ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΜΗΧΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Προστασία προσωπικών δεδομένων στις εφαρμογές «πράσινων» πιστοποιητικών

Αναστάσιος Χ. Παναγόπουλος

Επιβλέπων: **Κωνσταντίνος Λιμνιώτης,** Δρ. Εξωτερικός Συνεργάτης

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Προστασία προσωπικών δεδομένων στις εφαρμογές «πράσινων» πιστοποιητικών

Αναστάσιος Χ. Παναγόπουλος
Α.Μ.: EN3200007

ΕΠΙΒΛΕΠΩΝ: **Κωνσταντίνος Λιμνιώτης,** Δρ. Εξωτερικός Συνεργάτης

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ **Δημήτριος Κατσιάνης**, Επίκουρος Καθηγητής
Νίκος Πασσάς, ΕΔΙΠ

Οκτώβριος 2022

ΠΕΡΙΛΗΨΗ

Η μεγάλη εξάπλωση του Κορωνοϊού SARS-CoV-2/Covid-19 τα τελευταία τρία χρόνια, έχει δημιουργήσει μεγάλες αναταραχές στον πλανήτη μας, τόσο στον τομέα της υγείας, όσο και σε αυτόν της οικονομίας. Πολλές επιχειρήσεις αναγκάστηκαν να κλείσουν και εκατοντάδες άνθρωποι υπέφεραν από κατάθλιψη, εξαιτίας του φόβου που επικρατούσε αλλά και των lockdown στα οποία προέβηκαν οι κυβερνήσεις για τον περιορισμό του ιού. Η επιστροφή στην κανονικότητα ξεκίνησε να έρχεται με την εμφάνιση των πρώτων εμβολίων, τα οποία μπορούσαν να δημιουργήσουν την ανοσία που είχε ανάγκη η ανθρωπότητα. Η κανονικότητα αυτή, θα επέτρεπε στους ανθρώπους να κυκλοφορούν ελεύθερα, τόσο μέσα στην χώρα τους, όσο και εντός ΕΕ.

Τη διευκόλυνση αυτή την παρέχουν τα λεγόμενα πράσινα πιστοποιητικά (green pass), τα οποία αποτελούν την ψηφιακή απόδειξη ότι κάποιος είτε έχει εμβολιαστεί για τον κορωνοϊό, είτε έχει κάνει τεστ για τον ιό με αρνητικό αποτέλεσμα, είτε έχει αναρρώσει από τη νόσο Covid-19, με γνώμονα πάντα την προστασία των προσωπικών τους δεδομένων. Τα πιστοποιητικά αυτά, έγιναν ευρέως γνωστά σε όλη την Ευρώπη. Χάρη στην καλή συνεργασία μεταξύ των χωρών, δεν άργησαν και τα πρώτα ταξίδια από την μία χώρα στην άλλη. Οι πολίτες, απέκτησαν πλέον τη δυνατότητα να επισκέπτονται, εν μέσω πανδημίας, όχι μόνο όποιο μέρος στη χώρα τους επιθυμούν, αλλά και άλλες χώρες, υπακούοντας όμως στους νόμους τους σχετικά με τον Covid-19. Οι χώρες τις ΕΕ, αποφάσισαν τη δημιουργία εφαρμογών, οι οποίες θα μπορούν να ελέγχουν την εγκυρότητα των πιστοποιητικών και έτσι να κάνουν πιο εύκολη τη ζωή των πολιτών.

Η συγκεκριμένη διπλωματική αφορά τις εφαρμογές πράσινων πιστοποιητικών που χρησιμοποιούνται στα κράτη-μέλη της Ευρώπης, δίνοντας έμφαση στην ιδιωτικότητά τους και στο κατά πόσο τα δεδομένα των χρηστών διαρρέουν σε ιχνηλάτες. Κύριος άξονας της εργασίας, είναι ο έλεγχος της ασφάλειας και της ιδιωτικότητας των εφαρμογών αυτών, καθώς και των απαιτήσεων (permissions) που έχουν απο τους χρήστες (privacy policies). Επίσης, θα αξιολογηθεί η τρέχουσα κατάσταση υπό το πρίσμα του σχετικού νομικού πλαισίου, που είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων(GDPR- 2016/679) της ΕΕ, αλλά και η e-Privacy οδηγία. Οι δύο αυτές οδηγίες, θα αναλυθούν αρχικά ξεχωριστά, έτσι ώστε να γίνουν πιο εύκολα κατανοητές στον αναγνώστη. Περαιτέρω, οι εφαρμογές μελετώνται, με χρήση κατάλληλων εργαλείων λογισμικών, ως προς τη λειτουργία τους σε πραγματικό χρόνο, με σκοπό να διαπιστωθεί η αποτελεσματικότητά τους, το τι πρέπει να ικανοποιούν, αλλά και τυχόν ζητήματα ιδιωτικότητας που εγείρουν. Επιπλέον, θα αναφερθούν κενά και προβλήματα που έχουν υπάρξει, τόσο από τα ίδια τα πράσινα πιστοποιητικά, όσο και από τις εφαρμογές που χρησιμοποιούνται. Τα συμπεράσματα της παρούσας διατριβής, έχουν ιδιαίτερη σημασία και για τη γενικότερη περίπτωση που έξυπνες εφαρμογές θα χρησιμοποιηθούν για μια περίοδο έκτακτης κρίσης, όπως μια πανδημία, αφού πάντοτε, προκειμένου οι χρήστες να έχουν εμπιστοσύνη σε αυτές, πρέπει να γίνεται σαφές ότι ενεργούν υπό το πρίσμα του σεβασμού στα ατομικά δικαιώματα.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ιδιωτικότητα έξυπνων εφαρμογών

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Πράσινα πιστοποιητικά, ιδιωτικότητα, ΓΚΠΔ, προσωπικά δεδομένα, ιχνηλάτες

ABSTRACT

The great spread of the SARS-CoV-2 / Covid-19 in the last three years, has created great turmoil on our planet, both in the field of health and in that of the economy. Many businesses were forced to close and hundreds of people suffered from depression due to the prevailing fear and lockdowns that governments proceeded, to curb the virus. The return to normalcy began with the advent of the first vaccines, which could create the immunity that humanity needed. This regularity would allow people to move freely, both within their own country and within the EU.

This facility is provided by the so-called green pass certificates, which are digital proof that someone has either been vaccinated for the coronavirus, tested negative for the virus, or has recovered from Covid-19 disease, always with guidance to the protection of their personal data. These certificates became widely known throughout Europe. Thanks to the good cooperation between the countries, the first trips from one country to another were not long in coming. Citizens now have the right to visit not only any place in their country they wish, but also other countries, as long as they obey to their Covid-19 laws. EU countries have decided to create applications that will be able to check the validity of certificates and thus make the lives of citizens easier.

This dissertation studies the green certificate applications used in the European Member States, emphasizing on their privacy and whether user data is leaked to trackers. The main pillar of the study, is the security and privacy characteristics of these applications, as well as the requirements/permissions that they have from users (privacy policies) Moreover, the current situation will be assessed in the light of the relevant legal framework, which is the General EU Data Protection Regulation (GDPR- 2016/679), but also the e-Privacy Directive. These two legal instruments will be initially analyzed separately, so that they can be more easily understood by the reader. Furthermore, the applications are studied, using appropriate software tools, in terms of their operation in real time, in order to determine their effectiveness, what they should satisfy, but also any privacy issues that they raise. In addition, gaps and problems that have occurred, both from the green certificates themselves and from the applications used, will be reported. The conclusions of this study are of high importance for any case that smart applications will be used in case of an urgent situation like a pandemic, since towards ensuring the users trust it is essential to assure that human rights are being respected.

SUBJECT AREA: Security and privacy in smart applications

KEYWORDS: Green certificates, privacy, GDPR, personal data, trackers

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα εργασία αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Μηχανική Υπολογιστών, Τηλεπικοινωνιών και Δικτύων» με ειδίκευση την «Δικτύωση Υπολογιστών» του τμήματος Πληροφορικής και Τηλεπικοινωνιών του Εθνικού & Καποδιστριακού Πανεπιστημίου Αθηνών, εντός του ακαδημαϊκού έτους 2021-2022, υπό την επίβλεψη του Δρ. Κωνσταντίνου Λιμνιώτη.

Με την ολοκλήρωση της, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλαν στην εκπόνησή της. Πρωτίστως, ευχαριστώ θερμά τον επιβλέπων καθηγητή, κύριο Λιμνιώτη Κωνσταντίνο, ο οποίος είναι εξωτερικός συνεργάτης στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του ΕΚΠΑ, για την εμπιστοσύνη που μου έδειξε από την πρώτη κιόλας στιγμή, αναθέτοντάς μου το θέμα αυτό, για την καθοδήγησή του, τις υποδείξεις του, την διαθεσιμότητα και συνεισφορά του, και την συνεχή του υποστήριξη από την αρχή μέχρι το τέλος.

Τέλος, θα επιθυμούσα να πω ένα μεγάλο ευχαριστώ και να εκφράσω την αμέριστη ευγνωμοσύνη μου στην οικογένειά μου και στους ανθρώπους που βρίσκονται κοντά μου για όλη τη στήριξη και τη συμπαράσταση, καθ’ όλη τη διάρκεια των μεταπτυχιακών μου σπουδών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

Διανύουμε ήδη τον τρίτο χρόνο από το αρχικό μεγάλο ξέσπασμα της πανδημίας της αναπνευστικής νόσου 2019-nCov, που είναι μια μολυσματική ασθένεια, η οποία προκαλείται από τον κορωνοϊό SARS-CoV-2. Η πρώτη εμφάνιση του ιού, εντοπίστηκε στην Κίνα και πιο συγκεκριμένα στην πόλη Γιουχάν στα τέλη του 2019. Ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) αποφάσισε να κηρύξει την έξαρσή του ως γεγονός διεθνούς ενδιαφέροντος στις 30 Ιανουαρίου 2020 και ως πανδημία στις 11 Μαρτίου 2020. Η εξάπλωση την πανδημίας αυτής, έφερε μεγάλες και πρωτόγνωρες αλλαγές στην καθημερινή ζωή των ανθρώπων σε όλο τον πλανήτη. Οι κυβερνήσεις, αναγκάστηκαν να πάρουν πολλά και σκληρά μέτρα για να ελαττώσουν όσο μπορούν την εξάπλωση του ιού, όπως η επιβολή χρήσης μάσκας τόσο σε εσωτερικούς, όσο και σε εξωτερικούς χώρους, η απαγόρευση κυκλοφορίας (lock down), η απομόνωση των ανθρώπων που είναι νοσούντες (καραντίνα), η τηλεργασία και η συνεχής διενέργεια διαγνωστικών τεστ για λόγους εργασίας και κυκλοφορίας.

Η χρήση μάσκας ήταν ένα από τα πιο δύσκολα και συχνά μέτρα που παίρνουν οι κυβερνήσεις, έτσι ώστε να μειωθεί η διασπορά του ιού. Αυτό συμβαίνει, λόγω του μεγάλου αριθμού ασυμπτωματικών ανθρώπων, οι οποίοι δεν γνωρίζουν ότι έχουν τον ιό, μιας και δεν έχουν κανένα απολύτως σύμπτωμα. Τα lock down, έγιναν συνήθεια στην καθημερινότητά μας, μιας και ανα τακτά χρονικά διαστήματα, η απαγόρευση κυκλοφορίας έμπαινε στη ζωή μας. Το εκάστοτε Υπουργείο Υγείας κάθε χώρας, δυσκολευόταν όλο και περισσότερο να εντοπίσει τις επαφές του κάθε ατόμου που νοσεί, επειδή ο αριθμός των νοσούντων αυξανόταν μέρα με τη μέρα. Ήταν φανερό πώς αν δεν άλλαζε κάτι, όλα τα παραπάνω θα γίνονταν η καθημερινότητά μας για πολύ ακόμα, με συνέπεια όλο και περισσότεροι άνθρωποι να έπεφταν σε κατάθλιψη, αλλά και η ανεργία και τα φαινόμενα οικογενειακής βίας να συνεχίζουν να αυξάνονται.

Στις αρχές όμως του δεύτερου χρόνου της πανδημίας, τα πρώτα θετικά μηνύματα εμφανίστηκαν για την ανθρωπότητα. Τα πρώτα εμβόλια έκαναν την εμφάνισή τους και έδωσαν μετά από καιρό μια ελπίδα για επιστροφή στην κανονικότητα. Όλο και περισσότεροι άνθρωποι, με προτεραιότητα στους ηλικιωμένους και στους ανθρώπους με υποκείμενα νοσήματα, άρχισαν να εμβολιάζονται, με σκοπό να αποκτήσουν την πολυπόθητη ανοσία. Έτσι, είδαμε τα μέτρα σιγά σιγά να μειώνονται και πολλές φορές να ισχύουν μόνο για όσους δεν έχουν εμβολιαστεί. Έπειτα, οι κυβερνήσεις, αποφάσισαν να δημιουργηθεί ένα ψηφιακό πράσινο πιστοποιητικό, το οποίο θα βοηθούσε στο να επιστρέψουμε στην κανονικότητα. Τα πιστοποιητικά αυτά, θα αποτελούν την ψηφιακή απόδειξη ότι κάποιος είτε έχει εμβολιαστεί για τον κορωνοϊό, είτε έχει κάνει τεστ για τον ιό με αρνητικό αποτέλεσμα, είτε έχει αναρρώσει από τη νόσο Covid-19. Με αυτόν τον τρόπο, θα μπορούν οι πολίτες να εισέρχονται σε όλους τους χώρους, όπως εστιατόρια, κέντρα διασκέδασης, γήπεδα, μαγαζιά κ.α., αρκεί να επιδείξουν στην είσοδο το συγκεκριμένο πιστοποιητικό.

Για να μπορεί να γίνει ο έλεγχος και η επαλήθευση των πιστοποιητικών αυτών, οι χώρες της ΕΕ αποφάσισαν τη δημιουργία εφαρμογών για τα ψηφιακά πράσινα πιστοποιητικά. Οι εφαρμογές αυτές, σκανάρουν το QR code των πιστοποιητικών και εμφανίζουν πράσινη ένδειξη όταν ο χρήστης μπορεί να μπει στον χώρο που επιθυμεί ή κόκκινο, όταν ο χρήστης δεν έχει δικαίωμα εισόδου, γιατί το πιστοποιητικό του έχει λήξει (πέρας χρονικής διάρκειας εμβολίου, νόσησης ή τέστ). Ασφαλώς, οι εφαρμογές θα πρέπει να λειτουργούν πάντα με γνώμονα την προστασία των προσωπικών τους δεδομένων. Η ΕΕ, έχει δημιουργήσει μία ψηφιακή πύλη, που συνδέει όλες τις εθνικές βάσεις δεδομένων, έτσι ώστε να γίνεται πιο εύκολα η επαλήθευση των πράσινων

πιστοποιητικών μέσα στην ΕΕ. Έτσι, οι πολίτες μπορούν εύκολα να μετακινηθούν σε άλλες χώρες εντός της ΕΕ, χωρίς να υπάρχει πρόβλημα με το πιστοποιητικό τους. Τα προσωπικά δεδομένα των χρηστών ασφαλώς και δεν μεταφέρονται από αυτήν.

1.1 Βασικά Ερευνητικά Ερωτήματα

Η παρούσα διατριβή, έχει ως στόχο τη μελέτη των εφαρμογών πράσινου πιστοποιητικού, οι οποίες υπάρχουν σε κάθε χώρα της Ευρωπαϊκής Ένωσης, αλλά και πως οι χρήστες θα τις χρησιμοποιούν πάντα με γνώμονα την προστασία των προσωπικών τους δεδομένων. Από τη συγκεκριμένη μελέτη, προέκυψαν και τα παρακάτω ερευνητικά ερωτήματα, τα οποία θα γίνει προσπάθεια να απαντηθούν στην συνέχεια της εργασίας:

- Διαθέτουν όλες οι χώρες της Ευρωπαϊκής Ένωσης τη δικιά τους εφαρμογή πράσινου πιστοποιητικού;
- Είναι όλες οι εφαρμογές «καθαρά» εφαρμογές πράσινου πιστοποιητικού;
- Τι ζητήματα ιδιωτικότητας εγείρονται και πως αντιμετωπίζονται;
- Ποια επεξεργασία προσωπικών δεδομένων πραγματοποιείται με τη χρήση των εφαρμογών;
- Τηρούνται οι προϋποθέσεις νομιμότητας σύμφωνα με το νομικό πλαίσιο;
- Είναι οι εκάστοτε πολιτικές απορρήτου κατανοητές και σωστές, ή κρύβουν πράγματα από τους χρήστες;

1.2 Μεθοδολογία

Το πρώτο μέρος της διατριβής, βασίστηκε στην έρευνα και αποτύπωση των εφαρμογών πράσινου πιστοποιητικού των χωρών της Ευρωπαϊκής Ένωσης, μιας και την περίοδο έναρξης της διατριβής, δεν είχαν ακόμα αναπτύξει όλες οι χώρες τη δική τους εφαρμογή. Στη συνέχεια, πραγματοποιήθηκε η συλλογή και επιλογή της κατάλληλης βιβλιογραφίας, έτσι ώστε να αποτυπωθούν καλύτερα οι πληροφορίες που ήταν σχετικές με τα ψηφιακά πράσινα πιστοποιητικά. Με τη βοήθεια της βιβλιογραφίας, καταγράφηκε ο τρόπος χρήσης των πράσινων πιστοποιητικών και των εφαρμογών τους, αλλά και τα θέματα ιδιωτικότητας και τα κενά που έχουν οι εφαρμογές αυτές.

Έπειτα, ακολούθησε θεωρητική έρευνα των έξυπνων εφαρμογών, έτσι ώστε να βρεθεί και να αποτυπωθεί υλικό, σχετικά με τα ζητήματα ασφάλειας και ιδιωτικότητας που εγείρονται από τη χρήση τους. Επίσης, έγινε έρευνα σχετικά με τους ιχνηλάτες και τον ρόλο τους στις έξυπνες εφαρμογές.

Στη συνέχεια της θεωρητικής έρευνας, μελετήθηκαν οι βασικοί κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων, που αποτελεί το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων εντός Ευρωπαϊκής Ένωσης. Η μελέτη τόσο του συγκεκριμένου Κανονισμού, όσο και της e-Privacy Οδηγίας είναι σημαντικές, έτσι ώστε να γίνει αντιληπτό ποια είναι η νόμιμη επεξεργασία προσωπικών δεδομένων στις εφαρμογές πράσινου πιστοποιητικού.

Περνώντας στο πρακτικό κομμάτι, πραγματοποιήθηκε πειραματική έρευνα, μέσω των εργαλείων exodus και lumen, έτσι ώστε να μελετηθεί σε πραγματικό χρόνο, το τι υποκείμενη επεξεργασία προσωπικών δεδομένων πραγματοποιείται από τις συγκεκριμένες εφαρμογές, το αν τα δεδομένα των χρηστών μεταφέρονται σε τρίτους και το αν είναι διαφανείς, εύχρηστες αλλά και φιλικές προς τον εκάστοτε χρήστη. Έτσι θα εξακριβωθεί το κατά πόσο οι πολιτικές απορρήτου της κάθε εφαρμογής, λένε όλη την

αλήθεια και αν βασίζονται στους κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων. Για την πραγματοποίηση της πειραματικής έρευνας, χρησιμοποιήθηκε ένας φορητός υπολογιστής για τη χρήση του exodus, καθώς και μία κινητή συσκευή, στην οποία εγκαταστάθηκε η εφαρμογή lumen.

Συνοψίζοντας, το αντικείμενο της εργασίας έχει πολύ μεγάλο ερευνητικό ενδιαφέρον, καθώς τα τελευταία χρόνια ο συγκεκριμένος ιός, έχει γίνει μέρος της καθημερινότητάς μας. Όσον αφορά τη βιβλιογραφία, είναι αρκετή μιας και διανύουμε τον τρίτο χρόνο της πανδημίας, αλλά υπάρχουν ελλείψεις όσον αφορά τις εφαρμογές των πράσινων πιστοποιητικών και το ποιες είναι για κάθε χώρα.

1.3 Δομή Διατριβής

Η παρούσα διπλωματική απαρτίζεται από 7 κεφάλαια, τα οποία έχουν ως στόχο να καλύψουν το αντικείμενο των εφαρμογών πράσινων πιστοποιητικών. Το συγκεκριμένο κεφάλαιο είναι η πρώτη επαφή του αναγνώστη με το αντικείμενο της μελέτης. Περιλαμβάνει μια μικρή εισαγωγή, τα ερευνητικά ερωτήματα που θα προσπαθήσει να απαντήσει, καθώς και τη μεθοδολογία που ακολουθήθηκε για την ολοκλήρωση της εργασίας.

Στο δεύτερο κεφάλαιο, θα πραγματοποιηθεί μια εισαγωγή στις βασικές έννοιες των έξυπνων εφαρμογών κινητών συσκευών. Επίσης, θα αναλυθούν τα ζητήματα ασφάλειας και ιδιωτικότητας που εγείρονται με τη χρήση των εφαρμογών, ενώ τέλος, θα γίνει αναφορά στους ιχνηλάτες και τις άδειες, που αιτούνται οι εφαρμογές για την καλύτερη λειτουργία τους.

Στο τρίτο κεφάλαιο, θα γίνει εισαγωγή ως προς την έννοια της ιδιωτικότητας και των προσωπικών δεδομένων και θα αναφερθούν οι απαιτήσεις και οι κίνδυνοι που υπάρχουν. Επίσης θα αναλυθούν εκτενέστερα τόσο ο Γενικός Κανόνας Προστασίας Δεδομένων με τις απαιτήσεις και κάποια από τα πιο σημαντικά άρθρα του, όσο και η e-Privacy οδηγία, που έχουν άμεση σύνδεση μεταξύ τους.

Στο τέταρτο κεφάλαιο, θα πραγματοποιηθεί ανάλυση των πράσινων πιστοποιητικών, ως προς τον τρόπο χρήσης τους, την προστασία των προσωπικών δεδομένων των χρηστών, αλλά και τα κενά που υπάρχουν τόσο σε αυτά, όσο και στις εφαρμογές πράσινων πιστοποιητικών, χρησιμοποιώντας αρκετά παραδείγματα.

Στο πέμπτο κεφάλαιο, θα γίνει αναφορά στα δύο εργαλεία που χρησιμοποιήθηκαν, έτσι ώστε να πραγματοποιηθεί το πρακτικό κομμάτι της εργασίας αυτής. Θα παρουσιαστεί ο τρόπος χρήσης τους βήμα βήμα, αλλά και το τι δεδομένα μπορούμε να λάβουμε από την ανάλυση που πραγματοποιούν.

Στο έκτο κεφάλαιο, θα παρουσιαστεί το πρακτικό σκέλος της διπλωματικής. Μέσω πινάκων, σχημάτων και εικόνων, θα παρουσιαστούν οι εφαρμογές που αναλύθηκαν, αλλά και σημαντικές πληροφορίες και ευρήματα που βρέθηκαν γι αυτές. Ο στόχος είναι να γίνει αντιληπτό, ποια προσωπικά δεδομένα παίρνουν οι εφαρμογές αυτές από τον χρήστη, αν τα δεδομένα αυτά παραχωρούνται σε τρίτους και κατά πόσο λειτουργούν με γνώμονα τους κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων.

Στο έβδομο και τελευταίο κεφάλαιο, θα παρουσιαστούν τα συμπεράσματα που λήφθηκαν από τον έλεγχο, αλλά και οι δυσκολίες που υπήρξαν για την ολοκλήρωση της παρούσας διπλωματικής.

2. ΕΞΥΠΝΕΣ ΕΦΑΡΜΟΓΕΣ

2.1 Έξυπνες Κινητές Συσκευές

Το επίθετο «έξυπνος», τα τελευταία χρόνια είναι η βασική λέξη του καθημερινού λεξιλογίου μικρών και μεγάλων. Ξεκίνησε με τα «έξυπνα» τηλέφωνα, που επιτρέπουν στο χρήστη να εγκαταστήσει και να χρησιμοποιήσει ένα μεγάλο εύρος εφαρμογών, με τις οποίες μπορεί να επικοινωνήσει και να φέρει εις πέρας καθήκοντα με απομακρυσμένο τρόπο (π.χ. πληρωμές). Στη συνέχεια, προχώρησε σε «έξυπνες» συσκευές, «έξυπνα» αυτοκίνητα, «έξυπνα» σπίτια, «έξυπνες» εφαρμογές. Τι μας οδήγησε όμως στην «έξυπνη» τεχνολογία και τι είναι αυτή; Οδηγηθήκαμε λόγω της συνεχούς τεχνολογικής προόδου λογισμικού και υλικού, με την οποία πολλές συσκευές μπορούν να συνδεθούν μεταξύ τους, μέσω του διαδικτύου ή Bluetooth. Με αυτόν τον τρόπο, γίνονται ανιχνεύσιμες και μπορούμε να τις παρακολουθούμε μέσω ενός υπολογιστή.

Με τη συνεχή τεχνολογική πρόοδο, επόμενο ήταν να επέλθει και πρόοδος στα κινητά τηλέφωνα, τα οποία περνώντας από πολλά στάδια αλλαγών, έφτασαν στα smartphones που όλοι ξέρουμε σήμερα. Αυτά τα «έξυπνα» τηλέφωνα, σε αντίθεση με τα συμβατικά κινητά τηλέφωνα, βασίζουν τη λειτουργία τους σε ένα λειτουργικό σύστημα που διαθέτει προηγμένη υπολογιστική ικανότητα. Ο χρήστης επιλέγοντας ένα smartphone, αυτόματα αποκτά όλες τις κλασσικές λειτουργίες ενός απλού κινητού, ενώ ταυτόχρονα, έχει τη δυνατότητα να αποφασίσει ο ίδιος για τον ακριβή αριθμό και το είδος των εφαρμογών που θα εγκαταστήσει σε αυτό. Με τον τρόπο αυτό, δημιουργεί μια κινητή συσκευή, προσαρμοσμένη απόλυτα στα θέλω του. Αυτό επιτυγχάνεται, χάρη στην ανοικτή αρχιτεκτονική των «έξυπνων» τηλεφώνων, με την οποία ο χρήστης, όχι μόνο μπορεί να χρησιμοποιήσει τις ήδη υπάρχουσες εφαρμογές, αλλά και να εγκαταστήσει νέες, ανάλογα με τις ανάγκες του. Κάτι τέτοιο, δεν ήταν δυνατό να συμβεί με τα κλασσικά κινητά τηλέφωνα, εξαιτίας του λογισμικού τους, στο οποίο δεν μπορεί να παρέμβει κανείς.

Τα smartphones, μπήκαν στη ζωή του παγκόσμιου πληθυσμού, αρχικά λόγω των χαρακτηριστικών που περιλαμβάνουν:

- Μεγάλη οθόνη αφής με μικρό βάρος (εύκολη μεταφορά)
- MicroSD κάρτες μνήμης μεγάλης χωρητικότητας
- Φωνητική επικοινωνία και βιντεοκλήση
- Ανταλλαγή SMS, MMS και email
- Ασύρματη διαδικτυακή σύνδεση (μέσω 4G, 5G, Wi-Fi)
- Προβολή φωτογραφιών, αναπαραγωγή βίντεο, αρχείων
- Ενσωματωμένη κάμερα
- Αναπαραγωγή ήχου
- Ενσωμάτωση εφαρμογών για κοινωνικές σελίδες

Επίσης, παρέχουν τη δυνατότητα εγκατάστασης νέων εφαρμογών, ανάλογες των αναγκών του κάθε χρήστη. Υπάρχουν πολλά είδη εφαρμογών, όπως διασκέδασης, επικοινωνίας, παιχνιδιών, υγείας κ.α. με τις οποίες οι χρήστες, εύκολα και γρήγορα ικανοποιούν την κάθε τους ανάγκη. Η πρόσβαση στις εφαρμογές αυτές, δίνεται μέσω των πλατφορμών διανομής εφαρμογών, όπως είναι το Google Play Store και το App Store.

Κάποιες από αυτές διατίθενται δωρεάν, ενώ άλλες επι πληρωμή. Η «έξυπνη» εφαρμογή έχει κάποια βασικά προτερήματα, όπως:

- Είναι συμβατή με όλες τις «έξυπνες» συσκευές
- Χρησιμοποιείται παντού, ανεξάρτητα με την τοποθεσία
- Είναι φιλική προς το χρήστη

Υπάρχει όμως και η άλλη όψη του νομίσματος, καθώς με τη χρήση της smart εφαρμογής, παρέχεται πρόσβαση σε προσωπικά δεδομένα του χρήστη, όπως επαφές, κλήσεις, τοποθεσία συσκευής κ.α, χωρίς πάντα τη συγκατάθεσή του. Άλλες εφαρμογές, ζητάνε άδεια από τον χρήστη, έτσι ώστε να κάνουν χρήση συγκεκριμένων εργαλείων του κινητού του, όπως η κάμερα ουσιαστικά «αναγκάζοντας» το χρήστη να εκχωρήσει άδεια. Θα αναφερθούμε εκτεταμένα στο κομμάτι των αδειών, στο ερευνητικό μέρος της εργασίας. Τέλος, με τον τρόπο αυτό δημιουργείται ένα ηλεκτρονικό προφίλ του χρήστη, άγνωστο σε αυτόν.

Όλα όσα αναφέραμε, σε συνδυασμό με τη σοβαρή μείωση του κόστους, είναι οι αιτίες που τα «έξυπνα» κινητά, από επαγγελματικό εργαλείο για λίγους, έφτασε να γίνει προέκταση του χεριού για όλους. Είναι πλέον καθημερινότητα, μας ακολουθούν όπου κι αν πηγαίνουμε και είναι συνεχώς συνδεδεμένα στο διαδίκτυο. Εξαιτίας αυτής της επιτυχίας, οι εταιρείες οδηγήθηκαν στη δημιουργία συσκευών (tablet) με παρόμοια χαρακτηριστικά με τα smartphones, με μεγαλύτερη οθόνη, που δεν χρησιμοποιούνται όμως για τηλεφωνική επικοινωνία, αλλά για εκπαίδευση, ψυχαγωγία κ.α. Αυτοί είναι οι λόγοι, που οι μονάδες παραγωγής «έξυπνων» συσκευών, παρά την παγκόσμια οικονομική κρίση, έχουν τεράστια έσοδα.

2.2 Παγκόσμιες Τάσεις και Υιοθέτηση στην Αγορά Κινητών Εφαρμογών

Αν και υπάρχει ήδη μεγάλος αριθμός διαθέσιμων εφαρμογών για κινητά, η ζήτηση για νέες εξακολουθεί να αυξάνεται, λόγω της ραγδαίας προόδου της τεχνολογίας και της ανάγκης των ανθρώπων για πιο καινοτόμες προσεγγίσεις. Αναμφίβολα, η κοινωνία μας εξαρτάται απόλυτα από φορητές συσκευές και κατ' επέκταση, εφαρμογές για κινητές συσκευές. Οι καινοτομίες στην τεχνολογία παρέχουν ευκαιρίες, όχι μόνο για την ανάπτυξη νέων λύσεων, αλλά και για τη βελτίωση των υπαρχουσών. Στην πραγματικότητα, σχεδόν το 90% του χρόνου που αφιερώνεται σε κινητές συσκευές σήμερα, χρησιμοποιείται σε εφαρμογές, κυρίως λόγω της πανδημίας και όλο το χρόνο που δαπανάται στο σπίτι. Αλλά αυτό δεν είναι κάτι καινούργιο. Οι εφαρμογές για κινητά είναι η πρώτη τάση εδώ και μερικά χρόνια. Ωστόσο, η τεχνολογία εξελίσσεται ολοένα και ταχύτερα κάθε χρόνο, με αποτέλεσμα να εμφανίζονται νέες και πιο απαιτητικές τάσεις για κινητά. Έτσι, η ενημέρωση με τις πιο πρόσφατες τάσεις ανάπτυξης εφαρμογών για κινητά, μπορεί να βοηθήσει στη δημιουργία μιας επιτυχημένης εφαρμογής, να προσελκύσει νέους χρήστες και να τους κάνει να τη χρησιμοποιούν τακτικά. Τέλος, θα παρέχονται νέες λύσεις με βάση τις ανάγκες των χρηστών και την ικανοποίηση αυτών.

<u>Οι κορυφαίες παγκόσμιες τάσεις κινητών εφαρμογών για το 2022 [3], [4]</u>

- **5G**: Όπως γνωρίζουμε, η τεχνολογία 5G υπάρχει εδώ και αρκετό καιρό, αν και δεν ήταν πάντα στο επίκεντρο μέχρι πολύ πρόσφατα. Το 5G είναι μια νέα γενιά καινοτομίας τηλεπικοινωνιακών δικτύων, που υποστηρίζει προηγμένες εφαρμογές σε Επαυξημένη Πραγματικότητα (Augmented Reality) και Εικονική Πραγματικότητα (Virtual Reality), 4K και 360 streaming video και διασυνδεδεμένες συσκευές IoT. Σε σύγκριση με προηγούμενες τεχνολογίες, το 5G υπόσχεται να προσφέρει αυξημένη ταχύτητα και εύρος ζώνης, χαμηλότερο

λανθάνοντα χρόνο και βελτιωμένη συνδεσιμότητα, εξασφαλίζοντας ελάχιστες διακοπές και ομαλή συνδεσιμότητα. Μπορούμε μόνο να φανταστούμε όλες τις αλλαγές που θα επιφέρει αυτή η νέα τεχνολογία, οπότε δεν είναι περίεργο που θεωρείται μια τάση από μόνη της.

- **Ενσωμάτωση επαυξημένης και εικονικής πραγματικότητας**: Οι τεχνολογίες κοινωνικής απόστασης σημείωσαν άνθηση από το 2020, όταν ο COVID-19 άρχισε να επηρεάζει ένα ευρύ φάσμα βιομηχανιών. Με τη χρήση τους, οι πωλητές και οι πάροχοι υπηρεσιών μπορούν να αλληλεπιδράσουν με τους πελάτες τους πιο προσωπικά. Χρησιμοποιώντας Augmented Reality (AR) και Virtual Reality (VR), οι επιχειρήσεις μπορούν να προβάλλουν τα προϊόντα και τις υπηρεσίες τους με τον καλύτερο δυνατό τρόπο. Επιπλέον, οι πελάτες μπορούν να δουν πώς θα είναι πάνω τους ένα συγκεκριμένο προϊόν, όπως ένα ρούχο πριν το αγοράσουν. Μαζί με τα εμπορικά οφέλη, το AR και το VR μπορούν να βελτιώσουν τις μαθησιακές εμπειρίες και να κάνουν τις εφαρμογές για κινητά πιο ελκυστικές.

- **Blockchain:** Η τεχνολογία Blockchain είναι μία από τις νεότερες τάσεις ανάπτυξης εφαρμογών για κινητά του 2022. Υπήρχε πάντα μεγάλη ανησυχία μεταξύ των χρηστών εφαρμογών, σχετικά με την ασφάλεια και την κακή χρήση δεδομένων. Ευτυχώς, το blockchain λύνει αυτά τα προβλήματα, δημιουργώντας αποκεντρωμένες βάσεις δεδομένων, γι' αυτό και αποτελεί μια αναδυόμενη τάση. Λόγω των χαρακτηριστικών της, οι εφαρμογές που χρησιμοποιούν αυτήν την τεχνολογία είναι πιο ασφαλείς, καθώς κανένα άτομο δεν μπορεί να αλλάξει τις βάσεις δεδομένων των χρηστών για πρόσβαση σε ευαίσθητες πληροφορίες.

- **Τεχνητή Νοημοσύνη (AI) και Μηχανική Μάθηση (ML):** Τα κινητά τηλέφωνα έχουν ήδη αρχίσει να χρησιμοποιούν AI και ML για την αναγνώριση προσώπου εδώ και αρκετό καιρό. Ωστόσο, αυτή η δυνατότητα ενσωματώνεται ολοένα και περισσότερο από εταιρείες ανάπτυξης εφαρμογών, για τη βελτίωση της ασφάλειας των χρηστών, της καλύτερης λειτουργικότητας και γενικά μιας μεγαλύτερης εμπειρίας χρήστη. Μπορεί να μειωθεί σημαντικά ο χρόνος ανάπτυξης της εφαρμογής, χρησιμοποιώντας τη μηχανική μάθηση. Ωστόσο, η AI και η ML μπορούν επίσης να μειώσουν τα λάθη στα οποία οι προγραμματιστές θα είχαν υποπέσει, αν τις είχαν χρησιμοποιήσει. Ορισμένες υπάρχουσες εφαρμογές, ενσωματώνουν πλέον στοιχεία τεχνητής νοημοσύνης, συμπεριλαμβανομένων των chatbot, καθώς και εξατομικεύουν ορισμένα στοιχεία της εμπειρίας χρήστη. Ως τάση ανάπτυξης εφαρμογών για κινητά το 2022, η τεχνητή νοημοσύνη και η μηχανική εκμάθηση θα χρησιμοποιηθούν εκτενώς, για την παροχή γεωγραφικής θέσης, καλύτερης εμπειρίας παιχνιδιού και προηγμένης ανάπτυξης λογισμικού στους χρήστες.

- **Beacon Technology**: Πολλές βιομηχανίες χρησιμοποιούν ήδη την τεχνολογία beacon, π.χ. υγειονομική περίθαλψη, ηλεκτρονικό εμπόριο, μουσεία, ξενοδοχεία κ.α. Παρόλο που εισήχθη το 2013, μόλις πρόσφατα έγινε δημοφιλής. Με τη χρήση αυτής της τεχνολογίας, οι online και οι offline κόσμοι μπορούν να συνδεθούν με έναν μοναδικό τρόπο. Χρησιμοποιώντας τεχνολογία Bluetooth χαμηλής ενέργειας, τα beacons στέλνουν σήματα σε άλλες έξυπνες συσκευές. Για παράδειγμα, ένας φάρος καταστήματος συνδέεται με το τηλέφωνο του πελάτη μέσω Bluetooth και προσφέρει εκπτώσεις και προσφορές. Ο πελάτης θα λάβει κάθε είδους πληροφορίες σχετικά με προϊόντα ή πωλήσεις κοντά. Ωστόσο, το κυρίαρχο πλεονέκτημα της τεχνολογίας beacon είναι η εγγύτητα.

- **Mobile Commerce (M-Commerce):** Το m-commerce ή κινητό εμπόριο είναι μια επέκταση του ηλεκτρονικού εμπορίου. Με απλά λόγια, η συναλλαγή γίνεται πλέον διαδικτυακά και ειδικά μέσω κινητής συσκευής. Το m-commerce ήταν μια εξαιρετικά αναπτυσσόμενη τάση τα τελευταία τρία χρόνια και θα συνεχίσει να είναι και το 2022. Μιας και ο COVID ώθησε το κινητό εμπόριο, όλο και περισσότεροι χρήστες το έχουν υιοθετήσει, πράγμα που σημαίνει, ότι η τάση των αγορών μέσω κινητών συσκευών δεν θα σταματήσει σύντομα.

- **Mobile wallets**: Ως ασφαλής και βολική επιλογή για την πραγματοποίηση αγορών, τα ψηφιακά «πορτοφόλια» χρησιμοποιούνται όλο και περισσότερο από τους σύγχρονους καταναλωτές. Σήμερα όμως, οι περισσότερες τράπεζες έχουν επίσης το δικό τους κινητό «πορτοφόλι», με το οποίο μπορεί να πραγματοποιείται εύκολα κάθε είδους χρηματοοικονομικών συναλλαγών, όπως πληρωμές λογαριασμών, ηλεκτρονικές μεταφορές, ηλεκτρονικές αγορές, ακόμη και να χρησιμοποιείται σε σούπερ μάρκετ και φυσικά καταστήματα ως αντικατάσταση της κάρτας. Η χρήση ανέπαφων πληρωμών μέσω κινητών «πορτοφολιών» αυξήθηκε κατά τη διάρκεια του COVID και η τάση θα συνεχιστεί, καθώς ο αριθμός τέτοιων «πορτοφολιών» θα αυξάνεται.

- **IoT and Cloud**: Η τεχνολογία Διαδικτύου των πραγμάτων (IoT) και τα έξυπνα αντικείμενα που συνδέονται με κινητά υπάρχουν εδώ και χρόνια, αλλά η αγορά αυξάνεται και οι δαπάνες για το IoT προβλέπεται να φτάσουν τα 1,1 τρισεκατομμύρια δολάρια έως το 2023, σύμφωνα με την Statista. Ο μεγαλύτερος μοχλός πίσω από την υιοθέτηση του cloud και του IoT είναι η ασφάλεια, μια αυξανόμενη ανησυχία για τις επιχειρήσεις. Με περισσότερα από 120 δισεκατομμύρια δολάρια, που δαπανήθηκαν για την ασφάλεια πληροφορικής το 2019 παγκοσμίως, είναι εύκολο να καταλάβει κανείς γιατί οι εταιρείες αναζητούν άλλες λύσεις. Το IoT και το cloud προσφέρουν άλλα οφέλη, όπως μειωμένο λειτουργικό κόστος, βελτιωμένη απόδοση και αυξημένες συνδέσεις με άλλες πλατφόρμες μέσω API.

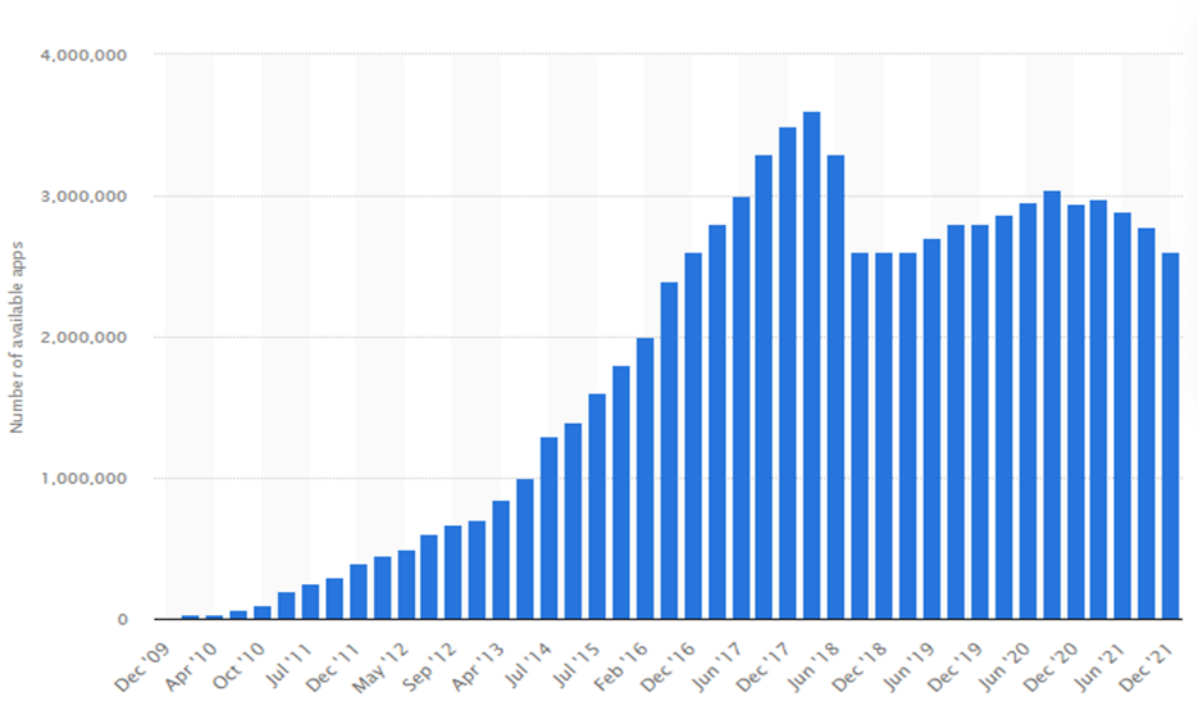
- **Wearables**: Η Statista προβλέπει ότι θα υπάρχουν 1,1 δισεκατομμύρια συνδεδεμένες φορητές συσκευές το 2022. Τα Wearables είναι ένας άλλος τρόπος διευκόλυνσης των χρηστών. Η δυνατότητα λήψης ειδοποιήσεων και μηνυμάτων στο smartwatch τους, ήταν η πιο συχνή λειτουργία των wearables για τους χρήστες των ΗΠΑ (Statista). Στην αγορά φορητών συσκευών, η παρακολούθηση της φυσικής κατάστασης έχει δει μια θετική και ανοδική τάση στη ζήτηση, με την αύξηση της ευαισθητοποίησης για την υγεία του γενικού καταναλωτικού πληθυσμού.

Με τον COVID-19 να επιταχύνει περαιτέρω την τάση των καταναλωτών να μετακινούν μεγάλο μέρος της ζωής τους στο Διαδίκτυο, υπάρχει μια νέα ώθηση για την παροχή πιο εξατομικευμένων εμπειριών σε κάθε καταναλωτή. Οι τάσεις ανάπτυξης εφαρμογών για κινητά για το 2022 αντικατοπτρίζουν αυτόν τον ψηφιακό μετασχηματισμό και επικεντρώνονται στην ικανοποίηση των χρηστών.

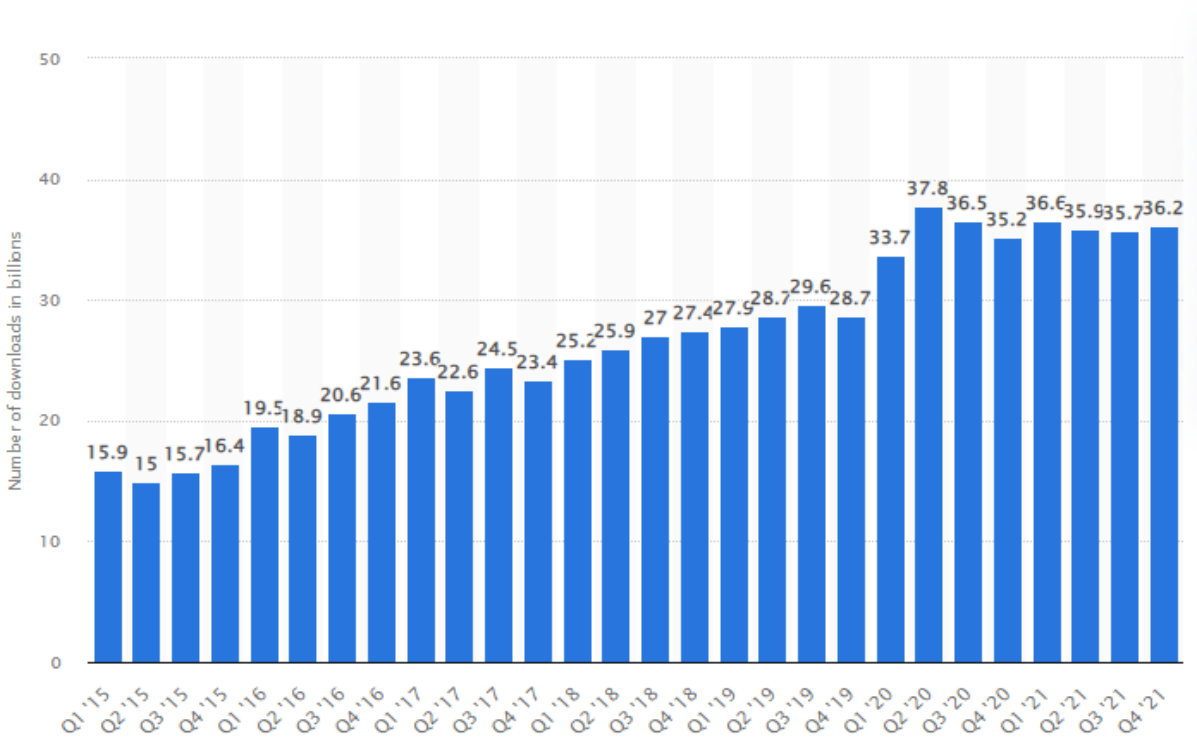
Οι αυξανόμενες απαιτήσεις των χρηστών, οδηγούν στην ανταγωνιστικότητα των εταιρειών, για αύξηση των χαρακτηριστικών των smartphones, με αποτέλεσμα την πολυπλοκότητά τους. Ο ανταγωνισμός στα ασύρματα δίκτυα και η αύξηση της αγοράς κινητών εφαρμογών, τις κάνουν αυτόματα έναν τομέα ανάπτυξης με μεγάλο ανταγωνισμό. Η συνεχόμενη αυτή αύξηση, οδήγησε στη δημιουργία της Οικονομίας

Εφαρμογών, που συνεχώς αυξάνεται και παίρνει τροφή από τις διαφημίσεις και τις πωλήσεις άλλων εφαρμογών.

Τα στατιστικά δεδομένα, σύμφωνα με την Statista, μας δείχνουν μια ραγδαία ανάπτυξη. Στο Google Play Store, οι διαθέσιμες εφαρμογές τον Ιούλιο του 2014 ήταν 1.3 εκατομμύρια, ενώ τον Μάρτιο του 2018 έφτασαν στα 3.6 εκατομμύρια. Ακολούθησε μια πτώση τα επόμενα χρόνια (Μάρτιος του 2019 στα 2.6 εκατομμύρια), αλλά με την εμφάνιση του COVID 19, βλέπουμε ότι υπήρξε εκ νέου μια αύξηση (Σεπτέμβριος του 2020 στα 3 εκατομμύρια), πριν αρχίσει πάλι η φθήνουσα πορεία λόγω κορεσμού.

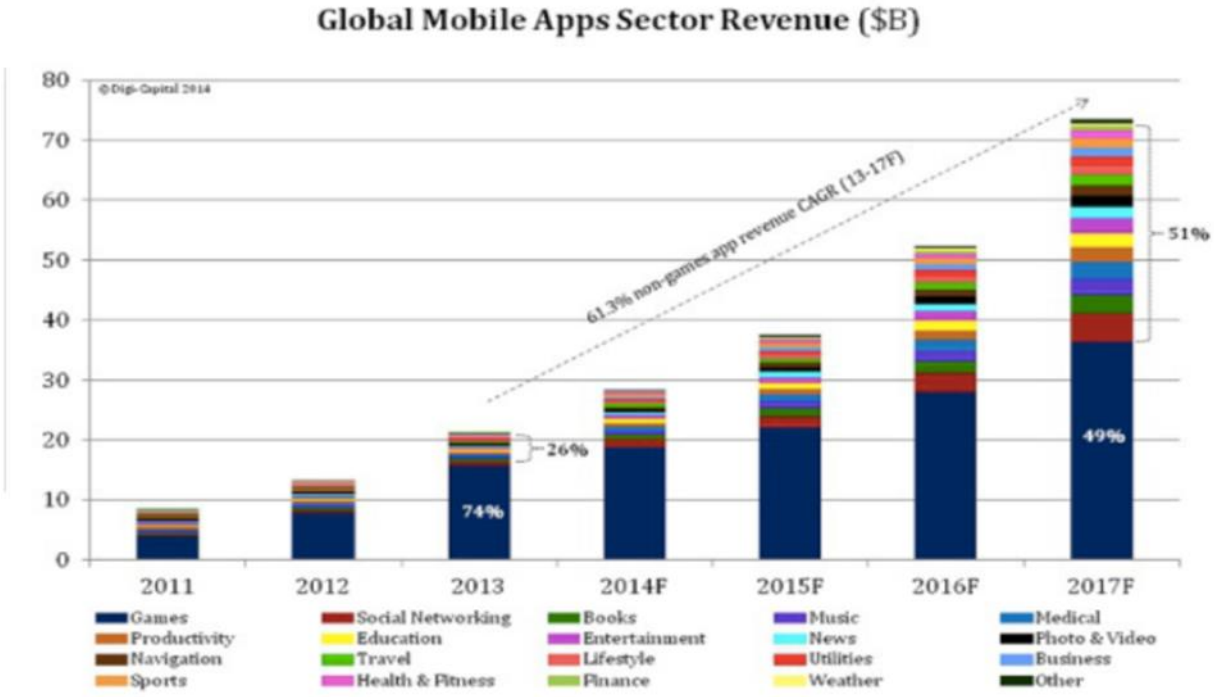


Οι σχετικοί δείκτες, δηλώνουν μια σταθερή άνοδο τα τελευταία χρόνια, αναφορικά με την απήχηση των εφαρμογών στο κοινό, φτάνοντας στο μέγιστο το δεύτερο τρίμηνο του 2020 (στην αρχή εγκλεισμού λόγω COVID) και μια σταθεροποίηση σε αρκετά μεγάλα νούμερα από το επόμενο τρίμηνο μέχρι και σήμερα (Statista 2021).



Εικόνα 2: Απήχηση Εφαρμογών στο Κοινό

Με το παρακάτω διάγραμμα, δικαιολογούμε την κερδοφορία της Οικονομίας Εφαρμογών. Καταλαβαίνουμε επίσης, τον μεγάλο αριθμό εργατικού δυναμικού που απασχολεί, καθώς και την εξασφάλιση μεγάλων εσόδων (Zinevych 2014).



Εικόνα 3: Μεγέθος της Αγοράς των Εφαρμογών

2.3 Ζητήματα Ιδιωτικότητας

Οι «έξυπνες» κινητές συσκευές που έχουν κατακλύσει τον κόσμο, έχουν σοβαρά ζητήματα ιδιωτικότητας, τα οποία ωφείλονται στις εφαρμογές. Αρχικά, υπάρχουν οι προ-εγκαταστημένες εφαρμογές, οι οποίες διαφέρουν ανάλογα με τον κατασκευαστή της κινητής συσκευής και που τις περισσότερες φορές ο χρήστης δεν μπορεί να τις απεγκαταστήσει. Κάποιες από αυτές τις εφαρμογές, συλλέγουν δεδομένα και παρακολουθούν το χρήστη χωρίς την άδειά του. Άλλες απ΄αυτές, είναι συνδεδεμένες με κακόβουλα λογισμικά, που πιθανόν να αποτελούν απειλή ασφάλειας για το χρήστη.

Το μεγαλύτερο πρόβλημα ιδιωτικότητας όμως, έγγειται αλλού. Στην κατανόηση αυτών των ζητημάτων, θα μας βοηθήσει μια μελέτη για το Smartphone Guidelines Tool, που διεξήχθη από την European Union Agency for Cybersecurity (ENISA) [8], στο πλαίσιο της έρευνας για την ασφάλεια και την ιδιωτικότητα των δεδομένων στις εφαρμογές για κινητά. Η μελέτη αυτή, συγκεντρώνει όλα εκείνα τα σημεία που απαιτούν προσοχή στην ανάπτυξη και συντήρηση εφαρμογών για κινητά, καθώς και προτάσεις για βελτιώσεις στις τρέχουσες διαδικασίες που ακολουθούνται κατά τη διάρκεια του κύκλου ζωής ανάπτυξης εφαρμογών. Ο ENISA, είναι ενας οργανισμός αφιερωμένος στην επίτευξη ενός υψηλού επιπέδου κυβερνοασφάλειας σε όλη την Ευρώπη. Συμβάλλει στην πολιτική της Ευρωπαϊκής Ένωσης στον κυβερνοχώρο, ενισχύει την αξιοπιστία των ICT προϊόντων, των υπηρεσιών και των διαδικασιών με συστήματα πιστοποίησης κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις αυριανές προκλήσεις στον κυβερνοχώρο.

Λαμβάνοντας υπόψη τη συνεχή και καθημερινή χρήση των κινητών τηλεφώνων από δισεκατομμύρια χρήστες, όπως επίσης και τον όγκο των δεδομένων που κυκλοφορούν μέσω αυτών, είναι απαραίτητο να μελετηθούν οι παράμετροι ασφαλείας που εφαρμόζονται σε όλο τον κύκλο ανάπτυξης μιας εφαρμογής για κινητά, καθώς και η συμμόρφωση με τις οδηγίες του GDPR (θα αναλυθεί παρακάτω). Αναλύοντας όλες τις σύγχρονες και ευέλικτες μεθοδολογίες ανάπτυξης, τις ευθύνες και τις διαδικασίες και γενικά ολόκληρο το οικοσύστημα εφαρμογών για κινητά, η μελέτη εντοπίζει τα κενά και προτείνει πιθανούς τρόπους για την επέκταση της κάλυψης, ώστε να συμπεριλάβει απαιτήσεις ιδιωτικότητας και προστασίας δεδομένων. Τα κύρια συμπεράσματα που προέκυψαν από αυτή τη μελέτη, με πρόσθετες συστάσεις για τη βελτίωση της προστασίας της ιδιωτικότητας των δεδομένων σε κινητά είναι:

- Παροχή καθοδήγησης στους προγραμματιστές εφαρμογών, σχετικά με τον τρόπο εφαρμογής των νομικών απαιτήσεων
- Ανάγκη για επεκτάσιμες μεθοδολογίες και βέλτιστες πρακτικές, για την προστασία δεδομένων από τον σχεδιασμό
- Ένα πλαίσιο DPIA για εφαρμογές για κινητά
- Βελτίωση της ιδιωτικότητας και της χρηστικότητας στο οικοσύστημα προγραμματιστών (όπως βιβλιοθήκες, API κ.λπ.)
- Απευθύνεται σε ολόκληρο το οικοσύστημα εφαρμογών για κινητά

Πριν από αυτό, υπάρχει μια ολοκληρωμένη ανάλυση για τους κινδύνους ιδιωτικότητας και προστασίας δεδομένων των εφαρμογών για κινητά, με βάση τη φύση των φορητών συσκευών και τις ιδιαιτερότητες ως προς την ανάπτυξη και την κατανομή του περιβάλλοντος των κινητών. Η ποικιλία των δεδομένων, οι πολλαπλοί αισθητήρες, οι διαφορετικοί τύποι αναγνωριστικών, οι συνεχώς συνδεδεμένες συσκευές, η περιορισμένη φυσική ασφάλεια και οι περιορισμένες διεπαφές χρήστη είναι μόνο μερικοί από τους λόγους που αυξάνουν τους κινδύνους προστασίας δεδομένων στα κινητά. Η χρήση τρίτων (3rd party software) είναι επίσης ένας από αυτούς τους κινδύνους, καθώς

οι περισσότερες εφαρμογές για κινητά «γράφονται» συνδυάζοντας διάφορες λειτουργίες που αναπτύχθηκαν από άλλες εταιρείες. Αυτές οι βιβλιοθήκες τρίτων, βοηθούν τους προγραμματιστές, για παράδειγμα να παρακολουθούν την αφοσίωση των χρηστών (analytics), να συνδέονται σε κοινωνικά δίκτυα και να παράγουν έσοδα από την προβολή διαφημίσεων. Ωστόσο, εκτός από τις προβλεπόμενες υπηρεσίες, οι βιβλιοθήκες μπορούν επίσης να συλλέγουν προσωπικά δεδομένα για δική τους χρήση. Οι ιδιοκτήτες των βιβλιοθηκών, μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να δημιουργήσουν λεπτομερή ψηφιακά προφίλ χρηστών, συνδυάζοντας τα δεδομένα που συλλέγουν από διαφορετικές εφαρμογές για κινητά. Επιπλέον, αυτές οι βιβλιοθήκες είναι συχνά ιδιόκτητες και κλειστού κώδικα και έτσι δεν μπορούν να αναλυθούν εύκολα. Συνεπώς, είναι σύνηθες ένας προγραμματιστής εφαρμογών για κινητά να μην κατανοεί πλήρως τα δεδομένα που πράγματι συλλέγουν αυτές οι υπηρεσίες. Περαιτέρω ανάλυση των τρίτων μερών, θα υπάρξει σε επόμενη ενότητα.

Στο περιβάλλον εφαρμογών για κινητά, όταν συλλέγονται δεδομένα για ή από μια κινητή συσκευή, η προσωπική φύση της χρήσης κινητής συσκευής συνεπάγεται ότι τέτοια δεδομένα πρέπει να θεωρούνται προσωπικά, σύμφωνα με την έννοια του GDPR. Έτσι, προσωπικά δεδομένα, δεν χαρακτηρίζονται μόνο τα δεδομένα της συσκευής που είναι προσωπικά και ιδιωτικά από τη φύση τους, όπως φωτογραφίες, μηνύματα, email, κ.α. Χαρακτηρίζονται επίσης, και δεδομένα που σχετίζονται με τη συσκευή, όπως αναγνωριστικά συσκευών, περιβαλλοντικές πτυχές, όπως η τοποθεσία της συσκευής και τα δεδομένα που σχετίζονται με τη χρήση της, συμπεριλαμβανομένων των αρχείων καταγραφής που περιέχουν δεδομένα χρήσης, τα οποία σχετίζονται σε συγκεκριμένες εφαρμογές. Μόλις ένας προγραμματιστής εφαρμογών συλλέξει (και επεξεργαστεί περαιτέρω) δεδομένα από και προς τη συσκευή και τον χρήστη της, συμπεριλαμβανομένων των μεταδεδομένων που σχετίζονται με τη συσκευή και τη συμπεριφορά του χρήστη, «πυροδοτεί» όλες τις βασικές απαιτήσεις προστασίας δεδομένων του GDPR. Εάν τα προσωπικά δεδομένα είναι πλήρως ανώνυμα, το πλαίσιο προστασίας δεδομένων δεν εφαρμόζεται, επειδή τα ανώνυμα προσωπικά δεδομένα είναι πανομοιότυπα με κάθε άλλο τύπο δεδομένων.

Κατά την πρόσβαση σε ευαίσθητα δεδομένα, ισχύουν αυστηρότερες απαιτήσεις βάσει του άρθρου 9 του GDPR. Οι σχετικές ειδικές κατηγορίες δεδομένων περιλαμβάνουν δεδομένα που σχετίζονται με φυλετική ή εθνική καταγωγή, πολιτικές απόψεις, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, γενετικά βιομετρικά δεδομένα και δεδομένα υγείας ή δεδομένα σχετικά με τη σεξουαλική ζωή ή τις σεξουαλικές προτιμήσεις ενός φυσικού προσώπου. Όταν η χρήση μιας εφαρμογής έχει ως αποτέλεσμα την επεξεργασία τέτοιων ευαίσθητων δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίσει ότι υπάρχει ρητή συγκατάθεση του χρήστη για την επεξεργασία αυτών των δεδομένων για συγκεκριμένους σκοπούς (εκτός αν συντρέχει κάποια από άλλες προϋποθέσεις, όπως ανάγκη διαφύλαξης ζωτικού συμφέροντος του χρήστη). Ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να συμμορφώνεται με τις κεντρικές νομικές υποχρεώσεις του GDPR όσον αφορά τη νόμιμη, δίκαιη και διαφανή επεξεργασία δεδομένων προσωπικού χαρακτήρα. Συνήθως, ο πάροχος της εφαρμογής θα χαρακτηρίζεται ως ο κύριος υπεύθυνος της επεξεργασίας προσωπικών δεδομένων, στο βαθμό που η εφαρμογή επεξεργάζεται τα προσωπικά δεδομένα των χρηστών για δικούς της σκοπούς. Σε πολλές περιπτώσεις, ο προγραμματιστής της εφαρμογής μπορεί να είναι ο ίδιος με τον πάροχο εφαρμογών, ενεργώντας έτσι ως υπεύθυνος επεξεργασίας δεδομένων, αλλά αυτό δε συμβαίνει πάντα, καθώς είναι δυνατό να έχει σύμβαση ανάπτυξης εκτός του οργανισμού. Σε ορισμένες περιπτώσεις, ενδέχεται να εμπλέκονται περισσότεροι από ένας ελεγκτές στην επεξεργασία προσωπικών δεδομένων στο πλαίσιο μιας εφαρμογής. Αυτό θα συμβαίνει, όταν μια εφαρμογή ενσωματώνει άλλες λειτουργικότητες (που βασίζονται σε δεδομένα) στην εφαρμογή,

όπως έναν τρίτο πάροχο υπηρεσιών (3rd party) για έλεγχο ταυτότητας χρηστών ή δικτύων διαφημίσεων για παροχή εσόδων. Επιπλέον, το λειτουργικό σύστημα μπορεί να συλλέγει δεδομένα κατά την χρήση των εφαρμογών.

Οι ευρωπαϊκές ρυθμιστικές αρχές προστασίας δεδομένων έχουν ερμηνεύσει τους ισχύοντες κανόνες, ώστε να υπονοείται ότι ο πάροχος ή ο προγραμματιστής της εφαρμογής (στον ρόλο του υπεύθυνου επεξεργασίας δεδομένων) έχει τη νομική ευθύνη σχετικά με την επεξεργασία δεδομένων τρίτων, καθώς και να συμβάλλει στη διευκόλυνσή της. Το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ), προσφάτως έχει αποφανθεί επί του θέματος για συγκεκριμένη περίπτωση[1], καταδεικνύοντας ότι η αλληλεπίδραση μεταξύ ενός υπεύθυνου επεξεργασίας δεδομένων (εν προκειμένω, κοινωνικού δικτύου) και ενός τρίτου μέλους, που παρέχει υπηρεσία, η οποία αξιοποιείται από τον αρχικό υπεύθυνο επεξεργασίας, συνεπάγεται από κοινού ευθύνη, βάσει της νομοθεσίας της ΕΕ για τη προστασία δεδομένων. Σε κάθε περίπτωση, είναι ένα ζήτημα για το οποίο σαφώς απαιτείται περαιτέρω καθοδήγηση, σχετικά με την ακριβή ευθύνη του πρώτου μέρους (1st party) να διασφαλίσει ότι τρίτα μέρη (3rd parties) επεξεργάζονται δεδομένα προσωπικού χαρακτήρα νόμιμα, δίκαια και με διαφάνεια. Ένα από τα βασικά προβλήματα στο περιβάλλον των κινητών, είναι ότι οι αρχιτεκτονικές αδειών, δεν προβλέπουν τη δυνατότητα χορήγησης άδειας στην εφαρμογή και στα ενσωματωμένα τρίτα μέρη χωριστά. Μερικές φορές, μια εφαρμογή μπορεί να ζητήσει πρόσβαση σε συγκεκριμένο τύπο δεδομένων στη συσκευή, μόνο επειδή ένα τρίτο μέρος θέλει ή χρειάζεται να αποκτήσει πρόσβαση σε αυτά τα δεδομένα. Οι δεσμεύσεις διαφάνειας, απαιτούν από τους προγραμματιστές εφαρμογών να είναι πλήρως διαφανείς σχετικά με την επεξεργασία των τρίτων μερών (3rd parties), την οποία διευκολύνει η εφαρμογή και αυτές οι λειτουργίες επεξεργασίας πρέπει να έχουν επαρκή νομική βάση.

2.4 Ασφάλεια

Για να υπάρξει θετική αξιολόγηση στις εφαρμογές κινητών συσκευών, είναι απαραίτητο να πληρούνται συγκεκριμένοι παράγοντες. Ένας από αυτούς και ίσως αυτός που δίνει το μεγαλύτερο θετικό πρόσιμο, είναι το επίπεδο ασφαλείας που δίνουν για τα δεδομένα που διαχειρίζονται. Η ασύρματη πρόσβαση, που κάνει συνεχώς άλματα εξέλιξης, η συνδεσιμότητα των κινητών συσκευών που είναι καθημερινή και συνεχόμενη, μεγαλώνουν τον κίνδυνο για κλοπή και κακόβουλες επιθέσεις από χρήστες, που δεν έχουν καμία εξουσιοδότηση. Αυτό οδηγεί τους προγραμματιστές των εφαρμογών, να φροντίζουν όχι μόνο να υπάρχει ασφάλεια στην πλατφόρμα που θα χρησιμοποιήσουν, αλλά και να δημιουργήσουν στην εκάστοτε εφαρμογή τους, κρυπτογραφημένες ενσωματωμένες λειτουργίες, με τις οποίες θα παρέχουν προστασία δεδομένων για τον εκάστοτε χρήστη.

Οι κινητές συσκευές για την κάλυψη των αναγκών του χρήστη, είναι συνεχώς συνδεδεμένες με υπηρεσίες cloud, με αγορές και πληρωμές, με τραπεζικές συναλλαγές και διάφορες άλλες υπηρεσίες, οι οποίες γίνονται εύκολα επιρρεπείς σε απειλές, εάν δεν πληρούνται οι προδιαγραφές ασφαλείας.

[1] Βλ. περιπτωση για FahionID, απόφαση ΔΕΕ της 29ης Ιουλίου 2019 στην υπόθεση C-40/17, Fashion ID, ECLI:EU:C:2019:629.

Κυκλοφορούν πολλοί και διάφοροι τύποι κακόβουλων επιθέσεων που αφορούν τις κινητές συσκευές. Κάποιοι από τους πιο γνωστούς είναι οι εξής:

- Οι ιοί, κατεβάζοντας και ενεργοποιώντας ο χρήστης κάποια εφαρμογή που είναι μολυσμένη, αυτομάτως ο ιός εισχωρεί στον κώδικά της και υποκλέπτει προσωπικά στοιχεία, όπως είναι ο κωδικός πρόσβασης κ.α..

- Botnet, εδώ μιλάμε για πολλούς υπολογιστές, οι οποίοι είναι μολυσμένοι με το ίδιο κακόβουλο λογισμικό και κάνουν συγχρονισμένη επίθεση, με μόνο σκοπό την εκτέλεση επιθέσεων Distributed Denial-of-Service (DDoS) και να υποκλέψουν προσωπικά δεδομένα. Αυτό μπορεί να επιτευχθεί συνήθως μέσω εισερχόμενων e-mail που έχουν επισυναπτόμενο μολυσμένο αρχείο, μέσω εφαρμογών ή μέσω μολυσμένων ιστοστελίδων, επιτρέποντας στον εισβολέα να έχει πρόσβαση στη συσκευή και στη σύνδεσή της.

- Phishing, εδώ ο επιτιθέμενος παριστάνει ότι είναι κάποιος άλλος, φυσικά αξιόπιστος, και βασιζόμενος στην άγνοια του χρήστη, προσπαθεί με έξυπνους τρόπους να του αποσπάσει προσωπικά δεδομένα όπως τραπεζικούς κωδικούς κ.α. (Kaspersky, 2020). Στην περίπτωση αυτή επιτίθενται μέσω άμεσου μυνήματος την ώρα που ο χρήστης κάνει κάποια πλοήγηση και τον οδηγούν σε σύνδεσμο, ο οποίος ενώ φαίνεται αξιόπιστος, στην ουσία τον οδηγεί σε κακόβουλη ιστοσελίδα.

- Spyware, είναι ένας τύπος κακόβουλου λογισμικού που εγκαθίσταται στον υπολογιστή ή στην κινητή συσκευή του χρήστη, χωρίς τη συγκατάθεσή του, το οποίο περισυλλέγει και μεταφέρει σε εξωτερικές πηγές ευαίσθητα προσωπικά δεδομένα όπως μηνύματα, φωτογραφίες, στοιχεία αλληλογραφίας, πληροφορίες τοποθεσίας και διάφορα άλλα.

Έχοντας ήδη μιλήσει για τα ζητήματα ιδιωτικότητας και τώρα για τους κινδύνους ασφαλείας, καταλαβαίνουμε ότι όσο χρήσιμες και αναγκαίες μπορεί να είναι οι έξυπνες εφαρμογές κινητών συσκευών, άλλο τόσο επικίνδυνες μπορούν να γίνουν αν δεν πληρούνται συγκεκριμένοι κανόνες. Θα συνεχίσουμε να αναλύουμε κάποια τέτοια ζητήματα στην πορεία της διπλωματικής.

2.5 Trackers και Third Parties

Ένας «ιχνηλάτης» (tracker), είναι ένα "κομμάτι" λογισμικού που είναι υπεύθυνο για τη συλλογή πληροφοριών για το άτομο που χρησιμοποιεί μια εφαρμογή ή σχετικά με τις χρήσεις ή το περιβάλλον αυτού του ατόμου. Ένας ιχνηλάτης, διανέμεται πολύ συχνά από μία εταιρεία με τη μορφή SDK (Software Development Kit), ένα είδος έτοιμου προς χρήση εργαλείου, που προορίζεται για να διευκολύνει το έργο των ανθρώπων που αναπτύσσουν εφαρμογές. Σημειώστε, ότι υπάρχουν οι λεγόμενοι ιχνηλάτες ανοιχτού κώδικα, των οποίων ο κώδικας είναι διαθέσιμος και μπορεί να αναζητηθεί από τον καθένα. Δεν έχουν όλοι οι ιχνηλάτες την ίδια λειτουργικότητα και μπορούν να παρουσιάζουν διαφορετικά επίπεδα εισβολής (απορρήτου).

- **Crash reporters:** αυτοί οι trackers ειδικεύονται στην αναφορά σφαλμάτων εφαρμογών. Με άλλα λόγια, στόχος τους είναι να ειδοποιήσουν τους προγραμματιστές εφαρμογών, ότι αντιμετωπίστηκε ένα πρόβλημα σε μια

εφαρμογή. Ως εκ τούτου, οι πληροφορίες που συλλέγονται κατά τη στιγμή του «κρασαρίσματος» της εφαρμογής, θα επιτρέψουν στον προγραμματιστή να διορθώσει το σφάλμα.

- **Analytics:** αυτοί οι trackers προορίζονται για να συλλέγουν τη χρήση των δεδομένων και να επιτρέπουν στον προγραμματιστή να έχει καλύτερη γνώση του «κοινού» του, όπως να ξέρει ποια σελίδα επισκέφτηκαν ή πόσο καιρό έμειναν σε μια συγκεκριμένη περιοχή της σελίδας.

- **Profiling:** στόχος αυτών των trackers είναι να συγκεντρώσουν όσο το δυνατόν περισσότερες πληροφορίες για τον χρήστη της εφαρμογής, έτσι ώστε να δημιουργήσει ένα εικονικό προφίλ. Για το σκοπό αυτό, ο tracker θα εστιάσει για παράδειγμα στο ιστορικό περιήγησης ή στη λίστα των εγκατεστημένων εφαρμογών κ.α.

- **Identication:** αυτοί οι trackers είναι υπεύθυνοι για τον προσδιορισμό της ψηφιακής ταυτότητας των χρηστών. Αυτή η ταυτότητα, μπορεί να αναφέρεται σε μια επίσημη ταυτότητα ή σε αφηρημένα αναγνωριστικά (ψευδώνυμο κ.α). Ο στόχος θα είναι για παράδειγμα, να μπορέσουν να συσχετιστούν οι εντός και εκτός σύνδεσης δραστηριότητες του ατόμου.

- **Ads:** αυτοί οι trackers στοχεύουν στην ταυτοποίηση του χρήστη της εφαρμογής, για να του προβάλλουν στοχευμένες διαφημίσεις. Αυτό είναι δυνατό, μόνο εάν ο χρήστης έχει ήδη ένα ψηφιακό προφίλ. Ο στόχος της ύπαρξης ενός τέτοιου tracker, είναι η δημιουργία εσόδων για την εφαρμογή τους μέσω διαφήμισης.

- **Location:** αυτοί οι trackers έχουν σχεδιαστεί για να προσδιορίζουν τη γεωγραφική θέση της κινητής συσκευής. Για να γίνει αυτό, αυτός ο τύπος tracker εκμεταλλεύεται αρκετούς αισθητήρες, όπως τσιπ GPS, περιβάλλουσες κεραίες κινητής τηλεφωνίας, δίκτυα Wi-Fi που υπάρχουν στην περιοχή, κοντινά Bluetooth beacon ή ακόμα και συγκεκριμένους ήχους που μεταδίδονται από μεγάφωνα.

Όσον αφορά τη λήψη απόφασης για την προσθήκη ενός tracker σε μια εφαρμογή ή ποιοι trackers θα προστεθούν, μπορούν να προκύψουν δύο πιθανά σενάρια. Στην πρώτη περίπτωση, ο οργανισμός που κατέχει το προϊόν αναθέτει την ανάπτυξη της εφαρμογής σε μια τρίτη εταιρεία. Η σύμβαση προσδιορίζει τι πρέπει να εκτελέσει η εφαρμογή και ποιες τεχνολογίες χρησιμοποιούνται για να γίνει αυτό. Μερικές φορές, ο εξωτερικός συνεργάτης, ήδη έχει ένα πρότυπο εφαρμογής που επαναχρησιμοποιεί για κάθε νέα εφαρμογή. Σε μία τέτοια κατάσταση, που όλες οι εφαρμογές που αναπτύσσονται θα περιλαμβάνουν αυτούς τους trackers, είτε καθορίζεται στη σύμβαση προγραμματισμού, είτε όχι. Στη δεύτερη περίπτωση, ο οργανισμός που κατέχει το προϊόν, αναπτύσσει την εφαρμογή εσωτερικά. Όταν συμβαίνει αυτό, οι εργαζόμενοί του υπό την έγκριση/εξουσιοδότηση της Διοίκησης, είναι υπεύθυνοι να αποφασίσουν εάν θέλουν ή όχι να συμπεριλάβουν ορισμένους τύπους tracker.

Όπως αναφέρθηκε στο [25], η συντριπτική πλειοψηφία των εφαρμογών χρησιμοποιεί βιβλιοθήκες τρίτων. Αυτές οι βιβλιοθήκες αποκτούν τα ίδια δικαιώματα πρόσβασης με την εφαρμογή που τις ενσωματώνει (host application). Ωστόσο, η χρήση τέτοιων βιβλιοθηκών ενδέχεται να ενέχει κάποιους κινδύνους για το απόρρητο των χρηστών. Επιπλέον, όπως αναλύεται στο [26], η χρήση πολλών δημοφιλών βιβλιοθηκών από πολλές διαφορετικές έξυπνες εφαρμογές, μπορεί να έχει ως αποτέλεσμα τη λεγόμενη συμπαιγνία εντός της βιβλιοθήκης. Με απλά λόγια, σε περίπτωση που μια βιβλιοθήκη

ενσωματώνεται σε πολλές εφαρμογές, εντός μιας συσκευής, μπορεί να συνδυάσει κατάλληλα το σύνολο αδειών που δίνονται από κάθε εφαρμογή, έτσι ώστε να αξιοποιήσει τα αποκτηθέντα προνόμια και να συγκεντρώσει μεγάλο όγκο προσωπικών πληροφοριών, χωρίς τη ρητή συγκατάθεση του χρήστη. Πιο συγκεκριμένα, όπως αναφέρεται επίσης στο [26], το τρέχον μοντέλο ασφάλειας Android, το οποίο δεν υποστηρίζει τον διαχωρισμό των προνομίων μεταξύ των εφαρμογών και των ενσωματωμένων βιβλιοθηκών, διευκολύνει τις ακόλουθες σχετικές απειλές απορρήτου χωρίς τη συγκατάθεση του χρήστη:

- Οι βιβλιοθήκες ενδέχεται να κάνουν κατάχρηση των προνομίων που παρέχονται στις οικοδέσποινες εφαρμογές.
- Οι βιβλιοθήκες μπορούν να παρακολουθούν τους χρήστες.
- Οι βιβλιοθήκες μπορούν να συγκεντρώνουν πολλαπλά σήματα για λεπτομερή σκιαγράφηση του προφίλ του χρήστη.

Οι υπηρεσίες τρίτων, βασίζονται συνήθως σε παραχωρημένες άδειες εφαρμογής για τη συλλογή των πληροφοριών, ορισμένες από τις οποίες μπορεί να είναι ευαίσθητου χαρακτήρα από πλευράς ιδιωτικότητας. Ενώ οι κινητές πλατφόρμες συνήθως επιτρέπουν στους χρήστες να παραχωρούν ή να απενεργοποιούν δικαιώματα για κάθε εφαρμογή, το μοντέλο αυτό έχει αρκετές ελλείψεις. Πρώτον, οι χρήστες συνήθως δεν γνωρίζουν πως με την παραχώρηση αδειών σε μια εφαρμογή, οι πληροφορίες τους ενδέχεται να συλλέγονται από υπηρεσίες τρίτων. Δεύτερον, οι χρήστες δεν ενημερώνονται για το ποιες εφαρμογές μοιράζονται τις ίδιες υπηρεσίες τρίτων. Αυτό έχει ως αποτέλεσμα να αγνοούν τα δυνητικά πλούσια δεδομένα που συγκεντρώνουν οι υπηρεσίες τρίτων. Αυτή η έλλειψη διαφάνειας, σημαίνει ότι το οικοσύστημα υπηρεσιών τρίτων, παραμένει ένα μυστήριο για τους χρήστες, τους ερευνητές και τις ρυθμιστικές αρχές, σε βαθμό που δεν έχουμε καν την πλήρη επίγνωση της ταυτότητας των μεγάλων παρόχων υπηρεσιών.

Τύποι Third-Party Apps

Υπάρχουν πολλές διαφορετικές περιπτώσεις, όπου μπορεί να συναντήσετε τον όρο "εφαρμογή τρίτου μέρους" (Third-Party App).

- Οι εφαρμογές που δημιουργήθηκαν για επίσημα καταστήματα εφαρμογών από προμηθευτές εκτός της Google (Google Play Store) ή της Apple (Apple App Store) και που ακολουθούν τα κριτήρια ανάπτυξης που απαιτούνται από αυτά τα καταστήματα εφαρμογών, είναι εφαρμογές τρίτων. Μια εγκεκριμένη εφαρμογή από έναν προγραμματιστή για μια υπηρεσία όπως το Facebook ή το Snapchat θεωρείται εφαρμογή τρίτου μέρους. Εάν το Facebook ή το Snapchat αναπτύξουν την εφαρμογή, τότε πρόκειται για εφαρμογή πρώτου κατασκευαστή.

- Οι εφαρμογές που προσφέρονται μέσω ανεπίσημων καταστημάτων εφαρμογών τρίτων ή ιστότοπων που δημιουργούνται από μέρη (parties) που δεν συνδέονται με τη συσκευή ή το λειτουργικό σύστημα, είναι επίσης εφαρμογές τρίτων. Θα πρέπει να είμαστε προσεκτικοί κατά τη λήψη εφαρμογών από οποιονδήποτε πόρο, ιδιαίτερα από ανεπίσημα καταστήματα εφαρμογών ή ιστότοπους, για να αποφύγουμε κακόβουλο λογισμικό.

- Μια εφαρμογή που συνδέεται με μια άλλη υπηρεσία (ή την εφαρμογή της), είτε για να παρέχει βελτιωμένες λειτουργίες, είτε για πρόσβαση σε πληροφορίες που σχετίζονται με το προφίλ του χρήστη, είναι μια εφαρμογή τρίτου μέρους. Ένα

παράδειγμα αυτού είναι το Quizzstar, μια εφαρμογή κουίζ τρίτου μέρους που απαιτεί άδεια για πρόσβαση σε ορισμένα μέρη ενός προφίλ στο Facebook. Αυτός ο τύπος εφαρμογής τρίτου μέρους δεν μπορεί να εγκατασταθεί. Αντίθετα, η εφαρμογή έχει πρόσβαση σε δυνητικά ευαίσθητες πληροφορίες, μέσω της σύνδεσής της με την άλλη υπηρεσία ή εφαρμογή.

Πώς τα First-Party Apps διαφέρουν από τα Third-Party Apps

Οι εφαρμογές πρώτου κατασκευαστή είναι εφαρμογές που δημιουργούνται και διανέμονται από τον κατασκευαστή της συσκευής ή τον δημιουργό λογισμικού. Μερικά παραδείγματα εφαρμογών πρώτου κατασκευαστή για το iPhone, είναι η Μουσική, τα Μηνύματα και τα Βιβλία.

Αυτό που κάνει αυτές τις εφαρμογές "πρώτου κατασκευαστή", είναι ότι οι εφαρμογές δημιουργούνται από έναν κατασκευαστή για τις συσκευές αυτού του ιδίου, χρησιμοποιώντας συχνά αποκλειστικό δικό του πηγαίο κώδικα. Για παράδειγμα, όταν η Apple δημιουργεί μια εφαρμογή για μια συσκευή Apple, όπως ένα iPhone, αυτή η εφαρμογή είναι πρώτου κατασκευαστή. Για συσκευές Android, επειδή η Google είναι ο δημιουργός του λειτουργικού συστήματος Android για κινητά, παραδείγματα εφαρμογών πρώτου κατασκευαστή περιλαμβάνουν την έκδοση των εφαρμογών Google για κινητές συσκευές, όπως το Gmail, το Google Drive και το Google Chrome.

Αν μια εφαρμογή είναι πρώτου κατασκευαστή για έναν τύπο συσκευής, δεν σημαίνει ότι δεν μπορεί να υπάρχει μια έκδοση αυτής της εφαρμογής διαθέσιμη για άλλους τύπους συσκευών. Για παράδειγμα, οι εφαρμογές Google έχουν μια έκδοση που λειτουργεί σε iPhone και iPad, η οποία προσφέρεται μέσω του Apple App Store. Αυτές θεωρούνται εφαρμογές τρίτων σε συσκευές iOS.

Γιατί μερικές υπηρεσίες απαγορεύουν τα Third-Party Apps

Ορισμένες υπηρεσίες ή εφαρμογές απαγορεύουν τη χρήση εφαρμογών τρίτων για λόγους ασφαλείας. Κάθε φορά που μια εφαρμογή τρίτου μέρους αποκτά πρόσβαση σε ένα προφίλ ή άλλες πληροφορίες από έναν λογαριασμό, παρουσιάζεται κίνδυνος ασφαλείας. Οι πληροφορίες σχετικά με τον λογαριασμό ή το προφίλ μπορούν να χρησιμοποιηθούν για την παραβίαση ή την αντιγραφή του λογαριασμού. Στην περίπτωση των ανηλίκων, μπορεί να εκθέσει φωτογραφίες και λεπτομέρειες για εφήβους και παιδιά σε δυνητικά επιβλαβή άτομα.

Στο παράδειγμα του κουίζ του Facebook, έως ότου αλλάξουν τα δικαιώματα εφαρμογής στις ρυθμίσεις του λογαριασμού Facebook, η εφαρμογή κουίζ μπορεί να έχει πρόσβαση στις λεπτομέρειες του προφίλ στο οποίο της παραχωρήθηκε άδεια πρόσβασης. Εάν δεν αλλάξουν τα δικαιώματα, η εφαρμογή έχει πρόσβαση στο προφίλ του Facebook, ακόμη και αφού ο χρήστης σταματήσει να χρησιμοποιεί την εφαρμογή. Συνεχίζει να συλλέγει και να αποθηκεύει λεπτομέρειες από το προφίλ του Facebook και αυτές οι λεπτομέρειες μπορεί να αποτελούν κίνδυνο για την ασφάλεια.

Η χρήση εφαρμογών τρίτων δεν είναι παράνομη. Ωστόσο, εάν οι όροι χρήσης για μια υπηρεσία ή εφαρμογή αναφέρουν ότι δεν επιτρέπονται εφαρμογές τρίτων, η απόπειρα χρήσης μιας για σύνδεση σε αυτήν την υπηρεσία θα μπορούσε να οδηγήσει σε κλείδωμα ή απενεργοποίηση ενός λογαριασμού.

Ποιος χρησιμοποιεί Third-Party Apps

Οι εφαρμογές τρίτων έχουν ποικίλες παραγωγικές, διασκεδαστικές και ενημερωτικές χρήσεις. Υπάρχουν εφαρμογές τρίτων που διαχειρίζονται πολλούς λογαριασμούς κοινωνικών μέσων ταυτόχρονα, όπως το Hootsuite και το Buffer. Άλλες εφαρμογές τρίτων, διαχειρίζονται τραπεζικούς λογαριασμούς από φορητή συσκευή, μετρούν θερμίδες ή ενεργοποιούν μια κάμερα ασφαλείας σπιτιού.

Ανοίγουμε την οθόνη του μενού εφαρμογών στο smartphone μας και πραγματοποιούμε κύλιση στις εφαρμογές που έχουμε λάβει. Έχουμε παιχνίδια, μέσα κοινωνικής δικτύωσης ή εφαρμογές για αγορές. Οι πιθανότητες αυτές να είναι εφαρμογές τρίτων είναι πολλές.

2.6 Άδειες σε Εφαρμογές για Κινητά

Ο σκοπός μιας άδειας είναι η προστασία του απορρήτου ενός χρήστη. Οι εφαρμογές πρέπει να ζητούν άδεια πρόσβασης σε ευαίσθητα δεδομένα χρήστη (όπως επαφές και φωτογραφίες), καθώς και σε ορισμένες λειτουργίες του συστήματος (όπως κάμερα και μικρόφωνο). Ανάλογα με τη δυνατότητα, το σύστημα μπορεί να χορηγήσει την άδεια αυτόματα ή μπορεί να ζητήσει από τον χρήστη να εγκρίνει το αίτημα. Ένα κεντρικό σημείο σχεδιασμού της αρχιτεκτονικής ασφαλείας του Android, είναι ότι καμία εφαρμογή, από προεπιλογή, δεν έχει άδεια να εκτελεί λειτουργίες που θα επηρεάσουν αρνητικά άλλες εφαρμογές, το λειτουργικό σύστημα ή τον χρήστη. Αυτό περιλαμβάνει την ανάγνωση ή την εγγραφή των προσωπικών δεδομένων του χρήστη (όπως επαφές ή μηνύματα ηλεκτρονικού ταχυδρομείου), την ανάγνωση ή την εγγραφή λέξεων άλλης εφαρμογής, την εκτέλεση πρόσβασης στο δίκτυο, τη διατήρηση της συσκευής ενεργή και ούτω καθεξής. Οι βασικές αρχές ανάπτυξης για την αίτηση αδειών είναι οι εξής:

- Η ζήτηση δικαιωμάτων όταν ο χρήστης αρχίσει να αλληλεπιδρά με τη λειτουργία που το απαιτεί.

- Ο μη αποκλεισμός του χρήστη. Να παρέχεται πάντα η επιλογή ακύρωσης μιας εκπαιδευτικής διεπαφής χρήστη που σχετίζεται με την άδεια.

- Εάν ο χρήστης αρνηθεί ή ανακαλέσει μια άδεια που χρειάζεται μια λειτουργία, πρέπει να υποβαθμιστεί η εφαρμογή, έτσι ώστε ο χρήστης να μπορεί να συνεχίσει να τη χρησιμοποιεί.

- Να δίνεται προσοχή στα δικαιώματα που απαιτούνται από τις βιβλιοθήκες. Όταν περιλαμβάνεται μια βιβλιοθήκη, η εφαρμογή κληρονομεί επίσης τις απαιτήσεις άδειας. Θα πρέπει λοιπόν ο χρήστης να γνωρίζει τι περιλαμβάνεται, τις άδειες που απαιτούνται και σε τι αυτές χρησιμοποιούνται.

- Να υπάρχει διαφάνεια. Όταν γίνεται ένα αίτημα αδειών, να είναι σαφές σχετικά με την άδεια που ζητάει και για ποιόν λόγο τη ζητάει, ώστε οι χρήστες να μπορούν να δώσουν τη συγκατάθεσή τους.

- Να μην θεωρείται δεδομένη, καμία συμπεριφορά του συστήματος.

Τα δικαιώματα χωρίζονται σε διάφορα επίπεδα προστασίας, όπου το καθένα από αυτά επηρεάζεται από την απαίτηση αιτήματος άδειας χρόνου εκτέλεσης. Υπάρχουν τρία επίπεδα προστασίας που επηρεάζουν τις εφαρμογές τρίτων: τα κανονικά δικαιώματα, τα δικαιώματα υπογραφής και τα επικίνδυνα δικαιώματα:

- Τα κανονικά δικαιώματα καλύπτουν περιοχές, όπου η εφαρμογή χρειάζεται πρόσβαση σε δεδομένα ή πόρους έξω από το sandbox της εφαρμογής, με πολύ

μικρό κίνδυνο για το απόρρητο του χρήστη ή τη λειτουργία άλλων εφαρμογών. Για παράδειγμα, η άδεια ρύθμισης της ζώνης ώρας είναι μια κανονική άδεια. Εάν μια εφαρμογή δηλώνει ότι χρειάζεται μια κανονική άδεια, το σύστημα εκχωρεί αυτόματα στην εφαρμογή αυτή την άδεια κατά τον χρόνο εγκατάστασης. Το σύστημα δε ζητά από το χρήστη να χορηγήσει κανονικά δικαιώματα και οι χρήστες δε μπορούν να ανακαλέσουν αυτές τις άδειες.

- Τα δικαιώματα υπογραφής όπου το σύστημα εκχωρεί αυτές τις άδειες εφαρμογής κατά την ώρα εγκατάστασης, αλλά μόνο όταν η εφαρμογή που επιχειρεί να χρησιμοποιήσει μια άδεια έχει υπογραφεί από το ίδιο πιστοποιητικό με την εφαρμογή που ορίζει την άδεια. Κάποια δικαιώματα υπογραφής, δεν προορίζονται για χρήση από εφαρμογές τρίτων.

- Τα επικίνδυνα δικαιώματα, καλύπτουν περιοχές όπου η εφαρμογή ζητά δεδομένα ή πόρους που αφορούν προσωπικά στοιχεία του χρήστη ή θα μπορούσαν ενδεχομένως να επηρεάσουν τα αποθηκευμένα στοιχεία του χρήστη ή τη λειτουργία άλλων εφαρμογών. Για παράδειγμα, η ικανότητα ανάγνωσης των επαφών του χρήστη είναι μια επικίνδυνη άδεια. Εάν μια εφαρμογή δηλώσει ότι χρειάζεται μια επικίνδυνη άδεια, ο χρήστης πρέπει να χορηγήσει ρητά την άδεια στην εφαρμογή. Έως ότου ο χρήστης εγκρίνει την άδεια, η εφαρμογή δεν μπορεί να παρέχει λειτουργικότητα που εξαρτάται από αυτήν την άδεια.

Μόνο τα επικίνδυνα δικαιώματα απαιτούν τη σύμφωνη γνώμη του χρήστη. Ο τρόπος που ζητάει το κινητό τη χορήγηση επικίνδυνων αδειών από το χρήστη, εξαρτάται από την έκδοση του Android που εκτελείται στη συσκευή του χρήστη και την έκδοση συστήματος που στοχεύει η εφαρμογή. Η εφαρμογή πρέπει να ζητήσει από τον χρήστη να εκχωρήσει τα επικίνδυνα δικαιώματα κατά το χρόνο εκτέλεσης. Όταν η εφαρμογή ζητά άδεια, ο χρήστης βλέπει ένα παράθυρο διαλόγου συστήματος, το οποίο λέει στον χρήστη σε ποια ομάδα αδειών προσπαθεί να έχει πρόσβαση η εφαρμογή. Ο διάλογος περιλαμβάνει ένα κουμπί «Άρνηση» και ένα «Αποδοχή». Εάν ο χρήστης αρνηθεί το αίτημα άδειας, την επόμενη φορά που η εφαρμογή θα ζητήσει την άδεια, το παράθυρο διαλόγου, θα περιέχει ένα πλαίσιο ελέγχου που όταν είναι επιλεγμένο, υποδεικνύει ότι ο χρήστης δεν θέλει να του ζητηθεί ξανά η άδεια. Εάν ο χρήστης επιλέξει το πλαίσιο «Να μην ερωτηθεί ξανά» και πατήσει «Άρνηση», το σύστημα δεν ζητάει πλέον άδεια από τον χρήστη. Ακόμα κι αν ο χρήστης παραχωρήσει στην εφαρμογή την άδεια που του ζητήθηκε, δεν μπορεί πάντα να βασίζεται στο ότι την έχει. Οι χρήστες έχουν επίσης την επιλογή ενεργοποίησης και απενεργοποίησης δικαιωμάτων ένα προς ένα στις ρυθμίσεις συστήματος. Παρακάτω αναφέρονται μερικές από τις επικίνδυνες άδειες, μαζί με τους λόγους που τις καθιστούν επικίνδυνες.

- **Ημερολόγιο:** Εάν ο χρήστης χρησιμοποιεί ενεργά τον ψηφιακό προγραμματιστή ημέρας, η εφαρμογή θα γνωρίζει τα πάντα για την καθημερινότητά του και μπορεί να τα μοιραστεί με εγκληματίες.

- **Κάμερα:** Μια εφαρμογή μπορεί να καταγράφει κρυφά βίντεο ή να τραβήξει φωτογραφίες ανά πάσα στιγμή.

- **Επαφές:** Μια εφαρμογή μπορεί να παγιδεύσει ολόκληρο το βιβλίο διευθύνσεών του. Αυτά τα δεδομένα είναι πολύ ελκυστικά σε spammers και απατεώνες. Αυτή η άδεια παρέχει επίσης πρόσβαση στη λίστα όλων των λογαριασμών που χρησιμοποιεί στις εφαρμογές αυτής της συσκευής, όπως Google, Facebook, Instagram και άλλους σαν αυτούς.

- **Τοποθεσία:** Η εφαρμογή ξέρει πού βρίσκεται ανά πάσα στιγμή.

- **Μικρόφωνο:** Η εφαρμογή μπορεί να καταγράψει όλα όσα συμβαίνουν κοντά στο τηλέφωνό του, όλες του τις συζητήσεις. Όχι μόνο όταν μιλάει στο τηλέφωνο, αλλά όλη μέρα.

- **Τηλέφωνο:** Όταν εκχωρεί άδειες τηλεφώνου, επιτρέπει στην εφαρμογή να πάρει σχεδόν οποιαδήποτε ενέργεια που σχετίζεται με φωνητικές επικοινωνίες. Η εφαρμογή θα γνωρίζει πότε και με ποιον μιλάει και μπορεί να καλέσει οπουδήποτε, συμπεριλαμβανομένων των αριθμών επί πληρωμή.

- **Αισθητήρες σώματος:** Εάν χρησιμοποιεί αξεσουάρ με αισθητήρες σώματος (όχι ενσωματωμένους στο τηλέφωνο αισθητήρες κίνησης), η εφαρμογή λαμβάνει δεδομένα σχετικά με το τι συμβαίνει με το δικό του σώμα.

- **SMS:** Επιτρέπει στην εφαρμογή να λαμβάνει και να διαβάζει τα εισερχόμενα μηνύματά του και επίσης, να του στέλνει άλλα με δική του χρέωση.

- **Αποθήκευση:** Η εφαρμογή μπορεί να διαβάσει, να αλλάξει ή να αφαιρέσει τυχόν αποθηκευμένα δεδομένα στο τηλέφωνό του.

Τώρα, εάν ο χρήστης αρνηθεί ένα αίτημα άδειας, η εφαρμογή θα πρέπει να τον βοηθήσει να κατανοήσει τις συνέπειες της άρνησης αυτής. Συγκεκριμένα, η εφαρμογή θα πρέπει να ενημερώνει τους χρήστες για τις λειτουργίες που δεν δουλεύουν, λόγω της άδειας που λείπει. Παρακάτω παρατίθενται οι βέλτιστες πρακτικές για τον χειρισμό μιας άρνησης άδειας χρήστη, όπως είθισται να διατυπώνονται προς τους χρήστες:

- Καθοδηγήστε την προσοχή του χρήστη. Επισημάνετε ένα συγκεκριμένο μέρος της διεπαφής χρήστη της εφαρμογής όπου υπάρχει περιορισμένη λειτουργικότητα, επειδή η εφαρμογή δεν έχει την απαραίτητη άδεια.

- Να είναι συγκεκριμένος. Μην εμφανίζεται ένα γενικό μήνυμα. Αντ' αυτού, αναφέρετε ποια χαρακτηριστικά δεν είναι διαθέσιμα, επειδή η εφαρμογή δεν έχει την απαραίτητη άδεια.

- Μην αποκλείετε τη διεπαφή χρήστη. Με άλλα λόγια, μην εμφανίζετε σε μια πλήρη οθόνη προειδοποιητικό μήνυμα, που εμποδίζει τους χρήστες να συνεχίσουν να χρησιμοποιούν την εφαρμογή.

Σε ορισμένες περιπτώσεις, η άδεια ενδέχεται να απορριφθεί αυτόματα, χωρίς ο χρήστης να κάνει οποιαδήποτε ενέργεια. Είναι σημαντικό να μην υποθέσουμε τίποτα για την αυτόματη συμπεριφορά. Ορισμένες εφαρμογές εξαρτώνται από την πρόσβαση σε ευαίσθητες πληροφορίες χρήστη, που σχετίζονται με αρχεία καταγραφής κλήσεων και μηνύματα. Σε αυτήν την περίπτωση, η εφαρμογή πρέπει να ζητήσει από τον χρήστη να την ορίσει ως προεπιλογή χειριστή για μια βασική λειτουργία συστήματος πριν ζητήσει αυτές τις άδειες χρόνου εκτέλεσης.

Λαμβάνοντας υπόψη τις ευαίσθητες πληροφορίες χρήστη στις οποίες έχει πρόσβαση μια εφαρμογή ενώ χρησιμοποιείται ως προεπιλογή χειριστή, η εφαρμογή δεν μπορεί να

γίνει προεπιλεγμένος χειριστής εκτός και αν πληρεί τις ακόλουθες απαιτήσεις καταχώρισης και βασικής λειτουργικότητας του Play Store:

- Η εφαρμογή πρέπει να μπορεί να εκτελεί τη λειτουργικότητα για την οποία έχει οριστεί ως προεπιλεγμένος χειριστής. Για παράδειγμα, ένας προεπιλεγμένος χειριστής SMS θα πρέπει να μπορεί να στέλνει μηνύματα.

- Η εφαρμογή πρέπει να παρέχει μια πολιτική απορρήτου η οποία θα πρέπει να είναι γραμμένη σε γλώσσα κατανοητή.

- Η εφαρμογή πρέπει να κάνει ξεκάθαρη τη βασική της λειτουργικότητα στην περιγραφή του Play Store. Για παράδειγμα, ένας προεπιλεγμένος χειριστής τηλεφώνου θα πρέπει να περιγράφει τις δυνατότητές του, που σχετίζονται με το τηλέφωνο στην περιγραφή.

- Η εφαρμογή πρέπει να δηλώσει τα δικαιώματα που είναι κατάλληλα για την περίπτωση χρήσης της.

- Η εφαρμογή πρέπει να ζητήσει να γίνει προεπιλεγμένος χειριστής, προτού ζητήσει τα δικαιώματα τα οποία σχετίζονται με το να είναι αυτή ο χειριστής.

Τέλος, τα δικαιώματα οργανώνονται σε ομάδες που σχετίζονται με τις δυνατότητες μιας συσκευής ή με τα χαρακτηριστικά της. Σύμφωνα με αυτό το σύστημα, τα αιτήματα αδειών αντιμετωπίζονται σε επίπεδο ομάδας και μια μεμονωμένη ομάδα αδειών, αντιστοιχεί σε πολλές δηλώσεις άδειας στο καταστατικό της εφαρμογής. Η ομαδοποίηση δικαιωμάτων με αυτόν τον τρόπο, επιτρέπει στο χρήστη να κάνει περισσότερο ουσιαστικές και τεκμηριωμένες επιλογές, χωρίς να κατακλύζεται από περίπλοκα και τεχνικά αιτήματα άδειας. Όλες οι επικίνδυνες άδειες Android ανήκουν σε ομάδες αδειών. Οποιαδήποτε άδεια μπορεί να ανήκει σε μια ομάδα αδειών, ανεξάρτητα από το επίπεδο προστασίας. Ωστόσο, η ομάδα μιας άδειας επηρεάζει την εμπειρία του χρήστη, μόνο εάν η άδεια είναι επικίνδυνη.

3. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

3.1 Έννοια Ιδιωτικότητας

Η έννοια της ιδιωτικότητας έχει τις ρίζες της πολύ βαθιά στην ιστορία. Ο Αριστοτέλης καταγράφει για πρώτη φορά την ανάγκη να διαχωριστεί ο δημόσιος βίος από τον ιδιωτικό[2]. Αιώνες μετά στην Γαλλική Επανάσταση, ο Saint Just διακύρηξε ότι η ελευθερία του ανθρώπου βρίσκεται στην ιδιωτική του ζωή και ότι αυτή θα πρέπει να προστατεύεται με κάθε τρόπο[3].Την έννοια της ιδιωτικότητας (privacy), τη συναντάμε για πρώτη φορά στις ΗΠΑ το 1890 στο άρθρο «Το δικαίωμα της ιδιωτικότητας» των Αμερικανών νομικών Samuel Warren και Louis Brandeis, με τον όρισμό «Το δικαίωμα να παραμένει κάποιος μόνος του». Για πρώτη φορά επίσης, τονίζεται πόσο αναγκαίο είναι να καταχωρηθεί συνταγματικά ως έννοια. Το 1984 ο F.Schoeman ορίζει την ιδιωτικότητα σαν μια περιορισμένη πρόσβαση στο άτομο και τις πληροφορίες που αφορούν την προσωπική του ζωή. Ο νομικός Alan F.Westin, δίνει έναν πιο αποδεκτό ορισμό για την έννοια της ιδιωτικότητας αναφέροντάς την ως την ικανότητα του ατόμου να ελέγχει κάτω από ποιες συνθήκες και ποιους όρους θα μπορεί κάποιος να αποκτά και να χρησιμοποιεί τις προσωπικές του πληροφορίες.

Το 1948 αναφέρεται το θέμα της ιδιωτικότητας από το Γενικό Συμβούλιο των Ηνωμένων Εθνών στην «Παγκόσμια Δήλωση των Ανθρωπίνων Δικαιωμάτων». Το 1950 η Ευρωπαϊκή Επιτροπή των Ανθρωπίνων Δικαιωμάτων, αναγνωρίζει ως θεμελιώδες ανθρώπινο δικαίωμα την προστασία της ιδιωτικής ζωής στο άρθρο 8 ως «Παν πρόσωπον δικαιούται εις τον σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του». Το 1981 το Συμβούλιο της Ευρώπης στη σύμβαση 108, αναφέρει ότι καμία προσωπική πληροφορία δεν μπορεί να γίνει αντικείμενο αυτοματοποιημένης επεξεργασίας εάν το εσωτερικό δίκαιο δεν προβλέπει κατάλληλες εγγυήσεις. Το ίδιο ισχύει και για τις πληροφορίες που έχουν να κάνουν με ποινικές καταδίκες.

Ανάλογα τώρα με το είδος των πληροφοριών, μπορούμε να χωρίσουμε την έννοια της ιδιωτικότητας σε κατηγορίες, κάποιες από αυτές είναι οι παρακάτω [24][25]:

- **Information privacy (ιδιωτικότητα πληροφοριών**): ελέγχει αν και με ποιο τρόπο μπορούν να συγκεντρωθούν, να αποθηκευτούν, να επεξεργαστούν ή και να διανεμηθούν οι προσωπικές πληροφορίες κάποιου.

- **Territorial privacy (εδαφική ιδιωτικότητα):** είναι η προστασία του φυσικού περιβάλλοντος ενός ατόμου, είτε αφορά το οικιακό περιβάλλον είτε το εργασιακό είτε κάποιο άλλο.

- **Bodily privacy (σωματική ιδιωτικότητα**): προστατεύει το άτομο από αδικαιολόγητες παρεμβάσεις όπως σωματικός έλεγχος, δοκιμή φαρμάκων ή οτιδήποτε παραβιάζει την ηθική του.

---

[2] «...απόσταση, χώρος και απομόνωση από τη δημόσια ζωή...», Αριστοτέλης «Ηθικά Νικομάχεια»

[3] «Saint Just «Fragments sur les institutions republicaines»

- **Communication privacy (ιδιωτικότητα επικοινωνίας):** προστατεύει από μη εξουσιοδοτημένη παρακολούθηση οποιασδήποτε επικοινωνίας του ατόμου.

Με την εισχώρηση της τεχνολογίας στην καθημερινή ζωή, το δικαίωμα της ιδιωτικότητας και η εξάσκησή του έγιναν ακόμα πιο σημαντικά. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, προστατεύει και δημιουργεί διαδικασίες άσκησης αυτού του δικαιώματος. Στην πληροφορική, η προστασία των προσωπικών δεδομένων είναι άρρηκτα συνδεδεμένη με την ιδιωτικότητα. Χωρίς το ένα δεν μπορεί να υπάρξει το άλλο, ωστόσο δεν ταυτίζονται – είναι δύο διαφορετικά θεμελιώδη ανθρώπινα δικαιώματα σύμφωνα με το Χάρτη Δικαιωμάτων της Ευρωπαϊκής 'Ενωσης (άρθρα 7 και 8 αντίστοιχα) [26].

3.2 Ιδιωτικότητα και Προσωπικά Δεδομένα

Η ανάγκη προστασίας της ιδιωτικής ζωής των ανθρώπων, της ανθρώπινης αξιοπρέπειας και κατά συνέπεια της ασφάλειας επεξεργασίας των προσωπικών τους δεδομένων, οδήγησε την Ευρωπαϊκή Ένωση να θεσπίσει την Οδηγία 95/46/ΕΚ, η οποία είχε ενσωματωθεί στην ένομη τάξη κάθε κράτους μέλους, και για περίπου δύο δεκαετίες αποτελούσε το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Η οδηγία αυτή έχει πλέον αντικατασταθεί από τον Κανονισμό 2016/679 (ΕΕ) Γενικός Κανονισμός Προστασίας Δεδομένων, γνωστός ως GDPR ο οποίος είναι σε εφαρμογή από τις 25 Μαΐου 2018 σε όλα τα Κράτη-Μέλη της ΕΕ.

Ήδη από το 2000, τόσο η ιδιωτικότητα όσο και η προστασία των προσωπικών δεδομένων αποτελούν θεμελιώδη ατομικά δικαιώματα για την ΕΕ, σύμφωνα με το Χάρτη Θεμελιωδών Δικαιωμάτων. Ειδικότερα, στο άρθρο 7 με τίτλο «Σεβασμός της ιδιωτικής και οικογενειακής ζωής» θεσπίζεται το ειδικότερο δικαίωμα της ιδιωτικότητας, ενώ στο άρθρο 8 με τίτλο «προστασία δεδομένων προσωπικού χαρακτήρα» θεσπίζεται το συναφές αλλά εν τέλει διαφορετικό δικαίωμα στην προστασία προσωπικών δικαιωμάτων: υπάρχει επικάλυψη μεταξύ των δύο δικαιωμάτων (π.χ. η αποκάλυψη ιδιωτικών συνομιλιών αποτελεί παραβίαση και των δύο δικαιωμάτων) αλλά πρόκειται για διαφορετικά ατομικά δικαιώματα.

Ο όρος «προσωπικά δεδομένα», αφορά κάθε πληροφορία που περιγράφει και αναφέρεται σε ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο (European Commission 2018) όπως: στοιχεία αναγνώρισης, φυσικά χαρακτηριστικά, εργασία, εκπαίδευση, οικονομικά στοιχεία, ενδιαφέροντα, συνήθειες. Επίσης, κάθε πληροφορία η οποία μπορεί συνδυαζόμενη να οδηγήσει έμμεσα στην ταυτοποίηση ενός ατόμου, χαρακτηρίζεται και αυτή ως προσωπικό δεδομένο. Κάθε προσωπική πληροφορία που έχει κρυπτογραφηθεί ή έχει αντιστοιχισθεί σε ψευδώνυμα και είναι ικανή να χρησιμοποιηθεί για την ταυτοποίηση του ατόμου, αυτόματα χαρακτηρίζεται ως «προσωπικό δεδομένο».

Το εύρος των προσωπικών δεδομένων είναι τεράστιο, καθένα από αυτά χρήζει διαφορετικής διαχείρισης και σε περίπτωση παραβίασής τους, υπόκεινται σε διαφορετικά νομικά πλαίσια. Για την καλύτερη κατανόησή τους έχουν κατηγοριοποιηθεί ως εξής:

- **Κοινά δεδομένα:** είναι τα προσωπικά δεδομένα τα οποία για να συλλεχθούν και να επεξεργαστούν χρειάζεται απλά η συγκατάθεση του χρήστη ή κάποια άλλη νομική βάση εξ αυτών που περιγράφονται στο άρθρο 6 του ΓΚΠΔ (π.χ. αν η

επεξεργασία επιβάλλεται από νόμο ή είναι αναγκαία για την εκτέλεση σύμβασης κ.α.). Τέτοια δεδομένα είναι:

- Ονοματεπώνυμο
- Επάγγελμα
- Διεύθυνση κατοικίας
- Ηλεκτρονική διεύθυνση (που ίσως δείχνει προσωπικά στοιχεία)
- Μορφωτικό επίπεδο
- Περιουσιακή κατάσταση
- Οικογενειακή κατάσταση
- Καταναλωτικές συνήθειες
- Τραπεζικοί λογαριασμοί
- Ύψος μισθού

- **Ευαίσθητα δεδομένα:** είναι τα δεδομένα που απορρέουν από την ιδιωτική ζωή του χρήστη, ανήκουν στον σκληρό πυρήνα της ιδιωτικότητας και χρειάζονται πρόσθετες προϋποθέσεις για να είναι επιτρεπτή η επεξεργασία τους. Αυτά τα δεδομένα αφορούν σε:
  - Φυλετική ή εθνική προσέλευση
  - Πολιτικά φρονήματα
  - Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
  - Συμμετοχή σε συνδικαλιστική οργάνωση
  - Υγεία
  - Ερωτική ζωή
  - Ποινικές διώξεις
  - Γενετικά δεδομένα
  - Βιομετρικά δεδομένα (δακτυλικά αποτυπώματα, γεωμετρία παλάμης, ανάλυση κόρης ματιού, χαρακτηριστικά προσώπου, φωνή εφόσον χρησιμοποιούνται για ταυτοποίηση)

- **Δημόσια δεδομένα:** δεδομένα και πληροφορίες που παράγονται από δημόσιους φορείς.

- **Κυβερνητικά δεδομένα:** είναι τα δεδομένα που παράγονται από τις κυβερνήσεις ή από φορείς υπό την επίβλεψη των κυβερνήσεων.

- **Ανοικτά:** είναι τα δεδομένα που μπορούν να χρησιμοποιηθούν ελεύθερα αρκεί να γίνεται αναφορά στους δημιουργούς.

- **Ανοικτά κυβερνητικά δεδομένα:** μιλάμε για δεδομένα ή πληροφορίες που παράγονται ή διατίθενται από την κυβέρνηση ή από φορείς υπό την επίβλεψή της, και χρησιμοποιούνται ή αναδιατίθενται από οποιονδήποτε αρκεί να αναφέρεται ή πηγή.

Υπάρχουν επίσης και τα Ανώνυμα δεδομένα τα οποία είναι πληροφορίες οι οποίες θα πρέπει να είναι απολύτως αδύνατον να μπορέσουν να ταυτοποιήσουν την ταυτότητα κάποιου. Τα ανώνυμα δεδομένα δεν θεωρούνται προσωπικά δεδομένα. Προσοχή όμως, γιατί πολλοί θεωρούν ότι έχουν κάνει ανωνυμοποίηση δεδομένων χωρίς όμως να το έχουν πετύχει, γιατί πολύ απλά δεν έχουν λάβει υπόψη όλα τα μέσα που μπορεί να

χρησιμοποιήσει κάποιος, όπως είναι το χρήμα, η τεχνολογία και ο χρόνος, για να καταφέρει άμεσα ή έμεσα να τον ταυτοποιήσει.

Πρέπει ακόμα να αναφέρουμε και τα ψευδωνυμοποιημένα δεδομένα. Αυτά τα δεδομένα είναι επεξεργασμένα, έτσι ώστε να μην μπορούν να ταυτιστούν με συγκεκριμένο πρόσωπο χωρίς να χρησιμοποιηθούν συγκεκριμένες πληροφορίες, οι οποίες διατηρούνται κάπου χωριστά και υπόκεινται σε οργανωτικά και τεχνικά μέτρα. Ο GDPR, προτρέπει τη χρήση των ψευδωνυμοποιημένων δεδομένων για μεγαλύτερη ασφάλεια της επεξεργασίας και της προστασίας των δικαιωμάτων. Η ψευδωνυμοποίηση είναι ευαίσθητο θέμα, γιατί δεν πρέπει για κανένα λόγο να μπορέσει κάποιος εισβολέας να κάνει ταυτοποίηση του χρήστη.

3.3 Απαιτήσεις Ασφαλείας και Προστασίας Προσωπικών Δεδομένων

Τα πληροφοριακά συστήματα έχουν την ανάγκη προστασίας των δεδομένων τους για να λειτουργήσουν σωστά. Γι αυτόν τον λόγο, υπάρχουν συγκεκριμένες απαιτήσεις ασφάλειας και ιδιωτικότητας, οι οποίες παρουσιάζονται παρακάτω [34][35]:

- Confidentiality (Εμπιστευτικότητα): Προστατεύει τα προσωπικά δεδομένα, έτσι ώστε να μην αποκαλυφθούν σε μη εξουσιοδοτημένα άτομα.
- Availability (Διαθεσιμότητα): Προστατεύει τα δεδομένα, έτσι ώστε να μην είναι διαθέσιμα στον οποιονδήποτε.
- Authenticity (Αυθεντικότητα): Όλα τα εμπλεκόμενα μέρη, μπορούν να εξασφαλίσουν και να διασφαλίσουν ταυτόχρονα την ταυτότητά τους.
- Integrity (Ακεραιότητα): Προστατεύει τα δεδομένα, έτσι ώστε να μην μπορεί να γίνει τροποποίηση, εισαγωγή, ή διαγραφή νέων χωρίς εξουσιοδότηση.
- Non-Repudiation (Μη-Αποποίηση): Σε τυχών ανταλλαγή πληροφοριών, μας προστατεύει από τη μη άρνηση του αποστολέα για την ταυτότητά του.

Υπάρχουν επιμέρους απαιτήσεις, οι οποίες επιτρέπουν στον ορισμό της ιδιωτικότητας, να περάσει από μια γενική έννοια, σε μια τεχνική απαίτηση. Αυτές είναι οι παρακάτω [34][35]:

- Authentication (Αυθεντικοποίηση): Είναι ο τρόπος με τον οποίο γίνεται επιβεβαίωση της ταυτότητας μιας οντότητας. Είναι απαίτηση για την ασφάλεια ενός πληροφοριακού συστήματος, αλλά βοηθάει πολύ και στις απαιτήσεις ιδιωτικότητας.
- Authorization (Εξουσιοδότηση): Με αυτόν τον τρόπο, μια οντότητα έχει το δικαίωμα πρόσβασης, σε ένα πληροφοριακό σύστημα.
- Identification (Αναγνώριση): Μέσω αυτής, γίνεται ο έλεγχος για την απαίτηση αυθεντικότητας και έπειτα εξουσιοδότησης ή όχι για την πρόσβαση σε δεδομένα.

- Anonymity (Ανωνυμία): Είναι ο τρόπος με τον οποίο ένας χρήστης μπορεί να επικοινωνήσει με άλλον ή να χρησιμοποιήσει μια υπηρεσία, χωρίς να αποκαλύψει την ταυτότητά του.
- Pseudonymity (Ψευδωνυμία): Με αυτόν τον τρόπο, μία οντότητα προστατεύει την ταυτότητά της από άλλες, μη εξουσιοδοτημένες.
- Unlinkability (Μη-συνδεσιμότητα): Με τον τρόπο αυτό, κανένας κακόβουλος χρήστης, δεν έχει την δυνατότητα να συλλέξει πληροφορίες, οι οποίες αν συνδυαστούν μπορούν να του παρέχουν στοιχεία για την ταυτότητα του χρήστη.
- Unobservability (Μη-παρατηρησιμότητα): Με τον τρόπο αυτόν, μία οντότητα προστατεύει την ιδιωτικότητά της, αφού οι κακόβουλοι χρήστες δεν έχουν την δυνατότητα να εντοπίσουν τα ίχνη της.
- Data Protection (Προστασία Δεδομένων): Από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), απαιτούνται κάποιες αρχές για την προστασία των προσωπικών δεδομένων. Κάποιες από αυτές τις αρχές οι οποίες αναλύονται περαιτέρω στην Ενότητα 3.5.2. είναι:
    - Αρχή της διαφάνειας, της αντικειμενικότητας και της νομιμότητας
    - Αρχή περιορισμού του σκοπού
    - Αρχή ελαχιστοποίησης των δεδομένων
    - Αρχή ακριβείας
    - Αρχή περιορισμού της περιόδου αποθήκευσης
    - Αρχή της ακεραιότητας και της εμπιστευτικότητας

3.4 Ρίσκα Ιδιωτικότητας για Κινητές Συσκευές

Στο συγκεκριμένο κεφάλαιο θα αναφερθούμε σε ορισμένους παράγοντες, οι οποίοι αποτελούν σημαντικό ρίσκο για την ιδιωτικότητα του χρήστη κινητών συσκευών.

- **Μεγάλο εύρος δεδομένων και αισθητήρων**: Οι χρήστες κινητών συσκευών, εγκαθιστούν όλο και περισσότερες εφαρμογές στην συσκευή τους, η οποία αποκτά πρόσβαση σε ένα μεγάλο εύρος προσωπικών δεδομένων του χρήστη, όπως ιατρικά δεδομένα κ.α. Οι νέες κινητές συσκευές, είναι εμπλουτισμένες με πολλούς αισθητήρες, όπως κάμερα, μικρόφωνο κ.α, μέσω των οποίων είναι εύκολη η δημιουργία δεδομένων, τα οποία μπορεί να έχουν συνέπειες στην ιδιωτικότητα του χρήστη. Αυτό μπορεί να αποδειχτεί και από την έρευνα των (M. Gadaleta & Rossi, 2018), όπου ο εντοπισμός ενός χρήστη γίνεται εύκολα, ακόμα και από τον τρόπο που περπατάει.

- **Το κινητό ως επέκταση του χεριού**: Στην σημερινή εποχή, το κινητό έχει γίνει επέκταση του χεριού όλων μας, έχοντας την πεποίθηση ότι είναι πολύ αξιόπιστο και ασφαλές. Τα έχουμε πάντα μαζί μας, είναι ενεργοποιημένα κάθε ώρα της ημέρας, με αποτέλεσμα να συνδέονται σε διάφορα δίκτυα. Όλοι μας, αποθηκεύουμε σε αυτό προσωπικά δεδομένα, τα οποία παραμένουν για αρκετά μεγάλο χρονικό διάστημα. Αυτό από μόνο του, κάνει τα κινητά τέλειους στόχους σε διαφημίσεις (που είναι το απλούστερο), αλλά και σε αναλυτές δεδομένων.

- **Τύποι αναγνωριστικών**: Οι εφαρμογές των κινητών συσκευών, μπορούν να κάνουν χρήση διαφόρων αναγνωριστικών ή δαχτυλικών αποτυπωμάτων που παρέχονται σε αυτά από το λειτουργικό σύστημα, έτσι ώστε να πραγματοποιείται ο εντοπισμός και η παρακολούθηση του χρήστη.

- **Εντοπισμός και δημιουργία προφίλ**: Ο γεωγραφικός εντοπισμός και η παρακολούθηση κινητών συσκευών είναι σύνηθες φαινόμενο στις μέρες μας. Αυτό, είναι κίνδυνος για την ιδιωτικότητα κάθε χρήστη, μιας και είναι εύκολο για κάθε ενδιαφερόμενο να υποκλέψει ευαίσθητα δεδομένα, που αφορούν για παράδειγμα την θρησκεία ή την υγεία του. Με την σύνδεσή τους στο διαδίκτυο, καθιστούν εύκολη την παρακολούθησή τους από τρίτους, οι οποίοι με την βοήθεια των third party βιβλιοθηκών, μπορούν να δημιουργήσουν ψηφιακά προφίλ των χρηστών (D. Arp et al. 2017).

- **Τεράστια συλλογή δεδομένων**: Καθημερινά σχεδόν τα κινητά εξελίσσονται και οι εφαρμογές αναβαθμίζονται, χρησιμοποιώντας κάθε νέο μέσο που τους δίνει την δυνατότητα να συλλέξουν δεδομένα, για την καλύτερη ανάλυση και λειτουργία των υπηρεσιών τους. Ο χρήστης, δεν μπορεί να απαγορεύσει την χρήση ενός αισθητήρα από την εφαρμογή, γιατί έτσι περιορίζει την πλήρη λειτουργία της. Αναγκασμένος λοιπόν να επιτρέψει την πρόσβαση σε όλους τους αισθητήρες, έχει ως αποτέλεσμα την τεράστια συλλογή δεδομένων προσωπικού χαρακτήρα από την εφαρμογή, η οποία τα αποθηκεύει σε third party βιβιοθήκες.

3.5 Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ), είναι ο νέος κανονισμός για την προστασία των προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης, που έρχεται να αντικαταστήσει την υπάρχουσα οδηγία περί προστασίας των δεδομένων (Data Protection Directive), η οποία ισχύει από το 1995. Η οδηγία 95/46/ΕΚ για την προστασία των δεδομένων έπρεπε να εφαρμοστεί από κάθε κράτος μέλος της ΕΕ και ενώ είχε σαν στόχο την ύπαρξη ενός εναρμονισμένου και σύγχρονου καθεστώτος προστασίας δεδομένων σε όλη την Ευρώπη, αυτός δεν επετεύχθη πλήρως, εξαιτίας των διαφορών που υπήρχαν σε διάφορες εθνικές εφαρμογές (Hansen, 2016).

Πέρασαν πάνω από 20 χρόνια συζήτησης και διαπραγμάτευσης και τελικά το 2016, εγκρίθηκε ο διάδοχος της οδηγίας για την προστασία των δεδομένων, ο οποίος ονομάστηκε Γενικός Κανονισμός Προστασίας Δεδομένων – General Data Protection Regulation (GDPR) (Regulation, 2016). Κύριοι στόχοι, ήταν και πάλι η εναρμόνιση και ο εκσυγχρονισμός που επιδιωκόταν με την παλιά οδηγία. Ο GDPR τέθηκε σε ισχύ στις 25 Μαΐου 2018. Η άμεση εφαρμογή του, σε όλα τα κράτη μέλη, συμβάλλει στην ενοποίηση του επιπέδου προστασίας δεδομένων. Ωστόσο, υπάρχουν περίπου 70 ρήτρες, άλλες υποχρεωτικές και άλλες προαιρετικές, οι οποίες δίνουν τα μέσα σε κάθε κράτος, για τις δικές τους εθνικές απαιτήσεις, με αποτέλεσμα να υπάρχει απόκλιση από μια κοινή στρατηγική για όλα τα κράτη μέλη της ΕΕ (Roßnagel & Nebel, 2016).

Το περιεχόμενο του κανονισμού έχει ως εξής: Στο 2ο τμήμα του αναφέρονται οι σημαντικές ιδιότητες του Ευρωπαϊκού Κανονισμού για την Γενική Προστασία Δεδομένων που προκύπτουν από την ευρωπαϊκή πρωτοβουλία, για μεταρρύθμιση της προστασίας δεδομένων. Στο 3ο τμήμα, αναφέρεται η έννοια της "προστασίας της ιδιωτικής ζωής από σχεδιασμό" και δίνει σύντομες πληροφορίες, αναφορικά με το ιστορικό και τους ορισμούς. Στο 4ο και 5ο τμήμα παρουσιάζονται οι νομικές

υποχρεώσεις, που αφορούν την προστασία των δεδομένων από το σχεδιασμό και την προστασία τους. Τέλος, στο 6ο και τελευταίο τμήμα απαριθμούνται τα συμπεράσματα και δίνεται μια κατακλείδα (Hansen, 2016). Θα πρέπει να τονίσουμε, ότι ο Γενικός Κανονισμός Προστασίας Δεδομένων δεν αποτελεί «απόλυτη» λύση για την προστασία των δεδομένων, μιας και από την μια, δεν είναι όλα καινούργια στον κανονισμό και από την άλλη στα 99 άρθρα του, υπάρχουν περιθώρια για διαφορετικές ερμηνείες. Στον κανονισμό, έχει επιλεγμένα αφαιρεθεί το νομικό κείμενο, όχι από σφάλμα, αλλά από καθαρή επιδίωξη. Υπάρχουν οι αφηρημένοι κανόνες, οι οποίοι για να μπορούν να εναρμονίζονται με τους συνεχώς μεταβαλλόμενους κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, πρέπει να τεκμηριώνονται κατάληλα και να είναι αποδεκτοί από τους Ευρωπαίους επιτρόπους προστασίας δεδομένων ως εποπτικές αρχές. Έτσι, ο GDPR ορίζει μια διαδικασία, η οποία θα επιτύχει μια συνεκτική ερμηνεία των νομικών υποχρεώσεων, που έχουν να κάνουν με τις διασυνοριακές συναλλαγές. Με αυτό τον τρόπο, ο κανονισμός θα είναι ανθεκτικός για πολλά χρόνια, σε αντίθεση με την προκάτοχό του οδηγία. Η συνεχής όμως διαπραγμάτευση για την τεκμηρίωση των αφηρημένων κανόνων είναι χρονοβόρα, με αποτέλεσμα να δεχτούν επιρροές από ομάδες πίεσης, οι οποίες δεν ενστερνίζονται τον ίδιο στόχο για την βέλτιστη προστασία των δεδομένων (Hansen, 2016). Οι ευρωπαίοι υπεύθυνοι επεξεργασίας δεδομένων, δεν είναι οι μόνοι στους οποίους απευθύνεται ο GDPR. Σκοπός του επίσης, είναι να εξασφαλίσει την προστασία των δεδομένων σε όλη την ευρωπαϊκή αγορά. Στο άρθρο 3 του κανονισμού, υπάρχει ο όρος της «αρχής της θέσης της αγοράς», ο οποίος απευθύνεται σε οργανισμούς που προσφέρουν υπηρεσίες ή αγαθά σε ανθρώπους στην ΕΕ ή σε οργανώσεις που παρακολουθούν τη συμπεριφορά των ανθρώπων, ακόμη και αν αυτές δεν έχουν έδρα στην επικράτεια της Ευρωπαϊκής Ένωσης. Συγκεκριμένα, οι εταιρείες οι οποίες κυριαρχούν στην ψηφιακή αγορά, ακόμα και αν δεν είναι μέλη της ΕΕ, πρέπει να συμμορφώνονται με τις απαιτήσεις του GDPR, για την προστασία των δεδομένων (Hansen, 2016).

Μια από τις σημαντικές αλλαγές που έχει επιφέρει ο GDPR, είναι ότι οι Ευρωπαίοι πολίτες έχουν πιο μεγάλο έλεγχο στα προσωπικά τους δεδομένα και οι οργανισμοί που τα συλλέγουν ή τα αναλύουν, έχουν υποστεί πολλές καινούργιες υποχρεώσεις. Με το GDPR, οι εθνικές ρυθμιστικές αρχές έχουν πάρει καινούργιες εξουσίες που τους δίνουν το δικαίωμα να επιβάλουν μεγάλα πρόστιμα σε όποιον παραβιάζει τον κανονισμό, ο οποίος έχει ενσωματωθεί ως εθνική νομοθεσία σε όλα τα κράτη μέλη της ΕΕ.

Ο GDPR, αν και είχε ψηφιστεί ως Ευρωπαϊκή νομοθεσία από τον Απρίλιο του 2016, η εφαρμογή του ξεκίνησε στις 25 Μάιου 2018. Η μεταβατική αυτή διετία ήταν απαραίτητη, γιατί οι εταιρείες και οι οργανισμοί, για να ευθυγραμμιστούν με τον κανονισμό, έπρεπε να προχωρήσουν σε σημαντικές αλλαγές.

3.5.1 Βασικές Καινοτομίες του GDPR

Ο GDPR έχει εισάγει αρκετές νέες καινοτομίες, οι οποίες βοηθούν στη ρύθμιση της προστασίας των προσωπικών δεδομένων των χρηστών. Επίσης, ορισμένες υπάρχουσες καινοτομίες ενισχύθηκαν, χάρη σε αυτόν. Κάποιες από αυτές είναι οι παρακάτω [41]:

- Δικαίωμα διαγραφής: Ένας χρήστης μπορεί να αιτηθεί την διαγραφή των δεδομένων του, που έχουν αποθηκευτεί και επεξεργαστεί από τρίτους, κατά την εκχώρηση άδειας σε αυτούς. Το δικαίωμα αυτό είναι ενισχυμένο σε σχέση με αυτό που οριζόταν στην Οδηγία 95/46/ΕΚ, υπό την έννοια ότι ο υπεύθυνος

επεξεργασίας, αν τα έχει παραχωρήσει και σε άλλους, θα πρέπει με την σειρά του να τους ενημερώσει για την απόφαση του χρήστη, έτσι ώστε να τα διαγράψουν κι αυτοί.

- Όταν η επεξεργασία είναι επιτρεπτή βάσει συγκατάθεσης, απαιτείται σαφής συγκατάθεση από τους χρήστες, όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων (σαφής συναίνεση από πλευράς χρήστη, η οποία πρέπει να προκύπτει με θετική ενέργεια του χρήστη κατόπιν πλήρους ενημέρωσης: προ-συμπληρωμένα «τετραγωνάκια» με δυνατότητα από-επιλογής δεν αποτελούν έγκυρη συγκατάθεση).

- Δικαίωμα μεταφοράς δεδομένων (π.χ. σε διαφορετικό υπεύθυνο επεξεργασίας).

- Ειδοποίηση παραβίασης προσωπικών δεδομένων (εντός 72 ωρών), τόσο της αρμόδιας αρχής, όσο και των προσώπων που παραβιάστηκαν τα δεδομένα τους.

- Υποχρέωση, για συγκεκριμένες περιπτώσεις, καθορισμού υπευθύνου προστασίας δεδομένων - Data Protection Officer (DPO).

- Πρόστιμα τα οποία κυμαίνονται από 0,5 έως 4% του συνόλου του παγκόσμιου ετήσιου τζίρου.

Στην παρακάτω εικόνα, απεικονίζονται ορισμένες βασικές καινοτομίες στην εφαρμογή του GDPR. Άξιο αναφοράς είναι πως η εφαρμογή του GDPR αναφέρεται αποκλειστικά σε προσωπικά δεδομένα.

3.5.2 Βασικοί Ορισμοί – Άρθρο 4

Ο ΓΚΠΔ, για να προσδιορίσει συγκεκριμένες έννοιες και ρόλους, που χρειάζονται σε μια επεξεργασία προσωπικών δεδομένων, χρησιμοποιεί συγκεκριμένους ορισμούς. Η λίστα

αυτών των ορισμών, περιλαμβάνεται στο άρθρο 4 του ΓΚΠΔ. Στην ενότητα αυτή, θα παρουσιάσουμε κάποιους βασικούς ορισμούς του Κανονισμού, οι οποίοι είναι απαραίτητοι για την κατανόηση της παρούσας διπλωματικής εργασίας [42].

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

- **Επεξεργασία**: 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.

- **Περιορισμός της επεξεργασίας**: η επισήμανση αποθηκευμένων δεδομένων προσωπικού χαρακτήρα με στόχο τον περιορισμό της επεξεργασίας τους στο μέλλον.

- **Υπεύθυνος επεξεργασίας**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

- **Εκτελών την επεξεργασία**: 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**: 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.

- **Υποκείμενο δεδομένων**: το φυσικό πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα.

- **Σύστημα αρχειοθέτησης**: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

- **Συγκατάθεση του υποκειμένου των δεδομένων**: 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.

- **Εποπτική αρχή**: ανεξάρτητη δημόσια αρχή που συγκροτείται από κράτος μέλος σύμφωνα με το άρθρο 51.

3.5.3 Αρχές που Διέπουν την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα και Νομιμότητα της Επεξεργασίας

Έχουμε ήδη αναφέρει τους κινδύνους για την ασφάλεια και την ιδιωτικότητα, οι οποίοι προκύπτουν από τις εφαρμογές, τόσο στα κινητά, όσο και σε οποιαδήποτε άλλη έξυπνη συσκευή. Οι κίνδυνοι αυτοί, οδήγησαν τον ΓΚΠΔ να συντάξει το άρθρο 5, στο οποίο αναφέρονται οι βασικές αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων. Ο GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων) περιγράφει τις αρχές προστασίας δεδομένων, στις οποίες συνοψίζονται οι πολλές απαιτήσεις του. Αυτές οι αρχές, είναι μια ουσιαστική πηγή για όσους προσπαθούν να κατανοήσουν πώς θα πετύχουν τη συμμόρφωσή τους με τους κανόνες προστασίας προσωπικών δεδομένων. Για παράδειγμα, οι μικροί οργανισμοί, οι οποίοι συχνά δεν διαθέτουν τους πόρους για να διορίσουν εμπειρογνώμονες προστασίας δεδομένων, οι οποίοι θα τους καθοδηγήσουν στη συμμόρφωση, μπορούν να βρουν τις αρχές αυτές ιδιαίτερα χρήσιμες [8][42].

- **Νομιμότητα, αντικειμενικότητα και διαφάνεια:** Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να επεξεργάζονται με σεβασμό της διαφάνειας και της δικαιοσύνης, απέναντι στο υποκείμενο των δεδομένων, καθώς και να τηρείται πάντοτε η απαίτηση ότι υπάρχει θεμιτός λόγος γι' αυτή την επεξεργασία.

- **Περιορισμός του σκοπού:** Για να γίνει η επεξεργασία προσωπικών δεδομένων από κάποια εφαρμογή, θα πρέπει να έχει συγκεκριμένο και νόμιμο σκοπό. Επίσης κρίνεται απαραίτητο να ενημερώνεται το υποκείμενο των δεδομένων, για το είδος του σκοπού αυτού. Η αρχή αυτή απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα, να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιεί σαφή και απλή γλώσσα.

- **Ελαχιστοποίηση των δεδομένων:** Τα δεδομένα προσωπικού χαρακτήρα, πρέπει να είναι κατάλληλα, επαρκή και συναφή. Είναι απαραίτητο να περιορίζονται σε ότι είναι αναγκαίο για την εξυπηρέτηση των σκοπών, για τους οποίους υποβάλλονται σε επεξεργασία.

- **Ακρίβεια:** Τα προσωπικά δεδομένα οφείλουν να είναι ακριβή και να ενημερώνονται όπου χρειάζεται. Επίσης, είναι απαραίτητο να λαμβάνεται κάθε εύλογο μέτρο, ώστε να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα που δεν είναι ακριβή θα διορθώνονται ή θα διαγράφονται, χωρίς χρονοτριβή και πάντα λαμβάνοντας υπ' όψην το σκοπό για τον οποίο γίνεται η επεξεργασία.

- **Περιορισμός της περιόδου αποθήκευσης:** Τα δεδομένα προσωπικού χαρακτήρα αποθηκεύονται σε τέτοια μορφή, ώστε να μπορεί να υπάρξει ταυτοποίηση του ατόμου και για τόσο χρονικό διάστημα, όσο χρειάζεται για την εξυπηρέτηση του σκοπού του οποίου γίνεται η επεξεργασία. Τα προσωπικά δεδομένα μπορούν να αποθηκευτούν για μεγαλύτερα διαστήματα, εφόσον αυτά θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς (άρθρο 89 παράγραφος 1) και εάν εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που ορίζονται από τον παρών κανονισμό, με σκοπό την διασφάλιση των δικαιωμάτων και ελευθεριών του ατόμου.

- **Ακεραιότητα και εμπιστευτικότητα:** Τα δεδομένα προσωπικού χαρακτήρα, θα πρέπει να υποβάλλονται σε επεξεργασία με τέτοιον τρόπο, ώστε να επιτυγχάνεται η εξασφάλιση της ασφάλειας και της προστασίας τους, από παράνομη ή μη εξουσιοδοτημένη επεξεργασία, καθώς και από τυχόν απώλεια, βλάβη ή καταστροφή τους. Αυτό μπορεί να επιτευχθεί, με τη χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

- **Λογοδοσία:** Οι παραπάνω θεμελιώδεις αρχές υπήρχαν και στην προηγούμενη νομική Οδηγία. Ο ΓΚΠΔ όμως, έρχεται να εισάγει την αρχή της λογοδοσίας (Αρ. 5 παρ. 2), που αποτελεί και τη βασική διαφορά τους. Σύμφωνα με αυτή την αρχή, οι υπεύθυνοι επεξεργασίας (πχ. οργανισμοί, επιχειρήσεις κ.α.), οι οποίοι συλλέγουν και επεξεργάζονται τα προσωπικά δεδομένα, είναι υποχρεωμένοι να φτιάχνουν τα τεχνικά και οργανωτικά τους μέτρα με τέτοιον τρόπο, ώστε να αποδεικνύουν όποτε χρειαστεί μπροστά στις αρχές, ότι συμμορφώνονται πλήρως με τις παραπάνω βασικές αρχές. Με αυτόν τον τρόπο, υπάρχει εγγύηση ότι τηρούνται οι αρχές που διέπουν τα προσωπικά δεδομένα και υπεύθυνοι γι αυτό πλέον είναι οι «υπεύθυνοι επεξεργασίας».

Στο άρθρο 6, καθορίζονται οι νομικές βάσεις της επεξεργασίας προσωπικών δεδομένων. Η επεξεργασία δεδομένων με προσωπικό χαρακτήρα, επιτρέπεται αν συντελλείται μια από τις παρακάτω περιπτώσεις [42]:

- Αν το άτομο στο οποίο ανήκουν τα προσωπικά δεδομένα έχει δώσει την συγκατάθεσή του για την επεξεργασία τους, για έναν ή περισσότερους συγκεκριμένους σκοπούς. Με τον όρο συγκατάθεση, εννοούμε ότι η συναίνεσή του πρέπει να είναι ρητή και ξεκάθαρη και να δίνεται με σαφή ενέργεια, χωρίς να υπονοείται.

- Η επεξεργασία δεδομένων είναι απαραίτητη για να εκτελεστεί μια σύμβαση, της οποίας το ένα συμβαλλόμενο μέρος είναι το πρόσωπο στο οποίο ανήκουν τα δεδομένα, ή για τη λήψη μέτρων πριν από τη σύναψη μιας σύμβασης, μετά από αίτηση του υποκειμένου των δεδομένων.

- Όταν η επεξεργασία δεδομένων είναι απαραίτητη, για να υπάρξει συμμόρφωση του υπευθύνου επεξεργασίας με τις νομικές υποχρεώσεις.

- Όταν η επεξεργασία δεδομένων γίνεται για να προστατέψει τα ζωτικά συμφέροντα του ίδιου προσώπου, του οποίου τα προσωπικά δεδομένα επεξεργάζονται, ή κάποιου άλλου ατόμου.

- Η επεξεργασία είναι απαραίτητη για την ολοκλήρωση ενός καθήκοντος, που γίνεται για το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, η οποία έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

- Η επεξεργασία είναι απαραίτητη για την ικανοποίηση των έννομων συμφερόντων του υπεύθυνου επεξεργασίας ή κάποιου τρίτου, εκτός αν υπερισχύει το συμφέρον ή οι ελευθερίες του υποκειμένου των δεδομένων. Όταν συμβαίνει αυτό,επιβάλλεται η προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως αν το πρόσωπο αυτό είναι παιδί.

3.5.4 Προστασία Δεδομένων από Σχεδιασμό και εξ' ορισμού

Στον κανονισμό, υπάρχει μια νέα απαίτηση από τον εκάστοτε υπεύθυνο επεξεργασίας, που έχει σαν στόχο την εναρμόνιση της συλλογής/επεξεργασίας των δεδομένων, από την αρχή, και με πρωταρχικό στόχο την προστασία των προσωπικών δεδομένων των υποκειμένων. Η απαίτηση αυτή, είναι η προστασία των προσωπικών δεδομένων από το στάδιο του σχεδιασμού και εξ ορισμού (privacy by default and privacy by design - Άρθρο 25 GDPR). Οι κατασκευαστές δηλαδή, θα πρέπει να παίρνουν τα κατάλληλα μέτρα προστασίας για τους χρήστες, στο στάδιο του σχεδιασμού και εξ ορισμού.

Ο υπεύθυνος επεξεργασίας, στη διάρκεια του σχεδιασμού των συστημάτων επεξεργασίας, θα πρέπει όχι μόνο να εφαρμόζει αλλά και να μπορεί να αποδείξει, ανά πάσα στιγμή, την λήψη των κατάλληλων μέτρων αλλά και τη χρησιμοποίηση τρόπων ενίσχυσης της ιδιωτικότητας. Για να πετύχει τη σωστή σχεδίαση πρέπει να λάβει υπόψη του όλες τις τελευταίες εξελίξεις που έχουν γίνει στην τεχνολογία, τη φύση και το σκοπό της επεξεργασίας καθώς και όλους τους πιθανούς κινδύνους κατά των δικαιωμάτων και των ελευθεριών των χρηστών που μπορεί να προκύψουν κατά τη διάρκεια της επεξεργασίας. Αυτό είναι απαραίτητο να γίνεται στην αρχή του σχεδιασμού/ανάπτυξης του συστήματος που θα κάνει την επεξεργασία και όχι εκ των υστέρων.

Επίσης, ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι εξ ορισμού, δέχονται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα, τα οποία είναι απαραίτητα για τον οποιοδήποτε σκοπό της επεξεργασίας. Ειδικότερα, τα μέτρα που θα ληφθούν, θα πρέπει να διασφαλίζουν ότι εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν είναι προσβάσιμα σε τρίτους, χωρίς την έγκριση του φυσικού προσώπου. Η υποχρέωση αυτή, αφορά το πλήθος των προσωπικών δεδομένων που αποθηκεύονται από το πρώτο λεπτό της συλλογής, έως και τη διαγραφή τους. Για παράδειγμα, οι κατασκευαστές των έξυπνων συσκευών θα πρέπει να εξασφαλίζουν τη διατήρηση της ανωνυμίας όλων των ατόμων που αγοράζουν τις συσκευές τους και η συλλογή πληροφοριών για τους χρήστες από τους σχεδιαστές εφαρμογών (applications), να γίνεται μόνο στο βαθμό που επιτρέπει ο Κανονισμός [43].

Στο προοίμιο του Κανονισμού, δίνεται ιδιαίτερη σημασία στα παιδιά. Αυτά, απαιτούν ειδική προστασία σε ότι έχει να κάνει με τα προσωπικά τους δεδομένα, γιατί έχουν μικρότερη επίγνωση των σχετικών κινδύνων, των συνεπειών, των εγγυήσεων και των δικαιωμάτων τους σε ότι αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το ίδιο ισχύει και για τους ηλικιωμένους. Η συγκατάθεση του γονέα ή κηδεμόνα δεν θα

πρέπει να είναι απαραίτητη σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε ένα παιδί. Εάν, π.χ., ένα παιδί θέλει να καταγγείλει μία πράξη κακοποιήσεως, δεν θα απαιτείται δικαιολογημένα η λήψη συγκαταθέσεως από τους γονείς ή κηδεμόνες. Το ερώτημα που προκύπτει είναι αν το δικαίωμα προστασίας όσον αφορά τα παιδιά θα πρέπει να είναι «επαυξημένο» έναντι του «κανονικού» για όλους τους άλλους. Δικαίωμα προστασίας δεδομένων δύο ταχυτήτων δηλαδή. Η απάντηση είναι, ότι η ενισχυμένη προστασία είναι δικαίωμα όλων, όχι μόνο των παιδιών, μιας και δεν είναι λίγοι οι «διαδικτυακά αναλφάβητοι» ενήλικες, που με πλήρη άγνοια κινδύνου εισέρχονται στο διαδίκτυο [44].

3.5.5 Ασφάλεια Επεξεργασίας

Το άρθρο 32 (ασφάλεια επεξεργασίας) του ΓΚΠΔ, ορίζει ότι οι υποχρεώσεις για την ασφάλεια επεξεργασίας μοιράζονται εξίσου, τόσο στον υπεύθυνο επεξεργασίας, όσο και στον εκτελών την επεξεργασία. Και οι δύο έχουν την ευθύνη να διασφαλίσουν το σωστό επίπεδο ασφαλείας, απέναντι στους κινδύνους που απειλούν τα δεδομένα προσωπικού χαρακτήρα και για να το πετύχουν αυτό, πρέπει να λάβουν όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα. Αφού ληφθεί υπόψη η φύση της επεξεργασίας και οι συνέπειες που θα υπάρξουν για τους χρήστες, σε περίπτωση που παραβιαστεί η ασφάλεια, τότε θα πρέπει να μπουν σε λειτουργία μέτρα, που θα περιλαμβάνουν κατά περίπτωση τα εξής [41]:

- Την ψευδωνυμοποίηση και την κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα, έτσι ώστε να μην μπορεί να γίνει ταυτοποίηση του υποκειμένου των δεδομένων από τρίτους.

- Την δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση. Ο υπεύθυνος της επεξεργασίας και ο εκτελών την επεξεργασία, υποχρεούνται να προστατεύσουν τα προσωπικά δεδομένα από αλλοίωση, διαρροή, απώλεια και παράνομη ή τυχαία καταστροφή, αλλά και να μπορούν ανα πάσα στιγμή να διαθέσουν τα συστήματά τους στο χρήστη.

- Σε περίπτωση φυσικού ή τεχνικού προβλήματος, να υπάρχει η δυνατότητα αποκατάστασης της διαθεσιμότητας, καθώς και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα.

- Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, θα πρέπει να έχουν σχεδιάσει μια διαδικασία, με την οποία ανα πάσα στιγμή θα μπορεί να δοκιμαστεί και να αξιολογηθεί η αποτελεσματικότητα των τεχνικών και οργανωτικών μέτρων που έχουν παρθεί, για την διασφάλιση της ασφάλειας της επεξεργασίας.

Με βάση το άρθρο 32 του ΓΚΠΔ, η αξιολόγηση στηρίζεται στην πιθανότητα εμφάνισης κινδύνου και στις σοβαρές επιπτώσεις που μπορεί να έχει αυτός, για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Αυτή η πιθανότητα και η σοβαρότητα του κινδύνου, θα πρέπει να καθορίζονται σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο (αιτία 76 άρθρου 32).

Η μεθοδολογία που εφαρμόζεται σήμερα είναι διαδεδομένη, λόγω της κλασσικής ανάλυσης και εκτίμησης κινδύνου.

3.5.6 Εκτίμηση Αντικτύπου Σχετικά με την Προστασία Δεδομένων – Data Protection Impact Assessment (DPIA)

Ο ΓΚΠΔ προστατεύει τα φυσικά πρόσωπα και ιδίως τα θεμελιώδη δικαιώματα και τις ελευθερίες τους, από την επεξεργασία προσωπικών δεδομένων και από την ελεύθερη κυκλοφορία τους. Ειδικότερα στο άρθρο 35, ορίζεται ότι κάθε δημόσιος ή ιδιωτικός οργανισμός, ο οποίος επεξεργάζεται συγκεκριμένα δεδομένα προσωπικού χαρακτήρα, είναι υποχρεωμένος να κάνει εκτίμηση των πιθανών επιπτώσεων των κινδύνων που ίσως προκύψουν από την επεξεργασία των δεδομένων, πριν να γίνει η επεξεργασία αυτή [41].

Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία, πρέπει κατά την επεξεργασία των δεδομένων να τηρούν την αρχή της λογοδοσίας. Οτιδήποτε κάνουν, πρέπει να είναι σύμφωνο με όσα ορίζει ο Κανονισμός και ταυτόχρονα, θα πρέπει να είναι πάντα έτοιμοι να αποδεικνύουν ότι έχουν πάρει όλα τα απαραίτητα μέτρα προς αυτή τη συμμόρφωση. Την εκπλήρωση και των δύο όρων της αρχής της λογοδοσίας, πραγματοποιεί η εκτίμηση αντικτύπου. Κατά την εκπόνηση της εκτίμησης αντικτύπου, θα προκύψουν οι ανάλογοι κίνδυνοι που ίσως προκληθούν από την επεξεργασία των δεδομένων. Τότε και μόνο τότε, θα μπορέσουν να προκύψουν και τα κατάλληλα μέτρα, για την αντιμετώπιση των κινδύνων αυτών.

Σύμφωνα με το [45], η DPIA είναι μια διαδικασία που λαμβάνει χώρα, κυρίως στο αρχικό στάδιο σχεδίασης μιας εφαρμογής και είναι φτιαγμένη, για να περιγράψει την επεξεργασία, να αξιολογήσει την αναλογικότητα και την αναγκαιότητά της, αλλά και να συνδράμει στην διαχείριση των κινδύνων για τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων, που συνεπάγονται από την επεξεργασία των προσωπικών δεδομένων.

Σαν αποτέλεσμα αυτής της διαδικασίας, είναι μια έκθεση που έχει:

- Τα στοιχεία και τα χαρακτηριστικά της επεξεργασίας.
- Την εκτίμηση των πιθανών κινδύνων.
- Προτεινόμενα μέτρα ασφαλείας, για την επίτευξη του περιορισμού ή της εξάλειψης των κινδύνων αυτών.

Στην Ελλάδα, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), ελέγχει αυτή την έκθεση και κατόπιν εκδίδει την απαραίτητη άδεια επεξεργασίας των συγκεκριμένων δεδομένων, όπως ακριβώς προβλέπεται από τον ΓΚΠΔ. Το ότι η εκτέλεση της προηγούμενης διαδικασίας γίνεται στο αρχικό στάδιο σχεδίασης, αποτελεί πλεονέκτημα για την πρόληψη και αντιμετώπιση κινδύνων, καθώς και αποφυγής οικονομικής ζημιάς για τον οργανισμό [46].

Επειδή η επεξεργασία κάθε φορά υπάρχει περίπτωση να έχει υψηλό κίνδυνο για τις ελευθερίες και τα δικαιώματα των φυσικών προσώπων, η DPIA είναι απαραίτητη. Σύμφωνα με τον ΓΚΠΔ (άρθρο 35 παρ. 2), πρέπει να γίνεται:

- Όταν γίνεται συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών των φυσικών προσώπων, με αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα, που αφορούν φυσικό πρόσωπο.
- Όταν γίνεται μεγάλης κλίμακας επεξεργασία των ευαίσθητων δεδομένων.
- Όταν παρακολουθούνται σε μεγάλη κλίμακα δημόσιοι προσβάσιμοι χώροι.

Όπως καταλαβαίνουμε, η επιτυχία της DPIA είναι ανάλογη του χρονικού σημείου που θα πραγματοποιηθεί. Όσο νωρίτερα γίνει, τόσο πρώιμα θα βρεθούν, από τον σχεδιασμό ενός έργου, δείγματα που ίσως οδηγούν σε κινδύνους για τα δεδομένα προσωπικού χαρακτήρα και έτσι, θα μπορέσουν να ληφθούν και να ενσωματωθούν αποτελεσματικότερα και ακριβέστερα μέτρα, για την προστασία των δεδομένων αυτών. Η επιτυχία της DPIA, εκτός από το χρονικό σημείο, εξαρτάται και από τη συμμετοχή των κατάλληλων ανθρώπων που θα έχουν κατάλληλη εμπειρία και γνώση. Αν και ο όρος DPIA, μεταφράζεται σαν εκτίμηση ή αξιολόγηση, δεν είναι μόνο αυτό. Δεν αφορά μόνο την ανάλυση των κινδύνων, αλλά και μία λίστα με τα απαραίτητα μέτρα ελέγχου ή ασφαλείας, που έχουν σχέση με τους πιθανούς κινδύνους [47].

3.6 e-Privacy Directive

Η οδηγία 2002/58/ΕΚ για το απόρρητο και τις ηλεκτρονικές επικοινωνίες, αλλιώς γνωστή ως οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (e-Privacy Directive), είναι μια οδηγία της ΕΕ για την προστασία των δεδομένων και το απόρρητο στην ψηφιακή εποχή. Παρουσιάζει τη συνέχιση των προηγούμενων προσπαθειών και ειδικά την Οδηγία για την Προστασία Δεδομένων. Ασχολείται με τη ρύθμιση μιας σειράς σημαντικών θεμάτων όπως το απόρρητο των πληροφοριών, την επεξεργασία δεδομένων κίνησης, τα ανεπιθύμητα μηνύματα και τα cookies. Αυτή η Οδηγία έχει τροποποιηθεί με την Οδηγία 2009/136, η οποία εισάγει αρκετές αλλαγές, ιδίως σε ό,τι αφορά τα cookies, τα οποία υπόκεινται πλέον σε προηγούμενη συναίνεση. [48]

Η νομοθεσία e-Privacy Directive, όπως ήδη αναφέραμε, βρίσκει απόλυτη εφαρμογή στα cookies. Αυτά είναι μικρά αρχεία κειμένου, που αποθηκεύονται στον φυλλομετρητή μας στη διάρκεια της πλοήγησής μας στο διαδίκτυο. Στόχο έχουν, να ειδοποιούν τον ιστότοπο που επισκεπτόμαστε, για την προηγούμενη δραστηριότητά μας. Τις περισσότερες φορές, περιγράφουν στοιχεία χρηστών όπως όνομα χρήστη και κωδικό πρόσβασης, με απότερο σκοπό, όταν επισκεφτούμε τον ίδιο ιστότοπο αργότερα, να μας "θυμάται" και να μην χρειαστεί να κάνουμε login. Ενώ φαινομενικά αυτή η τεχνολογία διευκολύνει, στην ουσία δίνει στους διαχειριστές της ιστοσελίδας τα προσωπικά μας δεδομένα, τα οποία ενδεχομένως να μην θέλαμε να είναι διαθέσιμα.

Τα cookies διακρίνονται σε:

- Μόνιμα cookies τα οποία αποθηκεύονται στον υπολογιστή και δεν διαγράφονται αυτόματα μόλις κλείσει το πρόγραμμα περιήγησης
- Cookies περιόδου λειτουργίας, τα οποία διαγράφονται μόλις κλείσει το πρόγραμμα περιήγησης.

- Cookies προβαλλόμενου ιστότοπου τα οποία τοποθετούνται από τον ιστότοπο που επισκεπτόμαστε. Μπορούν να αναγνωστούν μόνο από τον συγκεκριμένο ιστότοπο. Επίσης, ο ιστότοπος υπάρχει πιθανότητα να χρησιμοποιεί εξωτερικές

υπηρεσίες, οι οποίες να τοποθετούν και αυτές τα δικά τους cookies (cookies τρίτων) [50].

Σύμφωνα με την e-Privacy, τα cookies που δεν είναι απαραίτητα στην παροχή της υπηρεσίας που κάνει αίτηση ο χρήστης, θα πρέπει να εγκαθίστανται μόνο όταν ο χρήστης δώσει ρητή συγκατάθεση, αφού πρώτα έχει ενημερωθεί πλήρως. Επομένως, για τα cookies αυτά, η προκαθορισμένη (εξ ορισμού) ρύθμιση επιβάλλεται να είναι η μη εγκατάσταση τους.

Ο κανονισμός e-Privacy Regulation, έρχεται για να ρυθμίσει τη χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών εντός της Ευρωπαϊκής Ένωσης και προορίζεται να αντικαταστήσει την Οδηγία για το απόρρητο και τις Ηλεκτρονικές Επικοινωνίες (Οδηγία 2002/58/ΕΚ). Ο κανονισμός e-Privacy απευθύνεται κυρίως σε εταιρείες που δραστηριοποιούνται στην ψηφιακή οικονομία και καθορίζει πρόσθετες απαιτήσεις που πρέπει να πληρούν σε σχέση με την επεξεργασία προσωπικών δεδομένων. Η οδηγία για την προστασία της ιδιωτικής ζωής ηλεκτρονικών επικοινωνιών, διασφαλίζει την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών, ιδίως του σεβασμού της ιδιωτικής ζωής, του απορρήτου των επικοινωνιών και της προστασίας των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών. Εγγυάται επίσης την ελεύθερη κυκλοφορία δεδομένων, εξοπλισμού και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ένωση. Εφαρμόζει στο παράγωγο δίκαιο της Ένωσης το θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής, όσον αφορά τις επικοινωνίες, όπως κατοχυρώνεται στο άρθρο 7 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») [European Commission 2017].

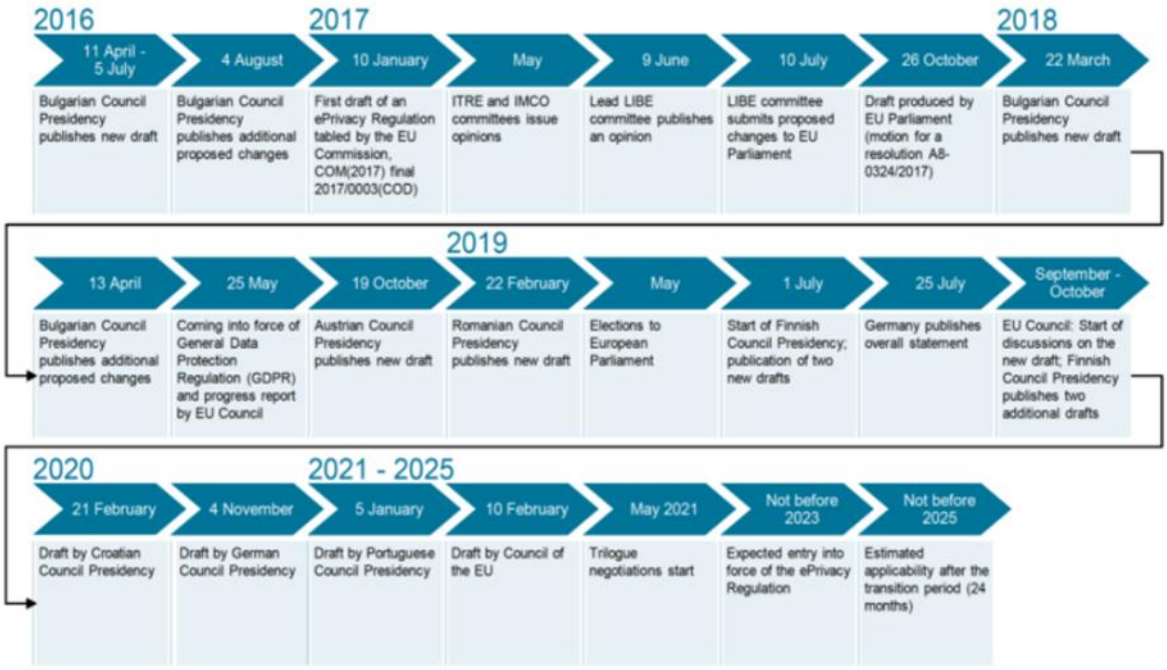
Αρχικά, ο Κανονισμός e-Privacy επρόκειτο να εφαρμοστεί από τις 25 Μαΐου 2018 μαζί με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR). Ωστόσο, σε αντίθεση με τον GDPR, τα κράτη μέλη της ΕΕ δεν έχουν ακόμη καταφέρει να συμφωνήσουν για το νομοσχέδιο. Αυτό σημαίνει, ότι οι διαπραγματεύσεις για τον Κανονισμό e-Privacy είναι ακόμη σε εξέλιξη.

Στις 10 Ιανουαρίου 2017, η Επιτροπή της ΕΕ παρουσίασε το πρώτο σχέδιο του κανονισμού για την προστασία της ιδιωτικής ζωής ηλεκτρονικών επικοινωνιών. Στις 26 Οκτωβρίου 2017, το Ευρωπαϊκό Κοινοβούλιο ενέκρινε τροποποιημένο σχέδιο και ψήφισε υπέρ των διαπραγματεύσεων με την Επιτροπή και το Συμβούλιο της Ευρωπαϊκής Ένωσης (τριμερείς διαπραγματεύσεις). Στις 5 Δεκεμβρίου 2017, η Εσθονική προεδρία του Συμβουλίου της ΕΕ δημοσίευσε το δικό της προσχέδιο. Ομοίως, ακολούθησαν προσχέδια από την Βουλγαρική, Αυστριακή, Ρουμανική, Φινλανδική, Κροατική και Γερμανική προεδρία του Συμβουλίου.

Πιο πρόσφατα, ο συμβιβασμός που πρότεινε η Γερμανία απέτυχε στις 4 Νοεμβρίου 2020. Μέχρι τότε, δεν υπήρχε έγκυρο σχέδιο κειμένου του Συμβουλίου Υπουργών. Ως αποτέλεσμα, οι τριμερείς διαπραγματεύσεις που ήταν προγραμματισμένες να ξεκινήσουν το δεύτερο εξάμηνο του 2018 καθυστέρησαν. Με την αλλαγή της Προεδρίας του Συμβουλίου της ΕΕ την 1η Ιανουαρίου 2021 και μετά από πολλά χρόνια, η Πορτογαλική προεδρία κατάφερε ωστόσο, να πείσει τα κράτη μέλη για την πρότασή της, την οποία έκανε στις 5 Ιανουαρίου 2021. Οι τριμερείς διαπραγματεύσεις με το Ευρωπαϊκό Κοινοβούλιο έχουν τώρα ξεκινήσει. Τα τελευταία, έγιναν γνωστά από μια έκδοση του Συμβουλίου Υπουργών της ΕΕ της 10ης Φεβρουαρίου 2021, που ανακοινώθηκε ότι επιτέλους βγήκε «λευκός καπνός».

Λαμβάνοντας υπόψη το γεγονός ότι υπάρχουν ορισμένα σημεία διαφωνίας σχετικά με το τρέχον κείμενο του κανονισμού, καταλαβαίνουμε ότι το e-Privacy ενδέχεται να μην προχωρήσει τόσο γρήγορα όσο η Πορτογαλική Προεδρία πιέζει. Ο Κανονισμός e-

Privacy δεν αναμένεται ασφαλώς να τεθεί σε ισχύ πριν από το 2023. Μια πιθανή μεταβατική περίοδος 24 μηνών σημαίνει ότι τυχόν νέοι κανονισμοί δεν θα τεθούν σε ισχύ πριν από το 2025 [51].



Εικόνα 5: e-Privacy Regulation - Χρονολογική επισκόπηση

Γενικότερα, αναφορικά με το τι πληροφορία μπορεί να εγκατασταθεί (και υπό ποιες προϋποθέσεις) στην κινητή συσκευή ενός χρήστη, καθώς και τι πρόσβαση μπορεί να αποκτηθεί σε πληροφορια που είναι ήδη αποθηκευμένη, εφαρμόζεται κατ' αρχάς η e-Privacy Οδηγία, ως ειδικότερη του GDPR. Στην Ελλάδα, ο νόμος που ενσωματώνει την εν λόγω Οδηγία στην εθνική νομοθεσία είναι ο ν. 3471/2006. Κάθε Κράτος-Μέλος έχει τη δική του νομοθεσία για την ενσωμάτωση της εν λόγω Οδηγίας – κάτι που συντελεί, εφόσον ακόμα δεν έχει οριστικοποιηθεί και ψηφιστεί ο e-Privacy Regulation, σε όχι απόλυτα συνεκτική εφαρμογή της εν λόγω νομοθεσίας στην Ευρώπη.

4. ΨΗΦΙΑΚΟ ΠΡΑΣΙΝΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

4.1 Τι είναι το Ψηφιακό Πράσινο Πιστοποιητικό

Οι πρώτες πληροφορίες για την εμφάνιση μιας νέας μεταδοτικής ασθένειας, έγιναν γνωστές στα τέλη του 2019. Από εκείνη τη στιγμή και μετά, οι εξελίξεις ήταν ραγδαίες. Ο

Covid-19 εξαπλώνεται, κρούσματα, θάνατοι, καραντίνα, τέλος οικονομικής και προσωπικής ζωής είναι τα καινούρια δεδομένα. Στα τέλη του 2020, λαμβάνουμε τα πρώτα θετικά δείγματα για τα εμβόλια και τότε είναι η στιγμή που η ΕΕ, αρχίζει να ψάχνει τρόπους, για την επιστροφή στην κανονικότητα. Η αποδεκτή πρόταση, είναι η δημιουργία του «ψηφιακού πράσινου πιστοποιητικού».

Το ψηφιακό πράσινο πιστοποιητικό είναι ένα έγγραφο, που διευκολύνει την ασφαλή και ελεύθερη κυκλοφορία εντός της ΕΕ στη διάρκεια της πανδημίας COVID-19. Αποδεικνύει ότι ο κάτοχός του έχει εμβολιαστεί κατά της νόσου COVID-19, ότι έχει εξεταστεί για COVID-19 με αρνητικό αποτέλεσμα ή ότι έχει αναρρώσει από την COVID-19. Η αρχική του χρήση, ήταν για όλα τα κράτη μέλη της ΕΕ, ενώ αργότερα επεκτάθηκε και για άλλες χώρες. Στη συνέχεια, θα αναφερθούν οι αρχικές σκέψεις και προτάσεις της επιτροπής, οι οποίες τελικά βρήκαν πλήρη εφαρμογή στο ψηφιακό πράσινο πιστοποιητικό που χρησιμοποιείται από όλους σήμερα.

Το ψηφιακό πράσινο πιστοποιητικό περιέχει τις απαραίτητες βασικές πληροφορίες, όπως ονοματεπώνυμο, ημερομηνία γέννησης, κράτος μέλος έκδοσης και έναν μοναδικό αναγνωριστικό κωδικό. Επίσης, περιλαμβάνει τρία διαφορετικά είδη πιστοποιητικών για την COVID-19 [52]:

- **Πιστοποιητικό εμβολιασμού:** Τα στοιχεία που αναγράφονται είναι το χορηγηθέν εμβόλιο και ο παρασκευαστής του εμβολίου, ο αριθμός των δόσεων, καθώς και η ημερομηνία εμβολιασμού.
- **Πιστοποιητικό εξέτασης:** Τα στοιχεία που αναγράφονται είναι το είδος της δοκιμασίας (PCR-RT/RAT), η ημερομηνία και η ώρα της δοκιμασίας, το κέντρο εξέτασης και το αποτέλεσμα.
- **Πιστοποιητικό ανάρρωσης:** Οι πληροφορίες που περιέχονται είναι η ημερομηνία θετικού αποτελέσματος δοκιμασίας, ο εκδότης του πιστοποιητικού, η ημερομηνία έκδοσης και η ημερομηνία λήξης ισχύος.

Όσον αφορά το πιστοποιητικό εξέτασης, για να εξασφαλιστεί η αξιοπιστία των αποτελεσμάτων των δοκιμασιών, επιλέξιμα για την έκδοση πιστοποιητικού εξέτασης βάσει του προτεινόμενου κανονισμού, πρέπει να είναι μόνο τα αποτελέσματα των λεγόμενων δοκιμασιών NAAT (πρόκειται για τις δοκιμασίες ενίσχυσης νουκλεϊκών οξέων που συμπεριλαμβάνουν τις δοκιμασίες RT-PCR) και των ταχειών δοκιμασιών αντιγόνων(RAT), που περιλαμβάνονται στον κατάλογο που καταρτίστηκε βάσει της σύστασης 2021/C 24/01 του Συμβουλίου.Οι αυτοδιαγνωστικές δοκιμασίες (self-test), δεν εκτελούνται σε ελεγχόμενες συνθήκες και θεωρούνται λιγότερο αξιόπιστες. Τα πιστοποιητικά θα πρέπει να εκδίδονται από τις υγειονομικές αρχές, οι οποίες, ωστόσο, δεν μπορούν να ελέγξουν δοκιμασίες που εκτελούνται, για παράδειγμα, στο σπίτι και επομένως, δεν μπορούν να εκδίδουν αξιόπιστα πιστοποιητικά γι' αυτές.

Η Επιτροπή πρότεινε τη δημιουργία, όχι μόνο διαλειτουργικού πιστοποιητικού εμβολιασμού, αλλά και πιστοποιητικών εξέτασης για την COVID-19, καθώς και πιστοποιητικών ανάρρωσης από αυτήν, για να διασφαλιστεί ο σεβασμός του δικαιώματος ελεύθερης κυκλοφορίας στην ΕΕ και η απουσία διακρίσεων εις βάρος ατόμων, που δεν έχουν εμβολιαστεί. Με τον τρόπο αυτό, μπορούν να επωφεληθούν από την έκδοση ψηφιακού πράσινου πιστοποιητικού, όσο το δυνατόν περισσότερα άτομα, όταν ταξιδεύουν.

Τα πιστοποιητικά μπορούν να εκδίδονται και να χρησιμοποιούνται σε όλα τα κράτη μέλη της ΕΕ για τη διευκόλυνση της ελεύθερης κυκλοφορίας. Όλοι οι πολίτες της ΕΕ και τα μέλη των οικογενειών τους, καθώς και υπήκοοι τρίτων χωρών που παραμένουν ή

διαμένουν σε κράτη μέλη της ΕΕ, είναι επιλέξιμοι για τη δωρεάν χορήγηση πιστοποιητικού. Το δικαίωμα της ελεύθερης κυκλοφορίας, ισχύει και για υπηκόους τρίτων χωρών που παραμένουν ή διαμένουν σε κράτη μέλη της ΕΕ και οι οποίοι έχουν το δικαίωμα να ταξιδέψουν σε άλλα κράτη μέλη. Το ψηφιακό πράσινο πιστοποιητικό διευκολύνει την άσκηση αυτού του δικαιώματος, μεταξύ άλλων μέσω πιστοποιητικού εξέτασης και πιστοποιητικού ανάρρωσης.

Τα πιστοποιητικά εκδίδονται σε ψηφιακή μορφή, ώστε να είναι δυνατή η εμφάνισή τους σε έξυπνο τηλέφωνο ή η εκτύπωσή τους, ανάλογα με την προτίμηση του κατόχου τους. Τα πιστοποιητικά περιέχουν διαλειτουργικό μηχαναγνώσιμο κωδικό QR που περιέχει τα απαραίτητα βασικά δεδομένα, καθώς και ψηφιακή υπογραφή. Ο κωδικός QR χρησιμοποιείται για την ασφαλή επαλήθευση της γνησιότητας, της εγκυρότητας και την ακεραιότητας του πιστοποιητικού. Για την καλύτερη διασυνοριακή αποδοχή, οι πληροφορίες στο πιστοποιητικό πρέπει να αναγράφονται στη γλώσσα ή στις γλώσσες του κράτους μέλους έκδοσης και στα αγγλικά. Ο κωδικός QR, που περιέχεται στο ψηφιακό πράσινο πιστοποιητικό, έχει ψηφιακή υπογραφή για την προστασία του από πλαστογράφηση. Όταν γίνεται έλεγχος στο πιστοποιητικό, σαρώνεται ο κωδικός QR και γίνεται η επαλήθευση της υπογραφής. Όλοι οι φορείς έκδοσης (π.χ. νοσοκομεία, κέντρα εξέτασης, υγειονομικές αρχές) διαθέτουν το δικό τους κλειδί ψηφιακής υπογραφής. Όλα αυτά αποθηκεύονται σε ασφαλή βάση δεδομένων στην κάθε χώρα.

Η Ευρωπαϊκή Επιτροπή δημιούργησε μια πύλη (μια ψηφιακή υποδομή η οποία συνδέει τις εθνικές βάσεις δεδομένων που περιέχουν δημόσια κλειδιά υπογραφής). Μέσω της πύλης αυτής, όλες οι υπογραφές των πιστοποιητικών μπορούν να επαληθευτούν σε όλη την ΕΕ. Τα προσωπικά δεδομένα του κατόχου του πιστοποιητικού δεν περνούν μέσω της πύλης, αφού αυτό δεν είναι αναγκαίο για την επαλήθευση της ψηφιακής υπογραφής. Η Ευρωπαϊκή Επιτροπή, προσφέρει επίσης λύσεις αναφοράς ανοικτού κώδικα, με σκοπό να υποστηρίξει τα κράτη μέλη στην ανάπτυξη λογισμικού, το οποίο μπορούν να χρησιμοποιούν οι αρχές για τη σάρωση και τον έλεγχο των κωδικών QR.

Η διάρκεια ισχύος των πιστοποιητικών εξαρτάται από επιστημονικά δεδομένα και θα καθορίζεται από τους αρμόδιους για την επαλήθευση σύμφωνα με τους εθνικούς τους κανόνες. Όταν ανακύπτουν νέα επιστημονικά δεδομένα, οι περίοδοι ισχύος των πιστοποιητικών για την εξαίρεση από τις ισχύουσες απαιτήσεις δημόσιας υγείας θα μπορούν να προσαρμοστούν. Τα πιστοποιητικά συνδέονται με την πανδημία COVID-19. Το σύστημα ψηφιακών πράσινων πιστοποιητικών θα ανασταλεί μόλις ο Παγκόσμιος Οργανισμός Υγείας (ΠΟΥ) κηρύξει το τέλος της διεθνούς κατάστασης έκτακτης ανάγκης στον τομέα της δημόσιας υγείας εξαιτίας της COVID-19. Ομοίως, αν ο ΠΟΥ κηρύξει εκ νέου διεθνή κατάσταση έκτακτης ανάγκης στον τομέα της δημόσιας υγείας εξαιτίας της COVID-19, παραλλαγής της ή παρόμοιας λοιμώδους νόσου, το σύστημα θα μπορούσε να ενεργοποιηθεί και πάλι.

Το ψηφιακό πράσινο πιστοποιητικό χορηγείται δωρεάν και η χρήση του δεν σταματάει στα ταξίδια. Τα κράτη μέλη της ΕΕ, μπορούν να χρησιμοποιούν το ψηφιακό πιστοποιητικό COVID της ΕΕ για εθνικούς σκοπούς, για παράδειγμα για την παροχή πρόσβασης σε πολιτιστικές εκδηλώσεις, σε εστιατόρια ή στον χώρο εργασίας. Η χρήση αυτή δεν καλύπτεται από τη νομοθεσία της ΕΕ και εναπόκειται στα κράτη μέλη της ΕΕ να την αποφασίσουν. Η Επιτροπή θα χρηματοδοτήσει τη δημιουργία της πύλης σε επίπεδο ΕΕ και θα υποστηρίξει τα κράτη μέλη για την ανάπτυξη λογισμικού που θα χρησιμοποιείται από τους αρμόδιους για την επαλήθευση που θα σαρώνουν τον κωδικό QR. Επομένως, η κάθε χώρα θα μπορεί να δημιουργήσει την δική της εφαρμογή, με σκοπό το σκανάρισμα του κωδικού QR και την επαλήθευση ή μη του εκάστοτε πιστοποιητικού. Επίσης, δημιουργείται άλλη μια εφαρμογή (wallet), η οποία δίνει το δικαίωμα στο χρήστη να αποθηκεύει στο έξυπνο κινητό του το εκάστοτε πιστοποιητικό για πιο εύκολη χρήση. Τέλος, ορισμένες χώρες διαθέτουν μια εφαρμογή, η οποία

καλύπτει και τις 2 περιπτώσεις (δηλαδή επαλήθευση και αποθήκευση). Οσον αφορά την προστασία προσωπικών δεδομένων, πρέπει να είναι γνωστός ο υπεύθυνος της επεξεργασίας, οι εκτελούντες την επεξεργασία, καθώς και τυχόν επεξεργασία προσωπικών δεδομένων, που τους έχει ανατεθεί. Επίσης θα πρέπει η εκτέλεση επεξεργασίας να καλύπτεται από απαραίτητες συμβάσεις, στις οποίες θα προβλέπονται οι κατάλληλες εγγυήσεις για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων. Με τον τρόπο αυτό, θα είναι σε θέση να εκπληρώνουν τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων, σύμφωνα με τον ΓΚΠΔ.

Από αυτές τις εφαρμογές, έχουμε κάποιες συγκεκριμένες λειτουργικές απαιτήσεις. Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, μεταξύ άλλων μέτρων για την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, τα δεδομένα που υποβάλλονται σε επεξεργασία θα πρέπει να περιορίζονται στο απολύτως ελάχιστο. Η εφαρμογή δεν θα πρέπει να συλλέγει άσχετες ή αχρείαστες πληροφορίες, οι οποίες μπορεί να περιλαμβάνουν την οικογενειακή κατάσταση, αναγνωριστικά επικοινωνίας, στοιχεία των καταλόγων αρχείων στον εξοπλισμό, μηνύματα, μητρώα κλήσεων, δεδομένα θέσης, αναγνωριστικά συσκευής κ.λπ. [53]. Επιπλέον, θα πρέπει να είναι έτσι δομημένες, έτσι ώστε μετά την επαλήθευση του εκάστοτε πιστοποιητικού, να απαγορεύεται στον ενδιαφερόμενο (αεροδρόμια, καταστηματάρχες κ.α.) να αποθηκεύσει τα στοιχεία της επαλήθευσης. Θα πρέπει επίσης, να γίνουν γνωστές οι κυρώσεις, που θα επιβάλλονται στον παραβάτη.

Σύμφωνα με τη Γνωμοδότηση 2/2021 της ελληνικής Αρχής Προστασίας Δεδομένων [54], ο σκοπός του ελέγχου των πιστοποιητικών είναι ο πολίτης που εισέρχεται σε έναν χώρο, να είναι «υγειονομικά ασφαλής», με τον τρόπο που η ασφάλεια αυτή ορίζεται στην κάθε περίπτωση. Ως εκ τούτου, η επαλήθευση των πιστοποιητικών μέσω της εφαρμογής θα πρέπει να οδηγεί στην ταυτότητα του κατόχου, καθώς και σε ένα αποτέλεσμα της μορφής «ναι/όχι» (π.χ. πράσινο ή κόκκινο χρώμα), έτσι ώστε να εξάγεται η πληροφορία αν ο πολίτης που εισέρχεται σε ένα χώρο είναι «υγειονομικά ασφαλής», χωρίς όμως να αποκαλύπτονται ειδικότερες πληροφορίες σχετικά με το εάν έχει εμβολιαστεί, αν έκανε τεστ ή αν έχει νοσήσει προηγουμένως από λοίμωξη με COVID-19. Πρέπει επίσης να ληφθεί υπόψη ότι η χρήση «έξυπνων» εφαρμογών εγείρει διάφορα ζητήματα ιδιωτικότητας, αν δεν ληφθούν εγκαίρως κατάλληλα μέτρα κατά την ανάπτυξή τους, όπως για παράδειγμα ο κίνδυνος διαρροής δεδομένων σε τρίτα μέλη (third parties), εάν και εφόσον χρησιμοποιηθούν έτοιμες βιβλιοθήκες κώδικα τρίτων μελών. Η DPIA, είναι υπεύθυνη για να απαριθμήσει τα τεχνικά και οργανωτικά μέτρα που σχεδιάστηκαν, έτσι ώστε να ελαχιστοποιηθούν οι εντοπισθέντες κίνδυνοι. Θα πρέπει να ληφθούν υπόψη στην ανάλυση, οι κίνδυνοι που απορρέουν από τη δόλια έκδοση, την παράνομη χρήση ή ακόμη και την παραποίηση των ψηφιακών στοιχείων που περιέχονται στα πιστοποιητικά. Οι κίνδυνοι αυτοί, μπορεί να έχουν αντίκτυπο στα δικαιώματα και τις ελευθερίες των ατόμων που επιθυμούν να έχουν πρόσβαση σε τόπους, εγκαταστάσεις ή εκδηλώσεις, που η είσοδός τους υπόκειται σε έλεγχο ως προς την υγειονομική τους κατάσταση. Τέλος, η χρήση της ηλεκτρονικής εφαρμογής πραγματοποιείται από τους ιδιοκτήτες ή διοργανωτές και από εξουσιοδοτημένους από αυτούς υπαλλήλους επιχειρήσεων (υπεύθυνοι Covid 19, οι οποίοι θα βρίσκονται στην είσοδο του εκάστοτε χώρου), έτσι ώστε να μην μπορεί ο οποιοσδήποτε να έρχεται σε επαφή με τα προσωπικά δεδομένα των ατόμων που ελέγχονται.

4.2 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) - European Data Protection Board (EDPB)

Το ΕΣΠΔ είναι ένα όργανο της ΕΕ επιφορτισμένο με την εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων και ιδρύθηκε στις 25 Μαΐου 2018. Αποτελείται από τον επικεφαλής κάθε ΑΠΔ και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) ή τους εκπροσώπους τους. Το ΕΣΠΔ, έχει σαν σκοπό να είναι στο επίκεντρο του νέου τοπίου, το οποίο διαμορφώνεται στην ΕΕ σχετικά με την προστασία των δεδομένων. Θα βοηθήσει στη διασφάλιση της νομοθεσίας για την προστασία των δεδομένων, έτσι ώστε να εφαρμόζεται με συνέπεια σε όλη την ΕΕ και θα καταβάλλει προσπάθειες για να εξασφαλίσει την αποτελεσματική συνεργασία των ΑΠΔ. Το ΕΣΠΔ θα εκδίδει κατευθυντήριες οδηγίες για την ερμηνεία βασικών εννοιών του ΓΚΠΔ, αλλά και θα καλείται να παίρνει δεσμευτικές αποφάσεις σε διαφορές, που προκύπτουν με ζητήματα διασυνοριακής επεξεργασίας, διασφαλίζοντας με αυτόν τον τρόπο την ομοιόμορφη εφαρμογή των κανόνων της ΕΕ, με σκοπό να αποφεύγεται το ενδεχόμενο η ίδια υπόθεση να αντιμετωπίζεται με διαφορετικό τρόπο στις διάφορες έννομες τάξεις [55].

Με τη σειρά του, ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων είναι μια ανεξάρτητη εποπτική αρχή, που πρωταρχικός στόχος της είναι να διασφαλίσει ότι τα ευρωπαϊκά θεσμικά όργανα και οργανισμοί σέβονται το δικαίωμα στην προστασία της ιδιωτικής ζωής και των δεδομένων, όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και αναπτύσσουν νέες πολιτικές. Τα καθήκοντα και οι εξουσίες του ΕΕΠΔ και του Αναπληρωτή Επόπτη, καθώς και η θεσμική ανεξαρτησία της εποπτικής αρχής, καθορίζονται από τον "Κανονισμό για την Προστασία των Δεδομένων". Στην πράξη, οι δραστηριότητες του ΕΕΠΔ μπορούν να χωριστούν σε τρεις κύριους ρόλους: εποπτεία, γνωμοδότηση και συνεργασία [56].

Η εμφάνιση του COVID-19, οδήγησε τον Απρίλιο του 2021 το ΕΣΠΔ και τον ΕΕΠΔ να εκδώσουν κοινή γνώμη σχετικά με τις προτάσεις για ένα ψηφιακό πράσινο πιστοποιητικό. Το πιστοποιητικό αυτό, έχει σαν στόχο να διευκολύνει την άσκηση του δικαιώματος της ελεύθερης κυκλοφορίας εντός της ΕΕ κατά τη διάρκεια της πανδημίας, με τη θέσπιση κοινού πλαισίου για την έκδοσή του, την επαλήθευση και την αποδοχή διαλειτουργικών πιστοποιητικών εμβολιασμού κατά της COVID-19, διαγνωστικών τεστ για την εν λόγω νόσο, καθώς και ανάρρωσης από αυτήν.

Το ΕΣΠΔ και ο ΕΕΠΔ, ζητούν από τους συννομοθέτες, να διασφαλίσουν ότι το ψηφιακό πράσινο πιστοποιητικό συμβαδίζει πλήρως με τη νομοθεσία της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα. Οι επίτροποι προστασίας δεδομένων από όλες τις χώρες της ΕΕ και του Ευρωπαϊκού Οικονομικού Χώρου, υπερτονίζουν την ανάγκη να μετριαστούν όσο πιο πολύ γίνεται οι κίνδυνοι για τα θεμελιώδη δικαιώματα των πολιτών και των κατοίκων της ΕΕ, οι οποίοι ενδέχεται να προκύψουν από την έκδοση του συγκεκριμένου πιστοποιητικού, συμπεριλαμβανομένων και των πιθανών ανεπιθύμητων δευτερογενών χρήσεών του. Το ΕΣΠΔ και ο ΕΕΠΔ υπογραμμίζουν επίσης, ότι η χρήση του πράσινου πιστοποιητικού δεν μπορεί και δεν πρέπει, σε καμία περίπτωση να οδηγήσει σε άμεσες ή έμμεσες διακρίσεις εις βάρος των φυσικών προσώπων. Ακόμα, θα πρέπει να είναι πλήρως σύμφωνο με τις θεμελιώδεις αρχές της αναγκαιότητας, της αναλογικότητας και της αποτελεσματικότητας. Επιπροσθέτως, το ΕΣΠΔ και ο ΕΕΠΔ πιστεύουν ότι η εισαγωγή του ψηφιακού πράσινου πιστοποιητικού θα πρέπει να συνοδεύεται από ένα ολοκληρωμένο νομικό πλαίσιο.

Η πρόταση για το ψηφιακό πράσινο πιστοποιητικό, θα πρέπει να θεσπίζει σαφείς και ακριβείς κανόνες που θα διέπουν το πεδίο και τον τρόπο εφαρμογής του, καθώς και να επιβάλλει κατάλληλες διασφαλίσεις. Έτσι, τα φυσικά πρόσωπα των οποίων τα

δεδομένα προσωπικού χαρακτήρα θίγονται, θα έχουν επαρκείς εγγυήσεις ότι θα προστατεύονται αποτελεσματικά από τον κίνδυνο πιθανών διακρίσεων. Επιπροσθέτως, αυτή η πρόταση, πρέπει να διαλαμβάνει ρητά ότι δεν επιτρέπονται η πρόσβαση σε δεδομένα φυσικών προσώπων και η επακόλουθη χρήση τους από τα κράτη μέλη της ΕΕ, με το πέρας της πανδημίας.

Η κοινή γνώμη ζητάει ειδικές συστάσεις για περαιτέρω διευκρινίσεις σχετικά με τις κατηγορίες δεδομένων που αφορά η πρόταση για το πιστοποιητικό, όπως την αποθήκευση των δεδομένων, τις υποχρεώσεις διαφάνειας και την ταυτοποίηση των υπευθύνων επεξεργασίας και όσων εκτελούν την επεξεργασία προσωπικών δεδομένων [57].

4.3 Προστασία Προσωπικών Δεδομένων στα Ψηφιακά Πράσινα Πιστοποιητικά

Η δημιουργία του πράσινου πιστοποιητικού, βασίστηκε πάνω στις κατευθυντήριες προτάσεις των ΕΣΠΔ και ΕΕΠΔ. Οι προτάσεις αυτές, ήταν σύμφωνες με τους κανόνες του ΓΚΠΔ, για την προστασία των προσωπικών δεδομένων.

Τα πιστοποιητικά, περιλαμβάνουν μόνο ένα ελάχιστο σύνολο πληροφοριών, απαραίτητων για την επιβεβαίωση και την επαλήθευση της κατάστασης του κατόχου τους, όσον αφορά τον εμβολιασμό, την εξέταση ή την ανάρρωση. Το ψηφιακό πιστοποιητικό COVID της ΕΕ έχει σχεδιαστεί για να προσφέρει πολύ υψηλό επίπεδο προστασίας των δεδομένων.

Χρησιμοποιεί αποκεντρωμένο σύστημα, το οποίο δεν απαιτεί μία κεντρική βάση δεδομένων της ΕΕ η οποία να περιέχει προσωπικά δεδομένα για όλα τα πιστοποιητικά που εκδίδονται, ούτε ανταλλαγές προσωπικών δεδομένων μεταξύ των αρχών. Τα δεδομένα στα οποία έχει πρόσβαση ο ελεγκτής δεν θα πρέπει να φυλάσσονται μετά από αυτόν (π.χ. κατά την επιβίβαση σε πτήση). Ο φορέας έκδοσης (π.χ. κέντρο εμβολιασμού) δεν μπορεί να διατηρεί τα δεδομένα για διάστημα μεγαλύτερο από το αναγκαίο, και σε καμία περίπτωση για διάστημα μεγαλύτερο από την περίοδο κατά την οποία οι κάτοχοι των πιστοποιητικών μπορούν να τα χρησιμοποιούν για να ασκούν το δικαίωμά τους να ταξιδεύουν. Το σύστημα, απαιτεί περιορισμένο μόνο όγκο προσωπικών δεδομένων. Για παράδειγμα, ο κατάλογος των κατηγοριών δεδομένων είναι συντομότερος από το αντίστοιχο περιεχόμενο στο «κίτρινο βιβλιάριο» του ΠΟΥ (που χρησιμοποιείται σε ορισμένα κράτη για την τεκμηρίωση των εμβολιασμών). Σύμφωνα με τις κατευθυντήριες γραμμές για τις τεχνικές προδιαγραφές, η διεπαφή του ελεγκτή πρέπει να παρουσιάζει το αποτέλεσμα της επαλήθευσης κατά τέτοιο τρόπο, ώστε να εμφανίζονται μόνο οι ελάχιστες απαιτούμενες πληροφορίες [58]:

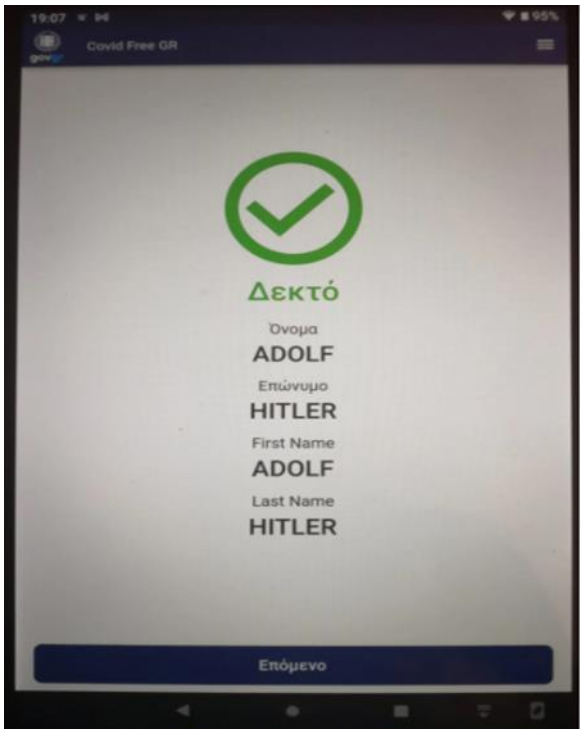
- για τις επιτυχείς επαληθεύσεις, οι πληροφορίες θα πρέπει να περιλαμβάνουν την ένδειξη ότι το πιστοποιητικό έχει όντως επαληθευτεί, καθώς και τα ελάχιστα προσωπικά στοιχεία που είναι απαραίτητα για τη σύνδεση του πιστοποιητικού με τον κάτοχό του.
- για τις μη επιτυχείς επαληθεύσεις, η διεπαφή θα πρέπει να αναφέρει την αιτία, καθώς και συναφείς λεπτομέρειες που δεν επέτρεψαν την επαλήθευση.

4.4 Κίνδυνοι Ιδιωτικότητας και Κενά στα Ψηφιακά Πράσινα Πιστοποιητικά

Όπως αναφέραμε ήδη, η δημιουργία του πράσινου πιστοποιητικού είναι σύμφωνη με τον ΓΚΠΔ και άρρηκτα συνδεδεμένη με την προστασία της ιδιωτικότητας. Από την πρώτη σχεδόν ημέρα λειτουργίας του όμως, φάνηκε ότι υπάρχουν κενά, τα οποία

πρέπει οι αρμόδιες αρχές να αντιμετωπίσουν. Αρκετοί είναι οι επιτήδειοι, που με διάφορους τρόπους κατέρρηψαν την προστασία τις ιδιωτικότητας.

Ένα τέτοιο παράδειγμα, είναι το πλαστό πιστοποιητικό του Αδόλφου Χίτλερ, το οποίο εμφανίστηκε. Όπως αναφέρεται στο [59], βρέθηκε στα λάθος χέρια το κρυπτογραφημένο κλειδί που χρησιμοποιείται για την πιστοποίηση ψηφιακών πιστοποιητικών εμβολιασμού κατά του κορονοϊού σε ορισμένες ευρωπαϊκές χώρες με αποτέλεσμα να έχουν πλαστογραφηθεί ψεύτικα πιστοποιητικά για πραγματικούς ανθρώπους. Έτσι, πέρα από πιστοποιητικά νεκρών ανθρώπων, βρέθηκαν και άλλα φανταστικών χαρακτήρων όπως του Μίκι Μάους και του Μπόμπ Σφουγκαράκη. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, το πάσο περιέχει έναν κωδικό QR με ψηφιακή υπογραφή για την προστασία του από παραποίηση, με αποτέλεσμα τα παραπάνω περιστατικά να εγείρουν ερωτήματα σχετικά με την ασφάλεια του συστήματος του "εμβολιαστικού διαβατηρίου" της ΕΕ. Με τον ίδιον τρόπο, κάποιος επιτήδειος μπορεί να χρησιμοποιήσει το όνομα του καθενός σε ένα πλαστό πιοστοποιητικό χωρίς εμείς να το γνωρίζουμε. Όπως αναφέρει το [60], κατόπιν μιας σειράς συναντήσεων, αποφασίστηκε να ακυρωθούν όλα τα πιστοποιητικά που δημιουργήθηκαν με αυτά τα κλειδιά. Για να αποδειχθεί ότι πράγματι χάθηκαν τα κλειδιά κάποιος ανέβασε ένα QR που αν σκαναριστεί με μια επίσημη εφαρμογή πιστοποίησης, στην Ελλάδα το Covid Free GR app, βγάζει εμβολιασμένο τον Αδόλφο Χίτλερ. Όπως φαίνεται και από την παρακάτω εικόνα, ο μεγαλύτερος σφαγέας της Ευρώπης, που αυτοκτόνησε το 1945, δείχνει ακίνδυνος, τουλάχιστον από τον Covid-19.



Εικόνα 6: Αποτέλεσμα Ελέγχου του Πιστοποιητικού του Αδόλφου Χίτλερ

Παρόμοια περιτατικά πλαστών πιστοποιητικών εμφανίζονται κάθε μέρα στη Βουλγαρία και στη Ρουμανία, σύμφωνα με το [61]. Στις χώρες αυτές, ο αριθμός των αντιεμβολιαστών είναι αρκετά μεγάλος. Αυτό έχει ως αποτέλεσμα, να έχουν δημιουργηθεί οργανώσεις, οι οποίες βρήκαν τον τρόπο να δημιουργούν πλαστά πιστοποιητικά και να τα πουλούν έναντι 300 ευρώ. Επίσης, υπάρχουν και οικογενειακοί

γιατροί, οι οποίοι εκδίδουν πιστοποιητικά εμβολιασμού, με τα στοιχεία του κάθε πολίτη, χωρίς όμως να έχει δεχθεί τη δόση του εμβολίου.

Από την άλλη, δεν είναι μόνο οι επιτήδειοι που προκαλούν προβλήματα, αλλά και τα ίδια τα ψηφιακά πιστοποιητικά, γιατί όπως θα αναλύσουμε παρακάτω, οι εφαρμογές κάποιων χωρών για τον έλεγχο των πιστοποιητικών, περιέχουν «ιχνηλάτες». Αυτοί με τη σειρά τους, μπορεί να προκαλέσουν προβλήματα ιδιωτικότητας μιας και αντλούν πληροφορίες από τα κινητά των χρηστών.

Τα ανωτέρω, ο ρόλος της Επιτροπής, η πληροφορία εμβολιασμού, η διασυνοριακή λειτουργία του, είναι ενδεικτικά. Από εκεί και ύστερα, κάθε χώρα αναπτύσσει τη δική της εφαρμογή, που θα πρέπει να πληροί τις γενικές απαιτήσεις, ενώ η ακριβής χρήση του κάθε πιστοποιητικού έγκειται επίσης σε κάθε χώρα. Στην Ελλάδα, η εφαρμογή για τα ψηφιακά πράσινα πιστοποιητικά, συμπεριλαμβάνει το ΑΜΚΑ του κάθε πολίτη. Αυτό από μόνο του δημιουργεί ερωτήματα σχετικά με την προστασία των προσωπικών δεδομένων. Δηλαδή όποιος γνωρίζει αυτό τον προσωπικό κωδικό μπορεί να:

- βρει αρκετά προσωπικά στοιχεία όπως διεύθυνση, τηλέφωνο, ονοματεπώνυμο.
- ανακαλύψει στοιχεία που αφορούν τον ιατρικό φάκελο του ατόμου όπως αν έχει νοσηλευτεί, ποια ιατροφαρμακευτική περίθαλψη του έχει χορηγηθεί τι φάρμακα παίρνει κ.α.
- δημιουργήσει και να εκδόσει παράνομες συνταγές φαρμάκων, εάν και εφόσον είναι γνώστης (hacker) και μπορεί με παράνομο τρόπο να έχει πρόσβαση σε δεδομένα/βάσεις δεδομένων, στα οποία υπό κανονικές συνθήκες, η πρόσβαση είναι εφικτή μόνο από τους γιατρούς.

Όσον αφορά τα κενά των ψηφιακών πράσινων πιστοποιητικών, υπήρξαν άνθρωποι που δεν μπορούσαν να εκδώσουν το πιστοποιητικό, είτε νόσησης είτε εμβολιασμού, λόγω λαθών-κενών στο σύστημα καταγραφής. Επίσης, υπήρξαν περιπτώσεις ανεμβολίαστων ανθρώπων, οι οποίοι για να αποκτήσουν πρόσβαση σε μέρη που επιτρέπονται μόνο εμβολιασμένοι, χρησιμοποιούσαν πιστοποιητικά γνωστών τους, συγγενών ή φίλων. Αυτό οδήγησε τις κυβερνήσεις, στην υποχρεωτική ταυτοποίηση με ταυτότητα ή διαβατήριο. Επιπλέον, παρατηρήθηκε ένα ακομά κενό, αυτή τη φορά στις εφαρμογές επαλήθευσης πιστοποιητικών. Υπάρχουν περιπτώσεις, στις οποίες για να μπει κάποιος κάπου (πχ. σε νοσοκομείο ή παλιότερα σε καφετέρια), χρειαζόταν αρνητικό rapid test 48ώρου. Η έννοια του 48ώρου δεν ήταν ακριβής στις αρχές, καθώς η ισχύ του ήταν για δύο ημερολογιακές ημέρες και όχι ακριβώς 48 ώρες (δηλαδή δεν μέτραγε το 48ωρο από την ώρα που το έκανε κάποιος και για 48 ώρες μετά). Το πρόβλημα αυτό, δείχνει να έχει λυθεί με την πάροδο του χρόνου, μιας και τώρα ελέγχεται η ώρα διενέργειας του τέστ και όχι μόνο η ημερομηνία.

5. ΕΡΓΑΛΕΙΑ ΑΝΑΛΥΣΗΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΚΙΝΗΤΩΝ ΕΦΑΡΜΟΓΩΝ

Στο παρόν κεφάλαιο, θα παρουσιάσουμε τα εργαλεία που χρησιμοποιήθηκαν, για την υλοποίηση της παρούσας διπλωματικής εργασίας. Θα αναλυθεί βήμα βήμα ο τρόπος

χρήσης του κάθε εργαλείου, έτσι ώστε να φτάσουμε στην άντληση των δεδομένων που θα μας βοηθήσουν στην περάτωσή της.

5.1 Exodus

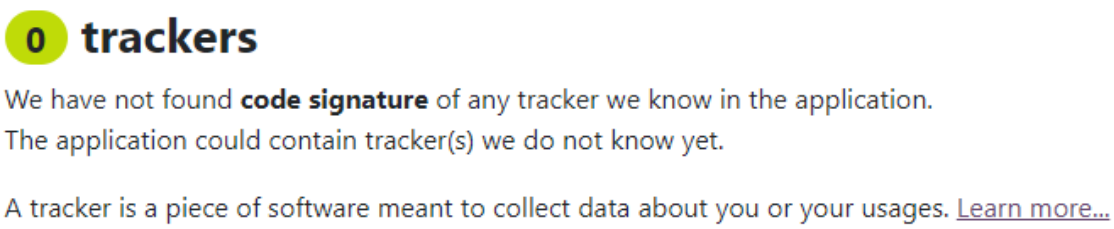
Το Exodus Privacy είναι ένας γαλλικός μη κερδοσκοπικός οργανισμός, ο οποίος στοχεύει στην προστασία του απορρήτου και διοικείται από τους hacktivists. Σκοπός του Exodus Privacy, είναι η ευαισθητοποίηση σχετικά με την παρακολούθηση που πραγματοποιείται από εφαρμογές Android, με τη βοήθεια εργαλείων ανάλυσης και διδακτικού υλικού. Αναλύει εφαρμογές Android και ψάχνει για ενσωματωμένους trackers, τους οποίους και παραθέτει στο χρήστη. Ένας tracker, είναι ένα κομμάτι λογισμικού, που συλλέγει δεδομένα σχετικά με τους χρήστες ή με το τι κάνουν. Το Exodus δεν απομεταγλωττίζει εφαρμογές. Η τεχνική ανάλυσής του είναι απολύτως νόμιμη και προσφέρει τις ακόλουθες επιλογές [62]:

- έλεγχο της αναφοράς μιας εφαρμογής Android, με τη χρήση της μηχανής αναζήτησης
- ανάλυση μιας νέας εφαρμογής Android, κατόπιν αίτησης για ανάλυση
- παροχή μιας λίστας με πράγματα που μπορεί ο χρήστης να κάνει, για να βελτιώσει το απόρρητό στο smartphone του

Στην παρακάτω εικόνα βλέπουμε την επισκόπιση της αναφοράς που μας έδωσε το exodus, σχετικά με την πράσινη εφαρμογή της Ελλάδας (Covid Free GR).

Εικόνα 7: Επισκόπηση Αναφοράς exodus για την Εφαρμογή Covid Free GR

Κάθε αναφορά περιέχει ποιοι trackers είναι ενσωματωμένοι στην εκάστοτε εφαρμογή. Για κάθε tracker, ο χρήστης μπορεί να δει περισσότερες λεπτομέρειες για αυτόν, καθώς και τη λίστα των εφαρμογών που το χρησιμοποιούν. Στην περίπτωση της Covid Free GR εφαρμογής, δεν υπάρχουν trackers, όπως φαίνεται από την εικόνα.



Εικόνα 8: Αριθμός Ιχνηλατών στην Εφαρμογή Covid Free GR

Μια αναφορά, θα παρέχει επίσης τη λίστα με τα δικαιώματα, τα οποία η εφαρμογή αιτείται για λειτουργία στο smartphone του χρήστη (όπως φαίνεται και από την παρακάτω εικόνα για την Covid Free GR εφαρμογή). Ορισμένες από αυτές τις άδειες, επισημαίνονται ως επικίνδυνες. Αυτό σημαίνει, ότι από την άποψη της Google, η εφαρμογή μπορεί να κάνει «κακόβουλα» πράγματα χρησιμοποιώντας αυτήν την άδεια. Επιπλέον, το exodus χρησιμοποιεί την ταξινόμηση αδειών Google.

Τέλος, το exodus δημοσίευσε μια εφαρμογή Android, η οποία έχει σχεδιαστεί για να απαριθμεί τις εφαρμογές, που είναι ήδη εγκατεστημένες στα κινητά τηλέφωνα, καθώς και τους ενσωματωμένους trackers σε κάθε μία εφαρμογή.

5.2 Lumen Privacy Monitor

Το Lumen Privacy Policy, είναι μια εφαρμογή που δημιουργήθηκε από το Haystack Project, μια ακαδημαϊκή πρωτοβουλία, η οποία είχε την καθοδήγηση ανεξάρτητων ακαδημαϊκών ερευνητών από το Διεθνές Ινστιτούτο Επιστήμης Υπολογιστών (ICSI), UC Berkeley και το IMDEA Networks. Η χρηματοδότηση έγινε από Εθνικό Ίδρυμα Επιστήμης (NSF – National Science Foundation) και το Εργαστήριο Διαφάνειας Δεδομένων (Data Transparency Lab). Το Lumen, είναι μια εφαρμογή Android, η οποία παρακολουθεί και αναλύει την εγκατεστημένη επισκεψιμότητα του κινητού. Ταυτόχρονα,

βοηθά τον χρήστη στον εντοπισμό των διαρροών του απορρήτου, οι οποίες είναι αποτέλεσμα των εγκατεστημένων εφαρμογών στο κινητό. Επίσης, δίνει την δυνατότητα στο χρήστη να πάρει πληροφορίες, σχετικές με τις εταιρείες που συλλέγουν τις πληροφορίες αυτές. Το Lumen δηλαδή, λειτουργεί ως ενδιάμεσο λογισμικό, ανάμεσα στις εφαρμογές και στη διασύνδεση του δικτύου, ενώ ταυτόχρονα καταγράφει κάθε κίνηση της εφαρμογής [63] [64].

Εγκαταστήσαμε την εφαρμογή Lumen, για να αξιολογήσουμε τις εφαρμογές πράσινου πιστοποιητικού, οι οποίες και θα αναλυθούν στο επόμενο κεφάλαιο. Η εφαρμογή, αμέσως μετά από την εγκατάσταση και την πρώτη της εκκίνηση, ζητάει από το χρήστη μια σειρά ενεργειών. Σε αυτές περιλαμβάνονται, η εγκατάσταση ενός πιστοποιητικού ρίζας (root certificate), πολλά δικαιώματα πρόσβασης, η από προεπιλογή παρακολούθηση της κρυπτογραφημένης και μη κίνησης και η ανώνυμη αποστολή των δεδομένων που έχουν συλλεχθεί στους ερευνητές του project, έτσι ώστε να γίνει ανάλυση και αξιολόγησή των δεδομένων όλων των χρηστών. Η εφαρμογή, για να αναγνωρίσει και να προσδιορίσει κάθε πιθανή διαρροή από άλλες εφαρμογές, απαιτεί να έχει δικαιώματα πρόσβασης, σε όλα τα δεδομένα προσωπικού χαρακτήρα του χρήστη, που υπάρχουν στη συσκευή του κινητού. Σύμφωνα με τους δημιουργούς της εφαρμογής, τα προσωπικά δεδομένα του χρήστη, δεν στέλνονται για διερεύνηση. Αυτό που αποστέλλεται, είναι μόνο στοιχεία πρόσβασης και τροποποίησης. Η εφαρμογή όμως, δεν είναι ανοικτού κώδικα και δεν μπορεί να πραγματοποιηθεί η διερεύνησή του. Αυτό έχει ως αποτέλεσμα, να δημιουργείται ανησυχία στους χρήστες, εξαιτίας των δικαιωμάτων και των απαιτήσεων που ζητάει από αυτούς. Το πιο σημαντικό γεγονός όμως και αυτό που θα πρέπει να εφησυχάσει πλήρως τους χρήστες, γιατί παρέχει μεγάλη ασφάλεια, είναι ότι η εφαρμογή δημιουργήθηκε από αναγνωρισμένο Πανεπιστήμιο και σε αμιγώς ακαδημαϊκό περιβάλλον. Επίσης, αξίζει να σημειωθεί ότι πολλοί ερευνητές έχουν χρησιμοποιήσει το Lumen, για την ανάλυση εξερχόμενης κίνησης από «έξυπνες» εφαρμογές. Αφού πραγματοποιηθούν οι παραπάνω ενέργειες, η εφαρμογή ξεκινάει την παρακολούθηση και την συλλογή πληροφοριών. Στη συνέχεια, δημιουργεί λεπτομερείς αναφορές, οι οποίες αφορούν τη δραστηριότητα και τις διαρροές των εφαρμογών που έχουν ήδη εγκατασταθεί [65].

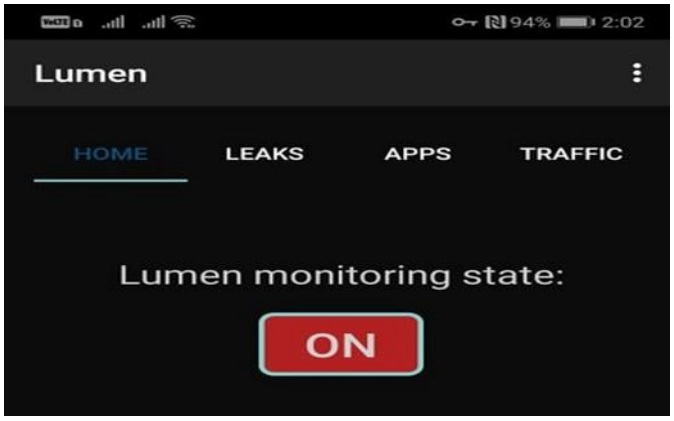
Η διεπαφή της εφαρμογής, αποτελείται από τρεις καρτέλες:

- Διαρροές (Leaks): Στην καρτέλα αυτή, εμφανίζονται οι πληροφορίες της συσκευής ή τα προσωπικά δεδομένα τα οποία έχουν διαρρεύσει, η εφαρμογή που προκάλεσε τη διαρροή αυτή, καθώς και η υπηρεσία ανάλυσης (analytics service) που πήρε τις διαρρέουσες πληροφορίες.

- Εφαρμογές (Apps): Στην καρτέλα αυτή, εμφανίζονται οι εφαρμογές, που έχει επιλέξει ο χρήστης να παρακολουθούνται. Το Lumen, φτιάχνει αναφορές κατανοητές και με κάθε λεπτομέρεια, έτσι ώστε ο χρήστης να καταλάβει τι κινδύνους επιφέρουν οι εφαρμογές που τρέχουν.
- Κίνηση (Traffic): Στην καρτέλα αυτή, εμφανίζεται μια γενικότερη εικόνα της κίνησης, που περνάει από τη συσκευή. Περιλαμβάνονται, πληροφορίες για το σύνολο των συνδέσεων, των διευθύνσεων IP που παίρνουν δεδομένα, το εύρος ζώνης που καταναλώθηκε, τα πρωτόκολλα χρήσης για τις επιμέρους συνδέσεις, καθώς και την επιβάρυνση που προκαλείται από διαφημίσεις και scripts που τρέχουν στο παρασκήνιο.

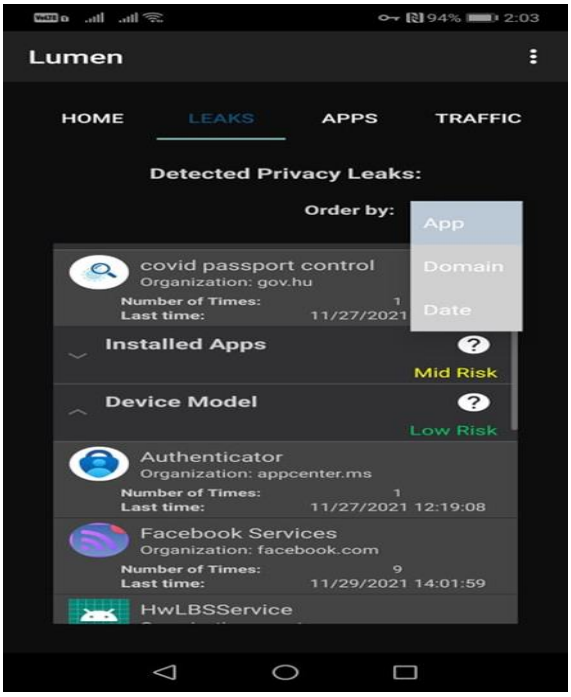
Το Lumen, για την παρακολούθηση της κίνησης μέσω των εφαρμογών που τρέχουν, χρησιμοποιεί τα δικαιώματα VPN. Το VPN, λειτουργεί τοπικά στη συσκευή ως ενδιάμεσο λογισμικό, ανάμεσα στις εφαρμογές και στα διαδικτυακά sockets. Με αυτό τον τρόπο, μπορεί να ανιχνεύσει τα τελικά σημεία όλων των πακέτων, τα οποία διακινούνται από την εφαρμογή [65].

Παρακάτω, θα δείξουμε βήμα βήμα τον τρόπο με τον οποίο ο χρήστης, αντλεί πληροφορίες για τα δεδομένα που μεταδίδουν οι εγκατεστημένες εφαρμογές.



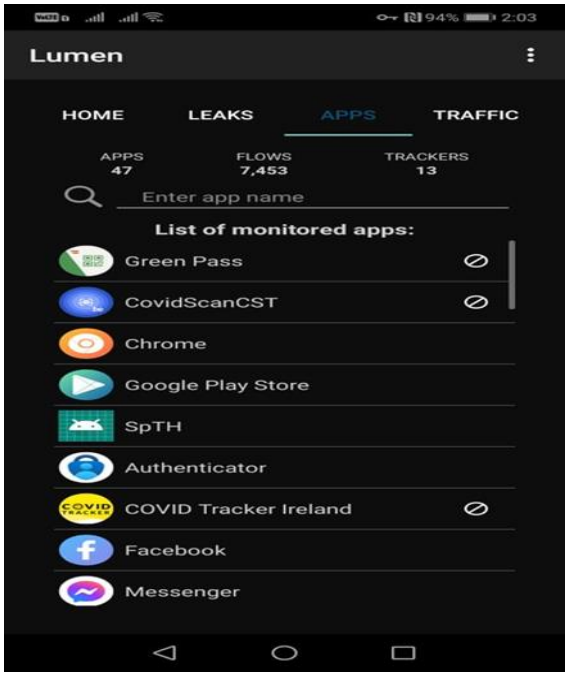
Εικόνα 10: Κεντρική Καρτέλα Ενεργοποίησης της Εφαρμογής lumen

Ο χρήστης, πρέπει να ενεργοποιήσει την εφαρμογή για να ξεκινήσει η ανίχνευση της κίνησης.



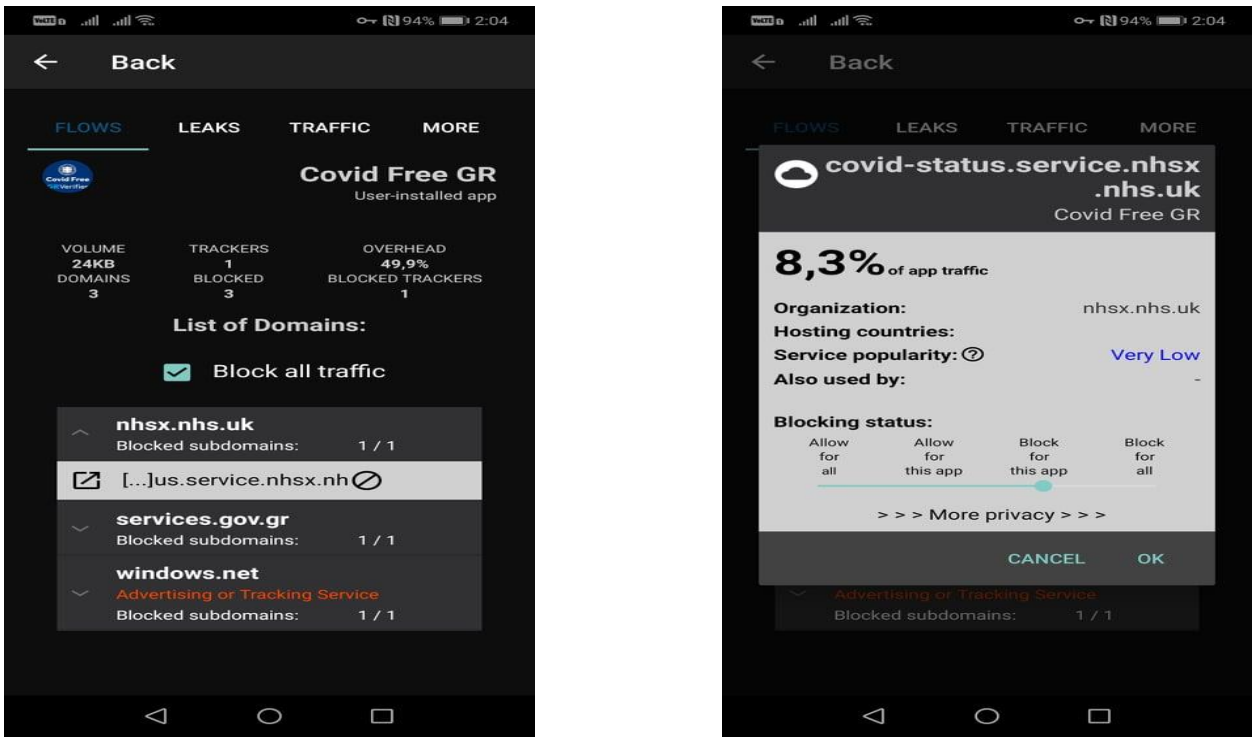
Εικόνα 11: Κεντρική Καρτέλα που Δείχνει τις Διαρροές Προσωπικών Δεδομένων από κάθε Εφαρμογή

Αυτή είναι η καρτέλα Leaks, στην οποία όπως αναφέραμε και παραπάνω, φαίνονται ποια προσωπικά δεδομένα χρησιμοποιούνται από εφαρμογές που τρέχουν στη συσκευή, καθώς και ποιες είναι οι εφαρμογές αυτές. Ο χρήστης, μπορεί να κατηγοριοποιήσει τις πληροφορίες κατά ημερομηνία, εφαρμογή ή domain. Στη συνέχεια, υπάρχει η δυνατότητα να δει σε τι κατηγορία κινδύνου βρίσκεται (high/medium/low), μαζί με μια κατανοητή και σύντομη επεξήγηση.



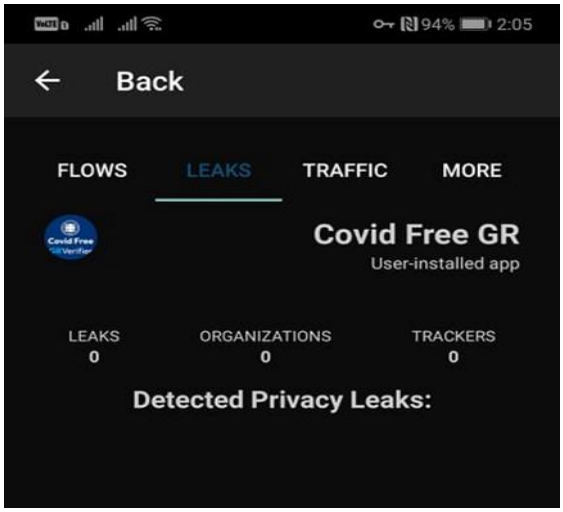
Εικόνα 12: Κεντρική Καρτέλα που Δείχνει τις Εφαρμογές της Συσκευής

Στην καρτέλα Apps, ο χρήστης μπορεί να δει τις εφαρμογές, τις οποίες έχει επιλέξει για να παρακολουθεί τις κινήσεις τους.



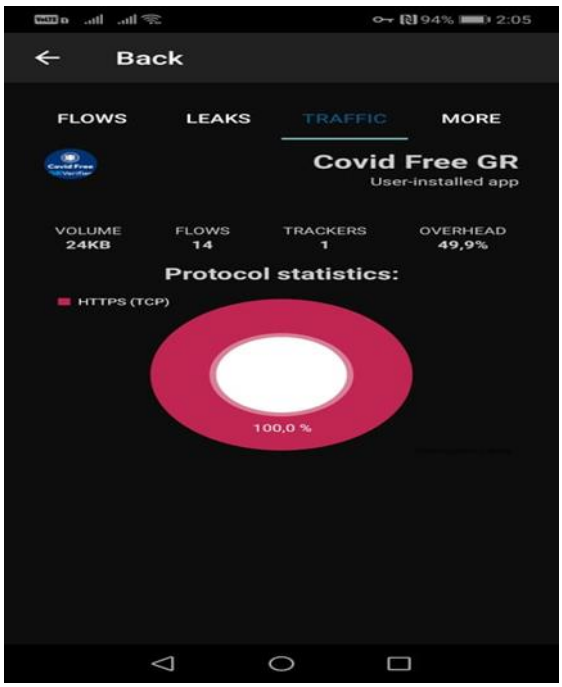
Εικόνα 13: Καρτέλα Εντός εφαρμογής που Δείχνει τις Ροές των Δεδομένων

Επιλέγοντας μια εφαρμογή, εμφανίζονται πληροφορίες, που αφορούν την κίνηση των δεδομένων όπως, το είδος των απεσταλμένων δεδομένων, τον παραλήπτη αυτών, τον όγκο τους, καθώς και τις μπλοκαρισμένες κινήσεις. Παράλληλα, ο χρήστης έχει την δυνατότητα να μπλοκάρει, όποια κίνηση θεωρεί επικίνδυνη. Επιλέγοντας μια ροή, ο χρήστης παίρνει περισσότερες πληροφορίες για αυτήν, μέσω των οποίων μπορεί να καταλάβει ποιος διαχειρίζεται τη συγκεκριμένη ροή.



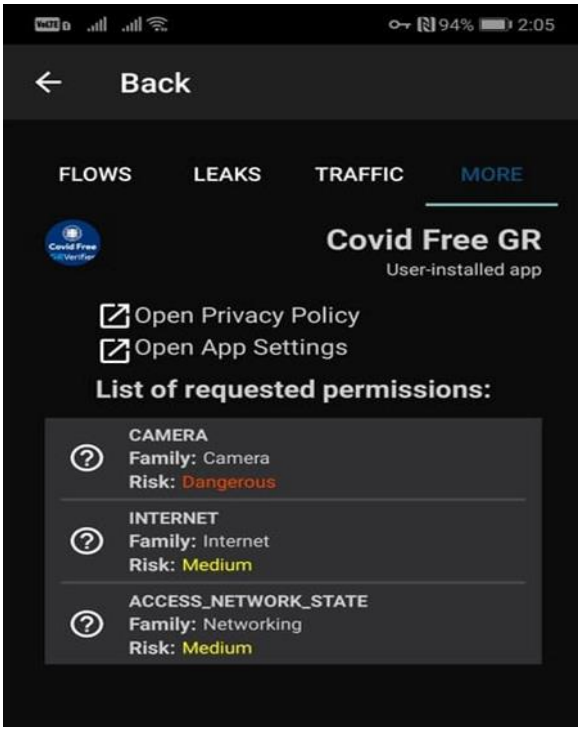
Εικόνα 14: Καρτέλα Εντός Εφαρμογής με τις Διαρροές της Συγκεκριμένης Εφαρμογής

Στην επιλογή Leaks, φαίνονται οι διαρροές της εκάστοτε εφαρμογής που έχουν καταγραφεί.



Εικόνα 15: Καρτέλα Εντός Εφαρμογής που Δείχνει την Κίνηση Μέσω της Εφαρμογής

Στην επιλογή Traffic, φαίνεται η κίνηση που γίνεται μέσω της εφαρμογής. Επίσης, φαίνεται ποιο ποσοστό κίνησης είναι κρυπτογραφημένο και ποιο όχι.



Εικόνα 16: Καρτέλα Εντός Εφαρμογής που Δείχνει τις Άδειες που Ζητούνται από τον Χρήστη

Στην επιλογή More, βλέπουμε τα δικαιώματα της εφαρμογής, καθώς και το πόσο επικίνδυνο είναι το καθένα. Επιλέγοντας ένα από αυτά, βλέπουμε μια σύντομη εξήγηση του κινδύνου.

6. ΜΕΛΕΤΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΠΡΑΣΙΝΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Τα τελευταία δύο χρόνια, έχουν σημαδευτεί από την απροσδόκητη πανδημία, που εξαπλώθηκε στον πλανήτη μας τον Νοέμβριο του 2019. Καθώς ο νέος κορωνοϊός,

γνωστός ως covid-19 εξαπλώνεται στον κόσμο, η τεχνολογία ακολούθησε τις ανάγκες αυτής της κρίσιμης περιόδου, συμβάλλοντας στην ενημέρωση και την ειδοποίηση του κοινού. Με αργά αλλά σταθερά βήματα, η ανθρωπότητα προσπαθεί να επιστρέψει στην κανονικότητα και να πάρει την ζωή της πίσω. Οι κυβερνήσεις, προσπάθησαν και συνεχίζουν να προσπαθούν να βρουν τρόπους στο να πραγματοποιηθεί η επιστροφή αυτή το συντομότερο δυνατό. Με τη βοήθεια των συχνότερων τεστ, αλλά και την ανακάλυψη εμβολίων κατά του ιού, άρχισε να φαίνεται εντονότερα φως στον ορίζοντα. Κάπως έτσι, δημιουργήθηκαν τα ψηφιακά πράσινα πιστοποιητικά, τα οποία επιτρέπουν την ασφαλή κυκλοφορία των ανθρώπων, τόσο εντός της χώρας τους, όσο και εντός της Ευρωπαϊκής Ένωσης.

Στο συγκεκριμένο κεφάλαιο, θα μελετήσουμε τις ψηφιακές πράσινες εφαρμογές που έχουν δημιουργηθεί από τις χώρες της ΕΕ. Θα παρατηρήσουμε το κατά πόσο αυτές εναρμονίζονται με τις διάφορες απαιτήσεις της νομοθεσίας, αναφορικά με την προστασία προσωπικών δεδομένων. Για τη συγκεκριμένη έρευνα, καταγράφθηκε ένα δείγμα 26 εφαρμογών πράσινων πιστοποιητικών Android των χωρών της Ευρωπαϊκής Ένωσης, που κυκλοφόρησαν στο Google Store και αναλύθηκαν στο πλαίσιο των χαρακτηριστικών χρήσης και απορρήτου. Οι συγκεκριμένες εφαρμογές δημοσιεύτηκαν από επίσημες τοπικές αρχές, όπως υπουργεία υγείας και κυβερνήσεις.

6.1 Ανάλυση Ιχνηλατών και Αδειών των Εφαρμογών Πράσινων Πιστοποιητικών

Για να πραγματοποιηθεί η ανάλυση αυτών των εφαρμογών, χρησιμοποιήθηκαν τα εργαλεία exodus και lumen. Η πρώτη εφαρμογή χρησιμοποιήθηκε μέσω της σελίδας του exodus στο ίντερνετ, ενώ το lumen εγκαταστάθηκε σε έξυπνη συσκευή. Η μάρκα του έξυπνου κινητού ήταν το Huawei P20 Lite και λειτουργικό σύστημα EMUI Android 9.1.0.

Για αυτό το πείραμα, το οποίο πραγματοποιήθηκε από το Μάρτιο μέχρι το Μάιο του 2022, χρησιμοποιήθηκε δείγμα 26 εφαρμογών Android από το Google Store και καταγράφηκαν μαζί με τον υπεύθυνο επεξεργασίας. Στη συνέχεια, χρησιμοποιώντας το εργαλείο Exodus για την παρακολούθηση και ανάλυση των αδειών μαζί με την εφαρμογή lumen, πραγματοποιήθηκε ανάλυση για κάθε εφαρμογή, διατηρώντας τον αριθμό των ενσωματωμένων ιχνηλατών και των αιτημάτων πρόσβασης αδειών. Κατά την εξέταση των πληροφοριών που είναι διαθέσιμες στο Google Play, εντοπίστηκαν τρεις κύριες κατηγορίες στις οποίες μπορεί να συσχετιστεί κάθε εφαρμογή:

- Εφαρμογές, οι οποίες είναι αποκλειστικά και μόνο εφαρμογές πράσινων πιστοποιητικών και έχουν ως στόχο την επαλήθευση του πιστοποιητικού του κάθε χρήστη. Πολλές από αυτές, έχουν την επιλογή αποθήκευσης του πράσινου πιστοποιητικού από τον κάθε χρήστη, για ευκολότερη πρόσβαση και επαλήθευση.
- Εφαρμογές, οι οποίες είναι εφαρμογές ιχνηλάτησης, με ενσωματωμένη την δυνατότητα επαλήθευσης πράσινων πιστοποιητικών.
- Εφαρμογές, οι οποίες είναι εφαρμογές ιχνηλάτησης με πρόσθετη δυνατότητα αποθήκευσης του πράσινου πιστοποιητικού.

Μετά από αναζήτηση και μελέτη των 27 χωρών της Ευρωπαϊκής Ένωσης, παρατηρήθηκε ότι το 85,2% αυτών, δηλαδή οι 23 από τις 27, διαθέτουν εφαρμογή, η οποία έχει ως στόχο την επαλήθευση του πράσινου πιστοποιητικού,ενώ πολλές από αυτές έχουν πρόσθετη τη δυνατότητα αποθήκευσής του. Το 3,7%, δηλαδή η μία χώρα από τις 27 (Γαλλία), διαθέτει εφαρμογή ιχνηλάτησης, η οποία έχει ενσωματωμένη την δυνατότητα επαλήθευσης του πράσινου πιστοποιητικού. 2 χώρες της ΕΕ (Ιρλανδία και

Εσθονία), δηλαδή το 7,4%, διαθέτουν σελίδα στο ίντερνετ για την επαλήθευση του πιστοποιητικού και όχι κάποια συγκεκριμένη εφαρμογή. Η μία από αυτές όμως (Ιρλανδία), μαζί με την 27η και τελευταία χώρα (Σλοβενία), ποσοστό 7,4%, διαθέτουν εφαρμογή ιχνηλάτησης, με πρόσθετη δυνατότητα αποθήκευσης του πράσινου πιστοποιητικού. Από τις 27 χώρες της ΕΕ, θα αναλυθούν οι παραπάνω εφαρμογές των 26 από αυτών. Εξαίρεση αποτελεί η Εσθονία, για την οποία δε βρέθηκε κάποια εφαρμογή που να ικανοποιεί κάποια από τις 3 προϋποθέσεις που αναφέρθηκαν.

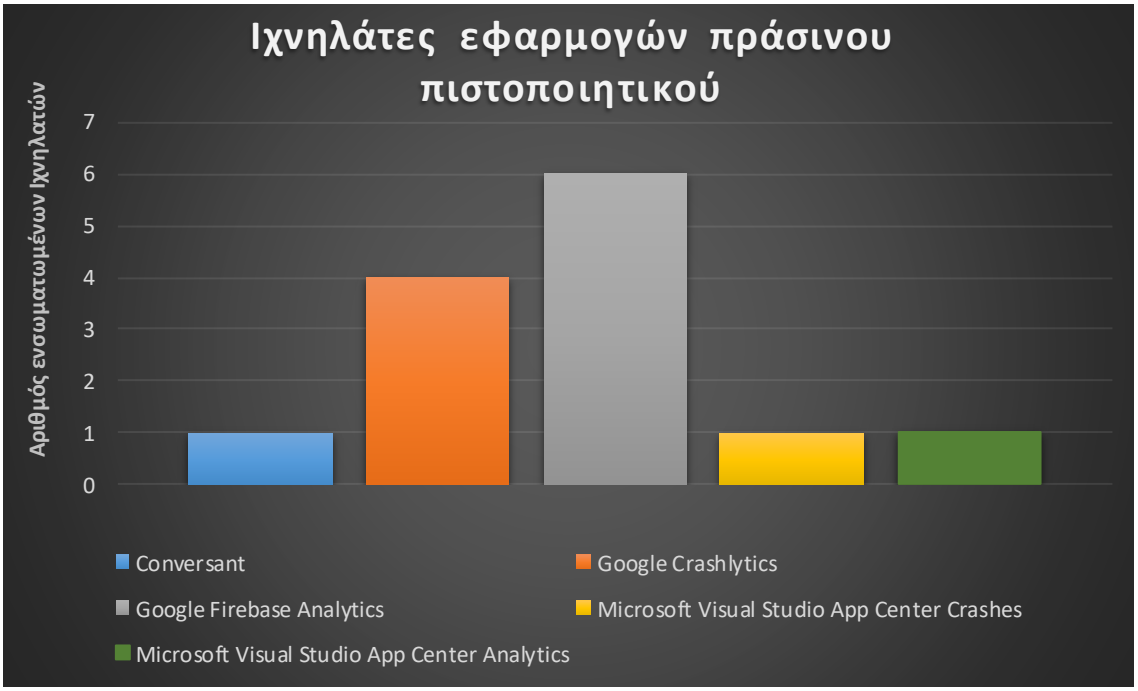
Οι εφαρμογές που ανήκουν στις 2 τελευταίες κατηγορίες, δηλαδή είναι και tracking εφαρμογές, εκτός από την ευχέρεια αποθήκευσης του πιστοποιητικού ή και επαλήθευσης αυτού, παρέχουν και άλλες δυνατότητες στο χρήστη. Το ίδιο, ισχύει και για την εφαρμογή της Ισπανίας. Στο παρακάτω πινακάκι θα αναφερθούν οι δυνατότητες αυτές για κάθε μία εφαρμογή.

Πίνακας 1: Δυνατότητες Εφαρμογών πέραν του Πράσινου Πιστοποιητικού

zVEM (Σλοβενία)	**COVID Tracker Ireland (Ιρλανδία)**	**TousAntiCovid (Γαλλία)**	**PassCOVID.gal (Ισπανία-Γαλικία)**
Γρήγορη και εύκολη πρόσβαση σε αποτελέσματα, συνταγές και άλλα έγγραφα στο σύστημα eHealth	Επιτρέπει το καθημερινό check-in, για την ενημέρωση σε περίπτωση συμπτωμάτων κρυολογήματος, γρίπης ή κορωνοϊού ή εάν κάποιος δεν αισθάνεται καλά	Χρησιμοποιεί τη σύνδεση Bluetooth του τηλεφώνου, για να ανιχνεύσει τα τηλέφωνα άλλων χρηστών όταν είναι κοντά στον χρήστη.	Επιτρέπει τη λήψη προειδοποιήσεων, την ενημέρωση για περιορισμούς, προτάσεις και ειδήσεις, καθώς και την αναφορά εάν ο χρήστης έχει βρεθεί σε μέρος με συγκέντρωση μετάδοσης, εάν βρίσκεται σε στενή επαφή ή εάν έχει διαγνωστεί με COVID-19.
Ανασκόπηση ιατρικής τεκμηρίωσης (αποτελέσματα, εξουσιοδοτήσεις και άλλα έγγραφα)	Χαρτογράφηση της εξάπλωσης του ιού στην Ιρλανδία	Ειδοποιεί όταν ο χρήστης βρεθεί κοντά σε χρήστη που έχει βγει θετικός στον COVID-19.	
Έλεγχος εκδομένων και χρησιμοποιημένων eRecipes	Χρήση της τεχνολογίας του τηλεφώνου για καταγραφή του πότε βρίσκεται κάποιος κοντά σε άλλους χρήστες της εφαρμογής. Εάν	Εάν ένας χρήστης κάνει ένα τεστ για COVID-19 που αποδειχθεί θετικό, το εργαστήριο θα του δώσει έναν κωδικό για να σαρώσει ή να τον	

	ένας χρήστης εφαρμογής βγει θετικός στον COVID-19, το HSE μπορεί να επικοινωνήσει μαζί του και να του δώσει τις συμβουλές και τη βοήθεια που χρειάζονται.	εισάγει χειροκίνητα για να στείλει μια ανώνυμη ειδοποίηση σε χρήστες που ήταν κοντά του.	
Προβολή eReferrals και eOrders			
Επανεξέταση των χρόνων αναμονής			

Μετά από προσεκτική ανάλυση των δεδομένων που συλλέχθηκαν, παρατηρήθηκε ότι μόλις 5 διαφορετικοί ιχνηλάτες βρέθηκαν στο δείγμα 26 εφαρμογών, οι οποίοι ήταν οι **Google Firebase Analytics, Google CrashLytics, Microsoft Visual Studio App Center Crashes, Microsoft Visual Studio App Center Analytics** και **Conversant** (σχήμα 2). Άξιο αναφοράς είναι ο μικρός αριθμός ιχνηλατών, κάτι που σημαίνει ότι οι κυβερνήσεις έχουν δώσει μεγάλη βάση στην προστασία δεδομένων. Ο μέγιστος αριθμός ιχνηλατών ανά εφαρμογή είναι **2** και εντωπίζονται στα **Skaner Certyfikatów Covid (Πολωνία)**, **Green Pass (Σλοβακία), CovScan (Κύπρος)** και **Tecka-prukaz bezinfekcnosti covid (Τσεχία)** (σχήμα 1). Επίσης, 17 από τις εφαρμογές αυτές, βρέθηκαν χωρίς ενσωματωμένους ιχνηλάτες. Αυτό σημαίνει ότι το 65% των εφαρμογών που έχει δημοσιευτεί από τις επίσημες αρχές δεν είχαν ενσωματωμένα προγράμματα παρακολούθησης. Το ποσοστό αυτό, έρχεται να ισχυροποιήσει το παραπάνω εύρημα σχετικά με τη σημασία που έχει δωθεί στην προστασία των δεδομένων.



Σχήμα 1: Κατανομή Ιχνηλατών σε Εφαρμογές Πράσινου Πιστοποιητικού

Σχήμα2: Ιχνηλάτες Εφαρμογών Πράσινου Πιστοποιητικού

Στον Πίνακα 2 συνοψίζονται οι εφαρμογές με μηδέν ιχνηλάτες, όπως βρέθηκαν κατά τη διάρκεια της ανάλυσης. Για να δοθούν περισσότερες πληροφορίες σε αυτήν τη λίστα, αναφέρεται ο υπεύθυνος επεξεργασίας της κάθε εφαρμογής και από ποιόν έχει εξουσιοδοτηθεί. Όπως φαίνεται και από τον πίνακα, οι εφαρμογές έχουν δημιουργηθεί από ινστιτούτα (όπως το National Institute for Research in Digital Sciences and Technologies για την Γαλλική εφαρμογή, το Finnish Institute for Health and Welfare για την Φινλανδική εφαρμογή και το Robert Koch-Istitut που είναι το ινστιτούτο εθνικής και δημόσιας υγείας που εκδίδει την εφαρμογή για λογαριασμό της Γερμανικής Ομοσπονδιακής Κυβέρνησης), υπουργεία υγείας (όπως της Βουλγαρίας της Ιταλίας και της Κύπρου), τα οποία έχουν εξουσιοδοτηθεί από επίσημες κυβερνητικές υπηρεσίες, αλλά και άλλες υπηρεσίες (όπως το Special Telecommunications Service της Ρουμανίας). Επίσης, βλέπουμε ότι υπάρχει εφαρμογή (Μάλτα), όπου η κυβέρνηση, είναι και ο υπεύθυνος επεξεργασίας.

Πίνακας 2: Εφαρμογές Πράσινου Πιστοποιητικού Χωρίς Ενσωματωμένους Ιχνηλάτες

Apps	Countries	Data Controllers	Notes	Trackers	Permissions

Gruner pass	Αυστρία	BRZ GmbH for Federal Ministry Republic of Austria		0	3 (access network state, camera, internet)
COVID CHECK BG	Βουλγαρία	Ministry of Health of the Republic of Bulgaria		0	6 (access network state, access wifi state, camera, flashlight, internet, write external storage)
TousAntiCovid	Γαλλία	National Institute for Research in Digital Sciences and Technologies (INRIA)	For General Directorate of Health of the Ministry of Solidarity and Health	0	12 (access coarse location, access fine location, access network state, access wifi state, Bluetooth, Bluetooth admin, camera, foreground service, internet, receive boot completed, request ignore battery optimizations, wake lock)
CovPass	Γερμανία	Robert Koch-Institut (RKI)	for the German federal governmen t	0	6 (access network state, camera, foreground service, internet, receive boot completed, wake lock)
Coronapas	Δανία	Statens Serum Institut		0	7 (access network state, camera, internet, use biometrics, use

					fingerprints, vibrate, wake lock)
Covid Free GR	Ελλάδα	Εθνική Αρχή Διαφάνειας (ΕΑΔ)	for the Hellenic Republic	0	3 (access network state, camera, internet)
COVID tracker Ireland	Ιρλανδία	Health Service Executive (HSE), Ireland and Department of Health (DoH)	HSE is responsible for the provision of health & personal social services in Ireland, with public funds.	0	8 (access network state, camera, access wifi state, bluetooth, foreground service, internet, receive boot completed, vibrate)
Verifica C19	Ιταλία	Ministry of Health through SOGEI		0	6 (access network state, camera, foreground service, internet, receive boot completed, wake lock)
CovidGO	Κροατία	Ministry of Health, & Ministry of the Interior in Zagreb		0	3 (camera, vibrate, internet)
Covid19Verify	Λετονία	Centre for Disease Prevention and Control of Latvia (CDPC) /Slimību profilakses un kontroles centrs, SPKC Latvia		0	5 (access network state, camera, internet, vibrate, foreground service)
Tikrinti COVID pažymėjimą / Verify COVID certificate	Λιθουανία	State Enterprise Centre of Registers	For Ministry of Health of the	0	6 (access network state, camera, foreground

			Republic of Lithuania		service, internet, receive boot completed, wake lock)
CovidCheck.lu	Λουξεμβούργο	State of the Grant Duchy of Luxemburg	For the Government Information Technology Center of the state of the Grant Duchy of Luxemburg	0	3 (camera, flashlight, internet)
CovPass-Malta	Μάλτα	Government of Malta		0	7(access network state, camera, foreground service, internet, NFC, receive boot completed, wake lock)
CoronaCheck	Ολλανδία	The Minister of Health, Welfare and Sport (VWS)		0	6 (access network state, camera, foreground service, internet, receive boot completed, wake lock)
Check DCC	Ρουμανία	Special Telecommunications Service		0	6 (access network state, camera, foreground service, internet, receive boot completed, wake lock)
zVEM	Σλοβενία	National Institute of Public Health (hereinafter: NIJZ)	Republic of Slovenia	0	9 (access network state, camera, flashlight, foreground service, internet, read external

					storage, use fingerprint, wake lock, write external storage)
Corona certificate reader	Φινλανδία	Finnish Institute for Health and Welfare		0	6 (access network state, camera, foreground service, internet, receive boot completed, wake lock)

Στον παρακάτω πίνακα, παρουσιάζονται οι εφαρμογές, οι οποίες έχουν ενσωματωμένους ιχνηλάτες. Όπως αναφέρθηκε παραπάνω, το 35% των εφαρμογών, δηλαδή 9 από τις 26 έχουν ενσωματωμένους ιχνηλάτες. Ο ιχνηλάτης **Google Firebase Analytics**, είναι αυτός που εμφανίζεται περισσότερες φορές, 6 εφαρμογές, ενώ ο **Google Crashlytics** εμφανίζεται 4 φορές. Τέλος, οι 2 ιχνηλάτες της **Microsoft**, εμφανίζονται μόνο στην εφαρμογή της Κύπρου ενώ ο ιχνηλάτης **Conversant** μόνο στην Πορτογαλία. Όπως φαίνεται στον πίνακα, 4 εφαρμογές έχουν υπεύθυνο επεξεργασίας τα αντίστοιχα υπουργεία υγείας της εκάστοτε χώρας, 2 εφαρμογές έχουν υπηρεσίες-εταιρείες υγείας, μία το συλλογικό όργανο λήψης αποφάσεων της κυβέρνησης (αυτόνομη κοινότητα Γαλικίας) και μία το Πορτογαλικό Νομισματοκοπείο (Πορτογαλία).

Πίνακας 3: Εφαρμογές Πράσινου Πιστοποιητικού με Ενσωματωμένους Ιχνηλάτες

Apps	**Countries**	**Data Controllers**	**Notes**	**Trackers**	**Permissions**
CovidScanBE	Βέλγιο	eHealth platform		1 (Google Crashlytics)	4 (access network state, camera, internet, vibrate)
PassCOVID.gal	Ισπανία-Γαλικία	XUNTA De Galicia	for Ministry of Health / Galician Health Service (Sergas)	1 (Google Firebase Analytics)	32 (access network state, call phone, camera, get accounts, flashlight, internet, read app badge, read contacts,

					read external storage, receive boot completed, request install packages, use biometric, use fingerprint, wake lock, write contracts, write external storage, update count, receive, read settings, update shortcut, change badge, read settings, write settings, update badge, read settings, write settings, read, write, broadcast badge, provider insert badge, badge count read, badge count write)
CovScan Cyprus	Κύπρος	Ministry of Health of Cyprus		2 (Microsoft Visual Studio App Center Analytics, Microsoft Visual Studio App Center Crashes)	7 (access network state, camera, foreground service, internet, receive boot completed, reorder tasks, wake lock)
EESZT Covid Control	Ουγγαρία	Electronic Health Service of Hungary	For the National Directorate General of Hospitals	1 (Google Firebase Analytics)	7 (access network state, camera, flashlight, internet, receive boot completed,

					wake lock, receive)
Skaner Certyfikatów Covid	Πολωνία	Ministry of Health		2 (Google CrashLytics, Google Firebase Analytics)	6 (access network state, camera, foreground service, internet, wake lock, bind get install referrer service)
Passe Covid	Πορτογαλία	Imprensa Nacional – Casa da Moeda (Official Printing Office – Portuguese Mint), hereinafter referred to as INCM	For Portoguese Government	1 (Conversant)	4 (access network state, camera, internet, flashlight)
Green Pass	Σλοβακία	Slovensko IT, SR and the Ministry of Health of the SR		2 (Google CrashLytics, Google Firebase Analytics)	11 (access network state, camera, foreground service, internet, receive boot completed, use biometric, use fingerprint, vibrate, wake lock, receive, bind get install referrer service)
Coronafree	Σουηδία	Giddir AB		1 (Google Firebase Analytics)	6 (access network state, foreground services, internet, vibrate, wake lock, bind get install referrer service)
Tecka-prukaz bezinfekcnosti	Τσεχία	Ministry of Health of the Czech		2 (Google CrashLytics,	7 (access network state, camera,

covid		Republic		Google Firebase Analytics)	internet, wake lock, use fingerprint, use biometric, bind get install referrer service)

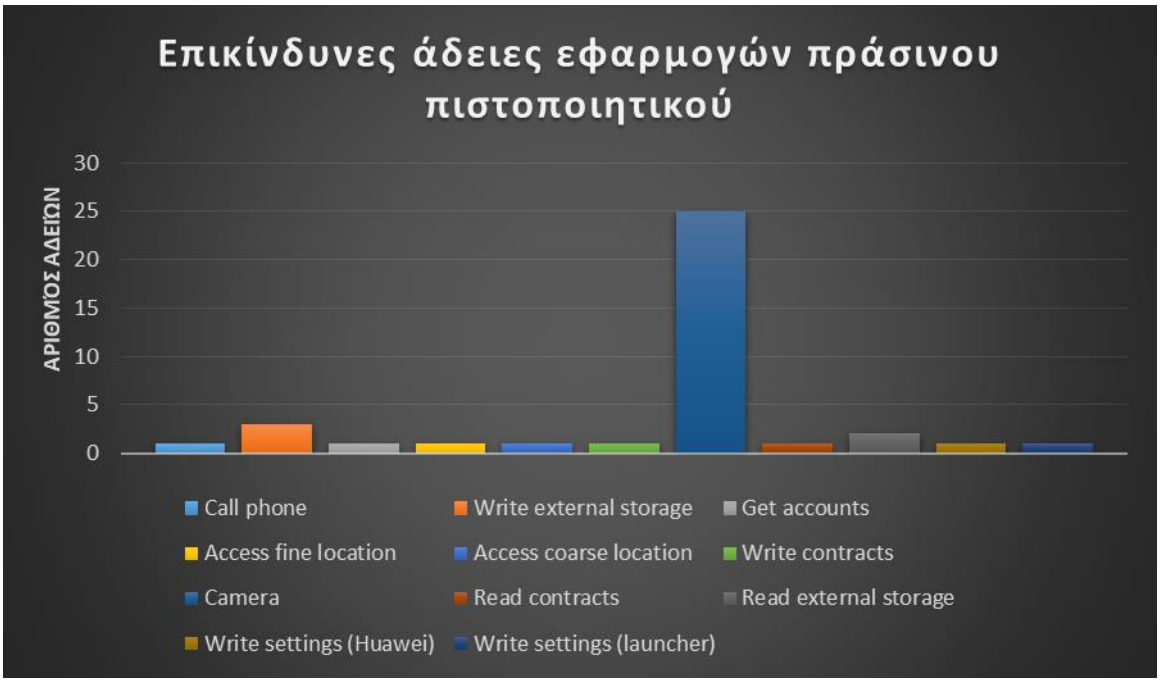
Στον παραπάνω πίνακα, παρατηρήσαμε ότι οι εφαρμογές ζητούν αρκετές άδειες από τους χρήστες, έτσι ώστε να μπορούν να λειτουργούν με σωστό τρόπο. Δεν είναι όμως όλες αυτές οι αιτήσεις αδειών επικίνδυνες. Από τον παρακάτω πίνακα, παρατηρούμε ότι μία εφαρμογή ζητάει πολλές επικίνδυνες άδειες και αυτή είναι η **PassCOVID.gal** της **Ισπανίας** (9 επικίνδυνες άδειες). Ακολουθούν η **TousAntiCovid** της **Γαλλίας** και η **zVEM** της **Σλοβενίας** με 3 επικίνδυνες άδειες και η **COVID CHECK** BG της **Βουλγαρίας** με 2. Όλες οι άλλες εφαρμογές, ζητούν μόνο μία και αυτή είναι η **CAMERA**, η οποία ζητείται από σχεδόν όλες τις εφαρμογές (25 από τις 26). Εντύπωση προκαλεί η εφαρμογή **Coronafree** της Σουηδίας, η οποία παρ ‘όλο που είναι μια εφαρμογή επαλήθευσης και αποθήκευσης πράσινου πιστοποιητικού, κατόπιν ελέγχου στο exodus και στο lumen, δεν εμφανίστηκε να ζητάει την άδεια της κάμερας (απαραίτητη για το σκανάρισμα του πιστοποιητικού). Τέλος, καμία άλλη επικίνδυνη άδεια δεν φάνηκε να χρησιμοποιείται σε πάνω από μία εφαρμογή, εκτός από τις **READ EXTERNAL STORAGE** και **WRITE EXTERNAL STORAGE**, που εμφανίζονται σε 2 και 3 εφαρμογές αντίστοιχα.

Πίνακας 4: Επικίνδυνες Άδειες Εφαρμογών Πράσινου Πιστοποιητικού

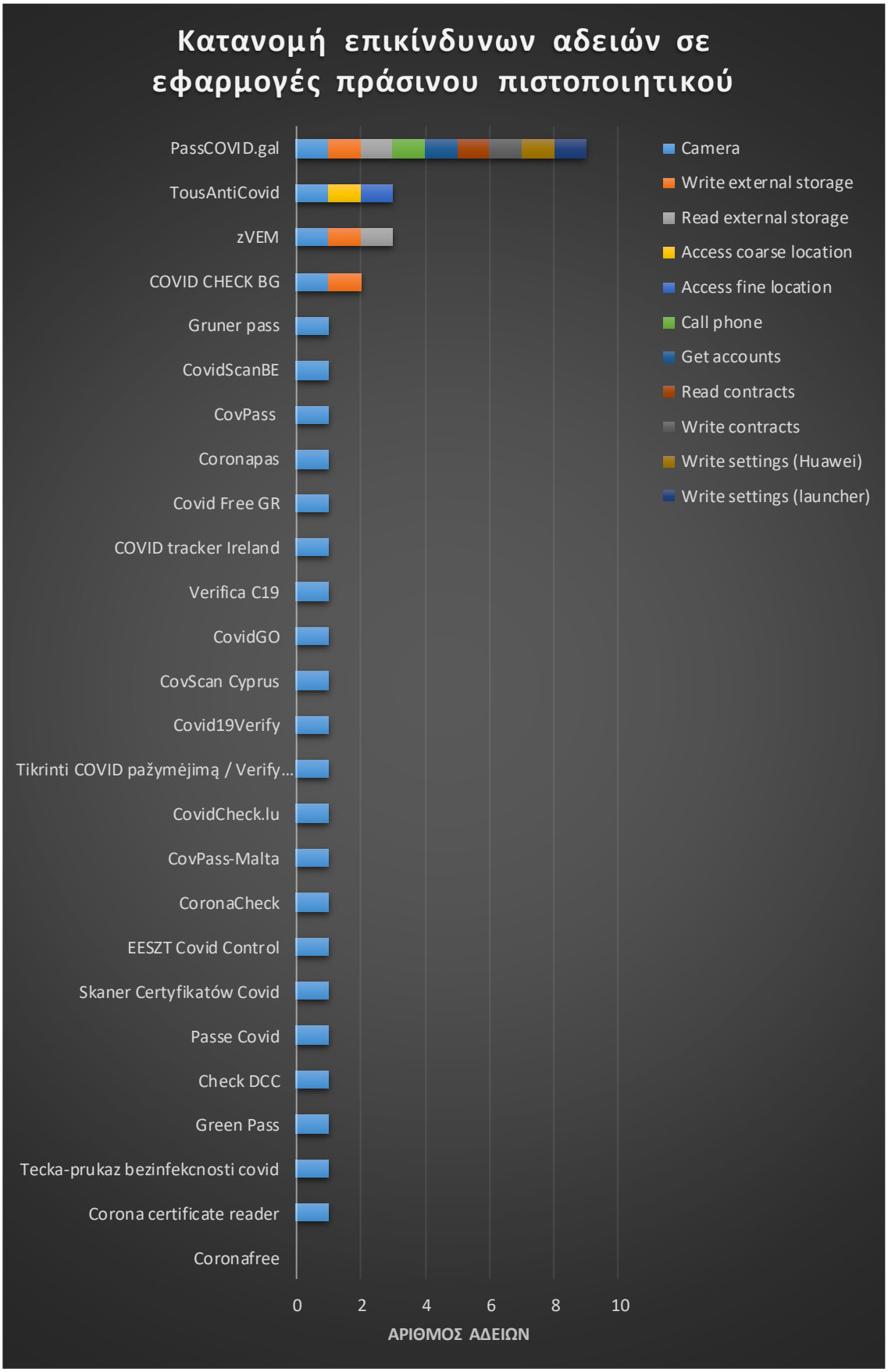
Apps	**Countries**	**Dangerous Permissions**
Gruner pass	Αυστρία	1 (camera)
CovidScanBE	Βέλγιο	1 (camera)
COVID CHECK BG	Βουλγαρία	2 (camera, write external storage)
TousAntiCovid	Γαλλία	3 (access coarse location, access fine location, camera)
CovPass	Γερμανία	1 (camera)
Coronapas	Δανία	1 (camera)

Covid Free GR	Ελλάδα	1 (camera)
COVID tracker Ireland	Ιρλανδία	1 (camera)
PassCOVID.gal	Ισπανία-Γαλικία	9 (call phone, camera, get accounts, read contacts, read external storage, write contacts, write external storage, write settings(huawei), write settings(launcher))
Verifica C19	Ιταλία	1 (camera)
CovidGO	Κροατία	1 (camera)
CovScan Cyprus	Κύπρος	1 (camera)
Covid19Verify	Λετονία	1 (camera)
Tikrinti COVID pažymėjimą / Verify COVID certificate	Λιθουανία	1 (camera)
CovidCheck.lu	Λουξεμβούργο	1 (camera)
CovPass-Malta	Μάλτα	1 (camera)
CoronaCheck	Ολλανδία	1 (camera)
EESZT Covid Control	Ουγγαρία	1 (camera)
Skaner Certyfikatów Covid	Πολωνία	1 (camera)
Passe Covid	Πορτογαλία	1 (camera)
Check DCC	Ρουμανία	1 (camera)
Green Pass	Σλοβακία	1 (camera)
Zvem	Σλοβενία	3 (camera, read external storage, write external storage)
Coronafree	Σουηδία	0
Tecka-prukaz bezinfekcnosti covid	Τσεχία	1 (camera)
Corona certificate reader	Φινλανδία	1 (camera)

Παρακάτω, είναι τα αναλυτικά γραφήματα για την κατανομή επικίνδυνων αδειών στις εφαρμογές πράσινων πιστοποιητικών, όπως εμφανίζονται στις πιο πρόσφατες αναφορές.



Σχήμα 3: Κατανομή Επικίνδυνων Αδειών σε Εφαρμογές Πράσινου Πιστοποιητικού



Σχήμα 4: Επικίνδυνες Άδειες Εφαρμογών Πράσινου Πιστοποιητικού

Όπως φαίνεται στον παραπάνω πίνακα, αλλά και στα γραφήματα, υπάρχουν 11 διαφορετικές άδειες στις εφαρμογές που εξετάσαμε. Παρακάτω θα επισημάνουμε το τι σημαίνει η κάθε μία από αυτές, με βάση το [66].

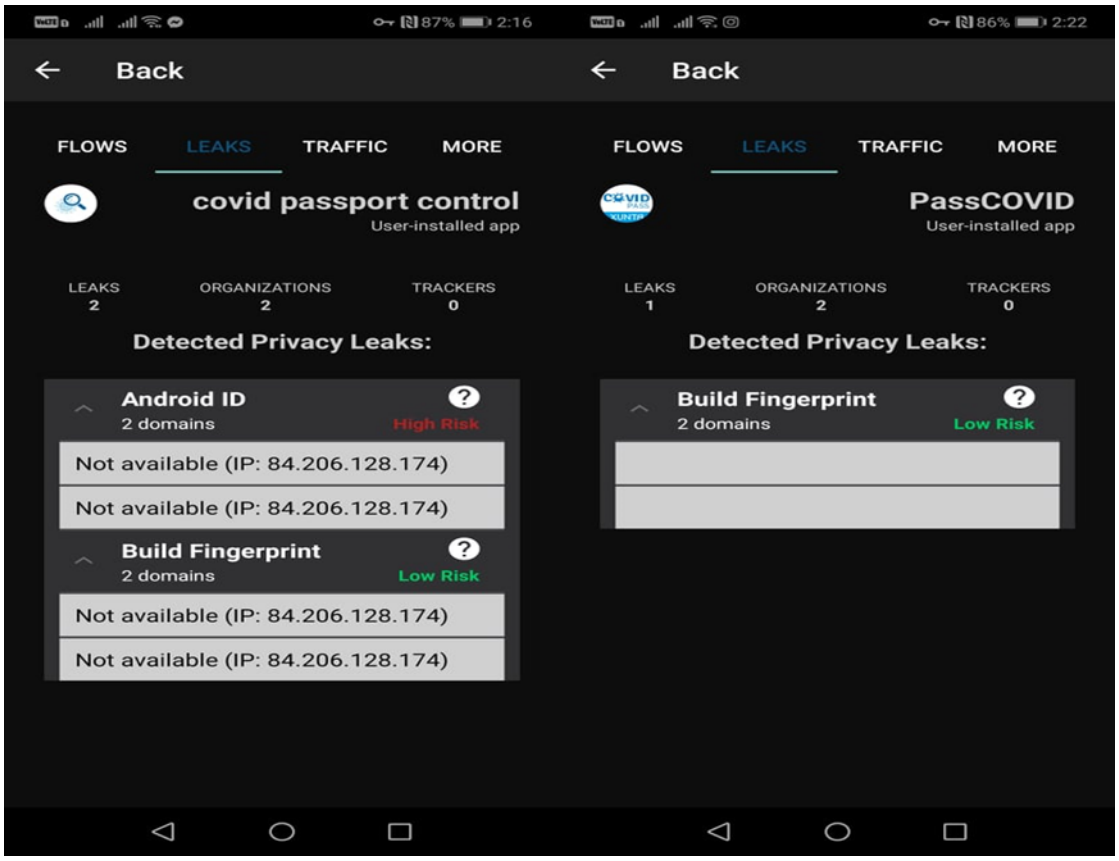
- **Camera:** Η συγκεκριμένη άδεια απαιτείται για να έχει πρόσβαση η εφαρμογή στην κάμερα της συσκευής και στην περίπτωσή μας να σκανάρει τα πιστοποιητικά με σκοπό την επαλήθευσή τους.
- **Write external storage:** Επιτρέπει σε μια εφαρμογή την εγγραφή σε εξωτερικό χώρο αποθήκευσης. Προορίζεται να χρησιμοποιηθεί από λίγες εφαρμογές που πρέπει να διαχειρίζονται αρχεία για λογαριασμό των χρηστών.
- **Read external storage:** Επιτρέπει σε μια εφαρμογή την ανάγνωση από εξωτερικό χώρο αποθήκευσης. Σε κάθε εφαρμογή που δηλώνει την άδεια WRITE_EXTERNAL_STORAGE χορηγείται σιωπηρά και αυτή η άδεια.
- **Access coarse location:** Επιτρέπει σε μια εφαρμογή την πρόσβαση σε κατά προσέγγιση τοποθεσία.
- **Access fine location:** Επιτρέπει σε μια εφαρμογή να έχει πρόσβαση σε ακριβή τοποθεσία. Χρησιμοποιείται εναλλακτικά της ACCESS_COARSE_LOCATION. Και οι δύο επιτρέπουν την πρόσβαση στην τοποθεσία στο παρασκήνιο.
- **Call phone:** Επιτρέπει σε μια εφαρμογή, να πραγματοποιήσει μια τηλεφωνική κλήση, χωρίς να περάσει από τη διεπαφή χρήστη του Dialer, ώστε ο χρήστης να επιβεβαιώσει την κλήση.
- **Get accounts:** Επιτρέπει την πρόσβαση στη λίστα λογαριασμών στην Υπηρεσία Λογαριασμών.
- **Read contacts:** Επιτρέπει σε μια εφαρμογή την ανάγνωση των δεδομένων επαφών του χρήστη.
- **Write contacts:** Επιτρέπει σε μια εφαρμογή την εγγραφή των δεδομένων επαφών του χρήστη.
- **Write settings (Huawei & launcher):** Επιτρέπει σε μια εφαρμογή να διαβάζει ή να γράφει τις ρυθμίσεις συστήματος.

Χωρίς να μπορεί να ειπωθεί με βεβαιότητα ότι κάποια εκ των ανωτέρω αδειών δεν χρειάζεται, γεννώνται ερωτηματικά από το γεγονός ότι σύνολο διαφορετικών εφαρμογών με ίδια λειτουργία έχουν «ποικιλία» στο είδος των δικαιωμάτων/αδειών που ζητούν για την ορθή λειτουργία τους, αφού θα ανέμενε κανείς ότι όλες οι εφαρμογές θα απαιτούσαν, περίπου, τα ίδια δικαιώματα. Το γεγονός ότι κάποιες εφαρμογές υποστηρίζουν και άλλες λειτουργίες ενδεχομένως να δικαιολογεί, σε κάποιο βαθμό, αυτήν την ποικιλία. Ωστόσο, κάθε εφαρμογή θα πρέπει σε κάθε περίπτωση να εξηγεί με σαφήνεια, στην πολιτική προστασίας δεδομένων της, την αναγκαιότητα κάθε επεξεργασίας δεδομένων – και, άρα, κάθε άδειας που αιτείται.

6.2 Ανάλυση Διαρροών στις Εφαρμογές Πράσινων Πιστοποιητικών

Στο επόμενο κομμάτι της έρευνας, επιχειρήθηκε να εντοπιστούν, τι είδος δεδομένα της συσκευής μας διαρρέουν (φεύγουν προς τα έξω), εξαιτίας των συγκεκριμένων εφαρμογών πράσινου πιστοποιητικού. Για την πραγματοποίηση αυτού του ελέγχου, χρησιμοποιήθηκε η εφαρμογή lumen, η οποία εγκαταστάθηκε στην κινητή συσκευή που επιλέχθηκε. Μέσω του Google Play Store, εγκαταστάθηκαν στο κινητό 22 από τις 26 εφαρμογές, στις οποίες και πραγματοποιήθηκε ο έλεγχος. Οι άλλες 4 εφαρμογές δεν ήταν δυνατό να εγκατασταθούν στη συσκευή **(COVID CHECK BG, CovPass, Skaner Certyfikatów Covid, Corona certificate reader).**

Μέσω της καρτέλας Leaks του lumen, έγινε προσπάθεια να εντοπιστούν οι εφαρμογές που προκάλεσαν διαρροή προσωπικών δεδομένων από την συσκευή. Επιλέγοντας λοιπόν μία μία τις εφαρμογές και κλικάροντας στην επιλογή leaks, εντοπίστηκε ότι μόνο 2 από τις 22 διαρρέουν δεδομένα. Όπως φαίνεται από τις παρακάτω εικόνες, αυτές είναι η **EESZT Covid Control** της **Ουγγαρίας** και η **PassCOVID.gal** της **Ισπανίας**. Οι διαρροές που βρέθηκαν, έχουν τις ονομασίες **Android ID** και **Build Fingerprint**.

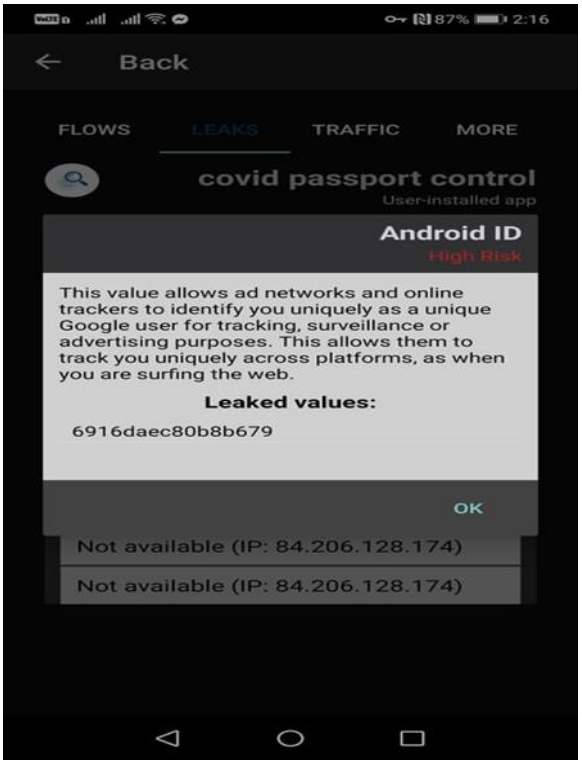


Εικόνα 17: Διαρροές που Εντοπίστηκαν στις 2 Εφαρμογές

Επίσης, πηγαίνοντας στην κεντρική καρτέλα των διαρροών, όπου φαίνονται συνολικά οι διαρροές όλων των εφαρμογών, εντοπίστηκε ακόμα μία διαρροή και για τις δύο αυτές εφαρμογές, με όνομα **Device Model**.

Ξεκινώντας την ανάλυση από την κατηγορία **Android ID**, που βρίσκουμε στην εφαρμογή της Ουγγαρίας, βλέπουμε από την εικόνα ότι πρόκειται για μια διαρροή υψηλού ρίσκου. Πατώντας πάνω στο ερωτηματικό (παρακάτω εικόνα), μπορούμε να βρούμε λεπτομέρειες σχετικά με τον λόγο που πραγματοποιείται η παρακολούθηση, ποια προσωπικά δεδομένα διαρρέουν από την συσκευή, αλλά και την υπηρεσία ανάλυσης που πήρε τις διαρρέουσες πληροφορίες. Αυτή η διαρροή, επιτρέπει στα δίκτυα διαφημίσεων και στους διαδικτυακούς ιχνηλάτες να προσδιορίζουν μοναδικά το χρήστη, ως μοναδικό χρήστη της Google για σκοπούς παρακολούθησης, ιχνηλάτησης ή διαφήμισης. Αυτό τους επιτρέπει να τον παρακολουθούν μοναδικά σε πλατφόρμες, όπως όταν σερφάρει στο διαδίκτυο. Όπως βλέπουμε, η διαρροή οδηγεί προς 2 domains, με IP 84.206.128.174. Η συγκεκριμένη IP, βρίσκεται σε ένα εύρος

διευθύνσεων, το οποίο ανήκει στην Εθνική Εταιρεία Πληροφοριών (National Infocommunications Service Company) της Ουγγαρίας. Χωρίς να γνωρίζουμε το νομικό πλαίσιο της εν λόγω χώρας, μία τέτοια διαρροή κρίνεται κατ' αρχάς «ανησυχητική» από τη σκοπιά της προστασίας δεδομένων, λαμβάνοντας υπόψη ότι ως υπεύθυνος επεξεργασίας της εφαρμογής δεν είναι η εν λόγω Υπηρεσία (και δεν θα μπορούσε και να είναι, αφού δεν φάινεται ότι είναι οργανισμός σχετικός με παροχή υπηρεσιών υγείας).

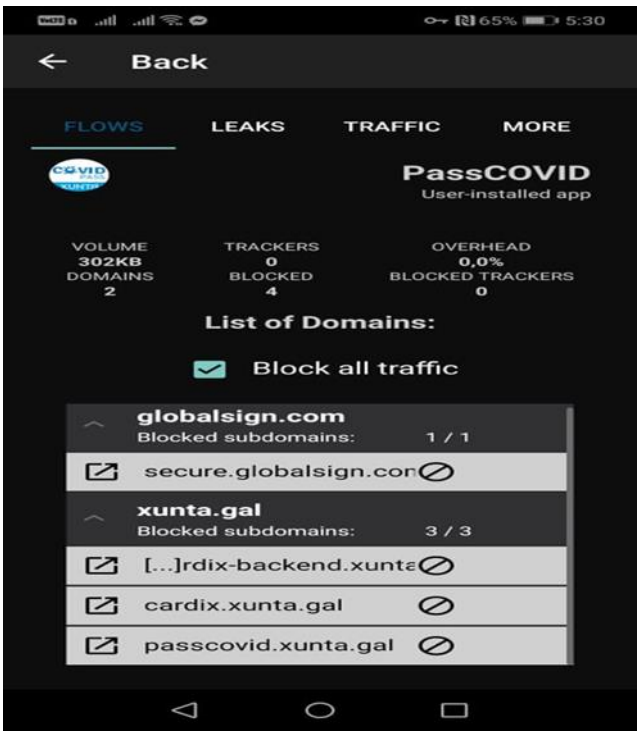


Εικόνα 18: Λεπτομερής Ανάλυση της Διαρροής (Android ID – Ουγγαρία)

Στη συνέχεια της ανάλυσης, εντοπίζουμε την κατηγορία **Build Fingerprint**, η οποία βρίσκεται και στις δύο εφαρμογές. Από την εικόνα βλέπουμε ότι πρόκειται για μια διαρροή μικρού ρίσκου. Αυτή η διαρροή, προσδιορίζει μοναδικά το λειτουργικό σύστημα Android του χρήστη και την έκδοση που εκτελείται. Οι εφαρμογές συνήθως χρησιμοποιούν αυτές τις πληροφορίες για να προσαρμόσουν το περιεχόμενο στην οθόνη του χρήστη ή για να βελτιώσουν την αποτελεσματικότητα της διαφήμισης. Ωστόσο, αυτές οι πληροφορίες, ειδικά όταν συνδυάζονται με άλλες διαρροές, μπορούν να αποκαλύψουν πράγματα για την προσωπικότητα, το γούστο, την ευημερία και τα δημογραφικά στοιχεία του χρήστη (εικόνα κάτω). Όπως είδαμε στις αρχικές εικόνες, και εδώ οι πληροφορίες οδηγούν προς τα ίδια 2 domain.

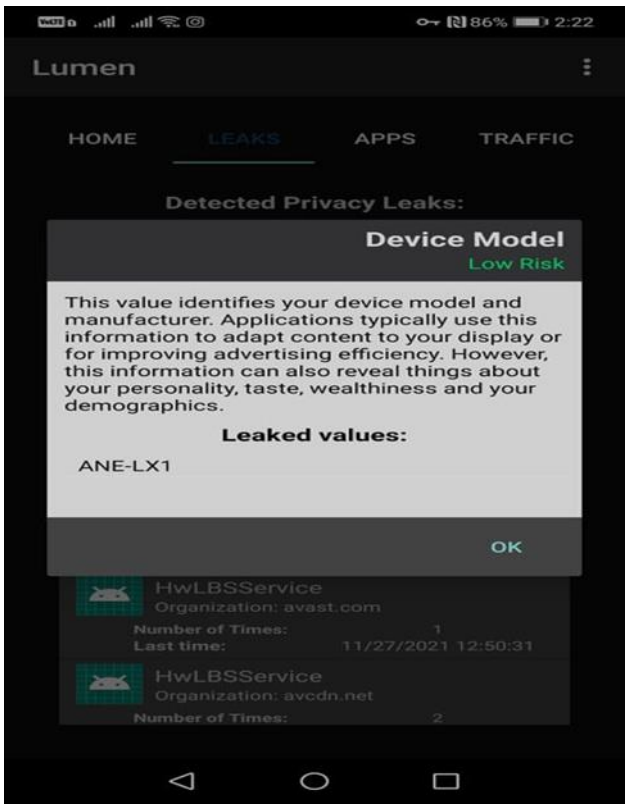
Εικόνα 19: Λεπτομερής Ανάλυση της Διαρροής (Build Fingerprint - Ουγγαρία)

Όσον αφορά την εφαρμογή της Ισπανίας, είδαμε πως εντοπίστηκε μόνο η κατηγορία Build Fingerprint, η οποία πρόκειται για μια κατηγορία μικρού ρίσκου. Οι πληροφορίες που συλλέγονται, οδηγούνται και εδώ σε δύο domain, για τα οποία όμως η καρτέλα leaks, δεν μας δίνει κάποια πληροφορία. Πατώντας πάνω στην επιλογή traffic, όπως φαίνεται στην παρακάτω εικόνα, η κίνηση πηγαίνει προς το xunta.gal που είναι και ο data controller της εφαρμογής, αλλά και προς το globalsign.com. Το δεύτερο, είναι ένας πάροχος αξιόπιστων λύσεων ταυτότητας και ασφάλειας που επιτρέπει σε επιχειρήσεις και παρόχους υπηρεσιών cloud σε όλο τον κόσμο, να ασφαλίζουν διαδικτυακές επικοινωνίες, να διαχειρίζονται εκατομμύρια επαληθευμένες ψηφιακές ταυτότητες και να αυτοματοποιούν τον έλεγχο ταυτότητας και την κρυπτογράφηση. Δηλαδή, βοηθάει την εφαρμογή του πράσινου πιστοποιητικού με την διασφάλιση των επικοινωνιών και την κρυπτογράφηση των ψηφιακών ταυτοτήτων.



Εικόνα 20: Λεπτομερής Ανάλυση της Διαρροής (Build Fingerprint - Ισπανία)

Στην εξωτερική καρτέλα των διαρροών, οι 2 αυτές εφαρμογές βρέθηκαν στην κατηγορία των διαρροών **Device Model.** Αυτή η κατηγορία διαρροών, προσδιορίζει το μοντέλο και τον κατασκευαστή της συσκευής του χρήστη. Οι εφαρμογές συνήθως χρησιμοποιούν αυτές τις πληροφορίες για να προσαρμόσουν το περιεχόμενο στην οθόνη του ή για να βελτιώσουν την αποτελεσματικότητα της διαφήμισης. Ωστόσο, αυτές οι πληροφορίες μπορούν επίσης να αποκαλύψουν πράγματα σχετικά με την προσωπικότητα, το γούστο, την ευημερία και τα δημογραφικά του στοιχεία. Η συγκεκριμένη διαρροή, αναφέρεται επίσης σαν χαμηλού ρίσκου. Αναφορά για το που πάνε τα δεδομένα αυτά δεν υπάρχει από την καρτέλα αυτή, αλλά κατά πάσα πιθανότητα έχουν τον ίδιο προορισμό με τις προηγούμενες περιπτώσεις, βάσει των ροών τους.



Εικόνα 21: Λεπτομερής Ανάλυση της Διαρροής (Device Model - Both)

Στην κεντρική καρτέλα των διαρροών, φαίνεται επίσης ποιος είναι ο οργανισμός που λαμβάνει τα δεδομένα (**gov.hu** για την **Ουγγαρία** και **globalsign.com** & **xunta.gal** για την **Ισπανία**). Τέλος, θα πρέπει να αναφέρουμε πως η εφαρμογή Lumen Privacy Monitor, δεν καταφέρνει να εντοπίσει όλες τις εξερχόμενες πληροφορίες από την συσκευή μας, εφόσον είναι κρυπτογραφημένη. Αυτό έχει ως αποτέλεσμα, τα ευρήματά μας μέσω του συγκεκριμένου εργαλείου να είναι περιορισμένα.

6.3 Έλεγχος των Privacy Policies

Στο τελευταίο κομμάτι της έρευνας, μελετήθηκαν τα privacy policies και των 26 παραπάνω εφαρμογών. Αυτό που έπρεπε να μελετηθεί σε αυτές, ήταν το αν είναι κατανοητό στον απλό χρήστη, ποια δεδομένα του θα υποστούν επεξεργασία ή θα αποθηκευτούν από την εφαρμογή και το αν οι πληροφορίες που συλλέξαμε από τα δύο προηγούμενα εργαλεία (exodus, lumen), αποτυπώνονται σε αυτές. Με απλά λόγια, το κατά πόσο ο χρήστης ενημερώνεται πλήρως, από τα συγκεκριμένα κείμενα ενημέρωσης.

Ξεκινώντας από τις 17 εφαρμογές πράσινου πιστοποιητικού, οι οποίες δεν εντοπίστηκαν να έχουν ενσωματωμένους ιχνηλάτες, παρατηρήθηκε πως τα νέα ήταν αρκετά θετικά. Ο χρήστης που θα επιχειρήσει να διαβάσει τα privacy policies τους, θα κατανοήσει ποια δεδομένα αποθηκεύει η εφαρμογή (π.χ. όνομα, επίθετο, «πράσινος ή κόκκινος» κ.α.), για ποιον λόγο το κάνει (π.χ. για εύκολη πρόσβαση σε συγκεκριμένους χώρους κ.α.), αλλά και για πόσον καιρό (συνήθως μέχρι το τέλος της πανδημίας). Όσον αφορά τις επικίνδυνες άδειες τις οποίες ζητούν οι εφαρμογές αυτές από τον χρήστη, έτσι ώστε να λειτουργούν με τον πιο αποτελεσματικό τρόπο, σχεδόν σε όλες τις

περιπτώσεις γίνεται φανερό στον χρήστη, με μια γρήγορη ανάγνωση. Για παράδειγμα, η άδεια της **κάμερας**, η οποία απαιτείται από όλες τις εφαρμογές, αναφέρεται σε όλα τα κείμενα ενημέρωσης. Η εφαρμογή με τις περισσότερες επικίνδυνες άδειες, όπως είδαμε και από τους παραπάνω πίνακες, ήταν η **PassCOVID.gal** της **Ισπανίας**. Παρ' όλα αυτά, όλες οι άδειες αναφέρονται στο αντίστοιχο privacy policy της εφαρμογής.

Το μοναδικό πρόβλημα το οποίο εντοπίστηκε, αφορά την εφαρμογή **COVID CHECK BG** της **Βουλγαρίας**. Στη συγκεκριμένη περίπτωση, ενώ η άδεια της κάμερας αναφερόταν, δεν υπήρχε ξεκάθαρη αναφορά στην άδεια write external storage. Αυτό έχει ως αποτέλεσμα, ο χρήστης να μην μπορεί εύκολα να καταλάβει αν η εφαρμογή έχει την δυνατότητα εγγραφής προσωπικών δεδομένων, σε εξωτερικό χώρο αποθήκευσης. Ένα άλλο ενδιαφέρον εύρημα, ήταν πως ορισμένες από τις εφαρμογές που μελετήθηκαν, όπως η **COVID tracker Ireland** της **Ιρλανδίας** και η **zVEM** της **Σλοβενίας**, συνεργάζονται με τρίτες οντότητες ή αλλιώς 3rd parties, οι οποίοι συνεισφέρουν στην καλή λειτουργία της εφαρμογής και έχουν την δυνατότητα πρόσβασης στα δεδομένα που συλλέγει η ίδια η εφαρμογή. Τα 3rd parties αυτά όμως, συμμορφώνονται με τις νομικές απαιτήσεις για τις συμβάσεις επεξεργασίας που ορίζονται από τον ΓΚΠΔ.

Τα σημαντικότερα προβλήματα όμως, βρέθηκαν στις 9 εφαρμογές πράσινου πιστοποιητικού, που διαθέτουν έναν ή περισσότερους ιχνηλάτες. Από τις 9, μόνο οι 3 ανέφεραν στην πολιτική απορρήτου την ύπαρξη ιχνηλατών, σε αντίθεση με τις επικίνδυνες άδειες, οι οποίες αναφέρονταν όλες. Πιο συγκεκριμένα:

- Η **CovidScanBE** εφαρμογή του **Βελγίου**, αναφέρει στην πολιτική απορρήτου, πως ενδέχεται να μεταφέρει δεδομένα που σχετίζονται με τη χρήση της εφαρμογής και της συσκευής στο Firebase (για τον εντοπισμό προβλημάτων στην εφαρμογή) με τη συγκατάθεση του χρήστη.
- Η **Skaner Certyfikatów Covid** της **Πολωνίας**, αναφέρει στην πολιτική απορρήτου, πως γίνεται χρήση των Google Analytics.
- Η **Tecka-prukaz bezinfekcnosti covid** της **Τσεχίας**, αναφέρει στην πολιτική απορρήτου πως προκειμένου να διασφαλιστεί η λειτουργικότητα της εφαρμογής, λειτουργεί επίσης με data «on its operation» (π.χ. αρχεία καταγραφής εφαρμογής και χρήση της εφαρμογής) και χρησιμοποιεί τυπικά εργαλεία (Firebase Crashlytics, Firebase RemoteConfig και Google Analytics) από την Google. Τα δεδομένα που αποστέλλονται από τις εφαρμογές σε αυτές τις υπηρεσίες δεν περιέχουν τα αναγνωριστικά του κατόχου του κινητού τηλεφώνου ή του ίδιου του κινητού τηλεφώνου (όπως ο αριθμός τηλεφώνου, IMEI, AdvertisingID) και υποβάλλονται σε επεξεργασία αποκλειστικά με σκοπό τον εντοπισμό και τη διόρθωση κρίσιμων λαθών, την καταγραφή ενημερώσεων της εφαρμογής και τη στατιστική χαρτογράφηση της εφαρμογής από τον χρήστη. Η εφαρμογή δεν γνωρίζει τα προσωπικά δεδομένα του χρήστη και αυτά τα τηλεμετρικά δεδομένα δεν μπορούν να συνδεθούν με κανέναν τρόπο με ένα συγκεκριμένο άτομο.

Όσον αφορά τις υπόλοιπες 6 εφαρμογές πράσινου πιστοποιητικού, δεν υπάρχει κάποια αναφορά στους ιχνηλάτες που εντοπίσαμε μέσω του εργαλείου exodus. Έτσι ο χρήστης, ακόμα κι αν διαβάσει την πολιτική απορρήτου, δεν θα είναι σε θέση να κατανοήσει αν υπάρχουν ιχνηλάτες και πόσοι είναι. Στις 5 από τις 6 εφαρμογές, γίνεται αναφορά σε αξιόπιστους και εξουσιοδοτημένους 3rd parties, αλλά χωρίς να αναφέρει τα ονόματά τους. Τέλος, στην πολιτική απορρήτου της εφαρμογής **Green Pass** της **Σλοβακίας**, αναφέρεται πως δεν υπάρχουν ούτε 3rd parties. Οι συγκεκριμένες εφαρμογές λοιπόν, μπορεί να αναφέρουν στα privacy policies τους, ότι ακολουθούν τους κανόνες του ΓΚΠΔ και πολλές φορές να επισημαίνουν και ορισμένους από αυτούς, όμως η αμέλειά τους να ενημερώσουν τους χρήστες, σχετικά με τους ιχνηλάτες που υπάρχουν μέσα σε αυτές,

καταπατάει την ιδιωτικότητά τους. Οι χρήστες των συγκεκριμένων εφαρμογών, δεν έχουν την δυνατότητα να γνωρίζουν, που καταλήγουν τα προσωπικά τους δεδομένα, ούτε και για ποιους σκοπούς αυτά δίνονται. Στις περισσότερες των περιπτώσεων, οι ιχνηλάτες είναι Google Analytics, τα οποία όπως είδαμε και στις 3 παραπάνω εφαρμογές χρησιμοποιούνται για την καλύτερη λειτουργικότητα της εφαρμογής και όχι για κάποιον πιο ύπουλο σκοπό. Αυτό όμως δεν σημαίνει πως δεν είναι άξιο αναφοράς από τους δημιουργούς των εφαρμογών αυτών.

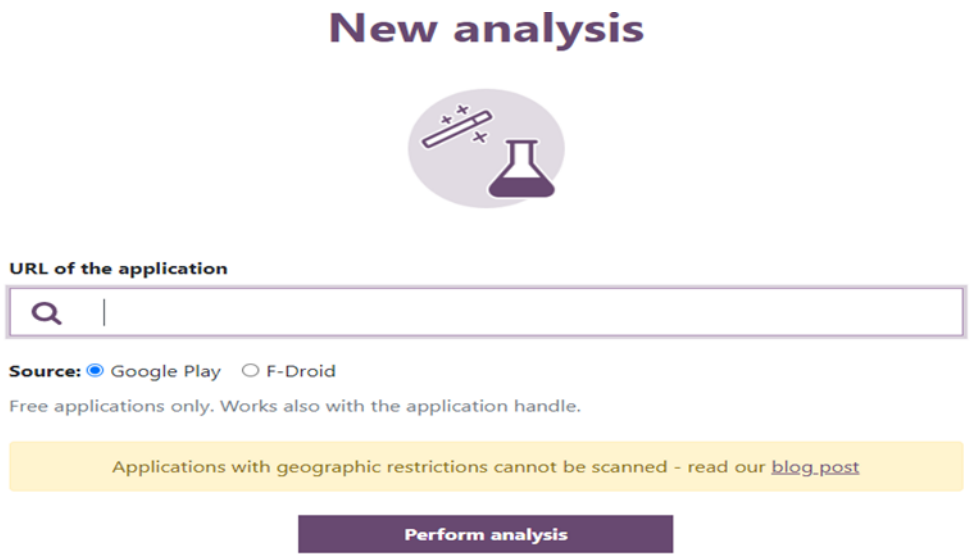
7. ΠΡΟΒΛΗΜΑΤΑ ΚΑΤΑ ΤΗΝ ΕΡΕΥΝΑ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

7.1 Προβλήματα και Περιορισμοί που Αντιμετωπίστηκαν κατά την Έρευνα

Κατά τη διάρκεια της έρευνας και τη χρήση των εργαλείων που αναφέρθηκαν και αναλύθηκαν σε προηγούμενα κεφάλαια, αντιμετωπίστηκαν κάποια προβλήματα, τα οποία στάθηκαν εμπόδιο στο να έχουμε ένα πιο σωστό και ολοκληρωμένο αποτέλεσμα. Αυτά είναι τα ακόλουθα:

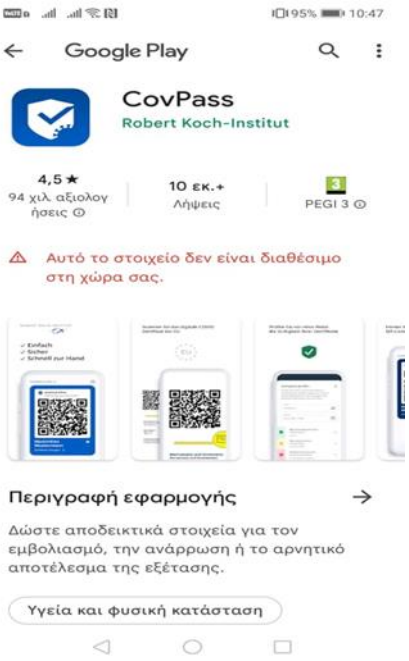
- Καθώς τα ψηφιακά πράσινα πιστοποιητικά είναι κάτι νέο αλλά και προσωρινό, οι πηγές σχετικά με τις εφαρμογές πράσινων πιστοποιητικών ήταν περιορισμένες. Βρέθηκε μόνο μία πηγή, η οποία ανέφερε ποιες χώρες έχουν δημιουργήσει εφαρμογή και ποιο είναι το όνομά της, αλλά ήταν σε αρκετά αρχικό στάδιο, οπότε εμπεριείχε λίγες εξ αυτών. Επίσης, λίγες χώρες ανέφεραν στις κυβερνητικές σελίδες τους, ή στις αντίστοιχες σελίδες των υπουργείων υγείας την ονομασία της εφαρμογής και πως μπορείς να τη βρεις σε Play Store και App Store. Αυτό είχε ως αποτέλεσμα, να πάρει πολύ χρόνο η εύρεση των εφαρμογών αυτών, με πολλές από αυτές να εντοπίζονται κατόπιν εξαντλητικής έρευνας. Η έλειψη επαρκών πηγών με πληροφορίες για τις εν λόγω εφαρμογές, οδήγησε στην αδυναμία εύρεσης εφαρμογής για την Εσθονία και στη χρήση εφαρμογής wallet για τις Ιρλανδία και Σλοβενία.

- Ένα δεύτερο, αλλά προσωρινό πρόβλημα, παρουσιάστηκε με το εργαλείο exodus. Ορισμένες εφαρμογές δεν ήταν αποθηκευμένες από παλαιότερους ελέγχους άλλων χρηστών, ή δεν τις εμφάνιζε. Έτσι, δεν ήταν δυνατή η καταγραφή των στοιχείων αυτών σχετικά με τις άδειες που ζητούν και τους ιχνηλάτες εφόσον υπάρχουν. Τελικά, βρέθηκε η επιλογή «Perform a new analysis», στην οποία τοποθετείτε το URL της εφαρμογής από το Play Store και πραγματοποιείται η ανάλυση.



Εικόνα 22: Νέα Ανάλυση Εφαρμογής - exodus

- Το τρίτο και τελευταίο πρόβλημα παρουσιάστηκε στον έλεγχο για διαρροές, μέσω του εργαλείου lumen. Ορισμένες από τις εφαρμογές, 4 από τις 26, (Βουλγαρία, Γερμανία, Πολωνία και Φινλανδία), δεν κατέστη δυνατό να εγκατασταθούν στο κινητό, διότι δεν επιτρεπόταν στη χώρα μας (Εικόνα 23). Το πρόβλημα αυτό, δημιούργησε ένα κενό στην έρευνά μας, καθώς δεν μπορούμε να έχουμε μια ολοκληρωμένη εικόνα για όλες τις εφαρμογές, σχετικά με τις διαρροές τους προς τρίτους.



Εικόνα 23: Αδυναμία Εγκατάστασης Εφαρμογής CovPass

7.2 Συμπεράσματα

Το θέμα που πραγματεύεται η παρούσα διπλωματική, έχει έντονο ερευνητικό ενδιαφέρον, μιας και η πανδημία, εξακολουθεί να υφίσταται μετά από σχεδόν τρία χρόνια. Όπως όλα δείχνουν, δε θα ξεφύγουμε εύκολα από αυτήν. Τα βήματα προς την κανονικότητα που έχουν γίνει είναι μεγάλα, ενώ τα lock down και η απαγόρευση κυκλοφορίας μοιάζουν μακρινές αναμνήσεις. Οι κυβερνήσεις, σε συνδυασμό με τα υπουργεία υγείας, έκαναν ότι περνούσε από το χέρι τους και μετά την ανακάλυψη των εμβολίων, επιχείρησαν να άρουν τις απαγορεύσεις με σταθερά βήματα. Μια σημαντική βοήθεια στο να επιτευχθεί αυτός ο σκοπός, ήταν τα ψηφιακά πράσινα πιστοποιητικά, τα οποία και υιοθέτησαν όλες οι χώρες τις Ευρωπαϊκής Ένωσης.

Οι πολίτες, μαθαίνουν να ζουν με αυτό και να το επιδεικνύουν σε κάθε μέρος που θέλουν να επισκεφτούν. Κάπως έτσι, μπήκαν στη ζωή των ανθρώπων και οι εφαρμογές πράσινων πιστοποιητικών, οι οποίες βοηθούν στην επαλήθευση των πιστοποιητικών του κάθε πολίτη. Όλοι οι ιδιοκτήτες καταστημάτων, εστιατορίων, γηπέδων και άλλων χώρων που δέχονται επισκέψεις από πολίτες, είναι αναγκασμένοι να διαθέτουν την συγκεκριμένη εφαρμογή και να ελέγχουν την εγκυρότητα των πιστοποιητικών. Τα σχόλια βέβαια για τις εφαρμογές αυτές στο Play Store, δεν είναι και τα καλύτερα, με πολλούς χρήστες να αναφέρουν διάφορα προβλήματα κατά τη λειτουργία τους.

Δεν είναι λίγοι οι πολίτες που ανησυχούν και δεν θέλουν να εγκαταστήσουν τη συγκεκριμένη εφαρμογή, καθώς φοβούνται για τους κινδύνους ιδιωτικότητας που εγείρονται από αυτές. Ο φόβος αυτός, μπορεί να προέρχεται από όσα ακούγονται για τις πιο γνωστές εφαρμογές κινητών, οι οποίες λαμβάνουν από τα κινητά προσωπικά δεδομένα και τα διαρρέουν σε τρίτους. Επίσης, βλέπουν το μεγάλο εύρος αδειών που ζητούν από αυτούς, με αποτέλεσμα να πιστεύουν ότι παρακολουθούνται. Τέλος, το γεγονός ότι τους παρέχουν τις εφαρμογές αυτές οι ίδιες οι κυβερνήσεις, οι οποίες τους ανάγκασαν να μένουν στα σπίτια τους, απαγορεύοντας τους την κυκλοφορία, τους κάνει ακόμα πιο καχύποπτους. Είναι γεγονός ότι οι πολίτες έχουν χάσει την εμπιστοσύνη τους στις κυβερνήσεις και τα υπουργεία υγείας, μιας και οι τελευταίοι αναιρούν συνεχώς αυτά που λένε. Αυτό έχει να κάνει, είτε με την αρχή της πανδημίας όπου η μια βδομάδα απαγόρευσης γινόταν 3 και 4, είτε πιο πρόσφατα όπου τα εμβόλια φαίνεται να μην κρατάνε για μεγάλο χρονικό διάστημα (με αποτέλεσμα να κάνουμε 3 ή και περισσότερες δόσεις), ενώ δε φαίνεται να εξασφαλίζουν και την πολυπόθητη ανοσία.

Μετά την έρευνα που πραγματοποιήθηκε στις εφαρμογές πράσινου πιστοποιητικού για τις χώρες τις Ευρωπαϊκής Ένωσης, παρατηρήθηκε πως επεξεργάζονται πολύ λίγες πληροφορίες χρηστών. Τα δεδομένα που λαμβάνουν, αφορούν το όνομα, το επίθετο και το αποτέλεσμα του πιστοποιητικού, καθώς και το πότε αυτό εκδόθηκε. Μπορεί αρκετές εφαρμογές να ζητούν πολλές άδειες, αλλά ελάχιστες θεωρούνται επικίνδυνες. Η πιο συνηθισμένη και σε πολλές περιπτώσεις και η μοναδική, είναι η χρήση της κάμερας. Αυτή, όπως γίνεται εύκολα αντιληπτό, είναι απαραίτητη για να πραγματοποιηθεί το σκανάρισμα του πιστοποιητικού. Στον τομέα λοιπόν αυτό, οι κυβερνήσεις των χωρών και οι προγραμματιστές των εφαρμογών έχουν κάνει ικανοποιητική δουλειά.

Όσον αφορά τους ιχνηλάτες, είδαμε ότι το ποσοστό των εφαρμογών που έχουν ενσωματωμένους, ήταν σχετικά μικρό. Επίσης σχεδόν όλοι, είχαν να κάνουν με τη Google. Οφείλεται βέβαια να παρέχεται στον χρήστη η δυνατότητα να διακόπτει τη χρήση των Google play services, καθώς οι συγκεκριμένες υπηρεσίες έχουν διαρροές σε τρίτους. Ένα τέτοιο παράδειγμα στη συγκεκριμένη έρευνα, ήταν οι εφαρμογές της Ισπανίας και της Ουγγαρίας, στις οποίες εντοπίστηκαν διαρροές και παρατηρήθηκε πως και οι δύο είχαν ενσωματωμένους ιχνηλάτες της Google.

Το πιο ανησυχητικό εύρημα, ήταν πως οι περισσότερες από τις εφαρμογές που έχουν ιχνηλάτες, 6 από τις 9, δεν έκαναν καμία αναφορά σε αυτούς στις πολιτικές απορρήτου τους. Αυτό έχει ως αποτέλεσμα, οι χρήστες που θα κατεβάσουν τις εφαρμογές, να μην γνωρίζουν την ύπαρξή τους, πράγμα που καταπατά τα δικαιώματά τους, αλλά και τους κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων. Ωστόσο, με μια περαιτέρω έρευνα σαν αυτή που πραγματοποιήθηκε στην παρούσα διπλωματική, θα ανακύψει το πρόβλημα αυτό, το οποίο αν πάρει διαστάσεις, θα κάνει τους πολίτες ακόμα πιο δύσπιστους. Παρ΄ ότι αποτελούν μειοψηφία, οι εφαρμογές αυτές, είναι ικανές να χαλάσουν τη φήμη του συνόλου των εφαρμογών πράσινου πιστοποιητικού και να χαρακτηριστούν αναξιόπιστες και επικίνδυνες για τους χρήστες στο σύνολό τους.

Το βασικό συμπέρασμα που βγήκε από την έρευνα, είναι πως οι εφαρμογές πράσινου πιστοποιητικού των χωρών της Ευρωπαϊκής Ένωσης, έχουν υιοθετήσει σε μεγάλο βαθμό και έχουν ταυτιστεί με τους κανόνες του Γενικού Κανονισμού Προστασίας Δεδομένων. Άξιο αναφοράς είναι πως όλες τον αναφέρουν σε σημεία των πολιτικών απορρήτου τους. Επίσης, γίνεται επισήμανση και σε συγκεκριμένα άρθρα που βασίζονται. Υπάρχουν βέβαια και οι εφαρμογές που έχουν ενσωματωμένους ιχνηλάτες ενώ δεν θα έπρεπε, όπως και τρίτα μέλη, με τα οποία όμως συνεργάζονται νόμιμα.

Τα αποτελέσματα στο σύνολό τους, ήταν πολύ ενθαρρυντικά καθώς το νομικό πλαίσιο δείχνει να τηρείται σε μεγάλο βαθμό και τα προσωπικά δεδομένα του χρήστη να μην καταπατούνται. Οι επικίνδυνες άδειες ήταν περιορισμένες και αναφέρονταν στις πολιτικές απορρήτου ενώ οι εφαρμογές που είχαν ενσωματωμένους ιχνηλάτες ήταν λίγες, χωρίς όμως αναφορά στις πολιτικές απορρήτου. Επιπλέον, οι διαρροές έκαναν και αυτές την εμφάνιση τους, αλλά μόνο σε δύο εφαρμογές. Φαίνεται πως τόσο οι κυβερνήσεις, όσο και οι προγραμματιστές των εφαρμογών, έβαλαν τα δυνατά τους και κατέβαλαν μια πολύ καλή προσπάθεια για να κερδίσουν την εμπιστοσύνη των πολιτών. Οι εξαιρέσεις όμως είναι πάντα αυτές που μένουν, ειδικά όταν υπάρχει καχυποψία. Θα πρέπει λοιπόν, να εναρμονιστούν όλες και όχι απλά οι περισσότερες εφαρμογές, με τους κανονισμούς και να σέβονται τα θεμελιώδη δικαιώματα της προστασίας των προσωπικών δεδομένων (να επεξεργάζονται με λίγα λόγια τα απολύτως απαραίτητα δεδομένα των χρηστών, χωρίς την ύπαρξη διαρροών δεδομένων, οι οποίες εκφεύγουν του νομικού πλαισίου προστασίας δεδομένων), έτσι ώστε οι χρήστες να χρησιμοποιούν τις εφαρμογές άφοβα. Επομένως, θα πρέπει να χρησιμοποιούμε τις εφαρμογές πράσινου πιστοποιητικού για το κοινό καλό, με την προϋπόθεση να υπάρχει διαφάνεια, αλλά και σεβασμός στους χρήστες και στα προσωπικά τους δεδομένα.

Σε κάθε περίπτωση, διαφαίνεται ότι η αξιοποίηση έξυπνων εφαρμογών για αντιμετωπίσεις κρίσεων - όπως μία πανδημία - θα είναι πλέον μία βασική επιλογή των κυβερνήσεων. Σε αυτό το πλαίσιο, είναι απόλυτα σημαντικό να αναπτύσσονται και να λειτουργούν οι εφαρμογές με πλήρη διαφάνεια και σεβασμό στα ατομικά δικαιώματα. Μόνο με αυτόν τον τρόπο οι πολίτες θα έχουν απόλυτη εμπιστοσύνη σε αυτές, η οποία εμπιστοσύνη με τη σειρά της θα συντελέσει στην αποτελεσματικότητά τους. Ακριβώς για αυτό, οι κυβερνήσεις θα πρέπει να καταβάλλουν κάθε προσπάθεια για να «πείθουν» τους πολίτες για την απόλυτα θεμιτή επεξεργασία των δεδομένων τους, ενώ και ο ρόλος των εποπτικών αρχών προστασίας δεδομένων πρέπει να είναι ουσιαστικός.

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ENISA	European Network and Information Security Agency
GDPR	General Data Protection Regulation
ICT	Information Communication Technologies
iOS	iPhone Operating System
IoT	Internet of Things
ML	Machine Learning
PCR	Polymerase Chain Reaction
RAT	Rapid Antigen Testing
RT	Real Time
SDK	Software Development Kit
VR	Virtual Reality
ΑΠΔ	Αρχή Προστασίας Δεδομένων
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΠΔ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΠΟΥ	Παγκόσμιος Οργανισμός Υγείας

ΑΝΑΦΟΡΕΣ

[1] Muhammad Sarwar, Tariq Rahim Soomro, “Impact of Smartphone’s on Society”, European Journal of Scientific Research, vol, 98, pp. 216-226, March 2013.

[2] Shraim, K., & Crompton, H. (2015, 1 1). Perceptions of Using Smart Mobile Devices in Higher Education Teaching: A Case Study from Palestine. Eric.ed.gov: https://files.eric.ed.gov/fulltext/EJ1105758.pdf

[3] Top 10 Mobile App Development Trends of 2022, Dec. 2017, by ADELA. Available: https://wiredelta.com/mobile-app-development-2022/

[4] 2022 is Coming: 8 Mobile App Development Trends to Look For, Dec. 2021, Available: https://saucelabs.com/blog/2022-is-coming-eight-mobile-app-development-trends-to-look-for

[5] Flora, H. W. (2014). (2014) An Investigation into Mobile Application Development Processes: Challenges and Best Practices. Στο H. W. Flora, Education and Computer Science (σελ. 1-9).

[6] Statista, Available: https://www.statista.com/accounts/pa

[7] Zinevych, S. (2014, 9 1). The Overview of Mobile Apps Market: Why You Should Enter Now. https://www.business2community.com/mobile-apps/overview-mobile-apps-market-enter-now-0994728#Wh9GTzDVdJWcxUoJ.97

[8] ENISA- European Union Agency for Network and Information Security, Privacy and Data Protection in mobile applications: A study on the app development ecosystem and the technical implementation of GDPR, Νοέμβριος 2017.

[9] Claude Castelluccia, Seda Guerses, Marit Hansen, Jaap-Henk Hoepman, Joris van Hoboken, and Barbara Vieira. Privacy and data protection in mobile applications. study, European Union Agency For Network and Information Security, 2017.

[10] AEPD. Guidelines for data protection by default. report, Spanish Data Protection Agency, 2020.

[11] AEPD. A guide to privacy by design. report, Spanish Data Protection Agency, 2020.

[12] Kaspersky, The dangers of phishing: Help employees avoid the lure of cybercrime, 2017, Available: https://go.kaspersky.com/rs/802-IJN-240/images/Dangers_Phishing_Avoid_Lure_Cybercrime_ebook.pdf

[13] Kaspersky, What is a Botnet?,2022, Available: https://usa.kaspersky.com/resource-center/threats/botnet-attacks

[14] Clare Stouffer, Spyware: What is spyware + how to protect yourself, Dec. 2021, Available: https://us.norton.com/internetsecurity-malware-spyware.html

[15] Exodus, “trackers”, Available: https://reports.exodus-privacy.eu.org/en/info/trackers/

[16] Stylianos Monogios, Konstantinos Limniotis, Nicholas Kolokotronis, and Stavros Shiaeles. A Case Study of Intra-library Privacy Issues on Android GPS Navigation Apps, pages 34{48. 01 2020.

[17] Son Sooel, Daehyeok Kim, and Shmatikov Vitaly. What mobile ads know about mobile users. 02 2016.

[18] Renee Lynn Midrack, What Is a Third-Party App?, Sep. 2021, Available: https://www.lifewire.com/what-is-a-third-party-app-4154068

[19] Developers, Request app permissions, 2022, Available: https://developer.android.com/training/permissions/requesting

[20] Developers, Permissions on Android, 2022, Available: https://developer.android.com/guide/topics/permissions/overview

[21] Developers, Permissions used only in default handlers, 2022, Available: https://developer.android.com/guide/topics/permissions/default-handlers

[22] “privacy”, Wikipedia. Mar. 01, 2022, Available: https://en.wikipedia.org/wiki/Privacy

[23] S. D. Warren and L. D. Brandeis, “The Right to Privacy”, Harv. Law Rev., vol. 4, no. 5, pp. 193-220, 1890.

[24] R. S. Rosenberg, The Social Impact of Computers. Elsevier, 2013

[25] Ε. Αλεξανδροπούλου – Αιγυπτιάδου, Πνευματική ιδιοκτησία και πληροφορική. Αθήνα: Θέμις, 2012.

[26] Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης "Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων", Dec. 18, 2000 Available: https://www.europarl.europa.eu/charter/pdf/text_el.pdf

[27] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Δέκα ερωτήσεις – απαντήσεις για τα προσωπικά δεδομένα", Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Available: https://www.dpa.gr/index.php/el

[28] European Commission, Commission. 2018. "Τι είναι τα δεδομένα προσωπικού χαρακτήρα;" Available: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_el

[29] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, "Ετήσια Έκθεση 2017 - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα," Αθήνα, 2018.

[30] "Ανοικτά Δεδομένα", Βικιπαίδεια. Mar. 02, 2022 Available: https://el.wikipedia.org/wiki/%CE%91%CE%BD%CE%BF%CE%B9%CF%87%CF%84%CE%AC_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CE%B1

[31] Κ. Λιμνιώτης, "Διαχείρηση Κινδύνων Ασφαλείας Πληροφοριακών και Επικοινωνιακών συστημάτων," Κύπρος, 2017.

[32] Ευρωπαϊκή Επιτροπή. Τι αποτελεί επεξεργασία δεδομένων; Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

[33] Yavuz CANBAY, Mehtap ULKER, Seref SAGIROGLU, "Detection of Mobile Applications Leaking Sensitive Data," Turkey 2017.

[34] Λ. Μήτρου, Σ. Κάτσικας, Σ. Γκριτζάλης και Κ. Λαμπρινουδάκης, Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών. Αθήνα: Παπασωτηρίου, 2010

[35] International Organization for Standardization, "ISO/IEC 27001:2013." International Organization for Standardization.

[36] M. Gadaleta, M. Rossi. 2018. "IDNet: Smartphone-Based Gait Recognition with Convolutional Neural Networks." Pattern Recognition 74 (February): 25-37. Available: https://www.sciencedirect.com/science/article/abs/pii/S0031320317303485?via%3Dihub

[37] D. Arp, E. Quiring, C. Wressnegger, and K. Rieck. 2017. "Privacy Threats through Ultrasonic Side Channels on Mobile Devices." IEEE Security and Privacy.

[38] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46". Official Journal of the European Union (OJ), 59, σσ. 1-88.

[39] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost. 2016 "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation. Available: http://friedewald.website/wp-content/uploads/2016/06/apf2016.pdf

[40] Roßnagel, A., & Nebel, M. (2016). Policy Paper: Die neue Datenschutzgrundverordnung. Ist das Datenschutzrecht nun fürheutige Herausforderungen gerüstet? (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt). Karlsruhe. Available: https://www.forum-privatheit.de/forum-privatheit-de/texte/veroeffentlichungen-desforums/positionspapiere-policy-paper/PolicyPaper-5-Die-neue-DSGVO_1.-Auflage_Mai_2016.pdf

[41] A. Skendzic, B Kovacic, E. Tijan, "General Data Protection Regulation-Protection of Personal Data in an Organization," Opatija Croatia, Μάϊος 2018.

[42] ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων περιεχομένων, Available: https://www.privacy-regulation.eu/el/index.htm

[43] Y. Matsuda, P. Rosenstein, K. Takamura, and C. Scovitch, "Data Collection: Defining the Customer", MIT Sloan School of Management, USA, Electronic Commerce and Marketing.

[44] F. Panagopoulou, “Τα νέα δικαιώματα για τους πολίτες βάσει του Γενικού Κανονισμού Προστασίας Δεδομένων: Μια πρώτη αποτίμηση και συνταγματική αξιολόγηση”, Εφημερίδα Διοικητικού Δικαίου, 2017.

[45] “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679” – Article 29 data protection working party WP 248 rev.01

[46] Κ. Σιασιάκος, Σ. Αναστασίου, Κ. Τούντας, “Εκτίμηση των επιπτώσεων σχετικά με την Προστασία των Προσωπικών Δεδομένων σε έργα Ηλεκτρονικής Διακυβέρνησης”, 2016.

[47] Λ. Κοτσαλής, Κ. Μενουδάκος, “Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων GDPR “νομική διάσταση και πρακτική εφαρμογή””, Νομική Βιβλιοθήκη, 2018.

[48] Privacy and Electronic Communications Directive 2002, Wikipedia, Available: https://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_Directive_2002

[49] European Commission, E. (2017, 1 10) Available in Regulation of the European Parliament and of the Council: Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[50] Πολιτική για τα cookies, “Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης”, Available: https://ec.europa.eu/info/cookies_el

[51] E-PRIVACY EUROPEAN REGULATION ON PRIVACY AND ELECTRONIC COMMUNICATIONS, (2021, 1 12) Available: https://cms.law/en/deu/insight/e-privacy

[52] Ευρωπαϊκή Επιτροπή, “Ερωτήσεις και απαντήσεις – Ψηφιακό πράσινο πιστοποιητικό”, Mar. 17 2021, Available: https://ec.europa.eu/commission/presscorner/detail/el/qanda_21_1187

[53] European Data Protection Board “Κατευθυντήριες γραμμές 04/2020 για τη χρήση δεδομένων θέσης και εργαλείων ιχνηλάτησης επαφών στο πλαίσιο της έξαρσης της νόσου COVID-19”, Apr. 21 2020, Available: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_el_0.pdf

[54] Γνωμοδότηση 2/21, Αρχή Προστασίας Δεδομένων, Αθήνα, July. 09 2021

[55] Τι είναι το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ);, “Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης”, Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_el

[56] Ευρωπαίος Επόπτης Προστασίας Δεδομένων 2021, Wikipedia, Available: https://el.wikipedia.org/wiki/%CE%95%CF%85%CF%81%CF%89%CF%80%CE%B1%CE%AF%CE%BF%CF%82_%CE%95%CF%80%CF%8C%CF%80%CF%84%CE%B7%CF%82_%CE%A0%CF%81%CE%BF%CF%83%CF%84%CE%B1%CF%83%CE%AF%CE%B1%CF%82_%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD

[57] Οι αρχές προστασίας δεδομένων της ΕΕ εκδίδουν κοινή γνώμη σχετικά με τις προτάσεις για το ψηφιακό πράσινο πιστοποιητικό, “Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης”, Apr. 2021, Available: https://edpb.europa.eu/news/news/2021/eu-data-protection-authorities-adopt-joint-opinion-digital-green-certificate_el

[58] Ευρωπαϊκή Επιτροπή, “Το ψηφιακό πιστοποιητικό COVID της ΕΕ, εμβολιασμοί και ταξιδιωτικοί περιορισμοί”, Available: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/movement-and-residence/eu-digital-covid-certificate-vaccinations-and-travel-restrictions_el

[59] “Ο "Αδόλφος Χίτλερ" έχει βγάλει ευρωπαϊκό πιστοποιητικό εμβολιασμού”, Oct. 30 2021 Available: https://www.news247.gr/kosmos/o-adolfos-chitler-echei-vgalei-eyropaiko-pistopoiitiko-emvoliasmoy.9406372.html?fbclid=IwAR1H8fJ3diVWmwQOldlx6HnrLt9lDo-ocdezycubM1hWiQPoDCY13OqC9V8

[60] “Κλάπηκαν ψηφιακά κλειδιά του πιστοποιητικού εμβολιασμού – Ο Χίτλερ φαίνεται εμβολιασμένος!”, Oct. 29 2021, Available: https://www.newscenter.gr/ellada/998562/klapikan-psifiaka-kleidia-toy-pistopoiitikoy-emvoliasmoy-o-chitler-fainetai-emvoliasmenos/

[61] “Δίνουν και παίρνουν τα πλαστά πιστοποιητικά εμβολιασμού… made in Βουλγαρία”, Nov. 03 2021, Available: https://www.newsit.gr/ellada/dinoun-kai-pairnoun-ta-plasta-pistopoiitika-emvoliasmou-made-in-voulgaria/3399648/?fbclid=IwAR0_XjoNPUbD5H1mjf6sLo2_qNJYnMapmU1NZtUz8jxG25S2vlwVxPsl4ds

[62] exodus “The privacy audit platform for Android applications”, 2022, Available: https://exodus-privacy.eu.org/en/page/what/

[63] “ICSI Haystack Project”, Oct. 2017, Available: https://haystack.mobi/

[64] A. Razaghpanah et al., “Apps, Trackers, Privacy and Regulators: A Global Study of the Mobile Tracking Ecosystem”, in Proceedings 2018 Network and Distributed System Security Symposium, San Diego, CA, 2018.

[65] Khanna, N. (2020, 6 2) “What is Lumen Privacy Monitor? How does it work?”, Available: https://candid.technology/lumen-privacy-monitor-review/

[66] Developers, Manifest.permission, 2022, Available: https://developer.android.com/reference/android/Manifest.permission