είναι το GET_ACCOUNTS, το οποίο ζητείται από δύο εφαρμογές. Μέσω αυτού, οι εφαρμογές αποκτούν πρόσβαση στα αποθηκευμένα accounts της συσκευής. Τέλος, το RECORD_AUDIO, το οποίο επίσης ζητείται να εκχωρηθεί σε δύο εφαρμογές, δίνει τη δυνατότητα στην εφαρμογή να καταγράψει ήχους μέσω του μικροφώνου.

Ιδιαίτερη αναφορά πρέπει να γίνει και για την περίπτωση του permission WRITE_EXTERNAL_STORAGE, την έγκριση του οποίου ζητούν οι μισές εφαρμογές. Το permission αυτό επιτρέπει στην εφαρμογή να αποκτήσει δικαίωμα ανάγνωσης / εγγραφής σε ολόκληρο τον εξωτερικό χώρο αποθήκευσης, επιπλέον του καταλόγου που της έχει παραχωρηθεί από το ίδιο το Android. Η εκχώρηση του συγκεκριμένου permission αποθαρρύνεται από την ίδια την Google για τις εκδόσεις Android 10 και μετά. [34]

Ένα άλλο χαρακτηριστικό που παρατηρείται, είναι η διαφοροποίηση των ζητούμενων permissions από εφαρμογές που θεωρητικά παρέχουν παρόμοιες λειτουργίες. Μία εφαρμογή ζητά πρόσβαση στο ημερολόγιο της συσκευής, μέσω των READ_CALENDAR και WRITE_CALENDAR. Επίσης, είναι διαδεδομένη η χρήση των permissions READ_MEDIA_AUDIO / READ_MEDIA_IMAGES / READ_MEDIA_VIDEO, μέσω των οποίων η εφαρμογή αποκτά τη δυνατότητα να διαβάσει αντίστοιχα αρχεία πολυμέσων από τον εξωτερικό χώρο αποθήκευσης. Δύο άλλες εφαρμογές περιλαμβάνουν λειτουργίες που ζητούν την έγκριση του READ_PHONE_STATE. Το dangerous permission αυτό εξασφαλίζει πρόσβαση στην κατάσταση του τηλεφώνου, όπως σε πληροφορίες για το δίκτυο του συνδρομητή ή την κατάσταση των κλήσεων σε εξέλιξη.

Οι διαφοροποιήσεις σε αυτά τα ζητούμενα permissions, αυξάνουν τον κίνδυνο της εμφάνισης intra-library collusion. Για παράδειγμα, μια βιβλιοθήκη η οποία έχει ενσωματωθεί στην εφαρμογή Booking και Pull & Bear, λειτουργεί με εγκεκριμένα όλα τα dangerous permissions, εκτός από 2 (αυτά που αφορούν τη συνδεσιμότητα μέσω bluetooth). Η λειτουργία μιας βιβλιοθήκης με όλα τα dangerous permissions σε

αποδοχή, είναι δυνατή, αν αυτή έχει ενσωματωθεί σε μια μόλις επιπλέον εφαρμογή, αυτή της Nike.

Όπως έχει περιγραφεί στην Ενότητα 4.4, η εμφάνιση του φαινομένου intra-library collusion θέτει ενδεχομένως σε ρίσκο την ιδιωτικότητα και την διαφύλαξη των δεδομένων προσωπικού χαρακτήρα του χρήστη, καθώς μια βιβλιοθήκη ο οποία έχει ενσωματωθεί σε όλες αυτές τις δημοφιλείς εφαρμογές αποκτά διευρυμένη πρόσβαση σε πόρους της συσκευής.

Η ύπαρξη permissions τα οποία δεν σχετίζονται άμεσα με την κύρια λειτουργία των εφαρμογών αυτών, η οποία είναι η αγορά προϊόντων ή υπηρεσιών μέσω διαδικτύου, δεν μπορεί να χαρακτηριστεί οπωσδήποτε περιττή. Τα επιπλέον permissions εμπλουτίζουν τη λειτουργικότητα της εφαρμογής.

Όμως είναι απαραίτητη η επαρκής και κατανοητή πληροφόρηση του χρήστη για την ανάγκη έγκρισης των permissions αυτών, μέσω των αντίστοιχων πολιτικών απορρήτου. Επίσης, η εκχώρησή τους πρέπει να γίνεται με βάση την αρχή της “προστασίας των δεδομένων εξ’ ορισμού”.

5.3.2 Εξέταση Ιχνηλατών Τρίτων Μερών

Στους δύο παρακάτω πίνακες παρατίθενται τα αποτελέσματα της στατικής ανάλυσης, μέσω του Exodus, καθώς και της δυναμικής ανάλυσης, μέσω του TC Slim, όσον αφορά την παρουσία ιχνηλατών στις προς εξέταση εφαρμογές. Στην αριστερή στήλη καταγράφεται το είδος του ιχνηλάτη, ενώ το σύμβολο “X” υποδηλώνει την ενσωμάτωση του ιχνηλάτη στην εκάστοτε εφαρμογή.

Πίνακας 4: Ενσωματωμένοι ιχνηλάτες, καθώς και χαρακτηρισμός τους, με βάση τη στατική ανάλυση του Exodus

ΕΙΔΟΣ TRACKER	CODE DETECTION RULE	**ONOMA TRACKER**	AB	Booking	e-Food	Germanos	Nike	Pull & Bear	Wolt	Zara
CRASH REPORT	org.acra	**Acra**						X		X
CRASH REPORT	ch.acra	**Acra**						X		X
ANALYTICS	com.adjust.sdk	**Adjust**			X			X		
ANALYTICS	com.adjust.android.sdk	**Adjust**			X			X		
	com.adobe.marketing.mobile	**Adobe Experience Cloud**	X				X			
	org.altbeacon.beacon	**AltBeacon**	X							
	com.altbeacon.beacon	**AltBeacon**	X							
	org.altbeacon.bluetooth	**AltBeacon**	X							
ANALYTICS	com.appsflyer	**Apps Flyer**		X				X	X	
	com.criteo	**Criteo**						X		
ANALYTICS	com.adobe.mobile.Analytics	**Demdex**					X			
ANALYTICS	com.adobe.mobile.Config	**Demdex**					X			

ANALYTICS & LOCATION	com.estimote	**Estimote**					X			
ANALYTICS	com.facebook. appevents	**Facebook Analytics**	X					X		
ANALYTICS	com.facebook. marketing	**Facebook Analytics**	X					X		
ANALYTICS	com.facebook. CampaignTracki ngReceiver	**Facebook Analytics**	X					X		
ANALYTICS	com.facebook. flipper	**Facebook Flipper**		X						
IDENTIFI-CATION	com.facebook. login	**Facebook Login**	X		X			X	X	
	com.facebook. share	**Facebook Share**			X			X	X	
ADVER TISEMENT	com.google.ads	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms.ads. AdView	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms.ads. AdActivity	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms.ads. AdRequest	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms.ads. mediation	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms.ads. doubleclick	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.ads	**Google AdMob**						X		
ADVER TISEMENT	com.google.unity .ads	**Google AdMob**						X		
ADVER TISEMENT	com.google. android.gms. admob	**Google AdMob**						X		
ADVER TISEMENT	com.google. firebase. firebase_ads	**Google AdMob**						X		
ANALYTICS	com.google. android.apps. analytics	**Google Analytics**		X	X			X		X
ANALYTICS	com.google. android.gms. analytics	**Google Analytics**		X	X			X		X
ANALYTICS	com.google. analytics	**Google Analytics**		X	X			X		X
CRASH REPORT	io.fabric	**Google Crash Lytics**	X	X	X			X	X	X
CRASH REPORT	com.crashlytics	**Google Crash Lytics**	X	X	X			X	X	X
CRASH REPORT	com.google .firebase.crashlyt ics	**Google Crash Lytics**	X	X	X			X	X	X

CRASH REPORT	com.google.firebase.crash	**Google Crash Lytics**	X	X	X			X	X	X
CRASH REPORT	io.invertase.firebase.crashlytics	**Google Crash Lytics**	X	X	X			X	X	X
ANALYTICS	com.google.firebase.analytics.FirebaseAnalytics	**Google Firebase Analytics**	X	X	X		X	X	X	X
ANALYTICS	com.google.android.gms.measurement	**Google Firebase Analytics**	X	X	X		X	X	X	X
ANALYTICS	com.google.firebase.firebase_analytics	**Google Firebase Analytics**	X	X	X		X	X	X	X
ANALYTICS	com.google.tagmanager	**Google Tag Manager**		X	X			X		X
ANALYTICS	com.google.android.gms.tagmanager	**Google Tag Manager**		X	X			X		X
	com.inmobi	**Inmobi**					X			
	in.inmobi	**Inmobi**					X			
CRASH REPORT	com.instabug	**Istabug**							X	
ANALYTICS & PROFILING	com.mopinion.mopinionsdk	**Mopinion**	X							
ANALYTICS	com.newrelic.agent	**New Relic**					X			
ANALYTICS	com.newrelic.mobile	**New Relic**					X			
ANALYTICS	com.optimizely	**Optimizely**					X	X		X
	com.salesforce.marketingcloud	**Salesforce Marketing Cloud**	X							
CRASH REPORT	io.sentry	**Sentry**							X	
CRASH REPORT	com.joshdholtz.sentry	**Sentry**							X	
ANALYTICS	com.singular.sdk	**Singular**					X			
ANALYTICS	com.snowpillowanalytics	**Snowpillow**						X		
	com.urbanairship	**Urban airship**					X			

Ο αντίστοιχος πίνακας, ο οποίος προέκυψε από τη δυναμική ανάλυση της εκτέλεσης της κάθε εφαρμογής, μέσω του TC Slim, παρατίθεται στη συνέχεια. Όπως και στην περίπτωση του Πίνακα 4, στην αριστερή στήλη καταγράφεται το είδος του ιχνηλάτη, ενώ το σύμβολο “X” υποδηλώνει την ενσωμάτωση του ιχνηλάτη στην εκάστοτε εφαρμογή.

Πίνακας 5: Ενσωματωμένοι ιχνηλάτες, καθώς και χαρακτηρισμός τους, με βάση τη δυναμική ανάλυση του TC Slim

ΕΙΔΟΣ TRACKER	CODE DETECTION RULE	**OMONA TRACKER**	AB	Booking	e-Food	Germanos	Nike	Pull & Bear	Wolt	Zara

FINGER PRINTING	app.adjust.com	**Adjust**			X					
UNCATEGORISED	assets.adobedtm.com	**Adobe**					X			
FINGER PRINTING	dpm.demdex.net	**Adobe**	X				X			
FINGER PRINTING	groupedelhaize.sc.omtrdc.net	**Adobe**	X							
UNCATEGORISED	combine.urbanairship.com	**Airship**					X			
UNCATEGORISED	device-api.urbanairship.com	**Airship**					X			
UNCATEGORISED	remote-data.urbanairship.com	**Airship**					X			
UNCATEGORISED	api.iterable.com	**api.iterable.com**							X	
UNCATEGORISED	sdk.iad-01.braze.com	**Braze**			X					
UNCATEGORISED	c.riskified.com	**c.riskified.com**		X						
ANALYTICS	bf36176aqn.bf.dynatrace.com	**Dynatrace**	X							
SOCIAL	graph.facebook.com	**Facebook**		X	X	X		X	X	
SOCIAL	platform-lookaside.fbsbx.com	**Facebook**		X						
UNCATEGORISED	o200274.ingest.sentry.io	**Functional Software Inc**							X	
FINGER PRINTING	ad.doubleclick.net	**Google**		X						
FINGER PRINTING	adservice.google.com	**Google**		X						
ANALYTICS	firebase-settings.crashlytics.com	**Google**	X	X	X	X		X	X	X
FINGER PRINTING	www.google-analytics.com	**Google**		X	X					
CONTENT	www.gstatic.com	**Google**					X			
UNCATEGORISED	img.riskified.com	**img.riskified.com**		X						
EMAIL	nexus-websocket-a.intercom.io	**Intercom**							X	
ANALYTICS	mobile-collector.newrelic.com	**New Relic**					X			
ADVERTISING	cdn.optimizely.com	**Optimizely**								X
ADVERTISING	logx.optimizely.com	**Optimizely**								X
UNCATEGORISED	sdkapicdn.applanga.com	**sdkapicdn.applanga.com**	X				X			
	q-xx.bstatic.com			X						

Από τα παραπάνω αποτελέσματα, τόσο της στατικής όσο και της δυναμικής ανάλυσης, παρατηρούμε ότι σε όλες τις εφαρμογές υπάρχει ενσωματωμένος τουλάχιστον ένας ιχνηλάτης. Οι ιχνηλάτες της Google (π.χ Google Firebase Analytics) και της Meta, μέσω του Facebook, βρίσκονται ενσωματωμένοι σχεδόν σε όλες τις εφαρμογές που εξετάσθηκαν.

Οι μικρές αποκλίσεις που παρατηρούνται, οφείλονται στον διαφορετικό τρόπο λειτουργίας του Exodus και του TC Slim. Η πρώτη εφαρμογή, εκτελώντας στατική ανάλυση, εξετάζει τον κώδικα της εφαρμογής, αναζητώντας δείγματα από γνωστούς ιχνηλάτες. Αντίθετα, η εφαρμογή TC Slim, παρακολουθεί σε πραγματικό χρόνο την εκτέλεση της προς εξέταση εφαρμογή. Στην περίπτωση της δυναμικής ανάλυσης, είναι λογικό αφενός κάποιες επικοινωνίες με ιχνηλάτες να μην πραγματοποιούνται κατά τη διάρκεια της εξέτασης, ενώ να εμφανίζονται άλλες, λόγω της δυναμικής φόρτωσης κώδικα (κάτι το οποίο είναι δύσκολο να εντοπιστεί μέσω στατικής ανάλυσης).

Η ύπαρξη ιχνηλατών, σε συνδυασμό με πολλά εκχωρημένα permissions, ενδέχεται να υποδηλώνει πιθανή απειλή στην ιδιωτικότητα και στην προστασία των δεδομένων προσωπικού χαρακτήρα του χρήστη.

Υπό αυτό το πρίσμα, παρατηρούμε ότι οι εφαρμογές Booking και Nike, συνδυάζοντας πολλά εκχωρημένα permissions, καθώς και πολλούς ενσωματωμένους ιχνηλάτες ενδεχομένως συμμετέχουν στην κοινοποίηση δεδομένων προσωπικού χαρακτήρα σε μεγαλύτερο βαθμό από τις άλλες εφαρμογές.

Αντίθετα, οι εφαρμογές e-Food και Wolt, έχοντας αποκτήσει λίγα permissions και ενσωματώνοντας σχετικά λίγους ιχνηλάτες, φαίνεται να είναι περισσότερο φιλικές στον χρήστη, όσον αφορά την ιδιωτικότητα και την προστασία των δεδομένων προσωπικού χαρακτήρα.

5.4 Εξέταση Πολιτικών Απορρήτου

Στην ενότητα αυτή εξετάζονται οι πολιτικές απορρήτου των εφαρμογών. Πέρα από την ευκολία κατανόησης, κάποια κύρια σημεία τα οποία πρέπει να καθορίζονται στο κείμενο τους, είναι:

- Εάν καταγράφονται τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται από την εφαρμογή.
- Εάν πραγματοποιείται κοινοποίηση σε τρίτα μέρη, ποια είναι αυτά και ποια δεδομένα κοινοποιούνται.
- Ποιος είναι ο σκοπός της κοινοποίησης του εκάστοτε δεδομένου.
- Εάν υπάρχει νομική βάση για την καταγραφή και επεξεργασία των δεδομένων.
- Στην περίπτωση όπου αυτή είναι η συγκατάθεση του χρήστη, τότε αν αυτή δίνεται ελεύθερα.
- Εάν ναι, τότε εξετάζεται αν αυτή δίνεται με βάση την αρχή προστασίας δεδομένων εξ’ ορισμού.
- Εάν η ανάκλησή της είναι εξίσου εύκολη με την αποδοχή της.
- Εάν καταγράφονται τα permissions τα οποία ζητούνται.

- Εάν δικαιολογείται η χρήση τους, κυρίως όσων εντάσσονται στην κατηγορία dangerous.
- Εάν ικανοποιείται η αρχή για data minimisation.
- Εάν στην περίπτωση μεγάλων εταιρειών υπάρχει 1 γενική πολιτική απορρήτου, ή αν υπάρχουν πολλές επιμέρους πολιτικές.
- Εάν υπάρχει ταύτιση των αποτελεσμάτων της στατικής και δυναμικής ανάλυσης με τις αντίστοιχες πολιτικές απορρήτου.

5.4.1 Πολιτική Απορρήτου Εφαρμογής AB

Η πολιτική απορρήτου της εφαρμογής AB βρίσκεται στο site της εταιρείας [37]. Η εταιρεία συλλέγει δεδομένα για τον χρήστη στις εξής περιπτώσεις: κατά την έκδοση της κάρτας μέλους, σε επισκέψεις στο site ή κατά τη χρήση της εφαρμογής. Ειδικά στην πρώτη περίπτωση, τα δεδομένα προσωπικού χαρακτήρα τα οποία καλείται να καταχωρήσει ο χρήστης, είναι το ονοματεπώνυμο, η διεύθυνση κατοικίας, ο τηλεφωνικός αριθμός, το e-mail και η ημερομηνίας γέννησης. Αναφέρεται ξεκάθαρα πως δεν συλλέγονται ευαίσθητα προσωπικά δεδομένα. Τα δεδομένα προσωπικού χαρακτήρα όσων συμμετέχουν στο πρόγραμμα μελών συνδυάζονται με τα στοιχεία συναλλαγών τους, για στατιστικούς λόγους.

Τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται η εταιρεία, καθώς και τρίτα μέρη, εξαρτώνται από το προφίλ του προγράμματος πιστότητας που έχει επιλέξει ο πελάτης. Με βάση την περιγραφή του προφίλ Basic, χωρίς να γίνεται κάποια αναφορά σε επεξεργασία δεδομένων, ο πελάτης συναινεί στη λήψη προωθητικών προσφορών και ενημερώσεων μέσω διαφόρων μέσων επικοινωνίας. Με βάση την περιγραφή του προφίλ Personal, ο πελάτης συναινεί στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με σκοπό την λήψη προσωποποιημένων προσφορών και ενημερώσεων. Τέλος, οι πελάτες του προφίλ Unique, λαμβάνουν παρόμοια μηνύματα και για συνεργάτες της εταιρείας. Σε αυτές τις περιγραφές, δεν γίνεται κάποια περεταίρω αναφορά στα είδη των δεδομένων που επεξεργάζονται επιπλέον αυτών που χρησιμοποιήθηκαν για την έκδοση της κάρτας (π.χ. ύψος αγορών, προϊόντα που αγοράζονται συνήθως, συχνότητα αγορών, καταστήματα στα οποία πραγματοποιούνται οι αγορές).

Επίσης, αναφέρεται ρητά ότι αν ο πελάτης επιλέξει αλλαγή του προφίλ, ενδέχεται να απολέσει πόντους ή προνόμια που είχε με βάση το προηγούμενο προφίλ. Αυτό προκαλεί προβληματισμό, αναφορικά με το κατά πόσο ο πελάτης θα επέλεγε ελεύθερα να αλλάξει το επιλεγμένο προφίλ, στην περίπτωση που αντιτίθεται στην επεξεργασία.

Τα δεδομένα προσωπικού χαρακτήρα του χρήστη παραμένουν στη διάθεση της εταιρείας για όσο διάστημα χρησιμοποιείται η κάρτα μέλους και έως το πολύ 5 χρόνια μετά την τελευταία χρήση της.

Η εταιρεία μοιράζεται τα δεδομένα προσωπικού χαρακτήρα με τρίτους. Όπως αναφέρεται, οι εταιρείες αυτές παρέχουν υπηρεσίες επικοινωνίας, διαφήμισης ή ενημέρωσης, χωρίς όμως να κατονομάζονται αυτές ή τα δεδομένα που κοινοποιούνται. Στην πολιτική απορρήτου αναφέρεται πως ο AB *“διασφαλίζει ότι από τις εταιρείες αυτές έχουν ληφθεί όλα τα απαραίτητα οργανωτικά και τεχνικά μέσα για την προστασία των δεδομένων”*.

Περισσότερο εκτενής αναφορά γίνεται στα cookies που χρησιμοποιεί το site της εταιρείας. Στην περίπτωση αυτή καταγράφονται αναλυτικά τα cookies που χρησιμοποιούνται, ο σκοπός τους, καθώς και ο χρόνος ζωής τους. Αναφέρεται ξεκάθαρα ότι τα cookies αυτά χρησιμοποιούνται για την πρόσβαση του χρήστη σε συγκεκριμένα προϊόντα και υπηρεσίες, για στατιστικούς λόγους ή για λόγους marketing (όπως η προβολή προσωποποιημένων διαφημίσεων). Ιδιαίτερη αναφορά γίνεται στην ενσωμάτωση των Adobe Analytics (για χρήση analytics) και Google Advertising (για την υποστήριξη προσωποποιημένων διαφημίσεων). Ένα σημείο που χρήζει προσοχής, είναι η μη τήρηση της αρχής της προστασίας εξ' ορισμού, καθώς, όπως αναφέρεται, αν ο χρήστης δεν κάνει κάποια επιλογή (αποδοχή η απόρριψη των cookies), αυτό θεωρείται ως αποδοχή της χρήσης τους.

Δεδομένα προσωπικού χαρακτήρα, τα οποία καταγράφονται αυτόματα κατά τη χρήση της εφαρμογής, είναι η γλώσσα, η τοποθεσία και οι ρυθμίσεις του προγράμματος περιήγησης. Επίσης, εάν ο χρήστης αποδεχθεί τα analytic cookies, καταγράφονται επιπλέον τμήμα της διεύθυνσης IP, η ανάλυση της οθόνης και το μοναδικό αναγνωριστικό της συσκευής.

Επιπλέον, κατά την υποβολή μιας παραγγελίας, τα απαραίτητα δεδομένα προσωπικού χαρακτήρα, είναι το ονοματεπώνυμο, η διεύθυνση παράδοσης και το τηλέφωνο επικοινωνίας. Αυτά κρίνονται απαραίτητα για την αποστολή της παραγγελίας. Όμως στους αποδέκτες αναφέρονται και τρίτες συνεργαζόμενες εταιρείες που έχουν αναλάβει την προβολή ή προώθηση προϊόντων ή /και υπηρεσιών, χωρίς να αναφέρεται η ταυτότητά τους ή ο λόγος για τον οποίο κοινοποιούνται σε αυτές τα συγκεκριμένα δεδομένα.

Τέλος, γίνεται αναφορά στο profiling του χρήστη. Ο χρήστης αρχικά μπορεί να προσδιοριστεί μοναδικά με χρήση των cookies, καθώς και ενός *"μοναδικού αριθμού που συνδέεται με την κινητή συσκευή"*, χωρίς να προσδιορίζεται ποιος είναι αυτός. Μέσω αυτών των παραμέτρων, είναι δυνατός ο συσχετισμός των πληροφοριών τις οποίες έχει κοινοποιήσει ο πελάτης στην εταιρεία κατά την εγγραφή του στο πρόγραμμα πελατών, με τις αναζητήσεις και τις αγορές που πραγματοποιεί. Όπως περιγράφεται ξεκάθαρα στην πολιτική απορρήτου, για αυτό απαιτείται η έγκριση του χρήστη. Με βάση τη διατύπωση της πολιτικής, έχει υιοθετηθεί η αρχή προστασίας δεδομένων εξ' ορισμού, με τη συγκεκριμένη δυνατότητα να είναι απενεργοποιημένη από προεπιλογή. Εφόσον ο χρήστης αποδεχθεί το profiling, εντάσσεται σε μια *"ομάδα πελατών με παρόμοια προφίλ ενδιαφέροντος"*, με σκοπό την προβολή εξατομικευμένων διαφημίσεων.

5.4.2 Πολιτική Απορρήτου Εφαρμογής Booking

Η πολιτική απορρήτου της Booking είναι η πιο εκτεταμένη και μια από τις ευκολότερα κατανοητές στο σύνολο των εφαρμογών που εξετάστηκαν [38]. Τα δεδομένα προσωπικού χαρακτήρα, τα οποία καταγράφονται από την εφαρμογή, χωρίζονται σε 3 κατηγορίες: τα υποχρεωτικά που πρέπει να καταχωρήσει ο χρήστης, κάποια προαιρετικά τα οποία ενδεχομένως είναι απαραίτητα για κάποια είδη κρατήσεων, καθώς και αυτά που συλλέγονται αυτόματα από την εφαρμογή. Στην πρώτη κατηγορία, ανήκουν το ονοματεπώνυμο και το e-mail, τα οποία κρίνονται απαραίτητα για την πραγματοποίηση μιας κράτησης. Στη δεύτερη κατηγορία συμπεριλαμβάνονται τα στοιχεία πληρωμής (αν η κράτηση εξοφληθεί μέσω της εφαρμογής) ή ο αριθμός ταυτότητας ή διαβατηρίου ή άδειας οδήγησης (αν πραγματοποιηθεί αγορά εισιτηρίου ή ενοικίαση μεταφορικού μέσου). Στην τρίτη κατηγορία ανήκουν, μεταξύ άλλων, η

διεύθυνση IP, το αναγνωριστικό της συσκευής, η έκδοση του λειτουργικού συστήματος και οι ρυθμίσεις γλώσσας.

Επίσης, αναφέρεται ότι κατά τη χρήση της εφαρμογής, ενδέχεται να αποστέλλονται επιπλέον πληροφορίες που αφορούν την τοποθεσία του χρήστη και τις επαφές του. Οι πληροφορίες αυτές, όπως αναφέρεται στην πολιτική απορρήτου, βοηθούν στην *"καλύτερη δυνατή εξυπηρέτηση και εμπειρία [...] προτείνοντας τα πλησιέστερα στην τοποθεσία σας εστιατόρια ή αξιοθέατα ή κάνοντας άλλες προτάσεις"*. Με βάση αυτή την περιγραφή, η πρόσβαση στην τοποθεσία ενδέχεται να κρίνεται χρήσιμη, όμως η πρόσβαση στις επαφές δεν φαίνεται να εξυπηρετεί το σκοπό της εφαρμογής.

Επιπροσθέτως, γίνεται αναφορά στην ανταλλαγή δεδομένων προσωπικού χαρακτήρα με τρίτους ή θυγατρικές. Τέτοιες εταιρείες είναι τα ίδια τα καταλύματα, τα τοπικά γραφεία της εταιρείας ή εταιρείες υποστήριξης πελατών. Ένα σημείο άξιο αναφοράς είναι το γεγονός ότι οι πληροφορίες που ανταλλάσσονται με υπηρεσίες marketing (e-mail, διεύθυνση IP) έχουν υποστεί κατακερματισμό (hashing) για την αποτροπή χρήσης τους για άλλους σκοπούς. Όμως υπάρχουν και ανταλλαγές δεδομένων η χρησιμότητα των οποίων δεν είναι προφανής: για παράδειγμα η αποστολή των στοιχείων της κράτησης (χωρίς να κατονομάζονται ποια είναι αυτά) στον πάροχο διαφημίσεων, εφόσον ο χρήστης πραγματοποιήσει κράτηση στην Booking αφότου χρησιμοποίησε διαφήμιση του συγκεκριμένου παρόχου.

Στην περίπτωση τηλεφωνικής επικοινωνίας με το κατάλυμα μέσω της εφαρμογής, ενδέχεται να συλλεχθούν μετα-δεδομένα της επικοινωνίας, όπως είναι η ταυτότητα του χρήστη, από πού τηλεφώνησε, η ημερομηνία της κλήσης καθώς και η διάρκειά της. Τέλος, κατά την σύνδεση του λογαριασμού Booking με λογαριασμό σε μέσο κοινωνικής δικτύωσης, ενδέχεται να υπάρξει ανταλλαγή δεδομένων μεταξύ της Booking και του παρόχου μέσων κοινωνικής δικτύωσης.

Η καταγραφή και επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται για διάφορους σκοπούς. Μεταξύ αυτών, είναι η πραγματοποίηση της κράτησης, η εξυπηρέτηση πελατών, λόγοι marketing (ως παράδειγμα αναφέρεται η αποστολή εξατομικευμένων μηνυμάτων), η βελτίωση υπηρεσιών (για παράδειγμα η δημιουργία και εξέλιξη μοντέλων τεχνητής νοημοσύνης) και η διαφοροποίηση της τιμής ανάλογα με τοποθεσία (επεξεργασία με βάση τη διεύθυνση IP).

Για όλα τα παραπάνω, αναφέρεται ξεκάθαρα η νομική βάση στην οποία βασίζεται η επεξεργασία. Για παράδειγμα, η εκτέλεση του συμβολαίου (πραγματοποίηση κράτησης) και το έννομο συμφέρον. Στην περίπτωση του marketing μέσω εξατομικευμένων μηνυμάτων, αναφέρεται η λήψη της συγκατάθεσης του χρήστη. Επίσης, στην περίπτωση της βελτίωσης υπηρεσιών με χρήση τεχνητής νοημοσύνης, το έννομο συμφέρον βασίζεται στην βελτίωση της απόδοσης και της ποιότητας των υπηρεσιών. Όμως, η χρήση των προσωπικών δεδομένων του χρήστη για την διαφοροποίηση της τιμής με βάση την τοποθεσία του, ενδέχεται να επηρεάσουν δυσμενώς, ενώ δεν φαίνεται να υπάρχει δυνατότητα μέσω της εφαρμογής στον χρήστη να αντιταχθεί σε μια τέτοια επεξεργασία.

Επίσης, γίνεται αναφορά στην μεταφορά δεδομένων προσωπικού χαρακτήρα εκτός ΕΟΧ. Σε αυτή την περίπτωση, η εταιρεία δεσμεύεται στο να *"καθορίσει και εφαρμόσει κατάλληλα συμβατικά, οργανωτικά και τεχνικά μέτρα [...] μέσω της θέσπισης τυποποιημένων συμβατικών ρητρών που έχουν εγκριθεί από την Ευρωπαϊκή Ένωση, με την εξέταση των χωρών στις οποίες μπορούν να διαβιβαστούν τα δεδομένα και με την επιβολή συγκεκριμένων τεχνικών και οργανωτικών μέτρων ασφαλείας"*.

Όσον αφορά την αρχή προστασίας δεδομένων εξ'ορισμού, αυτή φαίνεται να έχει υλοποιηθεί σε σημαντικό βαθμό. Διατυπώσεις όπως *"μπορείτε να επιλέξετε να μας παρέχετε πρόσβαση στα δεδομένα τοποθεσίας"* ή για την περίπτωση της φωνητικής αναζήτησης *"θα χρειαστεί να μας δώσετε πρόσβαση στο μικρόφωνο της συσκευής"* υπονοεί ότι αυτές οι κοινοποιήσεις δεδομένων προσωπικού χαρακτήρα είναι από προεπιλογή απενεργοποιημένες.

Τέλος, στην πολιτική απορρήτου γίνεται ξεκάθαρη αναφορά στις τεχνικές cross-device tracking, τις οποίες χρησιμοποιεί η εταιρεία. Με τη χρήση τεχνικών όπως web beacons (κατηγορία fingerprinting με χρήση canvas), scripts ή άλλων τεχνολογιών, είναι δυνατός ο *"συνδυασμός των δεδομένων που συγκεντρώνονται από ένα συγκεκριμένο πρόγραμμα περιήγησης ή μια κινητή συσκευή με δεδομένα από άλλον υπολογιστή ή συσκευή που χρησιμοποιείται από τον ίδιο πελάτη"* με σκοπό την *"βελτιστοποίηση των υπηρεσιών μας και των ενεργειών marketing και για να διασφαλίσουμε ότι σας παρέχουμε μια συνεπή εμπειρία χρήστη"*. Όπως υπονοείται από τη διατύπωση *"αλλάζοντας τις ρυθμίσεις των cookies στη συσκευή σας μπορείτε να τροποποιήσετε και τις ρυθμίσεις της τεχνολογίας cross-device tracking"* η τεχνολογία αυτή είναι ενεργοποιημένη από προεπιλογή. Αυτό αντιτίθεται στην αρχή προστασίας των δεδομένων εξ' ορισμού.

5.4.3 Πολιτική Απορρήτου Εφαρμογής e-Food

Η πολιτική απορρήτου της εφαρμογής e-Food είναι ιδιαίτερα καλά δομημένη και κατανοητή. Είναι προσβάσιμη μέσω του site της εταιρείας και καταγράφει αναλυτικά τα διάφορα δεδομένα προσωπικού χαρακτήρα τα οποία συλλέγει και επεξεργάζεται η εταιρεία [39]. Αυτά είναι χωρισμένα σε κατηγορίες, με τις σημαντικότερες να είναι τα δεδομένα λογαριασμού (ονοματεπώνυμο, e-mail, αριθμός τηλεφώνου, χώρα, αναγνωριστικό χρήστη), τα δεδομένα παραγγελίας και παράδοσης (διεύθυνση και ημερομηνία παράδοσης, αναγνωριστικό παραγγελίας), τα δεδομένα τοποθεσίας (διεύθυνση, ταχυδρομικός κώδικας, πόλη, γεωγραφικές συντεταγμένες) και οι πληροφορίες της συσκευής (αναγνωριστικό συσκευής, διεύθυνση IP, λειτουργικό σύστημα).

Στο κυρίως σώμα της πολιτικής απορρήτου, περιγράφονται τα δεδομένα προσωπικού χαρακτήρα τα οποία καταχωρούνται και επεξεργάζονται σε κάθε φάση της αγοράς και παράδοσης του προϊόντος. Επίσης, παρατίθεται η νομική βάση για το κάθε στάδιο, καθώς και ο χρόνος διατήρησης των δεδομένων αυτών. Για παράδειγμα, για τη φάση τοποθέτησης προϊόντων στο καλάθι αγορών, η εταιρεία χρειάζεται πρόσβαση στα δεδομένα του λογαριασμού, στα δεδομένα της κατηγορίας "παραγγελία και παράδοση", καθώς και στα δεδομένα που αφορούν την συσκευή. Η αναγκαιότητα των δεδομένων των δύο πρώτων κατηγοριών είναι φανερή, ενώ τα δεδομένα της τελευταίας χρησιμοποιούνται για την υποστήριξη της δυνατότητας ο χρήστης να μπορεί να συνεχίσει την παραγγελία του ύστερα από το κλείσιμο της εφαρμογής. Ως νομική βάση για αυτή την επεξεργασία καταγράφεται η σύναψη και εκτέλεση σύμβασης. Τα δεδομένα προσωπικού χαρακτήρα διαγράφονται ύστερα από την οριστική υποβολή της παραγγελίας ή το άδειασμα του καλαθιού αγοράς.

Η εταιρεία δεσμεύεται στην κοινοποίηση των ελάχιστων απαιτούμενων δεδομένων προσωπικού χαρακτήρα σε τρίτους, με σκοπό την προετοιμασία και παράδοση της παραγγελίας. Για παράδειγμα, κατά τη φάση της παράδοσης, είναι απαραίτητο να κοινοποιηθούν στον διανομέα το ονοματεπώνυμο, η διεύθυνση παράδοσης και το τηλέφωνο του πελάτη. Συνεπώς φαίνεται να υιοθετείται η αρχή data minimisation.

Μέρος των δεδομένων προσωπικού χαρακτήρα χρησιμοποιούνται για την προβολή προσωποποιημένων διαφημίσεων. Τέτοια δεδομένα είναι αυτά που ανήκουν, μεταξύ άλλων, στις κατηγορίες “δεδομένα λογαριασμού”, “δεδομένα τοποθεσίας” και “πληροφορίες συσκευής”. Από αυτές τις πληροφορίες εξάγονται προβλέψεις σχετικά με τα δημογραφικά στοιχεία των χρηστών (ηλικία, φύλο) και τις καταναλωτικές προτιμήσεις τους, δεδομένα τα οποία χαρακτηρίζονται ως ψευδωνυμοποιημένα. Με βάση τη διατύπωση *“η εκ των προτέρων συγκατάθεση [...] ζητείται για να σας εμφανίσουμε τις δικτυακές στοχευμένες διαφημίσεις”* υποδηλώνει συμμόρφωση με την αρχή προστασίας δεδομένων εξ’ ορισμού.

Για την περίπτωση κοινοποίησης των δεδομένων προσωπικού χαρακτήρα εκτός ΕΟΧ, καταγράφονται διάφορες διασφαλίσεις για την προστασία των δεδομένων που εξάγονται, όπως αποφάσεις επάρκειας από την Ευρωπαϊκή Επιτροπή, τυποποιημένες συμβατικές ρήτρες ή άλλοι δεσμευτικοί κανόνες. Παρ’όλ’αυτά, δεν υπάρχει κάποια αναφορά στα δεδομένα τα οποία ενδέχεται να κοινοποιηθούν ή στους λόγους που θα οδηγούσαν στην κοινοποίηση.

Μαζί με την εφαρμογή Wolt, πρόκειται για την εφαρμογή με την εκτενέστερη καταγραφή των ιχνηλατών οι οποίοι χρησιμοποιούνται. Η περιγραφή αυτή είναι προσπελάσιμη, μέσω της ξεχωριστής πολιτικής cookies. Η καταγραφή αυτή είναι σε μεγάλο βαθμό σύμφωνη με τα πειραματικά αποτελέσματα της στατικής και δυναμικής ανάλυσης που παρατέθηκαν στην Ενότητα 5.3.2.

5.4.4 Πολιτική Απορρήτου Εφαρμογής Germanos

Η πολιτική απορρήτου της εφαρμογής Germanos παρέχεται ως αρχείο .pdf στο site της εταιρείας [40]. Τα δεδομένα προσωπικού χαρακτήρα τα οποία συλλέγονται και υπόκεινται σε επεξεργασία, χωρίζονται σε κατηγορίες ανάλογα με τις ενέργειες που επιθυμεί να πραγματοποιήσει ο χρήστης. Για παράδειγμα, για τη συμμετοχή του χρήστη στο πρόγραμμα πιστότητας, απαιτούνται δεδομένα όπως το ονοματεπώνυμο του χρήστη και ο αριθμός κινητής τηλεφωνίας. Επίσης, ειδικά για τη χρήση της εφαρμογής, καταγράφονται η ώρα και η διάρκεια της σύνδεσης, καθώς και το αναγνωριστικό της συσκευής, ο κατασκευαστής, το μοντέλο και η έκδοση της εφαρμογής. Ως νομική βάση για την συλλογή και επεξεργασία των δεδομένων αυτών δηλώνεται η εκτέλεση της σύμβασης μεταξύ της εταιρείας και του πελάτη.

Η εφαρμογή της εταιρείας είναι η μόνη από όσες εξετάστηκαν η οποία αναφέρει τα permissions τα οποία χρειάζεται να εγκρίνει ο χρήστης προκειμένου αυτή να εγκατασταθεί και να λειτουργήσει. Στη λίστα των permissions καταγράφονται τα δεδομένα τοποθεσίας (GPS) με σκοπό την ενημέρωση του χρήστη για κοντινά καταστήματα της εταιρείας, το δικαίωμα λήψης SMS για την υλοποίηση 2-factor authentication, το δικαίωμα πρόσβασης στην κάμερα για σάρωση κωδικών QR, καθώς και στους αποθηκευμένους λογαριασμούς της συσκευής για την υποστήριξη αυτόματου login στην εφαρμογή. Τα permissions αυτά εντοπίστηκαν και κατά τη στατική ανάλυση μέσω του Exodus. Παρ’όλ’αυτά, εντοπίστηκαν και άλλα, όπως η πρόσβαση στο Bluetooth και στον χώρο εξωτερικής αποθήκευσης (κάτι που αποθαρρύνεται από τη Google) [34], τα οποία δεν καταγράφονταν στην πολιτική απορρήτου.

Τα δεδομένα προσωπικού χαρακτήρα, όπως αναφέρεται στο κείμενο της πολιτικής απορρήτου, διατηρούνται για όσο χρονικό διάστημα παραμένει ενεργός ο λογαριασμός του χρήστη. Όμως δεν διευκρινίζεται τι ισχύει στην περίπτωση κατά την οποία ο

χρήστης δεν χρησιμοποιήσει την εφαρμογή για μεγάλο χρονικό διάστημα, οπότε και ο λογαριασμός συνεχίζει να παραμένει ενεργός.

Η εταιρεία, επίσης, υποστηρίζει τη δημιουργία προσωποποιημένων προτάσεων αγοράς. Για αυτή τη δυνατότητα, η εταιρεία ζητά τη συγκατάθεση του χρήστη για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως το ονοματεπώνυμο, το e-mail και ο αριθμός τηλεφώνου του, καθώς και πληροφορίες για το ιστορικό αγορών του (κωδικοί προϊόντων, κόστος αγοράς, μέθοδος πληρωμής, κατάστημα αγοράς). Παρ'όλ'αυτά, δεν αποσαφηνίζεται αν η επεξεργασία θα γίνει από την ίδια την εταιρεία ή από τρίτο μέρος.

Όσον αφορά την αποστολή δεδομένων προσωπικού χαρακτήρα σε τρίτους, ως μοναδική περίπτωση τέτοιας εταιρείας καταγράφεται η Niobium Labs, η οποία έχει αναλάβει την ανάπτυξη και υποστήριξη της εφαρμογής της εταιρείας. Αναφορικά με τη διαχείριση των δεδομένων προσωπικού χαρακτήρα, η εταιρεία Γερμανός αποτελεί την υπεύθυνη επεξεργασίας, ενώ η Niobium αποτελεί την εκτελούσα την επεξεργασία. Με βάση την πολιτική απορρήτου, η εταιρεία *"δεν δημοσιοποιεί τα προσωπικά δεδομένα σε τρίτους με εξαίρεση τις περιπτώσεις που η κοινοποίηση/διαβίβαση τους επιβάλλεται από την ισχύουσα νομοθεσία"*. Παρά την αναφορά για επικοινωνία μόνο με τη Niobium, με βάση τη δυναμική ανάλυση ανιχνεύθηκε επιπλέον επικοινωνία με την CrashLytics (Google) και το Facebook.

Παρότι η εταιρεία δηλώνει ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πραγματοποιείται εντός Ελλάδας και Ευρωπαϊκής Ένωσης, στη δήλωση απορρήτου υπάρχει η αναφορά πως στο ενδεχόμενο συνεργασίας με εταιρείες εκτός Ευρωπαϊκής Ένωσης *"αυτές θα επεξεργαστούν τα δεδομένα σας, μόνο μετά από εντολή μας και σε περίπτωση που υπάρχει απόφαση επάρκειας της Ευρωπαϊκής Επιτροπής ή εάν συμφωνηθούν οι κατάλληλες ρήτρες που διασφαλίζουν υψηλό επίπεδο ασφάλειας σε σχέση με την επεξεργασία των προσωπικών σας δεδομένων"*.

5.4.5 Πολιτική Απορρήτου Εφαρμογής Nike

Η πολιτική απορρήτου της Nike αποτελεί κείμενο το οποίο καλύπτει οποιαδήποτε αλληλεπίδραση με την εταιρεία: είτε αφορά επίσκεψη στο ηλεκτρονικό ή φυσικό της κατάστημα, είτε τη χρήση οποιασδήποτε εφαρμογής της εταιρείας [41]. Αυτό έχει σαν αποτέλεσμα το κείμενο να είναι ιδιαίτερα γενικό. Όλοι αυτοί οι τρόποι με τους οποίους ο χρήστης μπορεί να αλληλεπιδράσει με την εταιρεία, περιγράφονται με τον όρο "πλατφόρμες".

Υπάρχουν διάφορα δεδομένα προσωπικού χαρακτήρα, τα οποία χειρίζεται η εταιρεία, όπως το ονοματεπώνυμο του χρήστη, η διεύθυνση, το e-mail, ο αριθμός τηλεφώνου, το φύλο και η ημερομηνία γέννησης. Επίσης, ενδέχεται να ζητηθούν πληροφορίες για τα σωματικά χαρακτηριστικά του χρήστη, όπως το ύψος και το βάρος. Στην ίδια πολιτική απορρήτου, αναφέρεται επίσης η καταγραφή δεδομένων από αισθητήρα καρδιακών παλμών και από το επιταχυνσιόμετρο του κινητού. Η αναφορά των συγκεκριμένων δεδομένων προσωπικού χαρακτήρα, καθώς δεν σχετίζεται με της ανάγκες μιας εφαρμογής ηλεκτρονικών αγορών, δυσκολεύει τον ακριβή προσδιορισμό των δεδομένων τα οποία όντως συλλέγονται από μια τέτοια εφαρμογή. Επίσης, τα permissions τα οποία εντοπίστηκαν κατά τη στατική ανάλυση, δεν δίνουν τη δυνατότητα στη συγκεκριμένη εφαρμογή να προχωρήσει σε τέτοιου είδους συλλογές δεδομένων.

Επιπλέον, στην πολιτική απορρήτου καταγράφονται διάφορες παράμετροι που αποστέλλονται στην εταιρεία, αυτόματα με τη χρήση της πλατφόρμας (είτε μέσω

επικοινωνίας με χρήση φυλλομετρητή είτε μέσω της χρήσης οποιαδήποτε εφαρμογής της εταιρείας). Ενδεικτικά, μερικές τέτοιες παράμετροι, είναι το ID της συσκευής, η κατάσταση κλήσεων, η κατάσταση του δικτύου, διάφορες πληροφορίες για το χώρο αποθήκευσης και τη μπαταρία, η διεύθυνση IP, το λειτουργικό σύστημα και οι ρυθμίσεις συστήματος, η χώρα και η ζώνη ώρας, καθώς και διάφορες πληροφορίες για τον browser.

Τα δεδομένα αυτά χρησιμοποιούνται για διάφορους σκοπούς. Μεταξύ αυτών, αναφέρονται η παροχή των υπηρεσιών της πλατφόρμας, όπως είναι η αγορά ενός προϊόντος, η προβολή εξατομικευμένων διαφημίσεων, καθώς και η υλοποίηση analytics.

Στην πολιτική απορρήτου, καταγράφεται επίσης η νομική βάση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, για διάφορα σενάρια. Ενδεικτικά, κατά την αφορά ενός προϊόντος, η νομική βάση της επεξεργασίας είναι η εκτέλεση της σύμβασης με τον πελάτη. Επίσης, ως νομική βάση για την επεξεργασία δεδομένων σχετικά με την αποδοτικότητα των διαφημιστικών εκστρατειών και άλλων προωθητικών πρωτοβουλιών, αναφέρεται το έννομο συμφέρον της εταιρείας. Όμως παραμένει ασαφές το ποια ακριβώς δεδομένα είναι αυτά, καθώς και αν σε αυτά συμπεριλαμβάνονται και δεδομένα προσωπικού χαρακτήρα του χρήστη.

Επίσης, περιγράφονται τρίτες οντότητες, στις οποίες πραγματοποιείται κοινοποίηση δεδομένων προσωπικού χαρακτήρα από την εταιρεία. Τέτοιες περιπτώσεις είναι, μεταξύ άλλων, οντότητες έρευνας και ανάλυσης, οντότητες προώθησης προϊόντων ή πάροχοι εξατομικευμένων διαφημίσεων. Από τη διατύπωση της συγκεκριμένης παραγράφου, δεν γίνεται ξεκάθαρο το ποια δεδομένα προσωπικού χαρακτήρα κοινοποιούνται και σε ποιους τρίτους. Επίσης, μόνο σε δύο από τις επτά περιπτώσεις τρίτων οντοτήτων αναφέρεται η απαίτηση για συναίνεση του χρήστη στην κοινοποίηση. Τέλος, δεν φαίνεται να έχει υιοθετηθεί η αρχή της προστασίας δεδομένων εξ' ορισμού στην περίπτωση της μιας από αυτές, καθώς με βάση τη διατύπωση *"You may opt-out of personalized advertising and custom audiences by using the relevant settings in our Platform"*, υπονοείται ότι η κοινοποίηση δεδομένων προσωπικού χαρακτήρα για την περίπτωση αυτή είναι ενεργοποιημένη από προεπιλογή.

Όσον αφορά την εξαγωγή των δεδομένων προσωπικού χαρακτήρα των χρηστών εκτός ΕΟΧ, η πολιτική απορρήτου αναφέρει ότι λαμβάνονται μέτρα μέσω της υιοθέτησης ρητρών και κανόνων για την επαρκή προστασία των δεδομένων αυτών. Όπως αναφέρεται στην πολιτική, η εταιρεία αποθηκεύει και ενδεχομένως επεξεργάζεται τα δεδομένα αυτά στις ΗΠΑ και άλλες χώρες, χωρίς όμως να κατονομάζονται αυτές.

Τέλος, όσον αφορά τη χρονική περίοδο διατήρησης των δεδομένων προσωπικού χαρακτήρα, όπως αναφέρεται στην πολιτική απορρήτου, τα δεδομένα αυτά διατηρούνται για όσο χρόνο χρειαστεί για τον εκάστοτε σκοπό για τον οποίο συλλέχθηκαν, χωρίς να καθορίζεται ένα συγκεκριμένο χρονικό παράθυρο (κάτι που δεν είναι σύμφωνο με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων).

5.4.6 Πολιτική Απορρήτου Εφαρμογής Pull & Bear

Στην περίπτωση της εφαρμογής Pull & Bear, η πολιτική απορρήτου μοιάζει με την αντίστοιχη της Nike, με την έννοια ότι αποτελεί ένα κείμενο το οποίο καλύπτει τόσο την εφαρμογή όσο και την επίσκεψη μέσω φυλλομετρητή στην ιστοσελίδα της εταιρείας ή την επίσκεψη σε ένα φυσικό κατάστημα [42]. Ως υπεύθυνοι επεξεργασίας, δηλώνονται

από κοινού η εταιρεία Pull & Bear Espana, όσο και η ITX Hellas (η οποία δραστηριοποιείται στην πώληση προϊόντων της Pull & Bear στην Ελλάδα).

Στην πολιτική απορρήτου, παρατίθενται κατηγορίες δεδομένων προσωπικού χαρακτήρα τα οποία συλλέγονται και επεξεργάζονται από την εταιρεία. Αυτά, ανήκουν σε κατηγορίες όπως τα στοιχεία ταυτότητας (ονοματεπώνυμο, χώρα, στοιχεία επικοινωνίας, φωτογραφία προφίλ), τα δεδομένα σύνδεσης (τοποθεσία, αναγνωριστικό συσκευής) ή άλλες πληροφορίες για τις προτιμήσεις του χρήστη. Στην πολιτική απορρήτου δεν αποσαφηνίζεται το ποια από αυτά τα δεδομένα είναι απαραίτητα ή προαιρετικά για τη λειτουργία της εφαρμογής.

Επίσης, στην πολιτική απορρήτου παρατίθεται πίνακας με διάφορους σκοπούς για τους οποίους η εταιρεία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα. Ενδεικτικά, αναφέρονται η εγγραφή στην πλατφόρμα, η πραγματοποίηση της αγοράς ενός προϊόντος, λόγοι marketing και ανάλυσης ποιότητας υπηρεσιών. Ειδικά στην περίπτωση του marketing, ύστερα από συγκατάθεση του χρήστη, πραγματοποιείται επεξεργασία των δεδομένων προσωπικού χαρακτήρα με σκοπό την κατάρτιση προφίλ χρήστη, με σκοπό την αποστολή προσωποποιημένου ενημερωτικού δελτίου. Παρ'όλ'αυτά, δεν υπάρχει κάποια αναφορά σε συγκεκριμένα δεδομένα προσωπικού χαρακτήρα, τα οποία υπόκεινται σε επεξεργασία για τον εκάστοτε σκοπό, και κυρίως για τη δημιουργία προφίλ χρήστη.

Αντίθετα, περιγράφεται η νομική βάση για την κάθε επεξεργασία. Για παράδειγμα, στην περίπτωση της πραγματοποίησης αγοράς ενός προϊόντος, ως νομική βάση καταγράφεται η εκτέλεση της σύμβασης αγοράς. Επίσης, στην περίπτωση που ο χρήστης επιθυμεί την αποθήκευση των δεδομένων πληρωμής και για μελλοντικές αγορές, ως νομική βάση αναφέρεται η συναίνεση του χρήστη.

Το χρονικό διάστημα διατήρηση των δεδομένων αυτών, δεν καθορίζεται με σαφήνεια. Στις περισσότερες περιπτώσεις υπάρχει ο γενικός χαρακτηρισμός *"για όσο χρονικό διάστημα απαιτείται"*. Εξαίρεση αποτελούν η συμμετοχή σε προωθητικές ενέργειες, όπου ορίζεται χρονικό διάστημα 6 μηνών μετά τη λήξη της ενέργειας, καθώς και προφανώς η περίπτωση διαχείρισης της εγγραφής του χρήστη, όπου τα δεδομένα προσωπικού χαρακτήρα παραμένουν στη διάθεση της εταιρείας, μέχρι ο χρήστης να επιλέξει τη διαγραφή του προφίλ του.

Όσον αφορά την κοινοποίηση των δεδομένων προσωπικού χαρακτήρα σε τρίτους, δεν υπάρχει λεπτομερής καταγραφή των δεδομένων που ενδέχεται να κοινοποιηθούν. Επίσης, οι "τρίτοι" περιγράφονται γενικά, ως χρηματοοικονομικοί οργανισμοί, πάροχοι υπηρεσιών τεχνολογίας και ανάλυσης ή πάροχοι υπηρεσιών και συνεργάτες που σχετίζονται με το μάρκετινγκ και τη διαφήμιση.

Στην πολιτική cookies, αναφέρονται πάντως δύο περιπτώσεις τρίτων domains, τα οποία αποκτούν δεδομένα προσωπικού χαρακτήρα των χρηστών της εφαρμογής: αυτά είναι η Network Advertising Initiative και η Google Analytics. Οι πολιτικές απορρήτου των Pull & Bear και Zara είναι από τις λίγες που κατονομάζουν κάποια από τα τρίτα μέρη στα οποία κοινοποιούνται δεδομένα.

Στην περίπτωση διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτες εταιρείες εκτός ΕΟΧ, αναφέρεται ότι *"θα διαβιβάζουμε τα δεδομένα σας με επαρκείς εγγυήσεις και διατηρώντας πάντα την ασφάλεια των δεδομένων σας, χρησιμοποιώντας τα πιο κατάλληλα διεθνή εργαλεία μεταφοράς δεδομένων, για παράδειγμα τις Τυπικές Συμβατικές Ρήτρες και τυχόν σχετικά συμπληρωματικά μέτρα"*. Όπως συμβαίνει σχεδόν σε όλες τις πολιτικές απορρήτου, δεν υπάρχει περεταίρω πληροφόρηση του χρήστη για τις ρήτρες αυτές.

Τέλος, υπάρχουν διάφορα σημεία στην πολιτική απορρήτου, στα οποία υπονοείται ότι δεν έχει υιοθετηθεί πλήρως η αρχή προστασίας δεδομένων εξ' ορισμού. Τέτοια παραδείγματα είναι οι διατυπώσεις *"εάν εισέλθετε στην Πλατφόρμα μας, σας ενημερώνουμε ότι θα επεξεργαστούμε τα δεδομένα περιήγησής σας για σκοπούς ανάλυσης και στατιστικούς σκοπούς [...]"* και *"εάν δεν θέλετε να στέλνουμε πληροφορίες σε τρίτους για να σας εμφανίζουν διαφημίσεις, μπορείτε να το κάνετε με διάφορα μέσα [...]"*, οι οποίες υποδηλώνουν ότι τα analytics και οι κοινοποιήσεις σε τρίτα μέρη είναι από προεπιλογή ενεργοποιημένες.

5.4.7 Πολιτική Απορρήτου Εφαρμογής Wolt

Η πολιτική απορρήτου της εφαρμογής Wolt είναι προσπελάσιμη μέσω του site της εταιρείας [43]. Στην αρχή της πολιτικής απορρήτου, διευκρινίζεται πως υπεύθυνοι επεξεργασίας είναι από κοινού η Wolt Enterprises Oy (με έδρα το Σαν Φρανσίσκο) και η επιμέρους τοπική εταιρεία του ομίλου σε κάθε χώρα που δραστηριοποιείται η Wolt (στην Ελλάδα αυτή η εταιρεία είναι η Wolt Technologies Greece).

Στην ενότητα των δεδομένων χρήστη, περιγράφονται τα δεδομένα προσωπικού χαρακτήρα, τα οποία συλλέγει και επεξεργάζεται η εταιρεία. Συγκεκριμένα, απαραίτητα τέτοια δεδομένα, τα οποία ζητούνται από τον χρήστη κατά την εγγραφή του στην εφαρμογή, είναι μεταξύ άλλων το ονοματεπώνυμο, ο αριθμός τηλεφώνου και το e-mail. Άλλες πληροφορίες, τις οποίες μπορεί να κοινοποιήσει ο χρήστης προαιρετικά, είναι η φωτογραφία του, τα δεδομένα τοποθεσίας, καθώς και η ηλικία (απαραίτητη πληροφορία σε περίπτωση παραγγελίας προϊόντος η χρήση του οποίου διέπεται από ηλικιακό περιορισμό).

Στην περίπτωση κατά την οποία ο χρήστης συνδεθεί στον λογαριασμό Wolt μέσω των διαπιστευτηρίων του Facebook, η Meta κοινοποιεί στη Wolt την φωτογραφία προφίλ του χρήστη στο Facebook, ένα υποσύνολο των φίλων του χρήστη, καθώς και το Facebook ID. Δεν υπάρχει κάποια αναφορά σε δεδομένα προσωπικού χαρακτήρα, τα οποία ενδέχεται να κοινοποιούνται από τη Wolt στη Meta. Σε αυτή την περίπτωση, υπεύθυνος επεξεργασίας είναι από κοινού η Wolt και η Meta.

Επίσης, στην πολιτική απορρήτου καταγράφονται διάφορα δεδομένα προσωπικού χαρακτήρα, τα οποία αφορούν τη συσκευή του χρήστη και συλλέγονται αυτόματα. Ενδεικτικά, μερικά από αυτά είναι διάφορες πληροφορίες που περιγράφουν τη συσκευή και την εφαρμογή Wolt, πληροφορίες για τον ISP, τη διεύθυνση IP, αναγνωριστικά που παρέχονται από τη συσκευή, το αναγνωριστικό διαφήμισης της συσκευής, η χώρα καθώς και η ζώνη ώρας το χρήστη, καθώς και μια εκτίμηση της τοποθεσίας βάσει της διεύθυνσης IP. Παρότι η λίστα αυτή είναι αρκετά εκτενής, υπάρχουν σημεία τα οποία δεν διευκρινίζονται με ακρίβεια, όπως ποιες είναι οι *"πληροφορίες που περιγράφουν τη συσκευή"* (καθώς ο ενδεδειγμένος τρόπος προσδιορισμού του χρήστη, ο GAID, αποτελεί το "το αναγνωριστικό διαφήμισης της συσκευής").

Μια ακόμα αναφορά στην πολιτική απορρήτου, αφορά τη χρήση ψευδωνυμοποιημένων αναγνωριστικών με σκοπό την *"παρακολούθηση και πρόβλεψη της χρήσης και των προτιμήσεων των εφαρμογών και υπηρεσιών"*. Επίσης, αναφέρεται η χρήση 3rd party cookies, για διαφημιστικούς λόγους. Παρότι δεν δίνονται επιπλέον πληροφορίες για το ποια είναι τα ψευδωνυμοποιημένα αναγνωριστικά, στην πολιτική απορρήτου δίνονται γενικές οδηγίες για την απενεργοποίηση της χρήσης τους. Επίσης, υπάρχει αναλυτική καταγραφή των τρίτων μερών τα οποία συνεργάζονται με τη Wolt. Η λίστα αυτή συμπίπτει σε πολλά σημεία με τη δυναμική ανάλυση που έχει προηγηθεί, ενώ η

απουσία μερικών μπορεί να ερμηνευτεί, καθώς η ίδια η εταιρεία επισημαίνει ότι *"δεν είναι απαραίτητο να χρησιμοποιούνται όλοι οι παραπάνω πωλητές ανά πάσα στιγμή ή σε όλες τις περιοχές της αγοράς"*.

Σε ξεχωριστή ενότητα της πολιτικής απορρήτου, καταγράφεται η νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Ενδεικτικά, αναφέρεται η εκπλήρωση των συμβατικών υποχρεώσεων της εταιρείας προς τους χρήστες (όπως κατά τη διαχείριση και παράδοση της παραγγελίας) ή η συγκατάθεση του χρήστη (όπως στην περίπτωση της προβολής διαφημίσεων και άλλων ενεργειών marketing).

Παρότι τα δεδομένα προσωπικού χαρακτήρα αποθηκεύονται κυρίως εντός ΕΟΧ, όπως αναφέρεται στην πολιτική απορρήτου, κατά την περίπτωση διαβίβασης τέτοιων δεδομένων εκτός ΕΟΧ τα δεδομένα αυτά προστατεύονται μέσω *"μιας σειράς συμφωνιών με τους παρόχους υπηρεσιών μας βάσει των Τυποποιημένων Συμβατικών Ρητρών ή μέσω άλλων κατάλληλων διασφαλίσεων"*. Παρότι δεν διευκρινίζεται το ποια δεδομένα παραμένουν εντός ΕΟΧ και ποια ενδέχεται να διαβιβαστούν, η εφαρμογή είναι η μόνη που παρέχει σύνδεσμο για την ανάγνωση των ρητρών αυτών από την επίσημη ιστοσελίδα της Ευρωπαϊκής Επιτροπής.

Παρόμοια με την πολιτική απορρήτου της εφαρμογής e-Food, έτσι και στην περίπτωση της Wolt αναφέρονται περιπτώσεις κοινοποίησης δεδομένων προσωπικού χαρακτήρα σε τρίτους, για τις ανάγκες προετοιμασίας και παράδοσης της παραγγελίας στον πελάτη. Συγκεκριμένα, αναφέρεται ότι πραγματοποιείται κοινοποίηση του ονοματεπωνύμου και του αριθμού τηλεφώνου στο συνεργάτη που προετοιμάζει την παραγγελία, ενώ στην περίπτωση του διανομέα κοινοποιείται επίσης η διεύθυνση του πελάτη. Παρ'όλ'αυτά, όπως αναφέρεται στη δήλωση απορρήτου, *"όταν ο Συνεργάτης επεξεργάζεται τα εν λόγω στοιχεία [...], ο Συνεργάτης είναι ανεξάρτητος υπεύθυνος επεξεργασίας των Προσωπικών Δεδομένων και υπεύθυνος για τη νομιμότητα των πράξεων επεξεργασίας του"*. Αυτό σημαίνει ότι στην περίπτωση της εφαρμογής Wolt, η εταιρεία δεν φέρει νομική ευθύνη στο ενδεχόμενο καταχρηστικής εκμετάλλευσης των δεδομένων προσωπικού χαρακτήρα από τον συνεργάτη (κατάστημα αγοράς, διανομέας).

Τέλος, δεν καθορίζεται με σαφήνεια η μέγιστη περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα. Συγκεκριμένα, στο κείμενο της πολιτικής απορρήτου υπάρχει η διατύπωση ότι *"Η περίοδος αποθήκευσης εξαρτάται από τη φύση των πληροφοριών και τους σκοπούς της επεξεργασίας. Επομένως, η μέγιστη περίοδος μπορεί να ποικίλει ανάλογα με τη χρήση"*. Επίσης, για την περίπτωση κατά την οποία ο χρήστης διαγράψει τον λογαριασμό του, η εταιρεία τον πληροφορεί ότι *"τα προσωπικά δεδομένα μπορεί να αποθηκευτούν μόνο εφόσον η επεξεργασία αυτή απαιτείται από τον νόμο ή είναι εύλογα αναγκαία για τις νομικές μας υποχρεώσεις ή τα νόμιμα συμφέροντά μας"*. Μέσω της διατύπωσης αυτής, δεν είναι σαφές στον χρήστη το χρονικό διάστημα για το οποίο η εταιρεία διατηρεί τα δεδομένα προσωπικού του χαρακτήρα ύστερα από τη χρήση της εφαρμογής για την πραγματοποίηση μιας παραγγελίας ή ακόμα και ύστερα από τη διαγραφή του λογαριασμού του.

5.4.8 Πολιτική Απορρήτου Εφαρμογής Zara

Η πολιτική απορρήτου της εφαρμογής Zara είναι πρακτικά ίδια με την αντίστοιχη της εφαρμογής Pull & Bear [44]. Και οι δύο Ισπανικές εταιρείες ανήκουν στον ίδιο όμιλο (Inditex) και εκπροσωπούνται στην Ελλάδα από την ITX Hellas. Συνεπώς, και στην

περίπτωση της εφαρμογής Zara ισχύουν οι ίδιες παρατηρήσεις με αυτές που αφορούν την εφαρμογή Pull & Bear.

6. ΣΥΜΠΕΡΑΣΜΑΤΑ

6.1 Σύνοψη – Συμπεράσματα

Στο πλαίσιο της εργασίας αυτής εξετάστηκε ο τρόπος εκτέλεσης των εφαρμογών στο λειτουργικό σύστημα Android. Μέσω της υποστήριξης του μοντέλου των permissions, μια εφαρμογή μπορεί να υποστηρίξει εκτεταμένες λειτουργίες. Το αντιστάθμισμα για αυτά τα οφέλη, είναι η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, η συλλογή και επεξεργασία των οποίων ενδέχεται να επηρεάσουν δυσμενώς τον χρήστη. Αυτή η απειλή της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα, προστατεύεται μέσω του Γενικού Κανονισμού για την Προστασία των Δεδομένων.

Η εργασία επικεντρώθηκε στις εφαρμογές ηλεκτρονικών αγορών μέσω διαδικτύου, μέσω των οποίων μπορούν να πραγματοποιηθούν αγορές προϊόντων και υπηρεσιών σε εταιρείες οι οποίες δραστηριοποιούνται στην Ελλάδα. Για τις ανάγκες των προσομοιώσεων, επελέγησαν εφαρμογές από οκτώ δημοφιλείς εταιρείες, οι οποίες καλύπτουν ευρύ φάσμα προϊόντων και υπηρεσιών: από πολυκαταστήματα και καταστήματα ειδών ρουχισμού μέχρι την κράτηση τουριστικών καταλυμάτων και αγορές ειδών τεχνολογίας και παράδοσης ειδών διατροφής. Ένα αξιοσημείωτο πρώτο συμπέρασμα που προέκυψε κατά την αρχική επιλογή των εταιρειών, είναι η απουσία εφαρμογών για κινητά από πολλές μεγάλες εταιρείες που δραστηριοποιούνται στον χώρο της τεχνολογίας στην Ελλάδα.

Όσον αφορά τα ζητούμενα permissions, μέσω της στατικής ανάλυσης με χρήση του Exodus, παρατηρήθηκε γενικά μεγάλος αριθμός από ζητούμενα dangerous permissions. Τα permissions τα οποία χρειαζόταν η κάθε εφαρμογή κυμαίνονταν από 9 έως 23, με τις περισσότερες εφαρμογές να χρειάζονται περίπου 20 permissions. Επίσης, το ποσοστό των dangerous permissions ήταν υψηλό, σε όλες τις εφαρμογές. Ως επί του συνόλου των permissions, τα dangerous αποτελούσαν το 33,3 – 47,8 %. Χαρακτηριστικό είναι ότι το μικρότερο ποσοστό από dangerous permissions καταγράφεται σε εφαρμογές οι οποίες ήδη ζητούν λίγα permissions. Ισοδύναμα, εφαρμογές οι οποίες ήδη ζητούν πολλά permissions, πολλά από αυτά είναι dangerous.

Εξετάζοντας από κοντά τα dangerous permissions των εφαρμογών, παρατηρείται ότι κάποια από αυτά είναι δικαιολογημένα, προκειμένου οι εφαρμογές να εμπλουτίσουν τη λειτουργικότητά τους σε βαθμό που να διευκολύνεται ο χρήστης. Ένα παράδειγμα είναι η αίτηση για χρήση του δέκτη GPS, προκειμένου να μπορούν να πληροφορήσουν τον χρήστη για κοντινά φυσικά καταστήματα. Παρ'όλ'αυτά, υπάρχουν περιπτώσεις στις οποίες είναι δύσκολο να ερμηνευθεί η αναγκαιότητα συγκεκριμένων permissions. Υπάρχει εφαρμογή η οποία ζητά πρόσβαση στην τοποθεσία στην οποία λήφθηκαν φωτογραφίες του χρήστη, ενώ άλλες δύο ζητούν πρόσβαση στο μικρόφωνο της συσκευής. Επίσης, οι μισές εφαρμογές ζητούν το permission WRITE_EXTERNAL_STORAGE, η χρήση του οποίου αποθαρρύνεται από τη Google, ήδη από την έκδοση Android 10.

Ένα άλλο χαρακτηριστικό για το οποίο μπορούν να εξαχθούν χρήσιμα συμπεράσματα, είναι ο βαθμός ταύτισης των permissions των εφαρμογών. Από τη μια υπάρχουν εφαρμογές οι οποίες ανήκουν στον ίδιο όμιλο και χρησιμοποιούν σχεδόν τα ίδια permissions. Από την άλλη, παρότι εξετάζονται εφαρμογές με παρόμοια λειτουργία (αναζήτηση προϊόντων ή υπηρεσιών και αγορά τους), παρατηρείται σημαντική

απόκλιση στα ζητούμενα permissions. Αυτό το χαρακτηριστικό ενδέχεται να συμβάλλει στην εμφάνιση intra-library collusion

Τέλος, αξίζει να σημειωθεί ότι, γενικά, η έγκριση πολλών permissions δεν είναι εξ'ορισμού κακή, καθώς μπορεί να βελτιώνει την λειτουργικότητα της εφαρμογής. Όμως, είναι απαραίτητη η σαφής και κατανοητή πληροφόρηση του χρήστη, καθώς και η τήρηση της αρχής προστασίας των δεδομένων εξ' ορισμού.

Στη δεύτερη φάση των προσομοιώσεων, εξετάστηκαν οι ιχνηλάτες που είναι ενσωματωμένοι στον κώδικα των εφαρμογών, μέσω της στατικής ανάλυσης του Exodus, ή αυτοί με τους οποίους εντοπίστηκε επικοινωνία μέσω της δυναμικής ανάλυσης του TC Slim. Όπως προκύπτει και από τις δύο αναλύσεις, όλες οι εφαρμογές συμπεριλαμβάνουν τουλάχιστον έναν ιχνηλάτη. Ειδικά για την εφαρμογή της εταιρείας Γερμανός, δεν ήταν δυνατή η ανάλυση των ιχνηλατών μέσω του Exodus, συνεπώς η αντίστοιχη στήλη της στατικής ανάλυσης παραμένει κενή. Από τα αποτελέσματα, γίνεται φανερό ότι οι ιχνηλάτες των Google (Firebase Analytics) και Meta (Facebook) χρησιμοποιούνται σχεδόν από όλες τις εφαρμογές που εξετάσθηκαν.

Επίσης, παρατηρούνται διαφοροποιήσεις στους εντοπισμένους ιχνηλάτες μέσω της στατικής και της δυναμικής ανάλυσης. Αυτό οφείλεται στον τρόπο εντοπισμού τους: στη στατική ανάλυση ελέγχεται ο κώδικας της εφαρμογής για τον εντοπισμό ιχνηλατών οι οποίοι μπορεί και να μην προσπελαστούν ποτέ, ενώ στη δυναμική ανάλυση καταγράφονται ιχνηλάτες που προσπελαύνονται το χρονικό διάστημα της εξέτασης. Σε αυτούς, συμπεριλαμβάνονται και ιχνηλάτες οι οποίοι προσπελαύνονται ύστερα από dynamic loading κατά τη φάση της εκτέλεσης της εφαρμογής (γι αυτό δεν εντοπίζονται κατά τη στατική ανάλυση).

Τέλος, η συνδυασμένη έγκριση dangerous permissions με την παρουσία ιχνηλατών σε μια εφαρμογή, ενδεχομένως αυξάνει την απειλή για την ιδιωτικότητα και τα δεδομένα προσωπικού χαρακτήρα του χρήστη. Αυτό, διότι η εφαρμογή αποκτά προσβάσεις και είναι γνωστό ότι μεταδίδει δεδομένα σε τρίτους. Επίσης, λόγω του intra-library collusion, ακόμα και διαφορετικές εφαρμογές που όμως αποστέλλουν δεδομένα στον ίδιο ιχνηλάτη και εκτελούνται με διαφορετικά permissions, ενδέχεται να αποτελούν ακόμα μεγαλύτερη απειλή για το απόρρητο του χρήστη.

Τέλος, από την εξέταση των πολιτικών απορρήτου εξάγονται πολλά συμπεράσματα.

Σε όλες τις πολιτικές απορρήτου καταγράφονται τα δεδομένα προσωπικού χαρακτήρα τα οποία καλείται να παραχωρήσει ο χρήστης μέσω φορμών συμπλήρωσης. Ειδικά στην περίπτωση της εταιρείας e-Food, η λίστα αυτή είναι ιδιαίτερα αναλυτική. Παρόλ'αυτά, μόνο στις περιπτώσεις των AB, Wolt και εν μέρει και στην περίπτωση της Nike καταγράφονται οι παράμετροι που συλλέγονται αυτόματα από την εφαρμογή, κατά την εκτέλεσή της.

Ο σκοπός της επεξεργασίας των δεδομένων είναι ένα πεδίο στο οποίο παρατηρούνται σημαντικές διαφοροποιήσεις. Σε κάποιες περιπτώσεις εφαρμογών, όπως στις εταιρείες AB, e-Food, Germanos και Wolt περιγράφονται αναλυτικά τα δεδομένα τα οποία υφίστανται επεξεργασία, καθώς και ο σκοπός της επεξεργασίας αυτής. Αντίθετα, στις πολιτικές απορρήτου των άλλων εφαρμογών, δεν υπάρχει τόσο σαφής αντιστοίχιση του σκοπού επεξεργασίας με τα δεδομένα που υφίστανται την επεξεργασία. Σε κάθε περίπτωση, καταγράφεται η νομική βάση (είτε για την κάθε επεξεργασία είτε για κάθε κατηγορία επεξεργασίας).

Ένα σημείο το οποίο παραμένει επίσης ιδιαίτερα θολό, είναι το χρονικό διάστημα διατήρησης των δεδομένων προσωπικού χαρακτήρα του χρήστη σε κάθε εταιρεία. Στην εφαρμογή της εταιρείας AB καθορίζονται τα χρονικά παράθυρα, ενώ στην εφαρμογή Germanos αναφέρεται ότι τα δεδομένα θα παραμείνουν αποθηκευμένα για όσο παραμένει ενεργός ο λογαριασμό του χρήστη. Οι πολιτικές απορρήτου των Nike, Pull & Bear και Zara, σχεδόν για όλα τα δεδομένα προσωπικού χαρακτήρα αναφέρουν “για όσο χρειαστεί”, ενώ στις πολιτικές απορρήτου των άλλων εταιρειών δεν υπάρχει καμία αναφορά στο συγκεκριμένο τομέα.

Ένα σημείο στο οποίο παρατηρείται σημαντική διαφοροποίηση στις πολιτικές, είναι αυτό της καταγραφής των ιχνηλατών. Στις περιπτώσεις των e-Food και Wolt παρατίθενται αναλυτικές λίστες με τους ιχνηλάτες, οι οποίες σε πολύ μεγάλο βαθμό συμφωνούν με τα αποτελέσματα των αναλύσεων. Από τις υπόλοιπες εφαρμογές, στην περίπτωση της εφαρμογής AB αναφέρονται δύο ιχνηλάτες, ενώ σε όλες τις υπόλοιπες πολιτικές δεν υπάρχει καμία αναφορά στην παρουσία ιχνηλατών.

Ελλιπής παραμένει η πληροφόρηση και για τις κοινοποιήσεις δεδομένων σε τρίτους. Αν και σε πολλές περιπτώσεις δεν είναι πρακτική η παράθεση του κάθε μεμονωμένου συνεργάτη (όπως στις περιπτώσεις των Booking, e-Food και Wolt), συνήθως παρατίθενται κατηγορίες συνεργατών χωρίς όμως να κατονομάζονται κάποιοι ή να προσδιορίζονται τα δεδομένα τα οποία τους κοινοποιούνται. Μόνο η εφαρμογή Germanos αναφέρει την Niobium, όμως κατά την προσομοίωση καταγράφηκε επικοινωνία και με ιχνηλάτες των Google και Meta (Facebook).

Όσον αφορά την κοινοποίηση εκτός ΕΟΧ, σε όλες τις πολιτικές, εκτός της Wolt, υπάρχει η γενική διαβεβαίωση πως η εταιρεία εξασφαλίζει μέσω συμβατικών ρητρών την προστασία των δεδομένων ακόμα και μετά τη διαβίβασή τους εκτός ΕΟΧ. Η πολιτική απορρήτου της Wolt είναι η μόνη η οποία παρέχει σύνδεσμο στον ιστότοπο της Ευρωπαϊκής Επιτροπής, όπου περιγράφονται οι συγκεκριμένες ρήτρες.

Όπως προκύπτει από την ανάλυση των πολιτικών απορρήτου, υπάρχουν πολλές περιπτώσεις στις οποίες η αρχή προστασίας των δεδομένων εξ’ ορισμού μπορεί να βελτιωθεί. Για παράδειγμα, στην περίπτωση της εφαρμογής AB, εάν ο χρήστης δεν απορρίψει τα cookies, αυτά θεωρούνται αυτόματα ενεργοποιημένα. Επίσης, στην εφαρμογή Booking, το cross-site tracking είναι από προεπιλογή ενεργοποιημένο. Επιπροσθέτως, στην πολιτική απορρήτου της αναφέρεται η ενδεχόμενη διαφοροποίηση στην αναγραφόμενη τιμή ανάλογα με την τοποθεσία του χρήστη, κάτι για το οποίο ο χρήστης δεν έχει επιλογή απενεργοποίησης.

Άλλα δύο χαρακτηριστικά άξιας αναφοράς, είναι η καταγραφή των ζητούμενων permissions μόνο στην εφαρμογή Germanos, αν και κατά τη στατική ανάλυση βρέθηκαν και άλλα, επιπρόσθετα, permissions. Επίσης, τρεις από τις πολιτικές απορρήτου, αυτές των Nike, Pull & Bear και Zara καλύπτουν ένα εύρος μέσων με τα οποία ο χρήστης συναλλάσσεται με την εταιρεία, και δεν αναφέρονται μόνο στην εφαρμογή ηλεκτρονικών αγορών. Ιδιαίτερα η πρόσβαση στον αισθητήρα καρδιακών παλμών και στο επιταχυνσιόμετρο, θα ήταν περιττή αν χρησιμοποιούταν σε μια εφαρμογή ηλεκτρονικών αγορών.

Συνοψίζοντας, εξετάζοντας τις πολιτικές απορρήτου παρατηρούνται σημαντικές αποκλίσεις στο βαθμό υιοθέτησης των αρχών του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Στο ένα άκρο υπάρχουν εφαρμογές, όπως αυτές των e-Food και Wolt, οι οποίες είναι ιδιαίτερα σαφείς και καλογραμμένες, καταγράφουν αναλυτικά τα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία για την επίτευξη κάποιου στόχου, ενώ επίσης παραθέτουν τους ιχνηλάτες που χρησιμοποιούν.

Επίσης, υπάρχουν άλλες πολιτικές, όπως αυτή της Nike, οι οποίες είναι ιδιαίτερα γενικές και ως αποτέλεσμα αυτού δεν γίνεται ξεκάθαρο ποια δεδομένα προσωπικού χαρακτήρα υπόκεινται σε επεξεργασία και για ποιο λόγο.

Τέλος, όπως γίνεται σαφές από τις πολιτικές απορρήτου, σχεδόν όλες οι εφαρμογές χρησιμοποιούν τεχνικές fingerprinting του χρήστη, μέσω cookies και canvas.

6.2 Μελλοντική Έρευνα

Τα συμπεράσματα της εργασίας αυτής, μπορούν να χρησιμοποιηθούν για την εις βάθος μελέτη των δεδομένων προσωπικού χαρακτήρα, τα οποία ενδέχεται να συλλέγονται από τους ιχνηλάτες που εντοπίστηκαν. Καθώς, με βάσει προηγούμενες μελέτες, τα δεδομένα αυτά μεταδίδονται κρυπτογραφημένα, ανάλογα με τη μέθοδο κρυπτογράφησης ενδέχεται να είναι δυνατή η αποκρυπτογράφησή τους και ο προσδιορισμός των αναγνωριστικών που χρησιμοποιούνται για την ταυτοποίηση του χρήστη. Περαιτέρω, η ανάλυση που πραγματοποιήσαμε ήταν στατική, γεγονός που σημαίνει ότι χρήζουν περαιτέρω διερεύνησης τα εν λόγω ευρήματά μας και μέσω δυναμικής ανάλυσης, αφού η στατική ανάλυση ενδέχεται να φέρει ψευδώς θετική πληροφορία για μία άδεια πρόσβασης (π.χ. να εμφανίζεται στον κώδικα της εφαρμογής μία συγκεκριμένη άδεια, η οποία όμως, κατά τη λειτουργία της εφαρμογής, τελικά να μην ενεργοποιείται ποτέ). Επίσης, η μεθοδολογία που ακολουθήθηκε στα πλαίσια της εργασίας αυτής, μπορεί να φέρει αποτελέσματα και στη διερεύνηση των απειλών της ιδιωτικότητας και των δεδομένων προσωπικού χαρακτήρα και στην περίπτωση της πλατφόρμας iOS.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
2-Factor Authentication	Αυθεντικοποίηση 2 Παραγόντων
Accountability	Λογοδοσία
Accuracy	Ακρίβεια
Ad Library	Βιβλιοθήκη Προβολής Διαφημίσεων
Ad Provider	Πάροχος Διαφημιστικού Περιεχομένου
Anonymous Data	Ανώνυμα Δεδομένα
Certificate	Πιστοποιητικό
Component	Συστατικό Στοιχείο
Confidentiality	Εμπιστευτικότητα
Controller	Υπεύθυνος Επεξεργασίας
Data Minimisation	Ελαχιστοποίηση των Δεδομένων
Data Protection by Default	Προστασία Δεδομένων εξ' Ορισμού
Data Protection by Design	Προστασία Δεδομένων Ήδη από Σχεδιασμό
Data Subject Consent	Συγκατάθεση Υποκειμένου των Δεδομένων
Fairness	Αντικειμενικότητα
Graphical User Interface	Γραφική Διεπαφή Χρήστη
Hash Function	Συνάρτηση Κατακερματισμού
Hashing	Κατακερματισμός
Integrity	Ακεραιότητα
Inter-Process Communication	Δια-Διεργασιακή Επικοινωνία
Kernel	Πυρήνας
Lawfulness	Νομιμότητα
Library	Βιβλιοθήκη
Personal Data	Δεδομένα Προσωπικού Χαρακτήρα
Privacy Policy	Πολιτική Απορρήτου
Processing	Επεξεργασία
Processor	Εκτελών την Επεξεργασία
Profiling	Κατάρτιση Προφίλ
Pseudonymisation	Ψευδωνυμοποίηση
Pseudonymous Data	Ψευδωνυμοποιημένα Δεδομένα
Purpose Limitation	Περιορισμός του Σκοπού
Security Model	Μοντέλο Ασφαλείας
Sensitive Personal Data	Ευαίσθητα Δεδομένα Προσωπικού Χαρακτήρα
Storage Limitation	Περιορισμός της Περιόδου Αποθήκευσης
Third Party	Τρίτος
Tracker	Ιχνηλάτης
Transparency	Διαφάνεια

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ART	Android Runtime
EXIF	EXchangeable Image File
GAID	Google Advertising ID
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
HAL	Hardware Abstraction Layer
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
JVM	Java Virtual Machine
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
UID	User ID
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος

ΑΝΑΦΟΡΕΣ

[1] https://www.un.org/en/about-us/universal-declaration-of-human-rights [Προσπελάστηκε 07/06/2024].
[2] https://www.europarl.europa.eu/charter/pdf/text_el.pdf [Προσπελάστηκε 07/06/2024].
[3] https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679 [Προσπελάστηκε 07/06/2024].
[4] Kaminski M.: "A recent renaissance in privacy law", Commun. ACM 2020, 63, 24–27.
[5] Achilleos G., Limniotis K.: "Exploring personal data processing in video conferencing apps", Electronics 12(5), 1247 (2023).
[6] Limniotis K., "Network and Telecommunications Systems Security" module presentations, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, 2024
[7] Elenkov N.: "Android Security Internals - An In-Depth Guide to Android's Security Architecture", No Starch Press, 2015
[8] https://developer.android.com/guide/platform [Προσπελάστηκε 05/07/2024]
[9] https://www.geeksforgeeks.org/android-architecture [Προσπελάστηκε 05/07/2024]
[10] https://developer.android.com/guide/topics/manifest/permission-element.html [Προσπελάστηκε 05/07/2024]
[11] Gerasimou S., Limniotis K.: "A Study on Privacy and Security Aspects of Personalised Apps", International Journal of Information Security, Volume 23, pages 3217-3239, Springer (2024)
[12] Grammatikakis K.-P., Ioannou A., Shiaeles S., Kolokotronis N.: "WiP : Are cracked applications really free? An empirical analysis on Android devices", 16th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), pp. 730-735 (2018).
[13] https://developer.android.com/reference/android/Manifest.permission [Προσπελάστηκε 07/07/2024]
[14] Monogios S., Limniotis K., Kolokotronis N., Shiaeles S.: "A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps", Communications in Computer and Information Science, vol 1111. Springer, Cham, 2021.
[15] Pearce P., Felt A., Nunez D., Wagner D.: "Ad-Droid: Privilege separation for applications and advertisers in Android", ASIACCS, 2012.
[16] Shekhar S., Dietz M., Wallach D.: "AdSplit: Separating smartphone advertising from applications", USENIX Security, 2012.
[17] Stevens R., Gibler C., Crussell J., Erickson J., Chen H.: "Investigating user privacy in Android ad libraries", MoST, 2012.
[18] Son S., Kim D., Shmatikov V.: "What Mobile Ads Know About Mobile Users", Proceedings of the Network and Distributed System Security Symposium, San Diego, CA, USA, 21–24 February 2016.
[19] https://support.google.com/googleplay/android-developer/answer/6048248?hl=en [Προσπελάστηκε 20/08/2024]
[20] https://1nce.com/en-us/resources/iot-knowledge-base/iot-hardware/iot-hardware-devices/what-does-imei-number-signify [Προσπελάστηκε 20/08/2024]
[21] https://www.efani.com/blog/difference-between-imei-imsi-iccid-and-msisdn-numbers [Προσπελάστηκε 20/08/2024]
[22] Bujlow T., Carela-Espanol, V., Sole-Pareta, J., Barlet-Ros, P.: "A Survey on Web Tracking: Mechanisms, Implications, and Defenses", Proceedings of the IEEE, vol. 105, pp. 1476-1510 (2017).
[23] Binns R., Lyngs U., Van Kleek M., Zhao J., Libert T., Shadbolt N.: "Third Party Tracking in the Mobile Ecosystem", [cs.CY] (2018).
[24] Mikians J., Gyarmati L., Erramilli V., Laoutaris N.: "Detecting price and search discrimination on the internet", Proceedings of the 11th ACM Workshop on Hot Topics in Networks (Hotnets'12). ACM New York, Seattle, Washington, USA, October 2012, pp. 79–84.
[25] https://abcnews.go.com/GMA/TheLaw/gma-answers-credit-card-companies-financially-profiling-customers/story?id=6747461 [Προσπελάστηκε 23/06/2024]
[26] http://www.linksandlaw.com/news-update49-job-applicants-finland.htm [Προσπελάστηκε 23/06/2024]
[27] Li T.-C., Hang H., Faloutsos M., Efstathopoulos P.: "TrackAdvisor: Taking back browsing privacy from Third-Party Trackers", Proceedings of the 16th Passive and Active Measurement Conference (PAM 2015), Proceedings Series: Lecture Notes in Computer Science 8362. Springer International Publishing Switzerland, New York, USA, March 2015, pp. 1–12.
[28] Nikiforakis N., Kapravelos A., Joosen W., Kruegel C., Piessens F., Vigna G.: "Cookieless monster: Exploring the ecosystem of web-based device fingerprinting", S&P, 2013.
[29] https://docs.oracle.com/javase/tutorial/deployment/applet/security.html [Προσπελάστηκε 20/08/2024]
[30] https://speedof.me/api.html [Προσπελάστηκε 20/08/2024]
[31] https://www.speedtest.net [Προσπελάστηκε 20/08/2024]

[32] Acar G., Eubank C., Englehardt S., Juarez M., Narayanan A., Diaz C.: “The Web never forgets: Persistent tracking mechanisms in the wild”, CCS, 2014.
[33] Taylor V. F., Beresford A. R., Martinovic I.: “Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones”, [cs.CR] (2017).
[34] https://medium.com/@kezzieleo/manage-external-storage-permission-android-studio-java-9c3554cf79a7 [Προσπελάστηκε 10/10/2024]
[35] https://www.genymotion.com/product-desktop [Προσπελάστηκε 17/08/2024]
[36] https://www.virtualbox.org [Προσπελάστηκε 17/08/2024]
[37] https://www.ab.gr/el/privacy [Προσπελάστηκε 17/08/2024]
[38] https://www.booking.com/content/privacy.html [Προσπελάστηκε 17/08/2024]
[39] https://www.e-food.gr/page/privacy [Προσπελάστηκε 17/08/2024]
[40] https://www.germanos.gr/images/corporate/2.%20Data%20Privacy%20Notice_GApp_25.7.2023.pdf [Προσπελάστηκε 17/08/2024]
[41] https://agreementservice.svs.nike.com/gr/el_gr/rest/agreement?agreementType=privacyPolicy&uxId=com.nike.unite&country=GR&language=el [Προσπελάστηκε 17/08/2024]
[42] https://static.pullandbear.net/2/static2/policies/privacy_policy/pullandbear_privacy_policy_GR_el.pdf [Προσπελάστηκε 17/08/2024]
[43] https://explore.wolt.com/el/grc/privacy [Προσπελάστηκε 17/08/2024]
[44] https://static.zara.net/static/pdfs/US/privacy-policy/privacy-policy-en_US-20240923.pdf [Προσπελάστηκε 17/08/2024]