Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Η προστασία προσωπικών δεδομένων στο περιβάλλον «έξυπνων» κινητών συσκευών

Χρυσάνθη Τσιντέα

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Δεκέμβριος 2020

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Η προστασία προσωπικών δεδομένων στο περιβάλλον «έξυπνων» κινητών συσκευών

Χρυσάνθη Τσιντέα

Επιβλέπων Καθηγητής
Κωνσταντίνος Λιμνιώτης

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση
των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2020

Περίληψη

Στόχος της παρούσας έρευνας είναι η μελέτη σε θέματα προστασίας προσωπικών δεδομένων, στο περιβάλλον «έξυπνων» κινητών συσκευών. Θα διερευνηθεί, με γνώμονα τις εφαρμογές που χρησιμοποιεί ένας χρήστης από την κινητή του συσκευή, ποιοι κίνδυνοι εγείρονται ως προς την ιδιωτικότητα των χρηστών, καθώς επίσης και σε ποιο βαθμό οι χρήστες είναι ενήμεροι και σε επαγρύπνηση τόσο για τους κινδύνους αυτούς, όσο και με το σχετικό νομικό πλαίσιο αναφορικά με τη νόμιμη επεξεργασία προσωπικών δεδομένων και τα δικαιώματά τους.

Η μεθοδολογία που ακολουθήθηκε είναι η διεξαγωγή έρευνας με κατάρτιση ερωτηματολογίου για μελέτη χρηστών κινητών συσκευών, προκειμένου να αποτιμηθεί η ευαισθητοποίησή τους σε θέματα προστασίας της ιδιωτικότητας τους και των προσωπικών δεδομένων που συλλέγονται με ή χωρίς την συγκατάθεσή τους. Το ερωτηματολόγιο διαμοιράστηκε, μέσω κοινωνικών δικτύων, σε πλήθος χρηστών οι οποίοι αξιοποιούν «έξυπνες» εφαρμογές, προκειμένου να υπάρξει μία πρώτη αποτίμηση του βαθμού γνώσης τους επι των ανωτέρω και της επαγρύπνησής τους.

Το συμπέρασμα που ανακύπτει από την παρούσα διατριβή είναι ότι οι σύγχρονοι χρήστες δείχνουν να είναι ενημερωμένοι για το πώς τα προσωπικά τους δεδομένα διαχειρίζονται από τις εφαρμογές. Οι περισσότεροι έχουν γνώση για τους κινδύνους που εγκυμονεί η απόκτησή τους από κακόβουλους. Ωστόσο παραμένει ακόμα ένα σοβαρό ποσοστό χρηστών το οποίο δηλώνει άγνοια για τους κινδύνους και την νομοθεσία που διέπει τα προσωπικά δεδομένα που διαχειρίζονται οι διαδικτυακές εφαρμογές. Στις μεγαλύτερες ηλικίες το πρόβλημα είναι πιο έντονο. Συνεπώς, καθίσταται ακόμα επίκαιρη και σημαντική η ανάγκη διαρκούς ευαισθητοποίησης των χρηστών.

Summary

The aim of this thesis is to study privacy issues in the "smart" mobile world. The risks arising to the privacy of users will be investigated, as well as to what extent the users are aware of both of these risks and of the relevant legal framework regarding the lawful processing of personal data and their rights.

The methodology followed is to conduct research by compiling a questionnaire to evaluate how the mobile users are aware of privacy risks and of their personal data collected with or without their consent. The questionnaire was distributed, via social networks, to several users who use 'smart' applications in order to have an initial assessment of their degree of knowledge of the above and their vigilance.

The conclusion drawn from this thesis is that modern users seem to be informed about how their personal data is managed by applications. However, there is still a serious percentage of users who are unaware of the risks and legislation governing the personal data managed by online applications. At older ages the problem seems to be more pronounced. The need for continuous user awareness is therefore still relevant and important.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Κωνσταντίνο Λιμνιώτη που με την καθοδήγησή του συνέβαλε τα μέγιστα για την ολοκλήρωση της διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η σύγχρονη εποχή χαρακτηρίζεται από την έντονη χρήση των διαδικτυακών εφαρμογών από μεγάλο μέρος του παγκοσμίου πληθυσμού. Για την διαμόρφωση της κατάστασης αυτής σημαντικό ρόλο έπαιξαν κυρίως:

- Η ραγδαία ανάπτυξη των τεχνολογιών του διαδικτύου που το καθιστούν ελκυστικό κανάλι μετάδοσης πληροφορίας. Η ανάπτυξη αυτή οδήγησε σε σημαντική μείωση του κόστους πρόσβασης του μέσου χρήστη διαδικτυακών εφαρμογών σε ευρυζωνικές συνδέσεις.
- Για τη πρόσβαση στις διαδικτυακές εφαρμογές έπαψε να χρησιμοποιείται αποκλειστικά ο ηλεκτρονικός υπολογιστής αλλά πλέον χρησιμοποιείται μία ποικιλία συσκευών με διαφορετικά χαρακτηριστικά. Η πρόσβαση πλέον σε αυτές γίνεται ευέλικτη.

Οι διαδικτυακές εφαρμογές χρησιμοποιούνται σήμερα σε σχεδόν όλες τις ανθρώπινες δραστηριότητες. Το μεγαλύτερο ποσοστό των χρηστών τις χρησιμοποιεί στην καθημερινότητα του, ενώ πολύ συχνά χρησιμοποιούνται στον επαγγελματικό, οικονομικό, κοινωνικό και προσωπικό τομέα της δραστηριότητας τους.

Καθώς οι εφαρμογές των διαδικτυακών εφαρμογών καλύπτουν τόσο μεγάλο φάσμα της ανθρώπινης δραστηριότητας, είναι αναπόφευκτο να χειρίζονται ευαίσθητα προσωπικά δεδομένα των χρηστών τους. Απαιτείται συχνά η μετάδοση τους μέσω του διαδικτύου, η αποθήκευσή τους σε διατάξεις παρόχων διαδικτυακών υπηρεσιών και η επεξεργασία τους. Με τον τρόπο αυτό οι μεγάλες και ταχείς εξελίξεις στον τομέα της τεχνολογίας ανέδειξαν επιπτώσεις στα

δικαιώματα ιδιωτικότητας των χρηστών καθώς τα σχετικά με αυτήν δεδομένα ψηφιοποιούνται και μεταδίδονται στο νέφος του διαδικτύου. Όσο οι προσωπικές πληροφορίες ψηφιοποιούνται, τόσο μεγαλώνει και η ανησυχία των πολιτών σχετικά με το ποια δεδομένα τους συλλέγονται, ποιος είναι αυτός που τα συλλέγει, πού φυλάσσονται, πώς και από ποιους μπορούν να χρησιμοποιηθούν. Η ανησυχία αυτή αποτελεί το τίμημα για την διευκόλυνση και την ταχεία διεκπεραίωση λειτουργιών που εκτελούν οι χρήστες των διαδικτυακών εφαρμογών. Η ανησυχία γενικότερα αντιμετωπίζεται με γνώση, εμπειρία και τήρηση κανόνων για την μείωση των πιθανοτήτων εμφάνισης ανεπιθύμητων καταστάσεων. Με τον ίδιο τρόπο αντιμετωπίζονται οι ανησυχίες που πηγάζουν από την χρήση των διαδικτυακών εφαρμογών.

Η γνώση που απαιτείται να έχει ο χρήστης των διαδικτυακών εφαρμογών αναλύεται σε δύο συνιστώσες: αυτήν που αφορά το τεχνολογικό και αυτή που αφορά το νομικό επίπεδο. Η παρούσα μελέτη καταρχήν διερευνά το κατά πόσο ο πολίτης είναι ενημερωμένος πάνω σε θέματα ασφάλειας και ιδιωτικότητας τόσο σε νομικό όσο και σε τεχνολογικό επίπεδο. Επιπλέον αναζητείται να εντοπιστεί ο τρόπος με τον οποίο αντιδρά κατά την εγκατάσταση εφαρμογών στις κινητές του συσκευές – καθώς η πλειονότητα των χρηστών των διαδικτυακών εφαρμογών αποκτούν πρόσβαση μέσω αυτών. Με βάση το αποτέλεσμα της εξέτασης της συμπεριφοράς του κατά την εγκατάσταση και χρήση των διαδικτυακών εφαρμογών εντοπίζονται οι τρόποι με τους οποίους δύναται να ενισχύσει την ασφάλεια της ιδιωτικότητας του.

1.1 Σκοπός έρευνας

Σκοπός της παρούσας έρευνας είναι να μελετηθούν θέματα προστασίας προσωπικών δεδομένων, υπό το πρίσμα του σχετικού νομικού πλαισίου, στο περιβάλλον «έξυπνων» κινητών συσκευών. Η χρήση διαδικτυακών εφαρμογών μέσω έξυπνων κινητών συσκευών, εκ της φύσεως της, εγείρει πολλαπλά ζητήματα προστασίας της ιδιωτικότητας, τα οποία παραμένουν ανοιχτά.

Ειδικότερα, δεδομένου ότι υπάρχει συγκεκριμένο νομικό πλαίσιο στην Ευρώπη αναφορικά με τις προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων, θα διερευνηθεί η γνώση του χρήστη σχετικά με το παρόν GDPR νομικό πλαίσιο, καθώς και την άσκηση των δικαιωμάτων του που απορρέουν από αυτό. Πέραν της νομικής εξασφάλισης, αναζητείται και το κατά πόσο είναι ικανοί οι χρήστες των διαδικτυακών εφαρμογών να χρησιμοποιήσουν την τεχνολογία για να εξασφαλίσουν τα προσωπικά τους δεδομένα από μη εξουσιοδοτημένη πρόσβαση και επεξεργασία.

Η συνισταμένη του σκοπού της έρευνας είναι ο εντοπισμός των τρόπων με τους οποίους οι άνθρωποι θα πρέπει να χειρίζονται τις λειτουργίες των διαδικτυακών εφαρμογών ώστε να διασφαλίζουν την ιδιωτικότητά τους αλλά και το πώς θα πρέπει να αντιδρούν σε περιπτώσεις που αυτή τίθεται σε κίνδυνο.

1.2 Βασικά ερευνητικά ερωτήματα

Με βάση την παραπάνω περιγραφή τα βασικά ερευνητικά ερωτήματα που καλείται η παρούσα μελέτη να έχει απαντήσει με την ολοκλήρωση της είναι τα παρακάτω:

- Ποιοι οι κίνδυνοι που ελλοχεύουν από την απρόσεκτη χρήση εφαρμογών στις έξυπνες κινητές συσκευές
- Σε ποιο επίπεδο γνωρίζει ο πολίτης για το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και τα δικαιώματά τους.
- Σε ποιον βαθμό είναι ο χρήστης των διαδικτυακών εφαρμογών ενημερωμένος για τους τρόπους με τους οποίους μπορεί να χρησιμοποιήσει την σύγχρονη τεχνολογία για να εξασφαλίζεται η ιδιωτικότητά του.
- Πως μπορεί ο σύγχρονος χρήστης των διαδικτυακών εφαρμογών να θωρακίσει την ιδιωτικότητά του.

1.3 Αναγκαιότητα και σπουδαιότητα έρευνας

Οι ραγδαίες τεχνολογικές εξελίξεις, η χρήση διαδικτύου, η όλο και αυξανόμενη χρήση των κινητών συσκευών, οι νέες εφαρμογές, τα social media, είναι καθημερινότητα στους πολίτες, που οδηγούν στην διάχυση μεγάλου όγκου προσωπικών δεδομένων στο διαδίκτυο. Στο περιβάλλον αυτό είναι εκτεθειμένα σε δυνητική κακόβουλη χρήση τους. Μεγάλο ποσοστό των κινδύνων απορρέουν από την απρόσεκτη εγκατάσταση εφαρμογών σε κινητές συσκευές όπου ο χρήστης μπορεί να μην έχει αντίληψη ότι τα προσωπικά δεδομένα του χρησιμοποιούνται για επεξεργασία από τρίτους, ή την απρόσεκτη αποκάλυψη πληροφοριών του χρήστη, την οποία την πραγματοποιεί ο ίδιος ακριβώς λόγω της άγνοιας των κινδύνων και των συνεπειών που ενδεχομένως επέλθουν.

Ήδη είναι ευρέως γνωστό ότι πολλοί οργανισμοί ενδιαφέρονται να αποκτούν πρόσβαση σε προσωπικά δεδομένα συνηθέστερα για την μεγιστοποίηση της αποδοτικότητας προωθητικών ενεργειών ή για την μελέτη της συμπεριφοράς της κοινής γνώμης. Πολλές φορές οι οργανισμοί αυτοί αποφεύγουν να εξασφαλίζουν την συναίνεση των υποκειμένων. Δεν είναι ωστόσο λίγες οι φορές όπου οι σκοποί των συλλεκτών δεδομένων δεν είναι αθώοι με αποτέλεσμα να τίθενται σε κίνδυνο σημαντικά αγαθά των υποκειμένων. Κατά συνέπεια η ιδιωτικότητα και η ασφάλεια των προσωπικών και ευαίσθητων δεδομένων των πολιτών αποτελούν κρίσιμα ζητήματα. Ως εκ τούτου η θέσπιση του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR), ο οποίος είναι σε εφαρμογή από τον Μάιο του 2018, καθώς και ο νέος προτεινόμενος Κανονισμός E-Privacy (που θα αντικαταστήσει την τρέχουσα Οδηγία e-Privacy), που αποτελεί συμπλήρωση του πρώτου υπό την έννοια ότι αποτελεί εξειδίκευση σε συγκεκριμένο τομέα επεξεργασίας προσωπικών δεδομένων, επικεντρώνεται ιδιαίτερα στο θέμα της ιδιωτικότητας των ηλεκτρονικών επικοινωνιών και του διαδικτύου, ώστε να προστατευτούν τα ψηφιακά δεδομένα του πολίτη.

Η αναγκαιότητα και η σπουδαιότητα της έρευνας είναι να γίνει εκτίμηση των κινδύνων που απορρέουν από την εγκατάσταση μιας εφαρμογής μη ελεγμένης ,

να ενισχυθεί η προστασία των προσωπικών δεδομένων και η κουλτούρα που πρέπει να καλλιεργηθεί στους πολίτες για την ασφάλεια και ιδιωτικότητα τους σχετικά με την ασφάλεια των δεδομένων στις κινητές συσκευές τους. Αυτή θα πρέπει να περιλαμβάνει και τεχνική γνώση ώστε να αποτρέπεται – όσο το δυνατόν αποτελεσματικότερα – η έκθεση των ευαίσθητων δεδομένων στους κινδύνους του διαδικτύου. Παρόλο που τα ζητήματα ιδιωτικότητας είναι γνωστά στην επιστημονική και ερευνητική κοινότητα, αλλά και σε πλήθος χρηστών, εν τούτοις είναι επίσης γνωστό ότι τόσο αρκετοί πάροχοι εφαρμογών δεν συμμορφώνονται με τις προϋποθέσεις νόμιμης επεξεργασίας προσωπικών δεδομένων (π.χ. αποκτώντας πρόσβαση χωρίς ρητή συγκατάθεση του χρήστη σε προσωπικά του δεδομένα, για όχι διαφανείς σκοπούς) όσο και αρκετοί χρήστες δεν έχουν την απαραίτητη επαγρύπνηση ως προς τους κινδύνους αυτούς.

Η αντιμετώπιση των κινδύνων ξεκινάει με την επίγνωση της άγνοιας τους ώστε να ανακαλυφθούν οι τρόποι με τους οποίους ο σύγχρονος χρήστης θα γνωρίζει πώς να διασφαλίζει την ιδιωτικότητά του σε τεχνικό και νομικό επίπεδο. Στην περίπτωση αυτή θα μπορεί να απολαμβάνει τα αγαθά της τεχνολογικής προόδου σε όλη τους την έκταση.

1.4 Προτεινόμενη μεθοδολογία

Η μεθοδολογία της μελέτης περιλαμβάνει:

- Βιβλιογραφική έρευνα για τον προσδιορισμό του νομοθετικού και τεχνολογικού πλαισίου προστασίας της ιδιωτικότητας του μέσου χρήστης των διαδικτυακών εφαρμογών που είναι προσβάσιμες από έξυπνες κινητές συσκευές.
- Πρακτική μελέτη του χειρισμού των προσωπικών δεδομένων από τις διαδικτυακές εφαρμογές που είναι προσβάσιμες από έξυπνες κινητές συσκευές. Για τον σκοπό αυτό χρησιμοποιείται ενδεικτικά μια κατάλληλη εφαρμογή η οποία έχει την δυνατότητα να παρέχει σχετικές πληροφορίες.

- Διεξαγωγή ερωτηματολογίου για μελέτη της συμπεριφοράς των χρηστών έξυπνων κινητών συσκευών ως προς την ευαισθητοποίηση τους σχετικά με την προστασία της ιδιωτικότητας τους και των προσωπικών δεδομένων κατά την χρήση διαδικτυακών εφαρμογών. Η έρευνα εστιάζει στο πώς αντιλαμβάνονται την συλλογή των προσωπικών τους δεδομένων από τους παρόχους των διαδικτυακών εφαρμογών, λαμβάνοντας υπόψη τις γνώσεις τους σε τεχνολογικό και νομικό επίπεδο.

1.5 Δομή της Διατριβής

Η Διατριβή είναι διαρθρωμένη ως εξής:

- Κεφάλαιο 2: Στο πρώτο κεφάλαιο της μελέτης περιλαμβάνονται περιγραφή έξυπνων κινητών συσκευών και των χαρακτηριστικών τους που τις καθιστά ελκυστικές για το μεγαλύτερο μέρος του παγκοσμίου πληθυσμού. Εξετάζονται τα χαρακτηριστικά των πιο δημοφιλών κατηγοριών εφαρμογών και σκιαγραφείται το προφίλ των πιο χαρακτηριστικών τύπων χρηστών τους, ενώ καταγράφονται και χρήσεις των εφαρμογών που σχετίζονται κατά κάποιο τρόπο με την ιδιωτικότητα των χρηστών.
- Κεφάλαιο 3: Με την βοήθεια των στοιχείων του πρώτου κεφαλαίου περιγράφονται οι τρόποι με τους οποίους είναι πιθανό να εκτεθούν τα ευαίσθητα προσωπικά δεδομένα των χρηστών των διαδικτυακών εφαρμογών, σε μη εξουσιοδοτημένη πρόσβαση και χρήση. Για τους τρόπους αυτούς εξετάζονται τα νομικά και τεχνολογικά εργαλεία άμυνας των χρηστών. Παρουσιάζονται επίσης σε πρακτικό επίπεδο (με την χρήση κατάλληλης εφαρμογής) οι τρόποι με τους οποίους οι εφαρμογές μπορεί να χειρίζονται τα προσωπικά δεδομένα των χρηστών.
- Κεφάλαιο 4: Στην συνέχεια της μελέτης εξετάζεται ο βαθμός κατά τον οποίο οι χρήστες των διαδικτυακών εφαρμογών γνωρίζουν το πώς μπορούν να κατοχυρώσουν νομικά και τεχνολογικά την ιδιωτικότητα

τους. Για τον σκοπό αυτό διανεμήθηκε ερωτηματολόγιο σε ικανό πλήθος ανθρώπων ώστε να εντοπιστούν στην πράξη οι γνώσεις των μέσων χρηστών στα ζητήματα: Νομικό πλαίσιο και ασφάλεια, ενημέρωση - εκπαίδευση χρηστών.

- Κεφάλαιο 5: Στο τέλος της μελέτης καταγράφονται τα συμπεράσματα που προκύπτουν ως προς τον βαθμό προστασίας της ιδιωτικότητας από την χρήση διαδικτυακών εφαρμογών μέσω έξυπνων κινητών συσκευών. Με βάση τα συμπεράσματα αυτά προτείνονται αποτελεσματικοί τρόποι ενίσχυσης της προστασίας της

Κεφάλαιο 2
Έξυπνες Κινητές Συσκευές

2.1 Έξυπνες Κινητές Συσκευές

Το έξυπνο τηλέφωνο (smartphone) είναι μια σχετικά μικρή συσκευή που προσφέρει τις κλασικές λειτουργίες του απλού κινητού τηλέφωνου (κάμερα, βίντεο, πολυμέσα κ.α.), επιτρέποντας παράλληλα στον χρήστη να επιλέγει αυτός το εύρος των εφαρμογών που θα εγκαταστήσει και θα χρησιμοποιήσει. Με αυτόν τον τρόπο ο χρήστης αποκτά μια προσωποποιημένη κινητή συσκευή η οποία προσαρμόζεται στις προσωπικές και επαγγελματικές ανάγκες του. Τα κλασικά κινητά τηλέφωνα βάζουν ένα όριο στις εφαρμογές που μπορεί να χρησιμοποιήσει ο χρήστης λόγω της κλειστής αρχιτεκτονικής τους. Δηλαδή διαθέτουν δικό τους λογισμικό στο οποίο δεν μπορεί να παρέμβει ο χρήστης. Αντίθετα τα smartphones έχουν ανοικτή αρχιτεκτονική επιτρέποντας στον χρήστη να χρησιμοποιεί τις προ εγκατεστημένες εφαρμογές και να εγκαθιστά εφαρμογές που τον βοηθούν στις δραστηριότητες του. Γρήγορα τα smartphones έγιναν η δημοφιλέστερη συσκευή επικοινωνίας για το μεγαλύτερο μέρος του παγκοσμίου πληθυσμού καθώς στα χαρακτηριστικά τους περιλαμβάνονται:

- Διαθέτουν μεγάλη οθόνη αφής με εικονικό πληκτρολόγιο και μικρό βάρος, διευκολύνοντας την μεταφορά τους.
- Διαθέτουν ως αποθηκευτικά μέσα κυρίως microSD κάρτες μνήμης με μεγάλο χώρο .
- Υποστηρίζουν την αναπαραγωγή αρχείων, βίντεο και λοιπών αρχείων.
- Δέχονται και εκτελούν τηλεφωνικές κλήσεις και βιντεοκλήσεις.
- Παρέχουν συγχρονισμό και αποστολή δεδομένων με δικτυακές συσκευές.
- Έχουν δικό τους λειτουργικό σύστημα και επεξεργαστή ARM επιτρέποντας την ταυτόχρονη εκτέλεση εφαρμογών.

- Παρέχουν δυνατότητα ασύρματης διαδικτυακής σύνδεσης είτε μέσω 3G ή 4G δικτύων είτε μέσω Wi-Fi, παρέχοντας εύκολη περιήγηση και αναζήτηση πληροφοριών, προβολή τυποποιημένων και φορητών ιστοσελίδων, εγκατάσταση νέων εφαρμογών κ.α.
- Δίνουν στον χρήστη την δυνατότητα δημιουργίας, αποστολής και λήψης SMS, MMS και email.
- Παρέχουν την δυνατότητα χρήσης προ εγκατεστημένων εφαρμογών και εγκατάστασης νέων εφαρμογών που διευκολύνουν την εκτέλεση ενεργειών.
- Προστατεύουν τον χρήστη από επιθέσεις ιών και κακόβουλων λογισμικών.

Η επιτυχία των έξυπνων κινητών τηλεφώνων οδήγησε στην μαζική παραγωγή συσκευών με παρόμοια χαρακτηριστικά με αυτά των έξυπνων κινητών τηλεφώνων αλλά με πιο διευρυμένο προσανατολισμό χρήσης. Οι έξυπνες κινητές συσκευές χρησιμοποιούνται συχνότερα για ευέλικτη πρόσβαση σε διαδικτυακές εφαρμογές και σπανιότερα για τηλεφωνική επικοινωνία. Συνήθως διαθέτουν μεγαλύτερο μέγεθος οθόνης, ενώ το μεγαλύτερο μέγεθος τους σε σχέση με τα έξυπνα κινητά τηλέφωνα δίνει την δυνατότητα για την ανάπτυξη περισσοτέρων και ποιοτικότερων πόρων που τους δίνουν την δυνατότητα να εκτελούν απαιτητικές λειτουργίες. Τις περισσότερες φορές χρησιμοποιούνται για ψυχαγωγία, εκπαίδευση, περιπτώσεις όπου χρειάζεται η ασύρματη μετάδοση δεδομένων (Shraim & Crompton, 2015).

2.2 Παγκόσμιες τάσεις στην αγορά κινητών εφαρμογών

Η ταχύτητα ανάπτυξης του κλάδου κινητών εφαρμογών είναι αυξητική και είναι κατανοητό ότι το μέλλον τους ανήκει, με πολλές εταιρείες να επενδύουν σημαντικά ποσά για την ανάπτυξη τέτοιων εφαρμογών.

Ήδη έχουν ωριμάσει τεχνολογίες και μεθοδολογίες για την ανάπτυξη εφαρμογών για κινητές έξυπνες συσκευές για (apptentive, 2015):

- Με νέα έξυπνα εργαλεία για πιο γρήγορη ανάπτυξη.
- Αξιοποίηση του υπολογιστικού νέφους για το συγχρονισμό των δεδομένων μεταξύ των κινητών συσκευών.
- Ασφάλεια των εφαρμογών.
- Προσωποποιημένη εμπειρία πελάτη με περαιτέρω ανάπτυξη υπηρεσιών Beacon και Location based,
- Τεχνολογία για «wearable» συσκευές , όπως είναι τα ρολόγια
- Πληρωμές μέσω M-commerce, M-banking : η Apple και η Google κυκλοφορούν ήδη εφαρμογές οι οποίες αντικαθιστούν τις πιστωτικές κάρτες και χρησιμοποιούνται ως ηλεκτρονικά πορτοφόλια.
- Internet of Things (IoT): διασυνδεσιμότητα των συσκευών του χρήστη με στόχο την ικανοποίησή του.
- Big Data και Apps Analytics: συλλογή των δεδομένων που προέρχονται από τις εφαρμογές που χρησιμοποιεί ο χρήστης για περαιτέρω αξιοποίηση του.
- Mobile Gaming
- Mobile Marketing

Η σύγχρονη έρευνα στοχεύει επίσης (Hindi, 2020):

- Στην προσαρμογή των εφαρμογών για λειτουργία σε συσκευές με ιδιαίτερα περιορισμένους πόρους λόγω μικρών φυσικών διαστάσεων.
- Υιοθέτηση των δυνατοτήτων που προσφέρει η τεχνολογία 5G των ασύρματων επικοινωνιών.
- Εξυπηρέτηση της κινητότητας (mobility) στο μέγιστο εφικτό βαθμό
- Εκμετάλλευση της τεχνολογίας Beacon μέσω της οποίας συλλέγονται δεδομένα σχετικά με την γεωγραφική θέση των κινητών συσκευών.
- Χρήση των έξυπνων κινητών εφαρμογών για λειτουργίες που σχετίζονται με την τεχνητή νοημοσύνη και την μηχανική μάθηση.

- Χρήση των έξυπνων κινητών συσκευών για εφαρμογές επαυξημένης πραγματικότητας.
- Αναβάθμιση των μεθόδων επικοινωνίας των χρηστών
- Χρήση των έξυπνων κινητών συσκευών για οικονομική διαχείριση.

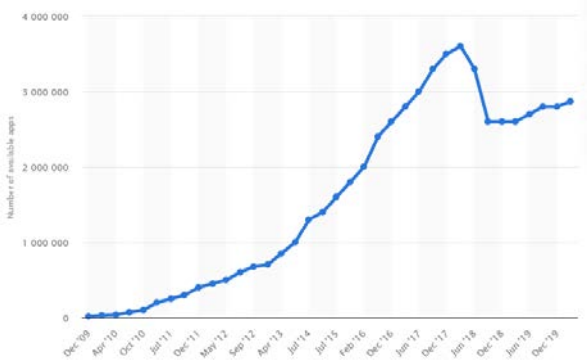
Φαίνεται ότι ο κλάδος των κινητών εφαρμογών θα παίξει ιδιαίτερα σημαντικό ρόλο στο εγγύς μέλλον και λόγω αυτής της ανάπτυξης θα πρέπει να δημιουργηθούν επιμέρους κλάδοι, με εξειδικευμένες εταιρείες. Είναι γεγονός ότι οι μικρομεσαίες εταιρείες δεν θα μπορούν να εξειδικευθούν σε όλους τους συναφείς κλάδους, λόγω έλλειψης πόρων.

2.3 Βαθμός υιοθέτησης των κινητών εφαρμογών

Η αυξανόμενη πολυπλοκότητα των κινητών συσκευών που κατακλύζουν την αγορά και οι απαιτήσεις των χρηστών ωθούν την ανταγωνιστικότητα στα χαρακτηριστικά των έξυπνων κινητών (smartphones). Η συνεχώς εξελισσόμενη αγορά κινητών εφαρμογών και ο αντίστοιχος ανταγωνισμός στα ασύρματα δίκτυα κάνουν τις κινητές εφαρμογές να είναι ένας ελκυστικός τομέας ανάπτυξης, με τον ανταγωνισμό να αυξάνεται συνεχώς. Οι προγραμματιστές αναλώνουν αρκετό χρόνο στην ανάπτυξη εφαρμογών και στην αντιμετώπιση πολλών προκλήσεων, ώστε να προσφέρουν επιπλέον δυνατότητες στους χρήστες, εργονομικό σχεδιασμό και διαφοροποίηση ανάμεσα σε παρόμοιες εφαρμογές. Όμως, η επιτυχία της ανάπτυξης μιας εφαρμογής εξαρτάται από την σχεδιασμένη σωστά στρατηγική και τον σωστό προγραμματισμό (Flora, 2014).

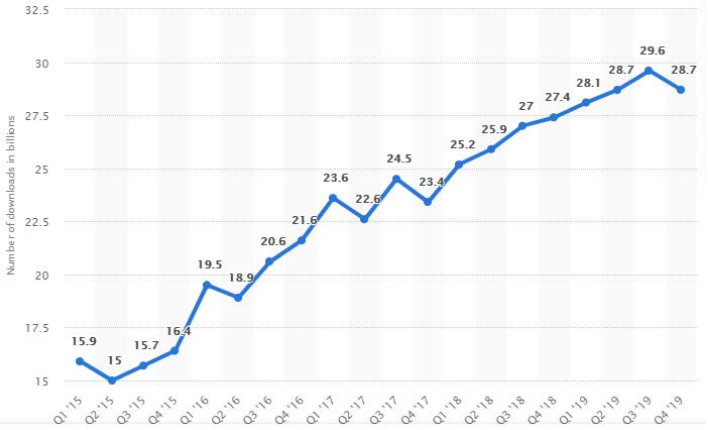
Η συνεχής αύξηση των smartphones και των κινητών εφαρμογών, οδήγησαν στην δημιουργία μιας νέας οικονομίας που ονομάζεται Οικονομία Εφαρμογών, η οποία ουσιαστικά τροφοδοτείται από τις διαφημίσεις και τις πωλήσεις άλλων εφαρμογών, μέσω των δωρεάν εφαρμογών. Αυτή η Οικονομία έχει ολοένα και αυξανόμενη τάση.

Στατιστικά δεδομένα καταδεικνύουν ότι η εν λόγω αγορά παρουσιάζει ραγδαία ανάπτυξη. Στο Google Play store οι διαθέσιμες εφαρμογές έφτασαν τα 2.80 εκατομμύρια τον Δεκέμβριο του 2019 (Statista, 2020) και τα 2.87 εκατομμύρια το Μάρτιο του 2020 (Statista, 2020), ενώ τον Μάιο του 2015 ο αριθμός ήταν στο 1.5 εκατομμύριο.



Διάγραμμα 1. Διαθέσιμες εφαρμογές στο Google App Store.

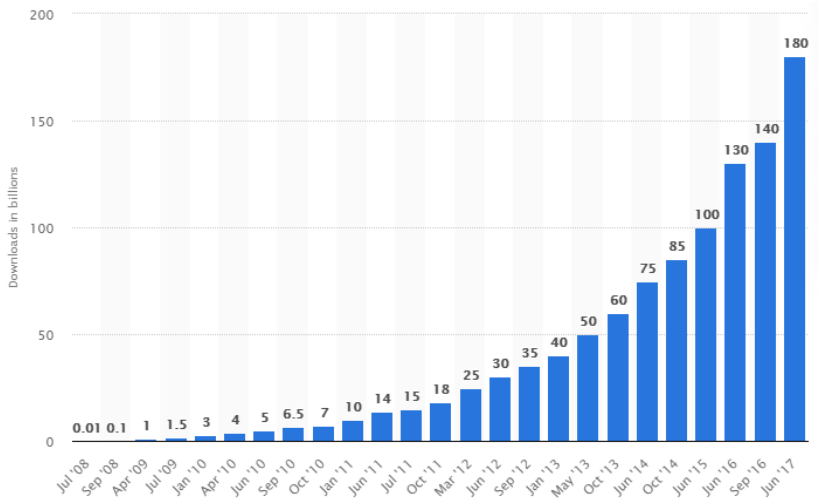
Η απήχηση των εφαρμογών στο κοινό αποδεικνύεται και από το πλήθος εκείνων που έχουν ληφθεί από χρήστες. Οι σχετικοί δείκτες δείχνουν σταθερή άνοδο τα τελευταία χρόνια η οποία δείχνει πλέον να φθάνει σε κορεσμό. (Statista, 2020):



Διάγραμμα 2. Απήχηση εφαρμογών στο κοινό.

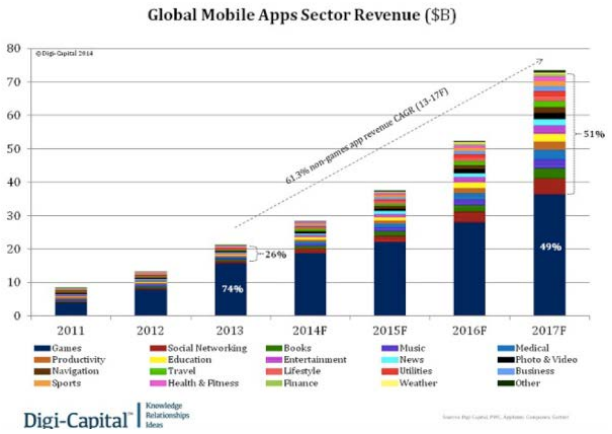
Ο αριθμός των εγκατεστημένων εφαρμογών το 2016 ανέρχονταν από το Google Play στα 55 δισεκατομμύρια εφαρμογές, ενώ το 2019 ο αριθμός έφθασε τα 84,3 δισεκατομμύρια. Με βάση τα εν λόγω στοιχεία υποδηλώνεται η εκθετική αύξηση

της δημοτικότητας των εφαρμογών. Κάτι το οποίο συμβαίνει αντίστοιχα και στο Apple Appl Store με παράδειγμα το έτη 2008 έως 2017 (Statista, 2020):



Διάγραμμα 3. Αριθμός εγκατεστημένων εφαρμογών.

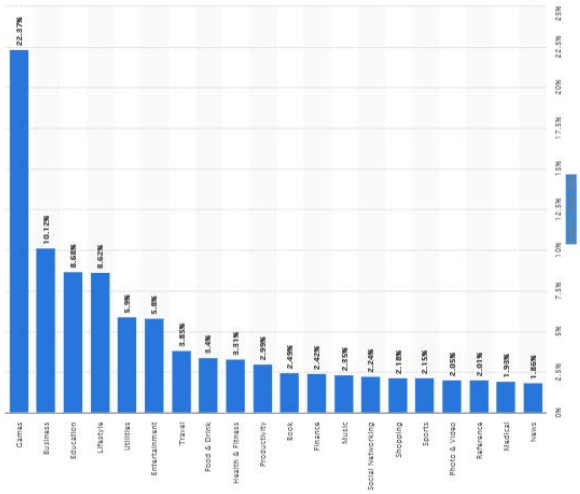
Η ανασκόπηση μέσω των στατιστικών στοιχείων επιτρέπει στον ερευνητή να προσδώσει στην Οικονομία Εφαρμογών (App Economy) τον τίτλο ενός κερδοφόρου κλάδου. Καθώς αλληλένδετα μπορεί να θεωρηθεί ότι ο κλάδος αυτό απασχολεί αρκετό δυναμικό στη σχεδίαση και προώθηση των εφαρμογών και παράλληλα εξασφαλίζει αρκετά έσοδα από κάθε κατηγορία εφαρμογών (Zinevych, 2014) (Statista, 2020).



Διάγραμμα 4. Μέγεθος της αγοράς των εφαρμογών.

Τα παιχνίδια αποτελούν την πλέον επικερδή κατηγορία εφαρμογών, καθώς διαφημίσεις ή αγορές εντός των παιχνιδιών μπορούν να αποφέρουν επιπλέον

κέρδος. Ακολουθούν οι εφαρμογές κοινωνικής δικτύωσης, ενώ οι υπόλοιπες κατηγορίες καταλαμβάνουν μικρότερα ποσοστά. Κάποιες εφαρμογές μοιράζονται δωρεάν από τους δημιουργούς τους, ενώ κάποιες άλλες έναντι ποσού. Όμως η εξασφάλιση των εσόδων δεν αφορά μόνο τη διάθεση της εφαρμογής επί πληρωμή, αλλά όπως αναφέρθηκε πρωτίστως οι διαφημίσεις ή αγορές εντός των παιχνιδιών μπορούν να αποτελέσουν πηγή εσόδων (statista, 2020).



Διάγραμμα 5. Μέγεθος της αγοράς των παιχνιδιών.

Οι εφαρμογές για έξυπνες κινητές συσκευές χρησιμοποιούνται εξίσου από άνδρες και γυναίκες. Οι χρήστες σε μεγαλύτερο ποσοστό ηλικιακά ανήκουν στην κατηγορία 25 έως 34 ετών (30%). Κατοικούν στα προάστια στο μεγαλύτερο ποσοστό τους (52%). Και η οικογενειακή κατάσταση που υπερτερεί είναι οι παντρεμένοι (47%) (Zinevych, 2014). Βέβαια το κοινωνικοοικονομικό- βιοτικό επίπεδο και άλλα κοινωνικά χαρακτηριστικά ανά περιοχή έρευνας σαφώς θα μπορούσαν να φέρουν διαφορετικά στατιστικά αποτελέσματα.

2.4 Τύποι εφαρμογών

Οι προγραμματιστές επιλέγοντας να αναπτύξουν μια εφαρμογή χρειάζονται παράλληλα να επιλέξουν διάφορες τεχνολογίες εφαρμογών οι οποίες χωρίζονται σε native και web-based . Αναλόγως ανάπτυξης εφαρμογής, επιλέγεται η κατάλληλη τεχνολογία που πρέπει να χρησιμοποιηθεί για να εξυπηρετήσει τον τιθέμενο στόχο. Παρόλα αυτά , επιλέγοντας την υβριδική ανάπτυξη , δηλαδή

συνδυασμός και των δύο τεχνολογιών, θεωρείται πλεονέκτημα γιατί προσφέρονται έτσι περισσότερες δυνατότητες και θα αναλυθεί παρακάτω.

Οι διαδικτυακές εφαρμογές χρησιμοποιούν γλώσσες προγραμματισμού CSS3, Javascript και HTML5 οι οποίες βασίζονται σε ιστοσελίδες για κινητές συσκευές. Αυτές είναι προσβάσιμες με χρήση περιηγητή από την κινητή συσκευή. Μια web-based εφαρμογή , επειδή χρησιμοποιεί τεχνολογία τύπου Javascript , κίνηση και δημιουργεί καλή διεπαφή με τον χρήστη, τέτοιου είδους εφαρμογές είναι συμβατές με οποιοδήποτε λειτουργικό, έχοντας ως μοναδικό προαπαιτούμενο τον περιηγητή. Το μόνο μειονέκτημα είναι ότι αυτού του είδους οι εφαρμογές δεν διατίθενται στα επίσημα App Stores, άρα οι πηγές εσόδων των δημιουργών βασίζεται στις διαφημίσεις της ιστοσελίδας ή στην συνδρομή (Hubbard, 2015).

Αντίθετα, οι native εφαρμογές , απευθύνονται σε συγκεκριμένη πλατφόρμα , παρέχοντας μεγαλύτερη λειτουργικότητα στους χρήστες . Κάθε τύπος πλατφόρμας χρησιμοποιεί την δική της γλώσσα, όπως για το IOS η Objective-C, για το Android η Java . Συμπληρωματικά , οι ενσωματωμένες εφαρμογές έχουν καλύτερη και πλήρη πρόσβαση στην συσκευή και περισσότερες δυνατότητες όπως είναι το ημερολόγιο, η κάμερα ή γενικά οι εφαρμογές των πολυμέσων. Οι native εφαρμογές έχουν ως πηγή εσόδων τις διαφημίσεις ή αγορά της εφαρμογής μέσω των καναλιών διανομής της κάθε πλατφόρμας (παράδειγμα Apple Store ή google play) (Kristijan, 2015).

Μία μέση λύση που ταιριάζει σε πολλές περιπτώσεις είναι οι υβριδικές εφαρμογές. Πρόκειται για εφαρμογές που χρησιμοποιούν τις ίδιες γλώσσες προγραμματισμού. Είναι web-based και λόγω αυτού έχουν τα πλεονεκτήματα και των δύο τύπων. Ενδεικτική υβριδική είναι το Titanium για HTML, Javascript και CSS δίνοντας ευελιξία για περισσότερες δυνατότητες στον προγραμματιστή. (Amatya, 2013).

2.5 Κύρια λειτουργικά συστήματα

Η αυξανόμενη χρήση των κινητών συσκευών, δημιούργησε την ανάγκη για ανάπτυξη λειτουργικών λογισμικών η οποία να καλύπτει διαφόρων ειδών συσκευές. Πλέον ο προγραμματιστής έχει να επιλέξει ποια πλατφόρμα θα χρησιμοποιήσει για την ανάπτυξη της εφαρμογής του και παρακάτω θα αναλυθούν οι πιο διαδεδομένες (Joseph & K, 2013).

2.5.1 Android

Το Android λειτουργικό λογισμικό είναι ανοικτού κώδικα , βασιζόμενο σε έκδοση Linux και έχει δημιουργηθεί για την Google πλατφόρμα. Διατίθεται δωρεάν και οι εφαρμογές του Android μπορούν να γραφτούν χρησιμοποιώντας άλλα λειτουργικά συστήματα όπως Mac OS, Linux και Windows. Σαν Linux προϊόν , το Android λειτουργικό λογισμικό, διαθέτει το χαμηλό στρώμα που περιλαμβάνει μνήμη, δίκτυο, ασφάλεια και οδηγούς και στο ανώτερο στρώμα διαθέτει τις βιβλιοθήκες για τα γραφικά , τα πολυμέσα και την βάση δεδομένων. Ο περιηγητής είναι ενσωματωμένος στο σύστημα, παρέχοντας γραμμή εργαλείων και μπάρα διευθύνσεων. Στο Google App Store υπάρχουν διαθέσιμοι και άλλοι περιηγητές για εγκατάσταση όπως είναι ο Mozilla.

2.5.2 iOS

Το iOS λειτουργικό λογισμικό δίνει έμφαση στην εμπειρία χρήστη μέσω της τεχνολογίας πολύ-αφής, δηλαδή ο χρήστης μπορεί να χρησιμοποιήσει περισσότερα από ένα δάκτυλα για διαφορετικές λειτουργίες. Ο κώδικας του iOS , σε σχέση με το Android, υπερτερεί αφετέρου λόγω περιορισμένων αναγκών σε μνήμη RAM , αφετέρου επειδή στις βασικές του λειτουργίες, ενσωματώνεται επιταχυνσιόμετρο, το οποίο είναι ικανό να εντοπίσει την θέση της συσκευής και ενώ αυτή κινείται να ελέγχει τις λειτουργίες του.

Και στο iOS , όπως στο Android υπάρχουν στρώματα, στα οποία μπορεί ο προγραμματιστής να προγραμματίσει:

- Core OS είναι το χαμηλότερο επίπεδο για το λειτουργικό λογισμικό
- Core Services που είναι βιβλιοθήκες για τις εφαρμογές και για την βάση δεδομένων
- Media που είναι βιβλιοθήκη που χρησιμοποιείται για τα γραφικά και για τα οπτικοακουστικά
- Cocoa Touch που είναι η βιβλιοθήκη που είναι υπεύθυνη για την διεπαφή του χρήστη και την οθόνη πολύ-αφής

Η iOS πλατφόρμα είναι πολύ δημοφιλής για τους προγραμματιστές , διαθέτοντας μεγάλη ποικιλία εφαρμογών για τις κινητές συσκευές.

Ο περιηγητής Safari είναι ενσωματωμένος στο σύστημα με σημαντικότερο πλεονέκτημα την ταχύτητα φόρτωσης των σελίδων που καλεί ο χρήστης. Στο application Store , υπάρχουν και άλλοι διαθέσιμοι περιηγητές για εγκατάσταση, όπως είναι ο Mozilla.

2.5.3 Windows Phone

Το Microsoft Windows λειτουργικό λογισμικό, είναι διαφορετικό από τα υπόλοιπα δύο που αναφέρθηκαν παραπάνω, λόγω του ότι για την δημιουργία του χρησιμοποιήθηκε σε μια νέα γλώσσα. Η αρχική οθόνη είναι μια λίστα από εικονίδια τα οποία δεν χωρίζονται σε σελίδες όπως στα υπόλοιπα δύο, αλλά η λίστα είναι κυλιόμενη προς τα κάτω. Κάθε εικονίδιο της λίστας, παρέχει πληροφορίες για την συγκεκριμένη εφαρμογή που ζητείται.

Τα στρώματα που μπορεί να αναφερθεί ο προγραμματιστής είναι:

- Το στρώμα που είναι ο πυρήνας των windows, του δικτύου και η αποθήκευση των δεδομένων
- Το στρώμα που είναι υπεύθυνο για τις εφαρμογές
- Το στρώμα διεπαφής του χρήστη
- Το στρώμα για το περιβάλλον εκτέλεσης των εφαρμογών

Ο ενσωματωμένος περιηγητής είναι ο γνωστός Internet Explorer με σημαντική βελτιστοποίηση για τις κινητές συσκευές. Στο Microsoft Store υπάρχουν και άλλοι διαθέσιμοι περιηγητές , όπως ο Mozilla.

Να σημειωθεί ότι κατά την περίοδο συγγραφής αυτής της Μεταπτυχιακής διατριβής, το Windows λειτουργικό για κινητές συσκευές που έγινε η αναφορά, αποσύρθηκε.

2.6 Δημοσιοποίηση εφαρμογής σε Google App Store

Για να δημοσιευθεί μια εφαρμογή στο Google App Store, ο προγραμματιστής θα πρέπει να ακολουθήσει κάποια ενδεδειγμένα βήματα που θα του υποδειχθούν από το app store. Αποδεχόμενος τους όρους ότι η εφαρμογή τους πληροί, τότε την υποβάλλει στην πλατφόρμα. Η Google απαιτεί το ποσό των 25 δολαρίων για μια φορά και η Apple το ετήσιο ποσό των 99 δολαρίων. Η εγκυρότητα της εφαρμογής για να ενταχθεί στην κάθε πλατφόρμα, στην Apple είναι πιο αυστηρή με αποτέλεσμα η διαδικασία έγκρισης να καθυστερεί για εβδομάδες και πολλές φορές να απορρίπτεται. Ο αντίστοιχος έλεγχος της Google είναι αυτοματοποιημένος με έλεγχο για ιούς και την δημοσίευση να καθυστερεί μερικές ώρες. Από την στιγμή που η εφαρμογή θα δημοσιευθεί , τότε ο προγραμματιστής έχει την δυνατότητα της αναβάθμισής της. Και εδώ η διαδικασία της Google είναι άμεση, ενώ στην Apple γίνεται επισκόπηση και κατόπιν πραγματοποιείται. Ο χρήστης της κινητής συσκευής, μπορεί οποτεδήποτε θελήσει να ελέγξει για τις διαθέσιμες ενημερώσεις των εφαρμογών του (Google, 2020) .

2.7 Προϋποθέσεις ανάπτυξης εφαρμογής

Οι προϋποθέσεις για την ανάπτυξη μιας εφαρμογής έως την δημοσίευσή της προς τους χρήστες είναι οι εξής:

- Ανάλυση της αγοράς ώστε να στοχεύσει το κοινό που θα απευθυνθεί η εφαρμογή και κατάλληλη χρηματοδότηση
- Συμβατότητα: Οι προγραμματιστές πρέπει να σχεδιάζουν και να αναπτύσσουν τις εφαρμογές τους με τέτοιο τρόπο ώστε να τρέχουν

αφενός σε πολλαπλές συσκευές και αφετέρου να είναι συμβατές με τις πιο γνωστές πλατφόρμες.

- Πολυπλοκότητα του υλικού: Οι ιδιαιτερότητες του υλικού των συσκευών διαφέρουν μεταξύ τους όσον αφορά τα χαρακτηριστικά τούς, δηλαδή την μνήμη, την ταχύτητα, την επεξεργασία γραφικών, ενώ οι διαθέσιμοι πόροι είναι περιορισμένοι.
- Εμπειρία χρήστη: οι εφαρμογές πρέπει να είναι κατάλληλα προσαρμοσμένες για κινητές συσκευές, ώστε να την προσφέρουν
- Δεδομένα : κατάλληλος προγραμματισμός ώστε σε περίπτωση αστοχίας διασύνδεσης , κατά την επανασύνδεσή του θα γίνει συγχρονισμός ώστε να ενημερωθούν τα δεδομένα.
- Ασφάλεια και έλεγχός της: βασική ευθύνη του προγραμματιστή να παρέχει την μέγιστη ασφάλεια. Σοβαρά προβλήματα εγείρονται με την πρόσβαση, μέσω κινητών συσκευών από μη εξουσιοδοτημένους χρήστες.
- Λειτουργικά συστήματα: Συμμόρφωση στις απαιτήσεις των λειτουργικών συστημάτων.

2.8 Ασφάλεια

Ένας παράγοντας που λαμβάνεται υπ' όψη για την θετική αξιολόγηση των εφαρμογών για κινητές συσκευές, είναι το επίπεδο ασφαλείας που παρέχουν για τα δεδομένα που διαχειρίζονται. Η ολοένα εξελισσόμενη ασύρματη πρόσβαση και η συνεχής συνδεσιμότητα των κινητών συσκευών , αυξάνει τον κίνδυνο για κακόβουλες πράξεις επιθέσεων και κλοπών από μη εξουσιοδοτημένους χρήστες. Ο προγραμματιστής εφαρμογών θα πρέπει , εκτός από την ασφάλεια που προσφέρει η πλατφόρμα που θα χρησιμοποιήσει, να παρέχει και ενσωματωμένες λειτουργίες κρυπτογράφησης στην εφαρμογή του, για την προστασία των δεδομένων του χρήστη .

Όπως αναφέρθηκε και παραπάνω , η συνεχής συνδεσιμότητα των κινητών συσκευών με υπηρεσίες cloud, τραπεζικές συναλλαγές, πληρωμές και άλλα, αν δεν πληρούν τις απαιτούμενες προδιαγραφές ασφάλειας, γίνονται εύκολος στόχος και τα καθιστά ευάλωτα σε απειλές.

Υπάρχουν διάφοροι τύποι κακόβουλων επιθέσεων στις έξυπνες κινητές συσκευές. Από τους πλέον γνωστούς είναι :

- οι ιοί, οι οποίοι, όταν ο χρήστης κατεβάσει κάποια μολυσμένη κακόβουλη εφαρμογή και κατά την ενεργοποίησή της, ενσωματώνεται στον κώδικά της και υποκλέπτει στοιχεία του χρήστη, όπως κωδικοί πρόσβασης και άλλα.
- spyware, με κύρια λειτουργία την συλλογή και την μεταφορά των δεδομένων όπως είναι η αλληλογραφία, το μήνυμα, οι φωτογραφίες ή τα στοιχεία των υπηρεσιών τοποθεσίας, σε εξωτερικές πηγές.
- botnet, όπου πρόκειται για στρατιά από υπολογιστές, μολυσμένοι όλοι με το ίδιο κακόβουλο λογισμικό όπου συνεργαζόμενα, επιτίθονται για να υποκλέψουν προσωπικές πληροφορίες και πολλά άλλα. Ο τρόπος που μπορεί να διανεμηθεί στην κινητή συσκευή του χρήστη είναι μέσω εφαρμογών , εισερχόμενης αλληλογραφίας με επισυναπτόμενα μολυσμένα αρχεία ή μολυσμένων ιστοσελίδων
    - phishing, όπου ο κακόβουλος υποδύεται μια αξιόπιστη οντότητα και εκμεταλλευόμενος την άγνοια του χρήστη, προσπαθεί να εκμαιεύσει προσωπικά του δεδομένα και κωδικούς (Kaspersky, 2020). Ο τρόπος επίθεσης και σε αυτήν την περίπτωση είναι κυρίως μέσω ηλεκτρονικής αλληλογραφίας ή άμεσου μηνύματος κατά την διάρκεια της πλοήγησης του χρήστη, όπου τον παραπέμπουν σε σύνδεσμο εμφανώς αξιόπιστο, αλλά τελικά οδηγούμενο σε διαφορετική και κακόβουλη ιστοσελίδα.

Πέραν όμως των κινδύνων ασφαλείας, υπάρχουν και κίνδυνοι που άπτονται της ιδιωτικότητας των χρηστών. Τέτοια ζητήματα καλύπτονται στα επόμενα κεφάλαια της παρούσας διατριβής.

Κεφάλαιο 3
Προσωπικά Δεδομένα και Εφαρμογές

3.1 Περιγραφή των προσωπικών δεδομένων

Ένας απλός ορισμός για την έννοια των δεδομένων προσωπικού χαρακτήρα είναι ότι αφορούν πληροφορίες για ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Επίσης όταν άλλου είδους πληροφορίες είναι ικανές συνδυαζόμενες, έμμεσα να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, τότε χαρακτηρίζονται και αυτές προσωπικά δεδομένα. Δεδομένα προσωπικού χαρακτήρα που αν και έχουν καταστεί ανώνυμα, κρυπτογραφηθεί ή έχουν αντιστοιχισθεί σε ψευδώνυμα, μπορούν να χρησιμοποιηθούν με κάποιον τρόπο για την ταυτοποίηση του ατόμου, περιγράφονται και αυτά ως προσωπικού χαρακτήρα. Ο χαρακτηρισμός των δεδομένων ως προσωπικού χαρακτήρα είναι ανεξάρτητος από το μέσο αποθήκευσης ή τον τρόπο επεξεργασίας τους. Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. (Ευρωπαϊκή Επιτροπή, 2020).

Χαρακτηριστικά παραδείγματα προσωπικών δεδομένων είναι:

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση που μπορεί να φανερώνει προσωπικά δεδομένα
- αναγνωριστικός αριθμός κάρτας οποιουδήποτε είδους

- δεδομένα τοποθεσίας θέσης ή κατοικίας ή εργασία ή γενικότερα χώρου που σχετίζεται με το άτομο
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να προσδιορίζουν μοναδικά ένα άτομο.

Για τα δεδομένα προσωπικού χαρακτήρα, η επεξεργασία αναφέρεται σε πράξεις που πραγματοποιούνται, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα και μπορεί να περιλαμβάνουν:

- Συλλογή: Ενέργειες που αφορούν την συγκέντρωση τους από διάφορες πηγές σε κάποιο αποθετήριο.
- Καταχώριση: Την καταγραφή τους σε κάποιο μέσο (συνήθως χειροκίνητα αλλά και αυτοματοποιημένα)
- Οργάνωση: Τον σημασιολογικό συσχετισμό τους
- Διάρθρωση: Την οργάνωση τους σε ιεραρχικές σχέσεις
- Αποθήκευση: Την με οποιοδήποτε τρόπο διατήρηση τους.
- Προσαρμογή: Την μεταμόρφωσή τους ώστε να είναι δυνατή η εκμετάλλευσή τους.
- Μεταβολή: Η αλλαγή της εμφάνισης και της σημασίας τους.
- Ανάκτηση: Η λήψη από την πηγή τους.
- Αναζήτηση πληροφοριών: Η χρησιμοποίηση τους για την δημιουργία πληροφοριών.
- Χρήση: Η με οποιοδήποτε χρήση τους για την επίτευξη οποιοδήποτε σκοπού.
- Κοινολόγηση με διαβίβαση: Η γνωστοποίηση του περιεχομένου τους στοχευμένα.
- Διάδοση ή κάθε άλλη μορφή διάθεσης: Η γνωστοποίηση τους σε ευρύ κοινό
- Συσχέτιση ή συνδυασμό: Η αναζήτηση συσχετίσεων ή δημιουργία συνδυασμών με σκοπό την παραγωγή συμπερασμάτων.
- Περιορισμό: Αποτροπή της πρόσβασης σε αυτά.

- Διαγραφή ή καταστροφή τους

Μερικά παραδείγματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι:

- Διαχείριση προσωπικού και μισθοδοσία·
- Προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών
- Αποστολή στοχευμένων σε συγκεκριμένο κοινό, διαφημιστικών ηλεκτρονικών μηνυμάτων
- Καταστροφή διά τεμαχισμού εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα·
- Δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο (Ευρωπαϊκή Επιτροπή, 2020)

3.2 Δεδομένα Ενδιαφέροντος

Οι σύγχρονες έξυπνες κινητές συσκευές μπορούν και διαχειρίζονται πολλά και ποικίλα προσωπικά δεδομένα. Αυτά που προσκαλούν περισσότερο το ενδιαφέρον τρίτων για πρόσβαση είναι τα εξής:

- Τοποθεσία: Τα περισσότερα σύγχρονα smartphones περιέχουν υλικό GPS, το οποίο μπορεί να εντοπίσει με ακρίβεια την τοποθεσία του χειριστή τους. Επιπροσθέτως η ευρεία περιοχή του σημείου στάσεως του μπορεί να εκτιμηθεί μέσω της σύνδεσης της συσκευής σε κοντινά δίκτυα WiFi ή κεραίες κινητής τηλεφωνίας. Ο κάτοχος τέτοιου είδους πληροφοριών μπορεί να εκτιμήσει με αρκετά μεγάλη ασφάλεια τις κινήσεις και τις συνήθειες του κατόχου της κινητής συσκευή και να τις εντάξει σε ένα πλαίσιο σκιαγράφησης του προφίλ του.
- Χρήση εφαρμογών: Το είδος των εφαρμογών καθώς και το μοτίβο χρήσης τους από τον κάτοχο της κινητής συσκευής μπορεί να παρέχουν σημαντικές πληροφορίες για την ανάπτυξη του προφίλ του. Οι εγκατεστημένες εφαρμογές αντανακλούν στα ενδιαφέροντά του

ενώ το πως τις χρησιμοποιεί καταδεικνύει την σημασία που έχουν για αυτόν αυτά τα ενδιαφέροντα.

- Πληροφορίες συσκευής: Οι έξυπνες κινητές συσκευές αποκαλύπτουν πληροφορίες που αφορούν τις προδιαγραφές και τις δυνατότητες τους. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της οικονομικής κατάσταση του κατόχου της συσκευής.
- Επικοινωνία: Από τα δεδομένα των συνδιαλλαγών ή των μηνυμάτων που ανταλλάσσει ο χρήστης της έξυπνης κινητής συσκευής, είναι εφικτό να δημιουργηθούν ασφαλείς εκτιμήσεις για τον κοινωνικό περίγυρο του χρήστη. Επιπλέον έχουν αναπτυχθεί μεθοδολογίες και τεχνικές που επιτρέπουν την ανάλυση των συναισθημάτων των εμπλεκομένων σε επικοινωνίες μέσα από το περιεχόμενο αυτών. Η διάρκεια των τηλεφωνικών κλήσεων μπορεί να οδηγήσει σε συμπεράσματα σχετικά με την κοινωνικότητα του χρήστη, ενώ το πλήθος των εισερχομένων κλήσεων μπορεί να είναι δηλωτικό για το πόσο δημοφιλής είναι.
- Χώρος Αποθήκευσης: Στον χώρο αποθήκευσης των έξυπνων κινητών συσκευών αποθηκεύονται αρχεία που πολλές φορές περιλαμβάνουν κρίσιμες πληροφορίες για τον χρήστη του. Προφανώς η πρόσβαση σε τέτοια αρχεία είναι πολύ σημαντική. Ωστόσο περισσότερο αθώες πληροφορίες που αφορούν το μέγεθος του δεσμευμένου από αρχεία χώρου αλλά και το είδος των αποθηκευμένων αρχείων μπορεί να παράξει πληροφορίες σχετικές με τα ενδιαφέροντα του χρήστη.
- Μικρόφωνο. Η εξαπάτηση των αντιπάλων έχει αποδειχθεί ειδικά με την κατάχρηση πρόσβασης στο μικρόφωνο της συσκευής. Δεν είναι πλέον απαραίτητο για έναν αντίπαλο να παρακολουθεί τις συνομιλίες ενός θύματος (αν και μπορεί να το κάνει ακόμα). Πράγματι, οι εφαρμογές είναι γνωστό ότι παρακολουθούν χρήστες σε όλες τις συσκευές που χρησιμοποιούν υπερήχους (Taylor, Beresford, & Martinovic, 2017).

3.3 Χρήση των Προσωπικών Δεδομένων

3.3.1 Πολίτες και Προσωπικά Δεδομένα

Στην Ευρώπη η χρήση του διαδικτύου είναι πολύ διαδεδομένη καθώς το 75% του πληθυσμού συνδέεται καθημερινά στο διαδίκτυο. Στις διάφορες χώρες το ποσοστό αυτό κυμαίνεται από περίπου 50 έως 97%. Στην Ελλάδα το 67% περίπου του πληθυσμού συνδέεται καθημερινά στο διαδίκτυο (Commission, Special Eurobarometer 487a, 2019). Παράλληλα τα στατιστικά στοιχεία της προσβασιμότητας στις διαδικτυακές εφαρμογές δείχνει μία τάση μικρής αύξησης των χρηστών του διαδικτύου στην Ευρώπη. Η χρήση των διαδικτυακών εφαρμογών είναι πιο διαδεδομένη στους ανθρώπους μικρότερης ηλικίας και στα αστικά κέντρα. Επίσης ένα από τα σημαντικότερα κίνητρα για χρήση των διαδικτυακών εφαρμογών αποτελούν οι εκπαιδευτικές ανάγκες. Το 80% περίπου των καθημερινών χρηστών του διαδικτύου έχουν υπ' όψη τους (τουλάχιστον ως προς τις βασικές του έννοιες) τον Γενικό Κανονισμό Προστασίας Δεδομένων (General Data Protection Regulation – GDPR).

Οι περισσότεροι άνθρωποι που χρησιμοποιούν τις διαδικτυακές εφαρμογές καθημερινά, συνδέονται σε εφαρμογές κοινωνικής δικτύωσης με τάση όσο περνούν τα χρόνια να αυξάνονται οι χρήστες τους. Οι συνεπείς χρήστες των κοινωνικών δικτύων δείχνουν στην συντριπτική τους πλειοψηφία και προτίμηση στις εφαρμογές ηλεκτρονικού εμπορίου. Ωστόσο, αν και το 75% των Ευρωπαίων έχει παραγγείλει αγαθά, τουλάχιστον μία φορά χρησιμοποιώντας κάποια διαδικτυακή εφαρμογή, μόλις το 25% περίπου, το κάνει με σχετικά μεγάλη συχνότητα χωρίς να φαίνεται να υπάρχουν αυξητικές τάσεις από το 2015 και μετά. Από αυτούς που κατέχουν την έννοια του GDPR το 93% είναι δυνητικοί χρήστες διαδικτυακών εφαρμογών ηλεκτρονικού εμπορίου.

Σε Πανευρωπαϊκό επίπεδο, ένας στους τρεις έχει ακούσει για τον GDPR αλλά μόνο οι μισοί από αυτούς γνωρίζουν τι ακριβώς είναι. Το ανησυχητικό στοιχείο

είναι ότι ένας στους τρεις Ευρωπαίους δεν γνωρίζει τι είναι. Οι νέοι άνθρωποι, εκείνοι που η εργασία τους αναγκάζει να χειρίζονται συχνά διαδικτυακές εφαρμογές, όπως επίσης και οι καθημερινοί χρήστες του διαδικτύου, είναι πιθανότερο να είναι ευαισθητοποιημένοι ως προς το GDPR. Πιο συγκεκριμένα, ως προς τα θέματα που χειρίζεται ο GDPR, ο βαθμός ενημέρωσης των Ευρωπαίων έχει ως εξής (Commission, Special Eurobarometer 487a, 2019) :

- Το 65% έχουν ακούσει για το δικαίωμα πρόσβασης στα δεδομένα τους
- Το 61% έχουν ακούσει για το δικαίωμα διόρθωσης των δεδομένων τους εάν είναι λάθος.
- Το 59% από τους ερωτηθέντες έχουν ακούσει για το δικαίωμα να αντιταχθούν στη λήψη άμεσου μάρκετινγκ
- Το 57% γνωρίζει για το δικαίωμα διαγραφής των δεδομένων τους
- Το 50% γνωρίζει τα περί του δικαιώματος μετακίνησης των δεδομένων τους από έναν πάροχο στον άλλο.
- Το 41% έχουν ακούσει για το δικαίωμα να έχουν λόγο όταν μεταβάλλονται οι τρόποι χειρισμού των δεδομένων τους.

Ως προς το κατά πόσο οι Ευρωπαίοι χρήστες έκαναν χρήση των δικαιωμάτων που απορρέουν από τον GDPR:

- Το 10% έχουν ασκήσει κάποιο ή κάποιο από τα δικαιώματα αυτά.
- Το 24% άσκησε το δικαίωμα να αντιταχτεί στο άμεσο μάρκετινγκ
- Το 18% άσκησε το δικαίωμα να έχει πρόσβαση στα δεδομένα του
- Το 16% άσκησε το δικαίωμα του να διορθώσει τα δεδομένα του αν είναι εσφαλμένα
- Το 13% άσκησε το δικαίωμα του να μεταφέρει τα δεδομένα του από έναν πάροχο σε άλλον.
- Το 8% άσκησε το δικαίωμα τους να έχουν άποψη όταν λαμβάνονται αυτοματοποιημένα αποφάσεις.

Περίπου το 60% των Ευρωπαίων γνωρίζει ότι η εφαρμογή των κανόνων του GDPR ελέγχονται από δημόσια αρχή. Παράλληλα στην πλειοψηφία τους

αναγνωρίζουν ότι όταν παρέχουν τα προσωπικά τους, δεν έχουν πλέον τον πλήρη έλεγχο της χρήσης τους. Η απώλεια αυτή του ελέγχου τους απασχολεί έντονα. Μόλις οι μισοί θεωρούν ότι όταν παρέχουν τα προσωπικά τους δεδομένα είναι ενημερωμένοι για τον τρόπο με τον οποίο θα χρησιμοποιηθούν. Αυτό κατά μεγάλο ποσοστό οφείλεται στο γεγονός ότι μόνο το 60% διαβάζει τις σχετικές ενημερώσεις πριν την χρήση των εφαρμογών. Οι λόγοι για τους οποίους οι Ευρωπαίοι δεν μπαίνουν στην διαδικασία να διαβάσουν τις ενημερώσεις των εφαρμογών περί ιδιωτικότητας των προσωπικών δεδομένων είναι:

- Συνήθως έχουν μεγάλη έκταση
- Είναι δυσνόητες για πολλούς από αυτούς
- Έχουν εμπιστοσύνη στους παρόχους των διαδικτυακών υπηρεσιών
- Θεωρούν ότι προστατεύονται από την ισχύουσα νομοθεσία

Πιο εξοικειωμένοι με τον GDPR φαίνεται να είναι οι άνθρωποι που κάνουν συχνή χρήση των κοινωνικών δικτύων. Ελέγχουν τις ρυθμίσεις ιδιωτικότητας των εφαρμογών και είναι ενημερωμένοι σε γενικές γραμμές τουλάχιστον για τα δικαιώματα τους. Επίσης οι γνώσεις περί προστασίας της ιδιωτικότητας είναι αντιστρόφως ανάλογη της ηλικίας και ανάλογη της βαθμίδας μόρφωσης. Από χώρα σε χώρα η αντιμετώπιση ων ζητημάτων ιδιωτικότητας γίνεται με διαφορετική ένταση. Αυτό έχει να κάνει κυρίως με το κατά πόσο ο τοπικός πληθυσμός χρησιμοποιεί διαδικτυακές εφαρμογές και με τον βαθμό κατά τον οποίο έχει ωριμάσει η διείσδυση τους σε κάθε χώρα (dataprivacymanager, 2020; eurostat, 2020) (Europa, 2020).

3.3.2 Χρήση εργαλείου Lumen

Το Lumen είναι ένα ακαδημαϊκό ερευνητικό έργο με επικεφαλής το Διεθνές Ινστιτούτο Επιστήμης Υπολογιστών (ICSI), το UC Berkeley και το IMDEA Networks. Υποστηρίζεται από το NSF (National Science Foundation) και το Data Transparency Lab. Η εφαρμογή Lumen Privacy Monitor αναλύει την κυκλοφορία της συσκευής στο διαδίκτυο και ενημερώνει τον χρήστη της για τα

χαρακτηριστικά της επικοινωνίας καθώς και για το αν αυτά δεν συνάδουν με τα γνωστά πρότυπα επικοινωνίας του χρήστη. Τα ευρήματα της σχετίζονται κυρίως με τον τρόπο κατά τον οποίο οι διάφορες διαδικτυακές εφαρμογές συλλέγουν τα ευαίσθητα προσωπικά δεδομένα σχετικά του χρήστη. Δίνει επιπλέον την δυνατότητα στον χρήστη να ρυθμίσει αυτές τις ροές με στόχο την προστασία των δεδομένων του. Η εφαρμογή ερευνά κυρίως το αν και τον τρόπο που επικοινωνούν οι εφαρμογές με διαδικτυακές υπηρεσίες παρακολούθησης και συλλογής προσωπικών στοιχείων. Έχει την δυνατότητα να ελέγξει και την κρυπτογραφημένη κίνηση. Δίνει επίσης την δυνατότητα στον χρήστη να αποκλείει ανεπιθύμητες ροές για μια δεδομένη εφαρμογή και να διαμορφώνει τις άδειες εφαρμογών για να διατηρήσετε τον έλεγχο του ποιος έχει πρόσβαση στα προσωπικά του δεδομένα. Για τον εντοπισμό διαρροών προσωπικών πληροφοριών, το Lumen απαιτεί ορισμένα δικαιώματα, ώστε να γνωρίζει ποιες τιμές και πληροφορίες πρέπει να αναζητήσει, όπως τον αριθμό τηλεφώνου, τα μηνύματα κειμένου, το IMEI και την τοποθεσία.

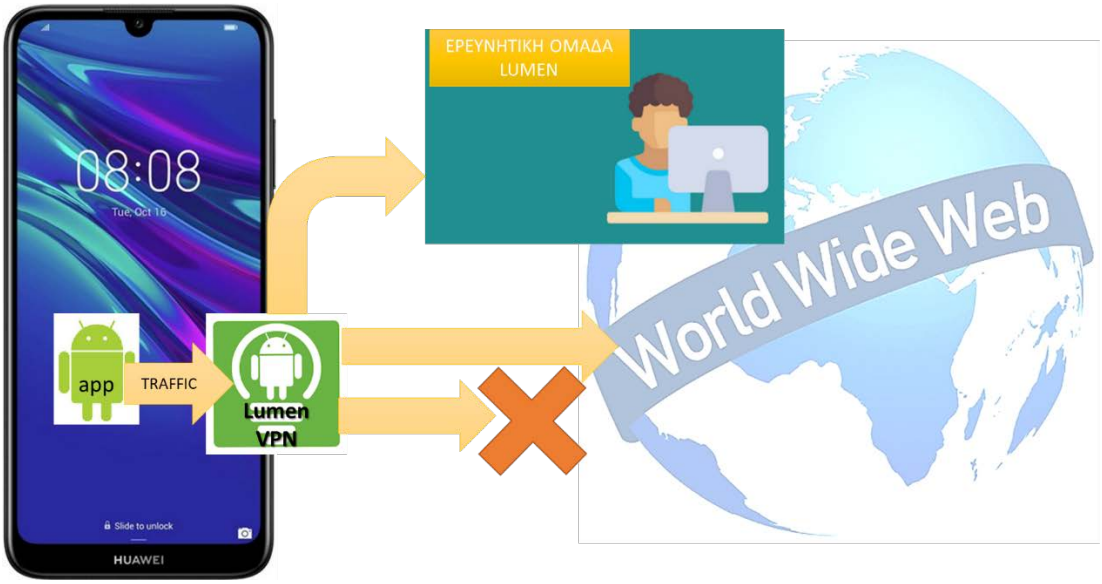
Για την παρούσα μελέτη, το εν λόγω εργαλείο λογισμικού χρησιμοποιήθηκε προκειμένου αναλυθεί η χρήση των προσωπικών δεδομένων από ένα σύνολο από δημοφιλείς εφαρμογές. Η εγκατάσταση της εφαρμογής απαιτεί την παροχή πολλών σχετικών δικαιωμάτων καθώς και την εγκατάσταση πιστοποιητικού για την παρακολούθηση της κρυπτογραφημένης και μη κίνησης. Τα στοιχεία που συλλέγει τα προωθεί ανώνυμα μέσω του διαδικτύου στην ερευνητική ομάδα που το υποστηρίζει. Για να λειτουργήσει θα πρέπει να της παρασχεθεί πρόσβαση σε προσωπικά δεδομένα της που αποθηκεύονται στην συσκευή καθώς διαφορετικά δεν είναι εφικτή η ανίχνευση των διαρροών. Αν και η ομάδα ανάπτυξης του εργαλείου δηλώνει ότι δεν συλλέγει τα προσωπικά δεδομένα των χρηστών, το γεγονός ότι πρόκειται για ένα έργο που δεν είναι ανοικτού κώδικα δημιουργεί ανησυχία σε οποίον επιλέξει να το χρησιμοποιήσει.

Με την ολοκλήρωση της εγκατάστασης της εφαρμογής, αυτή είναι πλέον σε θέση να παρέχει στον χρήστη της στοιχεία σχετικά με τη διαδικτυακή κίνηση

στην οποία συμμετέχουν οι εφαρμογές που είναι εγκατεστημένες στην συσκευή του. Η διεπαφή του αποτελείται από τρεις καρτέλες.

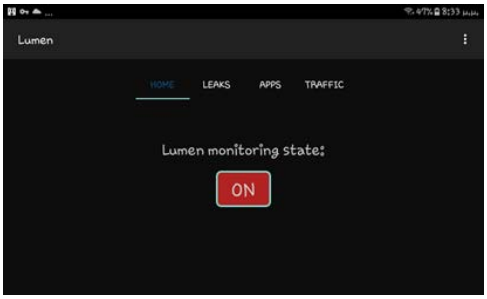
- Διαρροές (Leaks): Στην καρτέλα αυτή εμφανίζονται οι πληροφορίες περί του χρήστη ή της συσκευής οι οποίες μπορεί οι εγκατεστημένες εφαρμογές να δημοσιοποιούν.
- Εφαρμογές (Apps): Παρουσιάζονται στο τμήμα αυτό όλες οι εφαρμογές που ο χρήστης έχει επιλέξει να παρακολουθεί. Για αυτές το Lumen δημιουργεί λεπτομερείς και ευανάγνωστες αναφορές που είναι ικανές να δώσουν στον μέσο χρήστη έξυπνων κινητών συσκευών να κατανοήσει τους κινδύνους από τις εφαρμογές που τρέχουν.
- Κίνηση (Traffic): Στην καρτέλα αυτή περιλαμβάνονται στοιχεία που περιγράφουν ποιοτικά και ποσοτικά την κίνηση που περνάει από την συσκευή. Περιλαμβάνει πληροφορίες σχετικά με HTTPS και άλλες συνδέσεις, εύρος ζώνης και την επιβάρυνση που προκαλούν διαφημίσεις και scripts που τρέχουν στο παρασκήνιο και συνδέσεις σε διαδικτυακές υπηρεσίες.

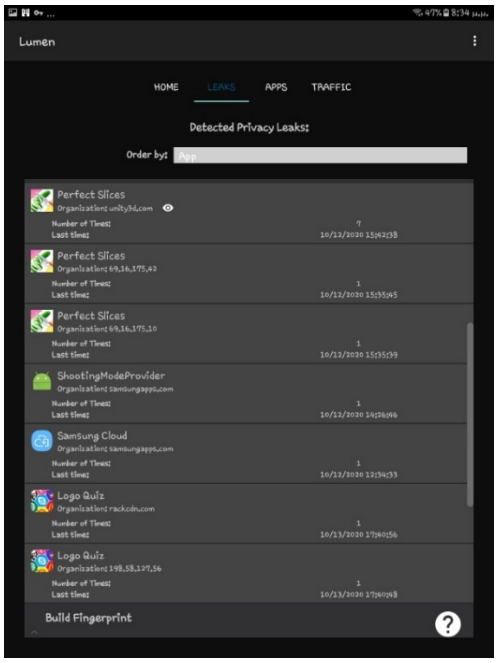
Το Lumen χρησιμοποιεί τα δικαιώματα VPN για να παρακολουθεί όλη την κίνηση που πραγματοποιούνται μέσω των εφαρμογών που τρέχουν. Αυτό το VPN λειτουργεί τοπικά στη συσκευή και λειτουργεί ως ενδιάμεσο λογισμικό μεταξύ εφαρμογών και των διαδικτυακών sockets. Λόγω αυτού, μπορεί να ανιχνεύσει τα τελικά σημεία (end points) όλων των πακέτων που διακινούνται από την εφαρμογή. Το πώς λειτουργεί σε γενικές γραμμές φαίνεται στην επόμενη εικόνα (Khanna, 2020).



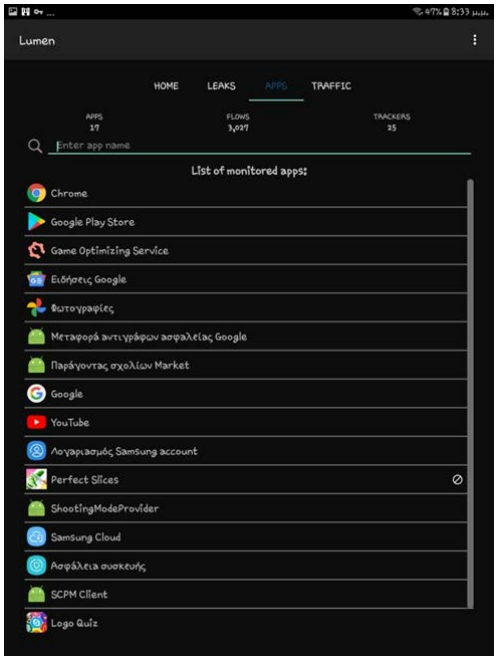
Εικόνα 1. Λειτουργία του Lumen.

Στον παρακάτω πίνακα φαίνονται το πως ο χρήστης κινητής συσκευής στην οποία είναι εγκατεστημένο το Lumen μπορεί να αντλήσει πληροφορίες για το τι δεδομένα μεταδίδουν οι εγκατεστημένες εφαρμογές.

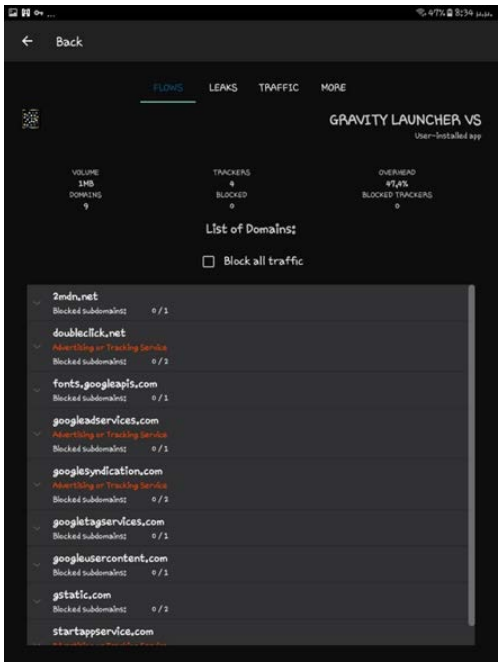
	Αρχικά ο χρήστης θα πρέπει να ενεργοποιήσει την εφαρμογή ώστε να είναι σε θέση να ανιχνεύει την κίνηση.



Στην καρτέλα Leaks προβάλλονται τα είδη των προσωπικών δεδομένων που χρησιμοποιούνται από εφαρμογές που τρέχουν στην συσκευή. Φαίνονται επίσης και οι εφαρμογές που τα χρησιμοποιούν. Ο χρήστης έχει την δυνατότητα να κατατάξει τις πληροφορίες κατά ημερομηνία, εφαρμογή ή domain. Όταν επιλέξει να προβληθούν κατά ημερομηνία, προσφέρεται η δυνατότητα να προβληθεί το επίπεδο του κινδύνου μαζί με μία σύντομη επεξήγηση σε γλώσσα και με όρους κατανοήσιμους από τον μέσο χρήστη έξυπνων κινητών συσκευών.



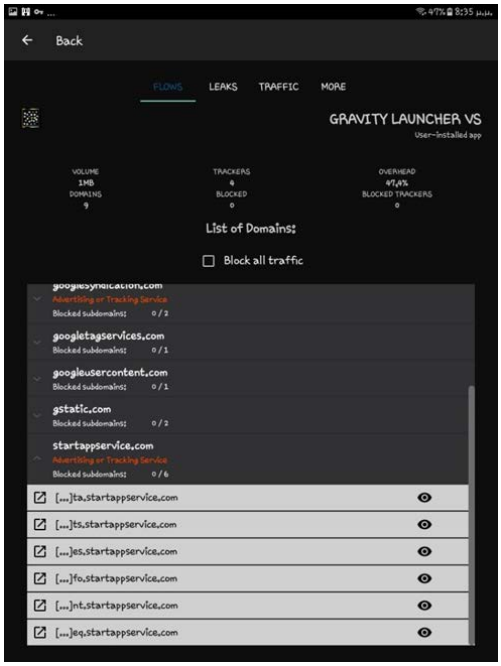
Στην οθόνη Apps φαίνονται οι εφαρμογές που ο χρήστης έχει επιλέξει να παρακολουθεί τις κινήσεις τους.



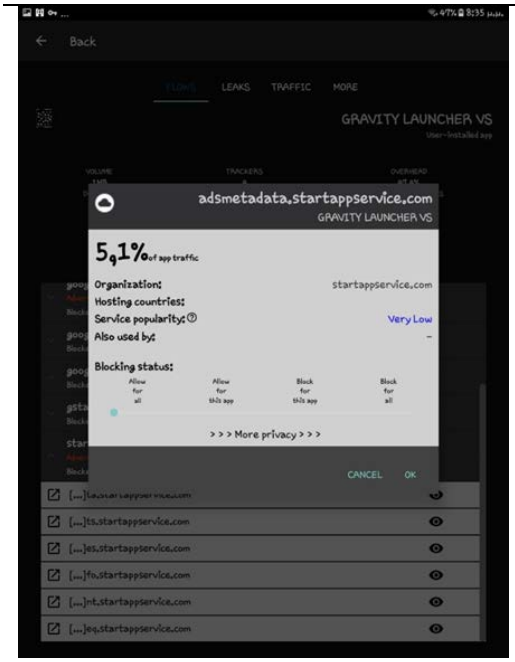
Με κλικ σε αυτές παρουσιάζονται πληροφορίες σχετικά με την κίνηση δεδομένων μέσω αυτών όπως:

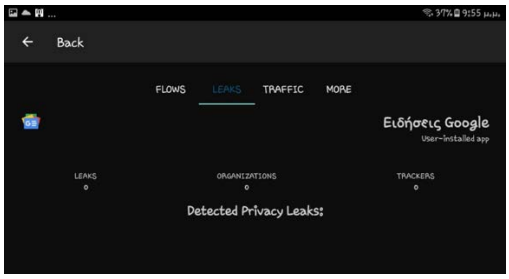
- Τι είδους δεδομένα στέλνουν
- Το ποιον έχουν παραλήπτη τα δεδομένα που στέλνουν
- Τον όγκο των δεδομένων που στέλνουν
- Ποια από την κίνηση αυτή έχει απαγορευθεί (block).

Παρέχεται επίσης η δυνατότητα στον χρήστη να μπλοκάρει την κίνηση αν την θεωρήσει επικίνδυνη.

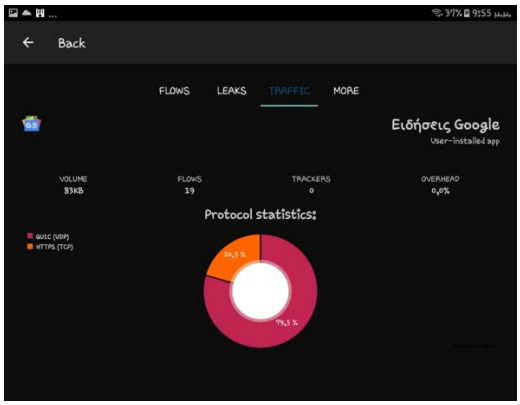


Με κλικ σε κάθε μία από τις ροές της εφαρμογής παρέχονται περισσότερες πληροφορίες για αυτή που βοηθούν κυρίως να προσδιοριστεί ποιος είναι ο διαχειριστής της ροής αυτής.

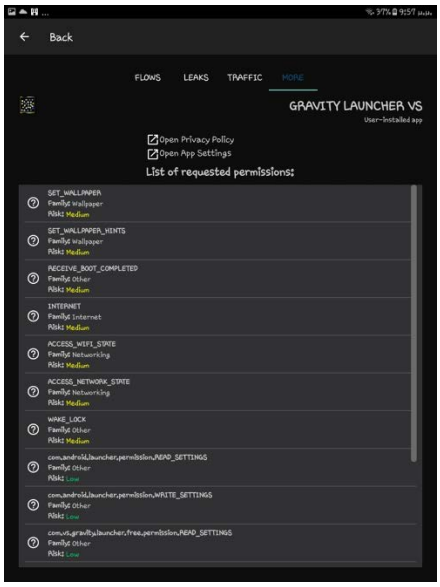




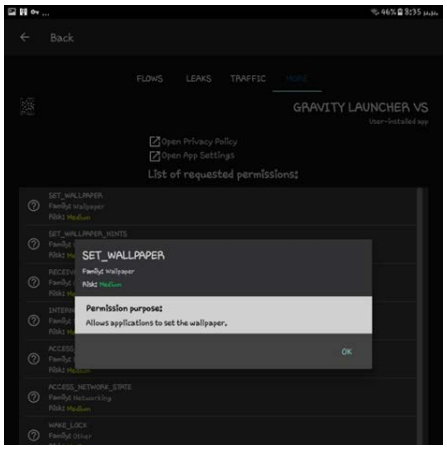
Στην επιλογή Leaks εμφανίζονται οι διαρροές που καταγράφηκαν μέσω της εφαρμογής



Στην επιλογή traffic καταγράφεται η κίνηση που περνάει μέσω της εφαρμογής. Εξετάζεται ποιο ποσοστό της κίνησης αυτής γίνεται υπό κρυπτογράφηση και ποιο όχι.



Στην καρτέλα More φαίνονται τα δικαιώματα της εφαρμογής σε βοηθήματα της συσκευής καθώς και το πόσο επικίνδυνο είναι αυτό.



Με κλικ σε κάθε ένα από αυτά παρέχεται μία σύντομη και περιεκτική επεξήγηση του κινδύνου.

3.4 Κίνδυνοι από τον χειρισμό προσωπικών δεδομένων

3.4.1 Μη εξουσιοδοτημένη (και ς) πρόσβαση

Οι έξυπνες κινητές συσκευές συνήθως έχουν εγκατεστημένες περισσότερες από είκοσι διαφορετικές εφαρμογές. Καθεμία από αυτές μπορεί να παρέχει διαφορετική πρόσβαση στις δυνατότητες και τα δεδομένα της συσκευής. Αυτά τα δικαιώματα συχνά αποδίδονται μέσω βιβλιοθηκών τρίτων που χρησιμοποιούν οι προγραμματιστές για να επιταχύνουν τον ρυθμό

ολοκλήρωσης των εφαρμογών ή/και να παρέχουν στους χρήστες ποιοτικές υπηρεσίες. Μερικά παραδείγματα από τις σχετικές υπηρεσίες είναι εκμετάλλευση των δυνατοτήτων της κοινωνικής δικτύωσης ή ο προσδιορισμός του σημείου στάσεως. Ωστόσο κάποιες φορές συμβάλλουν στην κατάρρευση του απορρήτου των χρηστών των συσκευών όπου χρησιμοποιούνται. Τα λειτουργικά συστήματα, κατά κανόνα, δεν έχουν την δυνατότητα να διαχωρίζουν την παροχή των δικαιωμάτων στην εφαρμογή ή στις βιβλιοθήκες που χρησιμοποιεί η εφαρμογή καθώς αντιλαμβάνονται τις εφαρμογές σαν ενιαίες οντότητες. Χαρακτηριστικές είναι οι αδυναμίες του Android να παρακολουθήσει την αποτελεσματικά την πρόσβαση των βιβλιοθηκών καθώς δεν μπορεί να επέμβει όταν οι βιβλιοθήκες:

- κάνουν κατάχρηση των προνομίων που τους παρέχονται από τις εφαρμογές.
- παρακολουθούν το σημείο στάσης των χρηστών χωρίς τη συγκατάθεσή τους.
- Ανταλλάσσουν δεδομένα με διαδικτυακές υπηρεσίες για τον σχηματισμό του προφίλ των χρηστών

Οι εφαρμογές που τρέχουν σε μία κινητή συσκευή δρουν με δύο βασικούς τρόπους προκειμένου να αποκαλύπτουν τα ευαίσθητα προσωπικά δεδομένα των χρηστών:

- Inter-Component Communication: Οι εφαρμογές που τρέχουν σε μία κινητή συσκευή διαμοιράζονται συστατικά τα οποία έχουν καθορισμένα δικαιώματα. Οι εφαρμογές ωστόσο έχουν την δυνατότητα να ανταλλάσσουν δεδομένα με συστατικά που καλούν ή από τα οποία καλούνται. Με τον τρόπο αυτό είναι πιθανό να διαρρέουν ευαίσθητες πληροφορίες που προέρχονται από κοινόχρηστα συστατικά.
- Inter-Library Communication (ICC): όντας μία βιβλιοθήκη μέρος εφαρμογών που είναι εγκαταστημένες στην ίδια συσκευή με διαφορετικό σύνολο δικαιωμάτων να τους έχουν ανατεθεί, έχουν την δυνατότητα να συνδυάσουν τα δικαιώματα που κληρονομούν από τις

εφαρμογές αυτές. Έχοντας αποκτήσει τον κατάλληλο συνδυασμό δικαιωμάτων πλέον είναι σε θέση να χειρίζονται ευαίσθητα δεδομένα των χρηστών. Στην επόμενη εικόνα φαίνεται σχηματικά ένα παράδειγμα τέτοιου είδους διαρροής δικαιωμάτων.

Ένας ακόμα τρόπος με το οποίο μπορεί να αποκτήσουν πρόσβαση σε προσωπικά δεδομένα χρηστών κινητών εφαρμογών αναρμόδιοι φορείς και οντότητες είναι με την αρπαγή τους από φορείς που τα διατηρούν συγκεντρωτικά (είτε έχουν εξουσιοδοτηθεί για αυτό είτε όχι). Τέτοια περιστατικά έχουν αναφερθεί πολλά τα τελευταία χρόνια με κάποια από αυτά να αφορούν μεγάλους οργανισμούς (Razaghpanah, et al., 2018).

3.4.2 Μη εξουσιοδοτημένη (αδιαφανής) επεξεργασία και χρήση

Έχουν πραγματοποιηθεί μελέτες που φανερώνουν την εφαρμογή χαλαρών πολιτικών εκμετάλλευσης – επεξεργασίας των ευαίσθητων δεδομένων. Τις περισσότερες φορές οι πολιτικές αυτές έχουν να κάνουν με την σχέση εμπιστοσύνης μεταξύ χρήστη-εφαρμογής η οποία παραβιάζεται με αποτέλεσμα τα προσωπικά δεδομένα να διαρρέουν προς τρίτους. Η διαρροή μπορεί να γίνει εν γνώσει των διαχειριστών των εφαρμογών. Στις περιπτώσεις αυτές εκμεταλλεύονται νομικές αστοχίες και διανέμουν τα ευαίσθητα δεδομένα κυρίως σε θυγατρικές τους εταιρείες ή σε συνεργάτες τους. Σε κάθε περίπτωση οι θιγόμενοι χρήστες αντιλαμβάνονται ότι τα προσωπικά τους δεδομένα έχουν διαρρεύσει όταν γίνονται δέκτες διαφημιστικών μηνυμάτων όταν χρησιμοποιούν τις εφαρμογές στην κινητή τους συσκευή. Επίσης ορισμένοι πάροχοι εφαρμογών δηλώνουν ρητά ότι διατηρούν το δικαίωμα να κοινοποιούν συγκεντρωτικά ή ανώνυμα δεδομένα σε συνεργάτες τους.

Τα προσωπικά δεδομένα, είτε ατομικά είτε συγκεντρωτικά, είναι πολύτιμα για την λήψη στρατηγικών και τακτικών αποφάσεων στα πλαίσια λειτουργίας των οργανισμών. Κατά συνέπεια η διάθεση τους από αυτούς που τα διατηρούν είναι μία πολύ προσοδοφόρα διαδικασία. Αυτή είναι και η βασική αιτία που αναζητούνται τρόποι να παρακαμφθεί η όποια νομική κατοχύρωση της

στεγανότητας των σχετικών βάσεων δεδομένων που διατηρούνται. Στην επόμενη εικόνα παρουσιάζεται μία ιστοσελίδα η οποία διαφημίζει την δυνατότητας παροχής δεδομένων σχετικών με καταναλωτές.

Εικόνα 2. Διαφήμιση διάθεσης προσωπικών δεδομένων.

3.5 Αντιμετώπιση Κινδύνων

3.5.1 Νομική κατοχύρωση και προστασία

Η ραγδαία ανάπτυξη της τεχνολογίας, κυρίως τις τελευταίες δύο δεκαετίες, βρήκε απροετοίμαστο τον νομικό κλάδο ως προς την αντιμετώπιση σχετικών ζητημάτων που προέκυψαν με την διευκόλυνση της πρόσβασης, επεξεργασίας και μετάδοσης προσωπικών δεδομένων. Για μεγάλο χρονικό διάστημα υπήρχε μεγάλο κενό στην νομική προστασία τους με αποτέλεσμα οι άνθρωποι να είναι ανοχύρωτοι στην έκθεση προσωπικών στοιχείων τους. Το κενό αυτό καλύπτεται σε μεγάλο βαθμό με τους κανόνες που είναι ευρέως γνωστοί ως General Data Protection Regulation (GDPR). Ο Γενικός Κανονισμός Προστασίας Δεδομένων – όπως είναι η απόδοση του όρου στην Ελληνική γλώσσα, τέθηκε σε εφαρμογή στην Ευρωπαϊκή Ένωση από τις 25 Μαΐου του 2018. Βασίζεται σε μέχρι τότε υφιστάμενες νομοθετικές πράξεις που σχετιζόταν με την προστασία των προσωπικών δεδομένων των ατόμων, ανεξάρτητα από τρόπο και την μορφή που χρησιμοποιούνται. Ισχύει όχι μόνο για εταιρείες και οργανισμούς στην ΕΕ, αλλά και για εταιρείες που εδρεύουν εκτός ΕΕ και που δραστηριοποιούνται στην ΕΕ ή παρακολουθούν τη συμπεριφορά πολιτών στην ΕΕ. Στοχεύει στην προστασία δεδομένων όπως:

- Το δικαίωμα πρόσβασης σε προσωπικά δεδομένα που συλλέγονται από εταιρείες ή οργανισμούς και την ενημέρωση αυτών.
- Η διαβίβαση προσωπικών δεδομένων σε άλλη οντότητα.
- Το δικαίωμα της διαγραφής των προσωπικών δεδομένων όταν πάψει να υφίσταται η ανάγκη που απαιτούσε την αποθήκευση τους.
- Το δικαίωμα ενημέρωσης για παραβιάσεις δεδομένων που ενδέχεται να αποτελούν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που αφορούν τα δεδομένα αυτά (Special Eurobarometer, 2019).

Ο Κανονισμός έχει άμεση ισχύ σε όλα τα Κράτη-Μέλη: για κάποια επιμέρους ζητήματα ωστόσο, εναποθέτει τη ρύθμισή τους στον εθνικό νομοθέτη. Στην Ελλάδα, τα ζητήματα αυτά ρυθμίστηκαν στην Ελληνική Νομοθεσία με τον Νόμο 4624 του 2019. Σύμφωνα με τον νόμο αυτό προβλέπεται η εφαρμογή των διατάξεων του, όπου πραγματοποιείται αυτοματοποιημένη επεξεργασία δεδομένων Προσωπικού Χαρακτήρα ή σε μη αυτοματοποιημένη επεξεργασία τους όταν περιλαμβάνονται στο παρόν ή τοπ μέλλον σε συστήματα δημοσίων και ιδιωτικών φορέων. Σε κάθε περίπτωση θα πρέπει σύμφωνα με τον νόμο να ορίζεται σε κάθε φορέα υπεύθυνος διαχείρισης και επεξεργασίας των προσωπικών δεδομένων με αντικείμενο την εξασφάλιση τήρησης των κανόνων του GDPR. Εποπτική αρχή για την τήρηση του νόμου ορίστηκε η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Στην Κύπρο, η αντίστοιχη εποπτική αρχή είναι το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Η εκάστοτε εποπτική αρχή συνεργάζεται σε υψηλότερο επίπεδο με τις αντίστοιχες αρχές των υπολοίπων κρατών μελών της ΕΕ και συμμετέχει στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και σε άλλα αντίστοιχα όργανα που έχουν ως αντικείμενο την προστασία δεδομένων προσωπικού χαρακτήρα. Συνεργάζεται επίσης και με τρίτες χώρες και διεθνείς οργανισμούς για το ίδιο αντικείμενο. Εξαιρέσεις στην

αρμοδιότητα της Αρχής τίθενται σε περιπτώσεις δεδομένων που σχετίζονται με δικαστικές πράξεις και την Εθνική Ασφάλεια. (Εφημερίδα της Κυβερνήσεως, 2019).

Εκ των σημαντικών διατάξεων του νόμου 4624/2019 στην Ελλάδα είναι η περίπτωση επεξεργασίας δεδομένων ανηλίκου στο πλαίσιο παροχής υπηρεσιών της Κοινωνίας της Πληροφορίας. Συγκεκριμένα, η επεξεργασία δεδομένων προσωπικού χαρακτήρα ανηλίκου, κατά την παροχή τέτοιων υπηρεσιών προς αυτόν, επιτρέπεται με συγκατάθεσή του αν έχει συμπληρώσει το 15ο έτος ή με συγκατάθεση των γονέων σε διαφορετική περίπτωση.

Σημαντική μνεία πρέπει να γίνει στον επερχόμενο Ευρωπαϊκό κανονισμό ePrivacy (σε αντικατάσταση της τωρινής Οδηγίας e-Privacy 2002/58/EC, όπως έχει αναθεωρηθεί με την Οδηγία 2009/136/ΕΨ) , ο οποίος αποτελεί ειδικό νόμο (lex specialis) και θα εξειδικεύσει , συμπληρώσει ή και αναμένεται να υπερισχύσει σε πολλά σημεία του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) ειδικότερα και όχι μόνο, στον τομέα των ηλεκτρονικών επικοινωνιών σε σχέση με την προστασία της ιδιωτικής ζωής των χρηστών (άρθρο 5 παράγραφος 3 και άρθρο 13). Δραστηριότητες οι οποίες παρουσιάζουν ιδιαίτερο ενδιαφέρον και άρα θα βρίσκονται στο πεδίο εφαρμογής του Ευρωπαϊκού Κανονισμού ePrivacy είναι οι IOT συσκευές, τα Cookies, τα Web Beacons μέσω των οποίων συλλέγεται η πλοήγηση των χρηστών, η Εμπορική Προώθηση με χρήση Email, καθώς και οι λεγόμενες Over-The-Top υπηρεσίες των άμεσων μηνυμάτων (Whatsup, Viber και άλλα). Ειδικά για τα Cookies, και σύμφωνα με το σχέδιο του Κανονισμού (αλλά και την τωρινή e-Privacy Οδηγία που είναι σε ισχύ), θα πρέπει να υπάρχει ρητή συγκατάθεση (consent) των χρηστών πριν την συλλογή των δεδομένων τους στις συσκευές τους, ενώ οι εταιρείες υποχρεούνται στην παροχή ακριβώς των ίδιων υπηρεσιών είτε οι χρήστες συναινέσουν είτε όχι . (COMMISSION, 2017)

3.5.2 Τεχνολογική προσέγγιση

Ο GDPR και οι προσαρμοσμένες σε αυτόν Εθνικές Νομοθεσίες, κατοχυρώνουν νομικά το δικαίωμα των Ευρωπαίων Πολιτών στο να έχουν τον έλεγχο της έκθεσης των προσωπικών τους δεδομένων. Ωστόσο η νομική κατοχύρωση δεν είναι από μόνη της αρκετή να εξασφαλίσει το απόρρητο των ευαίσθητων προσωπικών δεδομένων. Όσο περισσότερο χρησιμοποιούνται οι τεχνολογίες του διαδικτύου στην δραστηριότητα των ανθρώπων, τόσο περισσότερο ευάλωτα είναι τα δεδομένα τους στους κινδύνους του κυβερνοχώρου. Επομένως χρειάζεται να λαμβάνονται μέτρα τα οποία να προστατεύουν σε τεχνικό επίπεδο την έκθεση των προσωπικών δεδομένων των χρηστών των εφαρμογών.

Οι έξυπνες κινητές συσκευές και τα δημοφιλέστερα λειτουργικά τους συστήματα παρέχουν μηχανισμούς προστασίας. Ο βασικότερος από αυτούς είναι η παροχή δικαιωμάτων χρήσης των δυνατοτήτων των συσκευών. Όπως έχει ήδη αναφερθεί, οι εφαρμογές για κινητές συσκευές σχεδιάζονται και αναπτύσσονται με προδιαγραφές λειτουργίας που πολλές φορές απαιτούν την χρήση υποσυστημάτων τους όπως η φωτογραφική μηχανή, η ηχογράφηση. Ωστόσο τα λειτουργικά συστήματα είναι σχεδιασμένα έτσι ώστε η χρήση τους να γίνεται μόνο αν το επιτρέψει ο κάτοχος της συσκευής. Το Android προσφέρει μια κεντρική διεπαφή για ρυθμίσεις απορρήτου, καθώς και τη δυνατότητα αλλαγής δικαιωμάτων για μια συγκεκριμένη εφαρμογή. Επιπλέον, επιτρέπει στους χρήστες να αποφασίζουν για τις προεπιλεγμένες εφαρμογές για τις οποίες οι χρήστες μπορούν να προσαρμόσουν τα δικαιώματα που ταιριάζουν στις ανάγκες τους. Το IOS, από την άλλη πλευρά, χρησιμοποιεί «προνόμια» και «δικαιώματα». Τα προνόμια καθορίζονται στην ανάπτυξη μιας εφαρμογής και ορίζουν δυνατότητες που δεν είναι διαθέσιμες από προεπιλογή και είναι απαραίτητες για τη λειτουργία της εφαρμογής. Τα δικαιώματα υποβάλλονται στην Apple στο πακέτο εφαρμογών και δεν μπορούν να τροποποιηθούν μετά την υποβολή της αίτησης στο App Store. Τα δικαιώματα στο iOS εγκρίνονται μόνο κατά το χρόνο εκτέλεσης και χρησιμοποιούνται για να ζητήσουν από τον χρήστη τη χρήση περιορισμένων πόρων, όπου η πρόσβαση παρέχεται μόνο εάν ο χρήστης συμφωνήσει. Οι χρήστες ενδέχεται να ανακαλέσουν τα δικαιώματα

ανά πάσα στιγμή χρησιμοποιώντας τις ρυθμίσεις απορρήτου και ασφάλειας του iOS. Επίσης παρέχει την δυνατότητα ορισμού κοινής στάσης έναντι ομοίων αιτήσεων των εφαρμογών για δικαιώματα. Η ρύθμιση μιας στάσης επιτρέπει στους χρήστες να βλέπουν όλες τις εφαρμογές που ζητούν μια συγκεκριμένη άδεια ή όλες τις άδειες που ζητά κάθε εφαρμογή. Εάν οι χρήστες θέλουν να καταλάβουν γιατί απαιτείται άδεια, προωθούνται στην πολιτική απορρήτου. Με τις κεντρικές ρυθμίσεις ο χρήστης μπορεί να δώσει ή να άρει δικαιώματα μαζικά (enisa, 2017).

Οι προγραμματιστές και οι πάροχοι διαδικτυακών υπηρεσιών χρειάζεται να λαμβάνουν επιπλέον μέτρα για τον τεχνικό περιορισμό της διασποράς προσωπικών δεδομένων ως εξής:

- Περιορισμός διαχείρισης δεδομένων στα απολύτως απαραίτητα: με τις τακτικές αυτές αποφεύγεται γενικότερα η συλλογή και επεξεργασία προσωπικών δεδομένων εκτός από εκείνα που είναι εντελώς απαραίτητα. Επίσης όπου είναι εφικτό και δεν μειώνεται σε απαγορευτικό βαθμό η αποδοτικότητα των εφαρμογών, η επεξεργασία των δεδομένων γίνεται μερικώς και σε όση έκταση είναι απαραίτητο. Τέλος τα δεδομένα που δεν χρειάζονται πλέον, διαγράφονται άμεσα.
- Αποτροπή συσχέτισης προσωπικών δεδομένων μεταξύ τους ή με οντότητες διαχωρίζοντας την επεξεργασία λογικά ή φυσικά: Αυτό επιτυγχάνεται με διαμέριση προσωπικών δεδομένων ώστε να προσφέρεται σε λειτουργίες πρόσβαση μόνο σε αυτά που χρειάζεται, και με επεξεργασία τμημάτων προσωπικών δεδομένων ανεξάρτητα, χωρίς πρόσβαση ή συσχέτιση με δεδομένα άλλων τμημάτων.
- Υποβολή μόνο των απαραιτήτων λεπτομερειών για επεξεργασία: Τα δεδομένα, όποτε είναι εφικτό και δεν επηρεάζεται το αποτέλεσμα της επεξεργασίας, ομαδοποιούνται και η επεξεργασία γίνεται στα κοινά χαρακτηριστικά. Επίσης μπορεί να προστίθεται θόρυβος στα δεδομένα προκειμένου να είναι δυσκολότερο να συνδυαστούν με συγκεκριμένες οντότητες.

- Αποτροπή της δημοσίευσης των προσωπικών δεδομένων: όποτε είναι εφικτό τα προσωπικά δεδομένα αποκρύπτονται από τους δυνητικούς χρήστες των συστημάτων. Αυτό γίνεται με την εξουσιοδότηση της πρόσβασης των χρηστών μόνο για τον βαθμό που απαιτείται, την χρήση μηχανισμών κρυπτογράφησης τους και αφαίρεση κάθε στοιχείου που μπορεί να συσχετίσει διαφορετικών τμήματα προσωπικών δεδομένων.
- Ενημέρωση και εκπαίδευση των διαχειριστών ώστε να τηρούν τις διατάξεις του GDPR αλλά και τα μέτρα ασφαλείας στο διαδίκτυο. Θα πρέπει να έχουν πρόσβαση σε τεχνικές οδηγίες και νομικά κείμενα σχετικά με τα θέματα αυτά. Επίσης θα πρέπει να έχουν στην διάθεση τους απαραίτητους υλικοτεχνικούς πόρους και γνώσεις για να μπορούν να ανταποκρίνονται στις απαιτήσεις και τους κανόνες που αυτά ορίζουν.
- Παροχή μηχανισμών υποκειμένων δεδομένων για τον έλεγχο της επεξεργασίας των προσωπικών τους δεδομένων: Επεξεργασία μόνο των προσωπικών δεδομένων για τα οποία λαμβάνεται ρητή, ελεύθερη και ενημερωμένη συγκατάθεση. Θα πρέπει να επιτρέπεται την επιλογή της παροχής ή του αποκλεισμού προσωπικών δεδομένων, εν μέρει ή εξ ολοκλήρου, από οποιαδήποτε επεξεργασία. Τέλος θα πρέπει να δίνεται η δυνατότητα στα υποκείμενα των προσωπικών δεδομένων δυνατότητα να τα τηρούν ενημερωμένα ή να τα διαγράφουν (όπου αυτό είναι εφικτό).
- Προστασία του απορρήτου: Αναγνώριση της αξίας του απορρήτου και απόφαση σχετικά με πολιτικές που το διέπουν. Εξέταση του απορρήτου κατά το σχεδιασμό ή την τροποποίηση χαρακτηριστικών και την ενημέρωση πολιτικών και διαδικασιών για την καλύτερη προστασία των προσωπικών δεδομένων. Διασφάλιση της τήρησης των πολιτικών, αντιμετωπίζοντας τα προσωπικά δεδομένα ως περιουσιακό στοιχείο και το απόρρητο ως στόχο.
- Καταγραφή των ενεργειών επί της επεξεργασίας των προσωπικών δεδομένων: Παρακολούθηση όλης της επεξεργασίας δεδομένων, χωρίς αποκάλυψη προσωπικών δεδομένων, διασφάλιση και επανεξέταση των πληροφοριών που συλλέγονται για τυχόν κινδύνους. Εξέταση καθημερινών δραστηριοτήτων μέσω των αρχείων καταγραφής για τυχόν

κινδύνους για προσωπικά δεδομένα και σοβαρή απόκριση σε τυχόν ασυμφωνίες. Σε κάθε περίπτωση θα πρέπει να γίνεται λεπτομέρειες ανάλυση των στοιχείων που συλλέγονται (enisa, 2017).

Κεφάλαιο 4
Χρήστες Διαδικτυακών εφαρμογών – Αξιολόγηση της επαγρύπνησής τους

4.1 Γνώσεις – Στάση Χρηστών

Η νομική κατοχύρωση και οι τεχνικές δυνατότητες προσφέρουν σημαντική εξασφάλιση στην διαχείριση και την επεξεργασία των προσωπικών δεδομένων. Ωστόσο δεν είναι αρκετή για την επίτευξη υψηλού επιπέδου ασφαλείας τους καθώς οι χρήστες παίζουν τον σημαντικότερο ρόλο στον τομέα αυτό. Οι γνώσεις και η στάση των χρηστών απέναντι στα ζητήματα που έχουν να κάνουν με τα προσωπικά τους δεδομένα του δίνουν ανάλογες δυνατότητες για την εξασφάλιση τους. Πρωταρχικά το πώς αντιλαμβάνονται την ασφάλεια των προσωπικών τους δεδομένων και την σημασία τους καθορίζει τον βαθμό κατά τον οποίο ενδιαφέρονται για την διαχείριση και επεξεργασία τους. Όταν το υποκείμενο των δεδομένων θεωρεί ότι η διαρροή τους μπορεί με κάποιον τρόπο να είναι επιζήμια, εκτιμάται ότι θα αναζητήσει τους τρόπους με τους οποίους μπορεί να τα προστατεύσει ή να απαιτήσει την προστασία τους από την οντότητα στην οποία τα διαθέτει για επεξεργασία με συγκεκριμένο σκοπό. Σε αντίθετη περίπτωση η τελευταία μπορεί να ενεργεί ανεξέλεγκτα προς όφελος της ανεξάρτητα αν ο τρόπος που ενεργεί αποδεικνύεται επιζήμιος για το υποκείμενο.

Η ανησυχία για την διαχείριση και επεξεργασία των προσωπικών δεδομένων είναι απαραίτητο να συνδυάζεται με γνώση για τις νομικές και τεχνικές

δυνατότητες που υπάρχουν για να προστατευτούν. Έχοντας την σχετική γνώση ο χρήστης των διαδικτυακών εφαρμογών είναι σε θέση να λάβει τα μέτρα που μπορεί είτε σε νομικό είτε σε τεχνικό επίπεδο. Επίσης μπορεί να απαιτήσει και να ελέγχει την τήρηση των μέτρων που πρέπει να λαμβάνει ο διαχειριστής των διαδικτυακών εφαρμογών.

4.2 Μεθοδολογία έρευνας

Για την συλλογή ποσοτικών δεδομένων και προκειμένου να προσδιοριστεί το επίπεδο ευαισθητοποίησης του διαδικτυακού κοινού που αποκτά πρόσβαση με έξυπνες κινητές συσκευές σε αντίστοιχες εφαρμογές, διεξήχθη δειγματοληπτική έρευνα με την μορφή ηλεκτρονικού ερωτηματολογίου.

Το εργαλείο που χρησιμοποιήθηκε για τον σχεδιασμό και την διανομή του ήταν το Google Forms. Η επιλογή του συγκεκριμένου εργαλείου έγινε με γνώμονα την ευκολία σχεδίασης και δημιουργίας ερωτηματολογίων έναντι άλλων λογισμικών, σε συνδυασμό με την δωρεάν διάθεση και λειτουργία μέσω διαδικτύου με χρήση οποιουδήποτε προγράμματος περιήγησης, χωρίς επιπλέον εγκατάσταση λογισμικού στον υπολογιστή. Επιπλέον το Google Forms παρέχει και διαγραμματική παρουσίαση ανά απάντηση, ώστε τα αποτελέσματα των ερωτήσεων να εξάγονται εύκολα για χρήση τους από εφαρμογές στατιστικών αναλύσεων.

Όσον αφορά το ερωτηματολόγιο, για να περιοριστούν οι κίνδυνοι που απορρέουν από την αδυναμία κατανόησης των ερωτήσεων αλλά και την μείωση του χρόνου για την συμπλήρωση, επιλέχθηκε η όσο τον δυνατόν σαφέστερη διατύπωση κλειστού τύπου ερωτήσεων με προκαθορισμένες επιλογές για απαντήσεις για τους συμμετέχοντες.

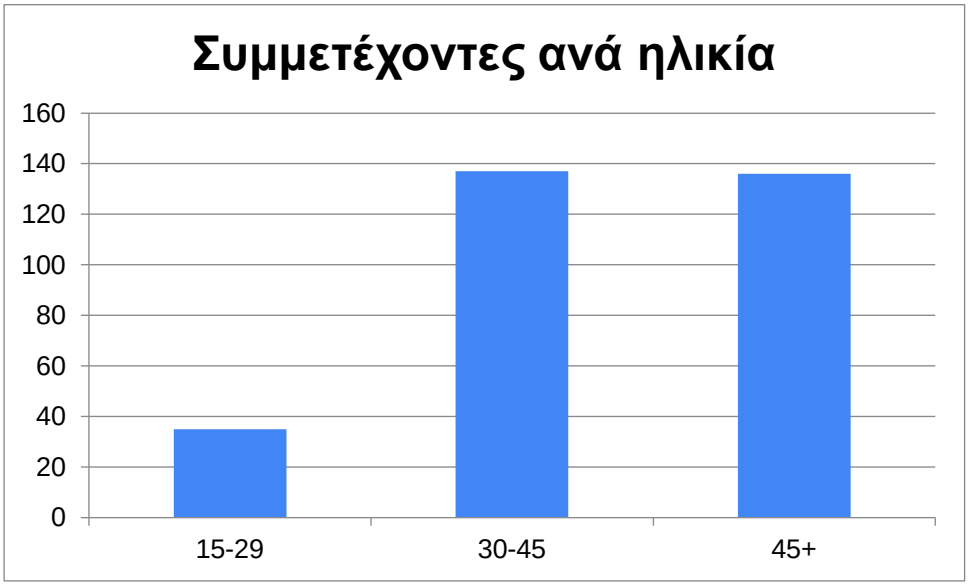
Αναλυτικότερα ο σχεδιασμός περιλάμβανε προαιρετικές και υποχρεωτικές ερωτήσεις, ερωτήσεις πολλαπλής επιλογής, ερωτήσεις προκαθορισμένων πολλαπλών σημείων καθώς και ερωτήσεις μορφής Likert με κλίμακα 1-5.

Σημαντικό είναι να αναφερθεί, ότι για την συμπλήρωση του ερωτηματολογίου, δεν ήταν απαιτητό από πλευράς συμμετέχοντα να διατηρεί οποιοδήποτε λογαριασμό σε κοινωνικά δίκτυα ή σε ηλεκτρονική αλληλογραφία και δεν ήταν απαιτητή η συμπλήρωση προσωπικών στοιχείων του, γεγονότα που επηρέασαν θετικά στην αύξηση του δείγματος αλλά και στην αξιοπιστία των δεδομένων της συλλογής.

Για την ανάλυση και την επεξεργασία των απαντήσεων του ερωτηματολογίου, χρησιμοποιήθηκε το Excel 2016 της Microsoft.

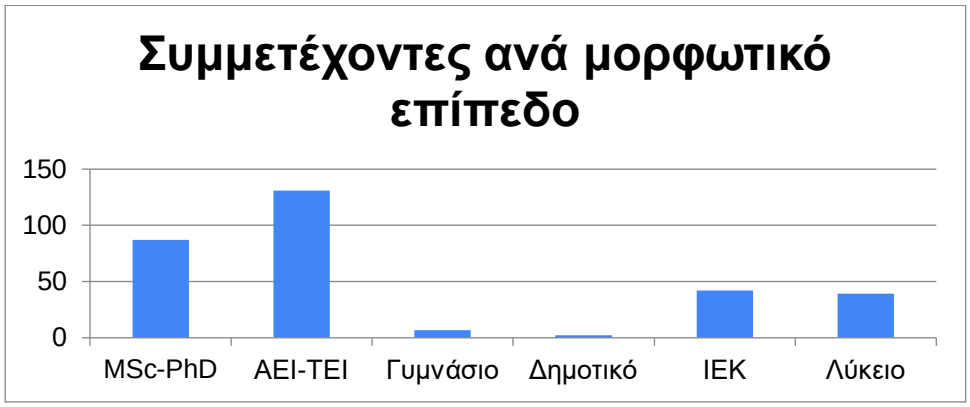
Συμμετείχαν 308 άνθρωποι οι οποίοι κλήθηκαν να ανταπαντήσουν στις ερωτήσεις του Παραρτήματος «Α». Για την επιλογή των ανθρώπων που θα συμμετέχουν χρησιμοποιήθηκε η τυχαία δειγματοληψία, η σύντομη έρευνα διενεργήθηκε με ανάρτηση του υπερσυνδέσμου του ερωτηματολογίου σε πλατφόρμα κοινωνικής δικτύωσης στο διαδίκτυο, για το διάστημα 31/3/2020-15/4/2020. Οι συμμετέχοντες ήταν κατανεμημένοι ομοιόμορφα στις ηλικιακές ομάδες των 30 ετών και άνω και στο επίπεδο γραμματικών γνώσεων που συνήθως έχουν οι σύγχρονοι ενήλικες. Αντίθετα η συντριπτική πλειοψηφία τους είναι ιδιωτικοί υπάλληλοι έναντι των άλλων επαγγελματικών ομάδων. Γενικά εκτιμάται ότι, ανεξάρτητα από την μέθοδο που ακολουθήθηκε, το δείγμα που προέκυψε είναι αντιπροσωπευτικό του διαδικτυακού κοινού, προκειμένου να καταδείξουμε μία τάση ως προς το επίπεδο ευαισθητοποίησης ενός τυπικού χρήστη.

Οι συμμετέχοντες ανά ηλικιακή ομάδα φαίνονται στο παρακάτω γράφημα.



Διάγραμμα 6. Συμμετέχοντες στην έρευνα ανά ηλικιακή ομάδα.

Οι συμμετέχοντες ανά μορφωτικό επίπεδο φαίνονται στο παρακάτω διάγραμμα.

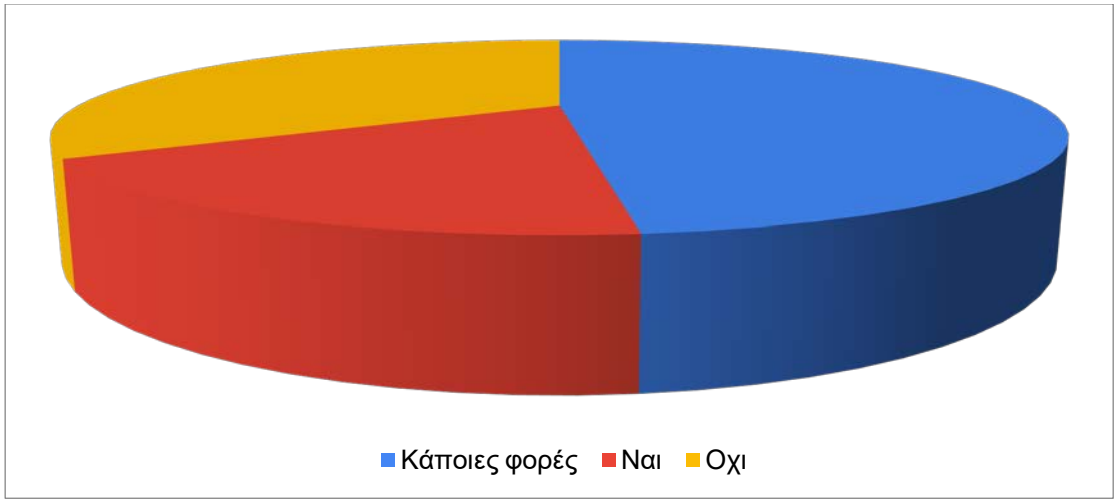


Διάγραμμα 7. Συμμετέχοντες στην έρευνα ανά μορφωτικό επίπεδο.

Οι συμμετέχοντες ανά επαγγελματική κατηγορία φαίνονται στο παρακάτω διάγραμμα.

Διάγραμμα 8. Συμμετέχοντες στην έρευνα ανά επαγγελματική ομάδα.

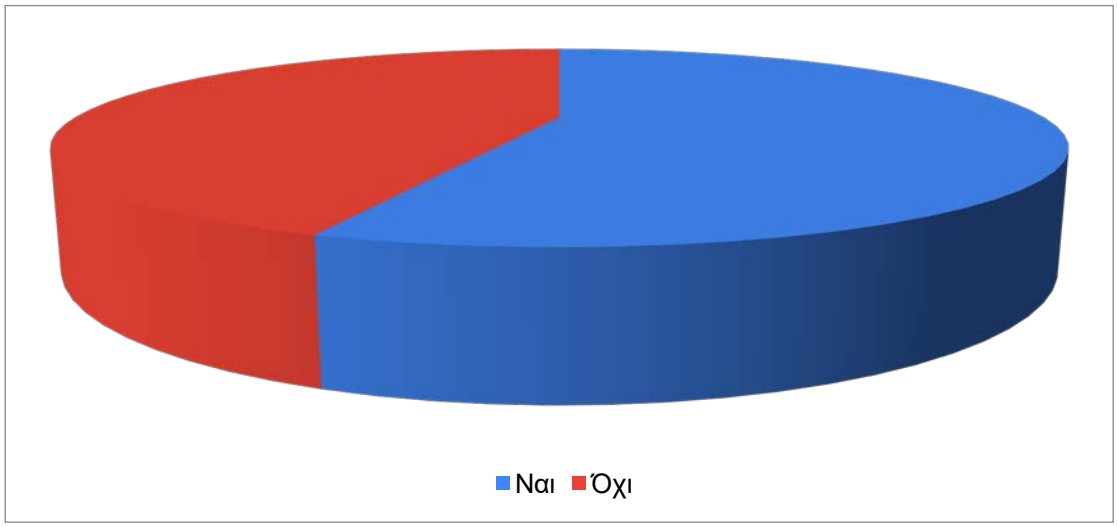
Η ερώτηση υπ' αριθμό 6 αναφέρεται στο ενδιαφέρον των χρηστών για την ενημέρωση τους σχετικά με τους όρους χρήσης και τις πολιτικές προστασίας δεδομένων των εφαρμογών που εγκαθιστούν στην συσκευή τους. Στο επόμενο διάγραμμα φαίνονται οι απαντήσεις τους.



Διάγραμμα 9. Απαντήσεις στην ερώτηση 6.

Από τις απαντήσεις προκύπτει ότι ένας στους τρεις χρήστες αδιαφορεί για αυτούς ενώ λιγότερο από το 20% φροντίζει πάντα να ενημερώνεται.

Η ερώτηση υπ΄ αριθμό 12 αναφέρεται στο κατά πόσο οι χρήστες των εφαρμογών προσέχουν το ποιες από τις δυνατότητες της συσκευής τους χρησιμοποιούν οι εφαρμογές που εγκαθιστούν στην συσκευή τους. Τα αποτελέσματα φαίνονται στο παρακάτω γράφημα.

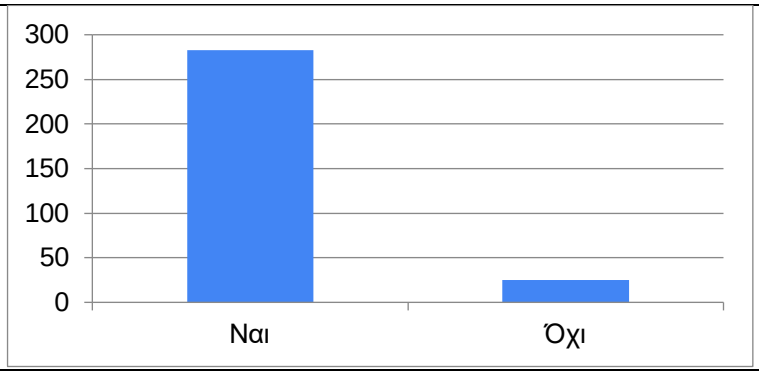


Διάγραμμα 10. Απαντήσεις στην ερώτηση 12.

Από τις απαντήσεις προκύπτει ότι πολύ σημαντικό μέρος των χρηστών δεν δίνει σημασία και αγνοεί το ποιες δυνατότητες χρησιμοποιούν οι εφαρμογές που εγκαθιστούν στις συσκευές τους.

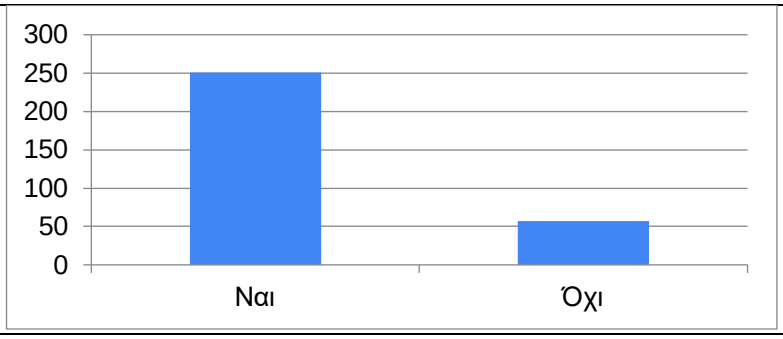
Μία σειρά από ερωτήσεις έχουν σκοπό την δημιουργία εκτιμήσεων για τον βαθμό κατά τον οποίο οι χρήστες των εφαρμογών για έξυπνες κινητές συσκευές είναι «υποψιασμένοι» για τους μη νόμιμους τρόπους που μπορεί να χρησιμοποιηθούν τα προσωπικά τους δεδομένα. Οι ερωτήσεις και οι απαντήσεις παρουσιάζονται στους παρακάτω πίνακες.

Ερώτηση 14: Πιστεύετε ότι οι επιλογές, οι πληροφορίες και η χρήση των εφαρμογών καταγράφονται από τους παρόχους των εφαρμογών;	
Ναι	283
Όχι	25



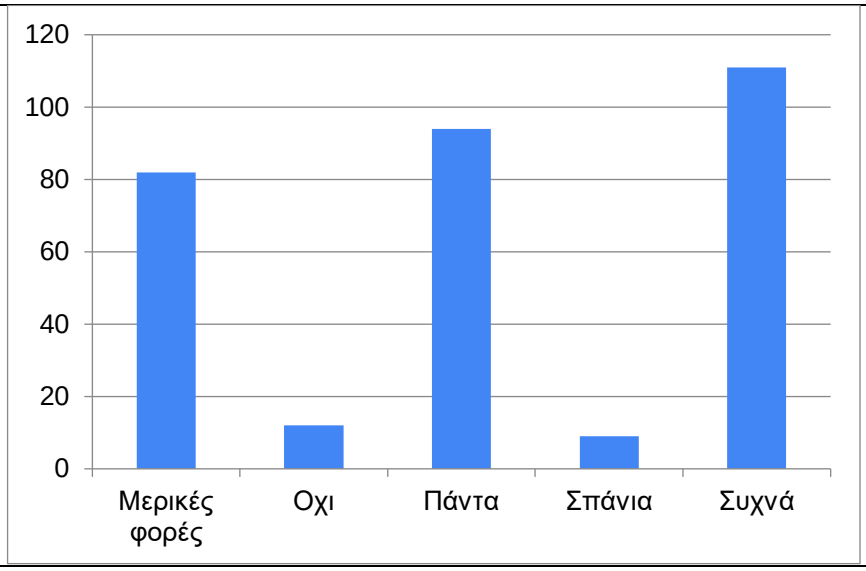
Πίνακας 1: Απαντήσεις ερώτησης 14

15. Πιστεύετε ότι οι επιλογές, οι πληροφορίες και η χρήση των εφαρμογών μοιράζονται σε τρίτους;	
Ναι	251
Όχι	57



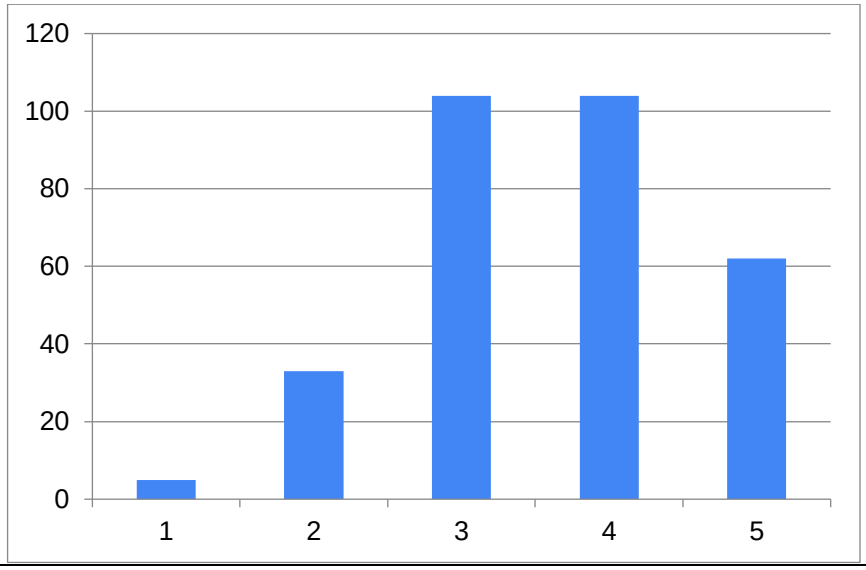
Πίνακας 2: Απαντήσεις ερώτησης 15

16. Ακόμα και μετά τη διαγραφή του ιστορικού περιήγησης, του λογαριασμού ή εφαρμογής, πιστεύετε διατηρούνται «κάπου» πληροφορίες για εσάς;	
Μερικές φορές	82
Όχι	12
Πάντα	94
Σπάνια	9
Συχνά	111



Πίνακας 3: Απαντήσεις ερώτησης 16

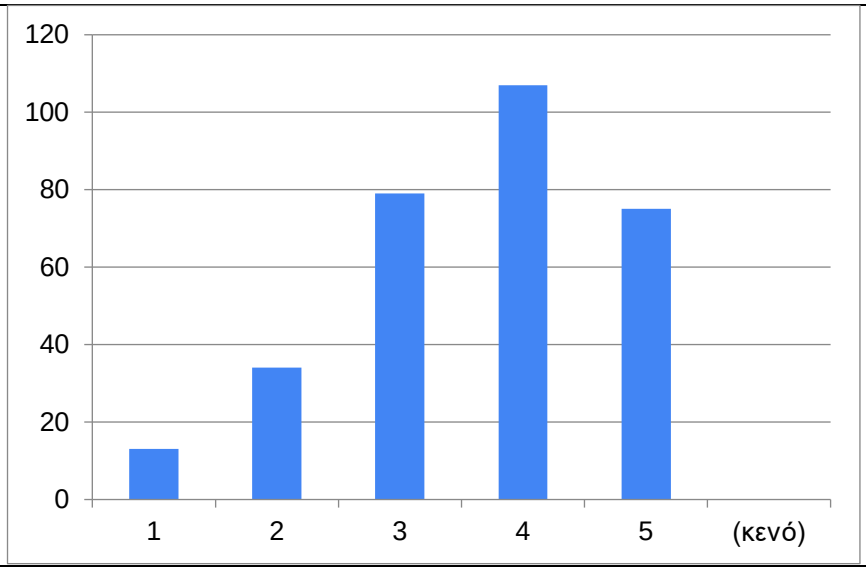
17. Πιστεύετε ότι παραβιάζεται η ιδιωτική σας ζωή στις ηλεκτρονικές επικοινωνίες μέσω των εφαρμογών;	
1 (Λίγο)	5
2	33
3	104
4	104
5 (Πολύ)	62



Πίνακας 4: Απαντήσεις ερώτησης 17

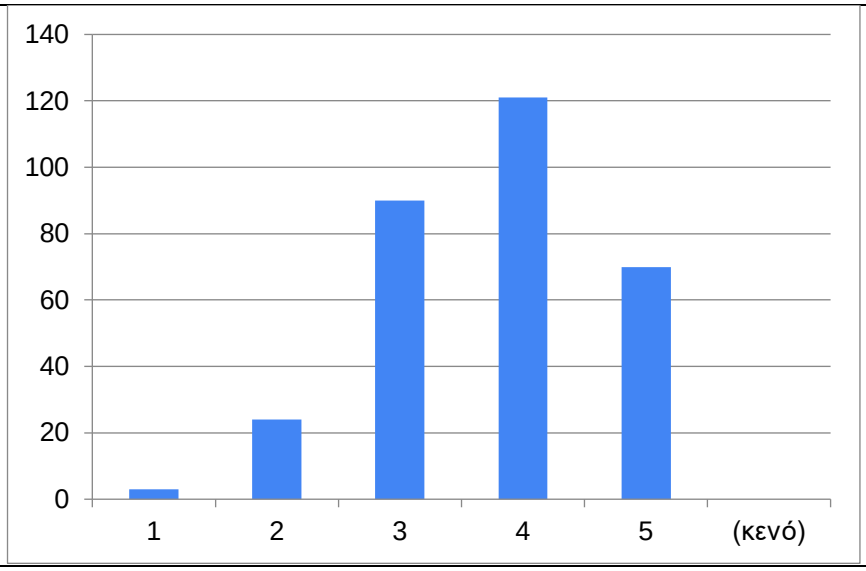
18. Πιστεύετε τα δεδομένα σας πωλούνται ή αξιοποιούνται για σκοπούς από τρίτους;	
1 (Λίγο)	13
2	34
3	79

4	107
5 (Πολύ)	75



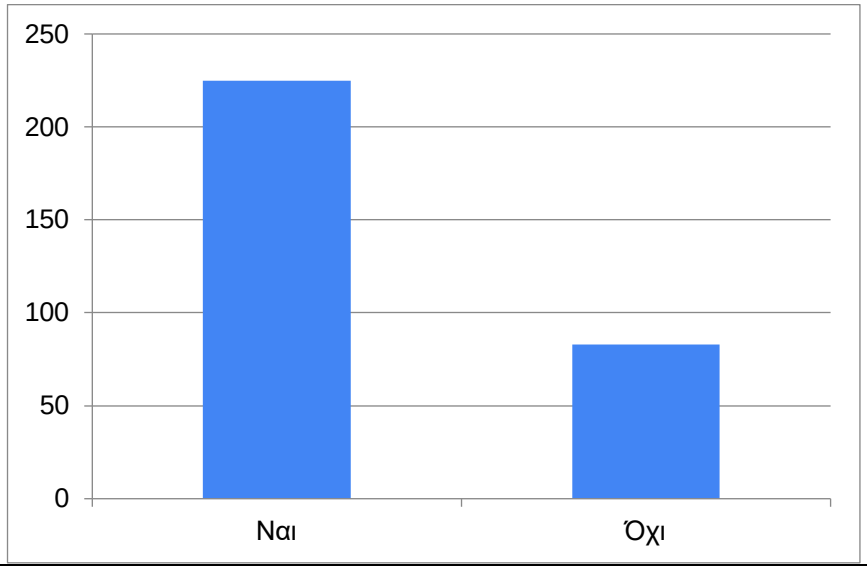
Πίνακας 5: Απαντήσεις ερώτησης 18

19. Πιστεύετε ότι ο συγχρονισμός συσκευών οδηγεί στην μεγαλύτερη απόκτηση δεδομένων για τους χρήστες	
1 (Λίγο)	3
2	24
3	90
4	121
5 (Πολύ)	70



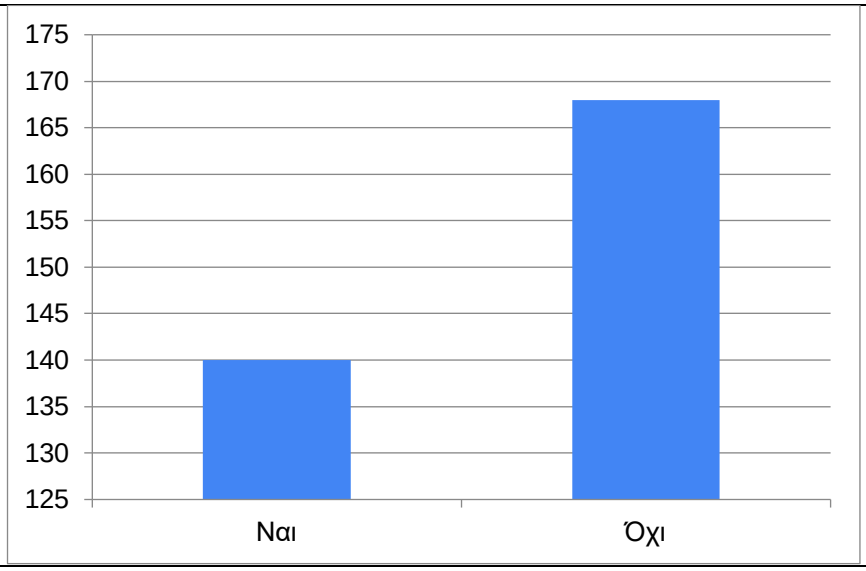
Πίνακας 6: Απαντήσεις ερώτησης 19

23. Πιστεύετε ότι η δυνατότητα φωνητικής γραφής θα μπορούσε μελλοντικά να συλλέγει επιπλέον δεδομένα για την προσωπική σας ζωή;	
Ναι	225
όχι	83



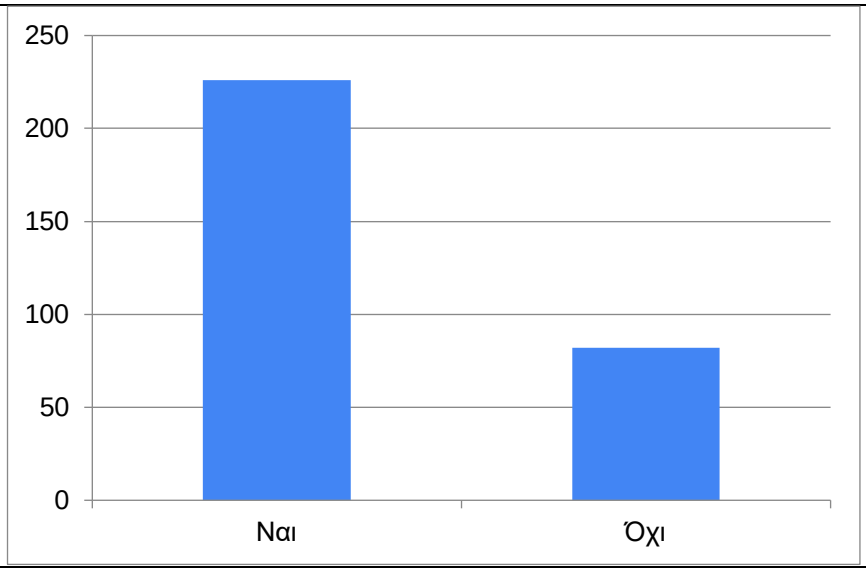
Πίνακας 7: Απαντήσεις ερώτησης 23

25. Πιστεύετε ότι το δαχτυλικό σας αποτύπωμα που εισάγετε για το ξεκλείδωμα του κινητού βρίσκεται καταχωρημένο και κάπου αλλού;	
Ναι	140
όχι	168



Πίνακας 8: Απαντήσεις ερώτησης 25

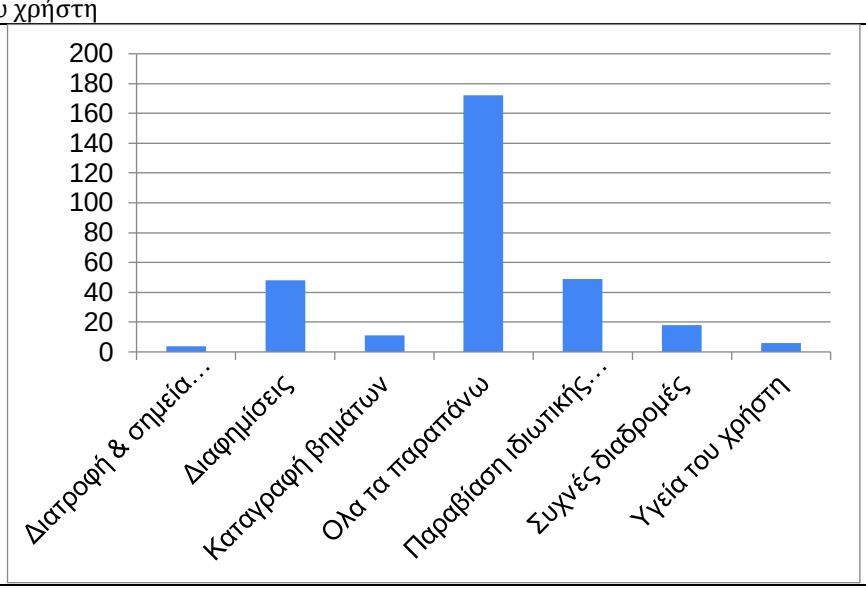
26. Πιστεύετε ότι οι συνομιλίες σας θα μπορούσαν να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων για εσάς;	
Ναι	226
όχι	82



Πίνακας 9: Απαντήσεις ερώτησης 26

27. Πιστεύετε ότι ο μόνιμος εντοπισμός της συσκευής σας συμβάλει στην:	
Διατροφή & σημεία συναλλαγών	4
Διαφημίσεις	48
Καταγραφή βημάτων	11
Όλα τα παραπάνω	172
Παραβίαση ιδιωτικής ζωής & ελευθερίας	49

Συχνές διαδρομές	18
Υγεία του χρήστη	6

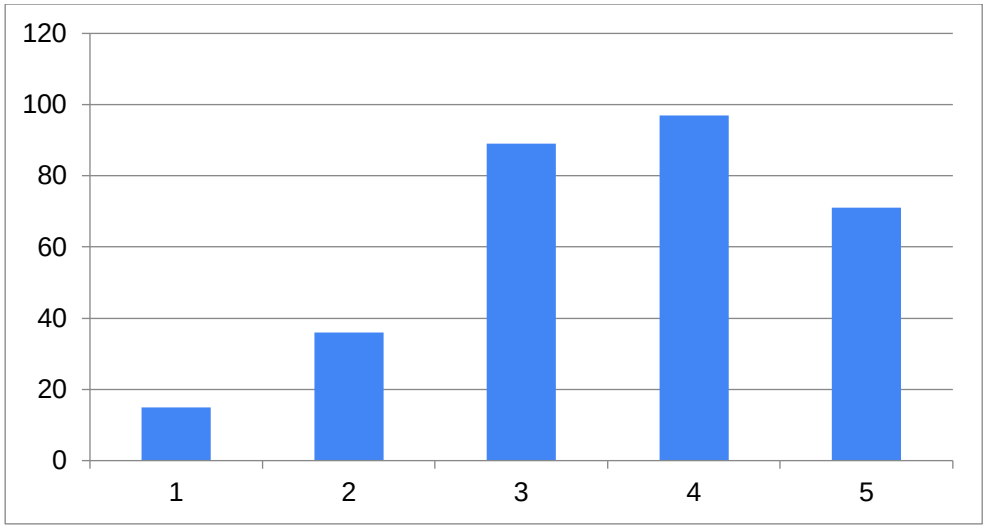


Πίνακας 10: Απαντήσεις ερώτησης 27

Από τα παραπάνω αποτελέσματα προκύπτει ότι ο μέσος χρήστης είναι «υποψιασμένος» για τις παράνομες ή/και κρυφές δυνατότητες διαχείρισης και επεξεργασίας των προσωπικών του δεδομένων. Ωστόσο ένα μεγάλο ποσοστό επιμένει να μην ελέγχει επαρκώς τις δυνατότητες των εφαρμογών που εγκαθιστούν ως προς την δυνατότητα τους να διαχειρίζονται και να επεξεργάζονται τα προσωπικά τους δεδομένα.

4.3 Γνώση επί του GDPR

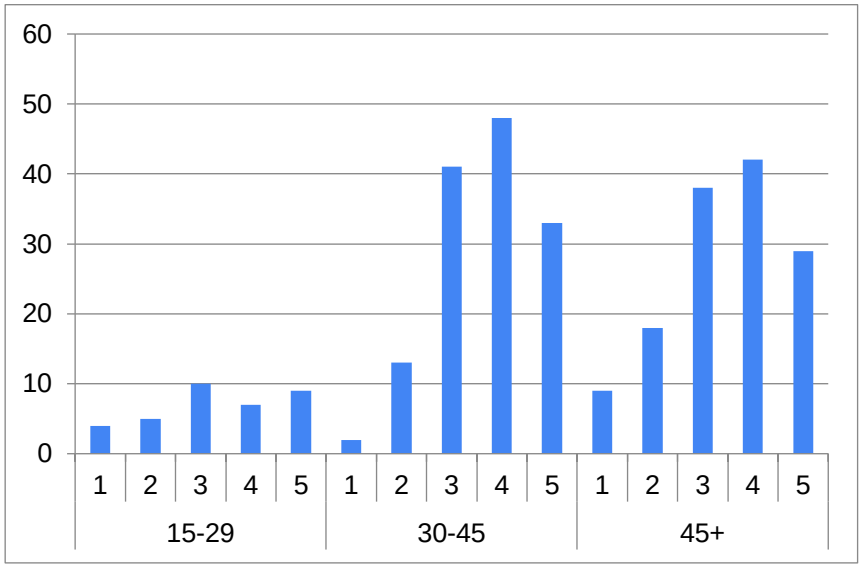
Μία ερώτηση του ερωτηματολογίου αφορούσε το κατά πόσο οι συμμετέχοντες γνωρίζουν τον Γενικό Κανονισμό που διέπει την διαχείριση και επεξεργασία των προσωπικών δεδομένων από τις εφαρμογές για κινητές συσκευές. Γενικά οι συμμετέχοντες απάντησαν όπως φαίνεται στο παρακάτω γράφημα (Κλίμακα 1 έως 5 αντιστοιχεί σε κλίμακας γνώσης από καθόλου ως απόλυτη).



Διάγραμμα 4: Επίπεδο γνώσης του GDPR

Από τα αποτελέσματα προκύπτει ότι σχεδόν οι μισοί χρήστες των εφαρμογών έχουν καλή γνώση του GDPR.

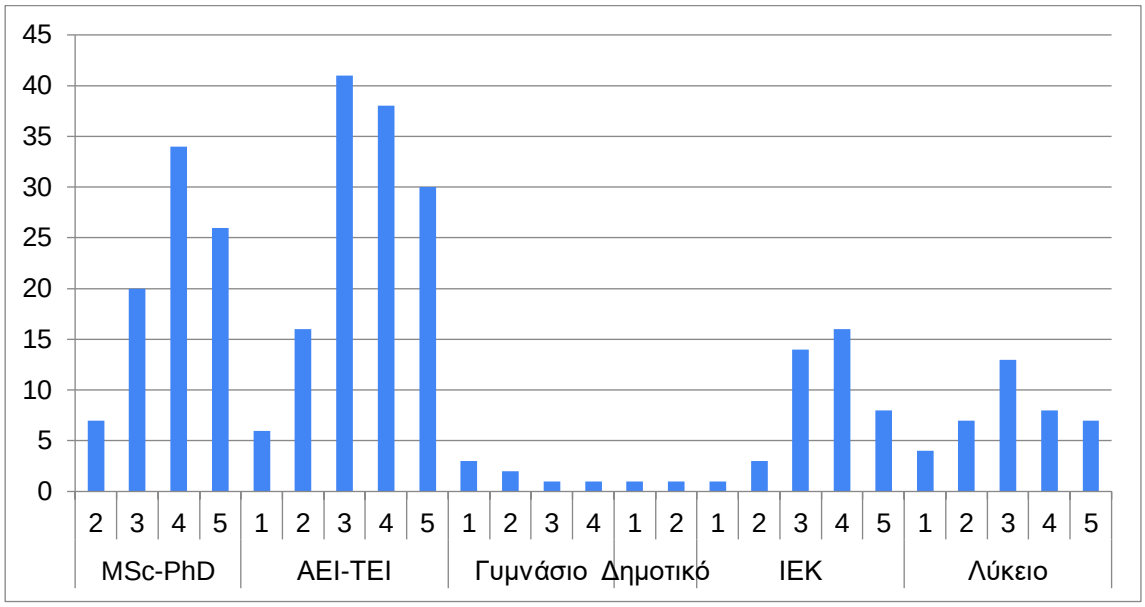
Ο βαθμός γνώσης σε σχέση με την ηλικιακή ομάδα των χρηστών φαίνεται στο παρακάτω γράφημα



Διάγραμμα 5: Επίπεδα γνώσης του GDPR σε σχέση με την ηλικιακή ομάδα

Αν και τα αποτελέσματα δεν διαφοροποιούνται πολύ σε σχέση με την γενική κατάσταση, φαίνεται οι άνθρωποι μικρότερης ηλικίας να είναι πιο ενημερωμένοι.

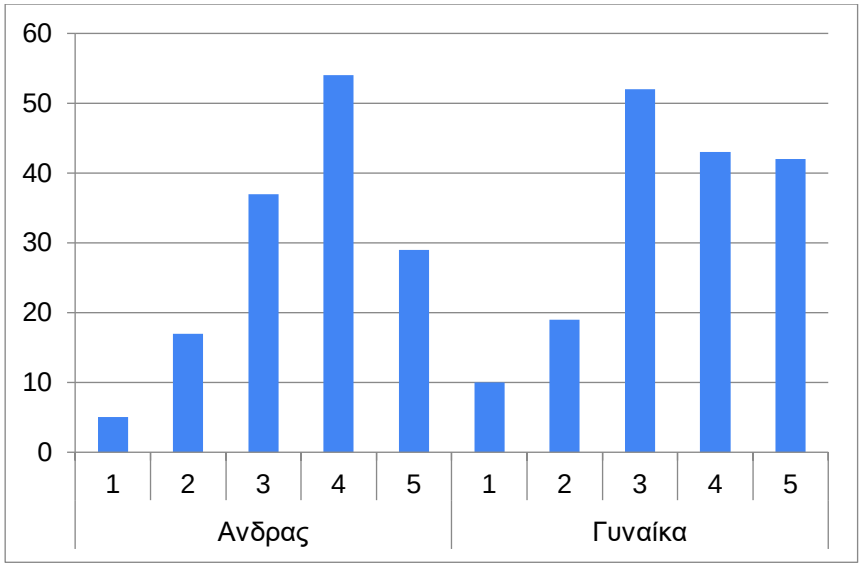
Στο παρακάτω γράφημα προβάλλεται η σχέση γνώσης του GDPR σε σχέση με τις γραμματικές γνώσεις.



Διάγραμμα 6: Επίπεδα γνώσης του GDPR σε σχέση με το επίπεδο μόρφωσης

Από τα αποτελέσματα προκύπτει ότι οι άνθρωποι με χαμηλότερο επίπεδο γραμματικών γνώσεων είναι πιο πιθανό να αγνοούν τον GDPR.

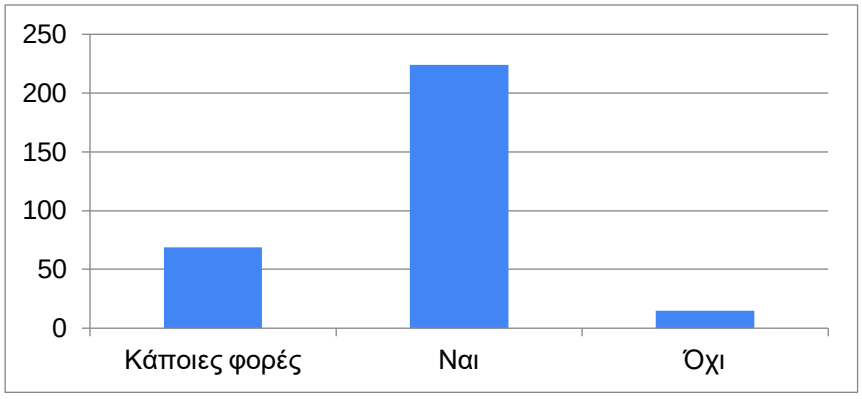
Στο επόμενο διάγραμμα φαίνεται το πώς σχετίζεται το φύλο του χρήστη με τον βαθμό γνώσης του GDPR.



Διάγραμμα 7: Επίπεδα γνώσης του GDPR σε σχέση με το φύλο.

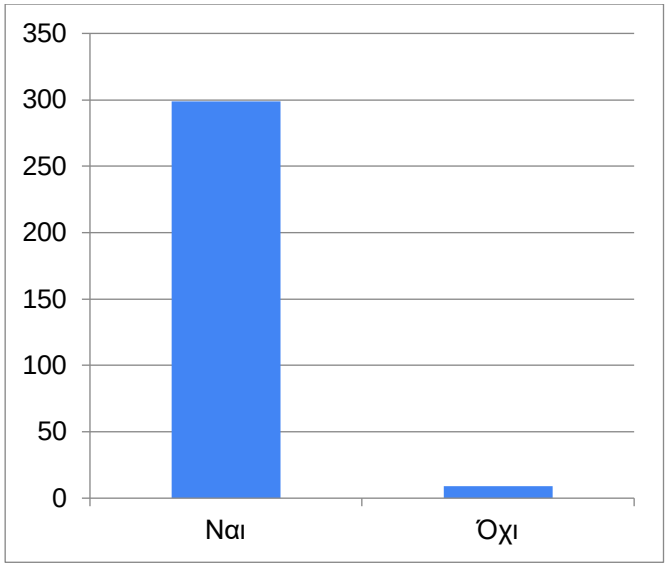
Από αυτό φαίνεται ότι οι άνδρες γενικότερα έχουν καλύτερη γνώση του GDPR.

Στην έρευνα αναζητήθηκε και το επίπεδο του ενδιαφέροντος των χρηστών για εφαρμογές που κατά κύριο λόγο διαχειρίζονται και επεξεργάζονται προσωπικά δεδομένων των χρηστών τους. Οι περισσότεροι χρήστες διαπιστώνουν ότι κατά την χρήση ορισμένων εφαρμογών εμφανίζονται διαφημίσεις, όπως φαίνεται στο επόμενο διάγραμμα.



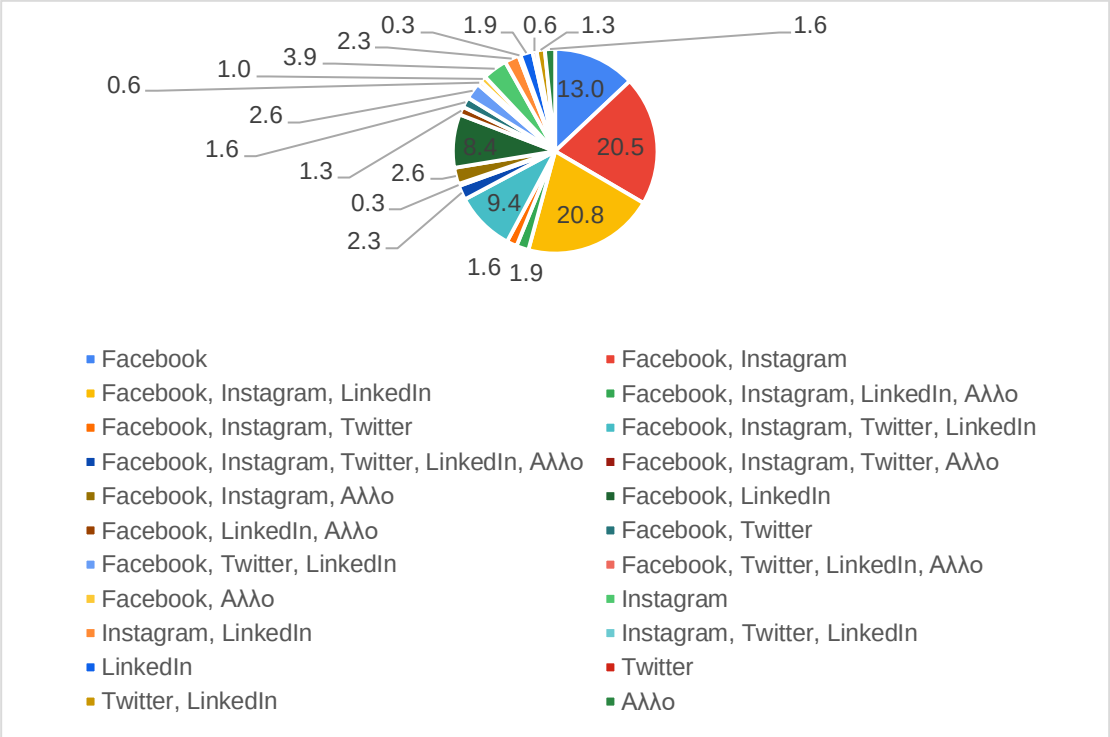
Διάγραμμα 8: Εμφάνιση διαφημίσεων στις εφαρμογές

Σχεδόν όλοι οι συμμετέχοντες δήλωσαν ότι εγκαθιστούν στην έξυπνη κινητή συσκευή τους εφαρμογές που διατίθενται από τα αντίστοιχα ηλεκτρονικά καταστήματα.



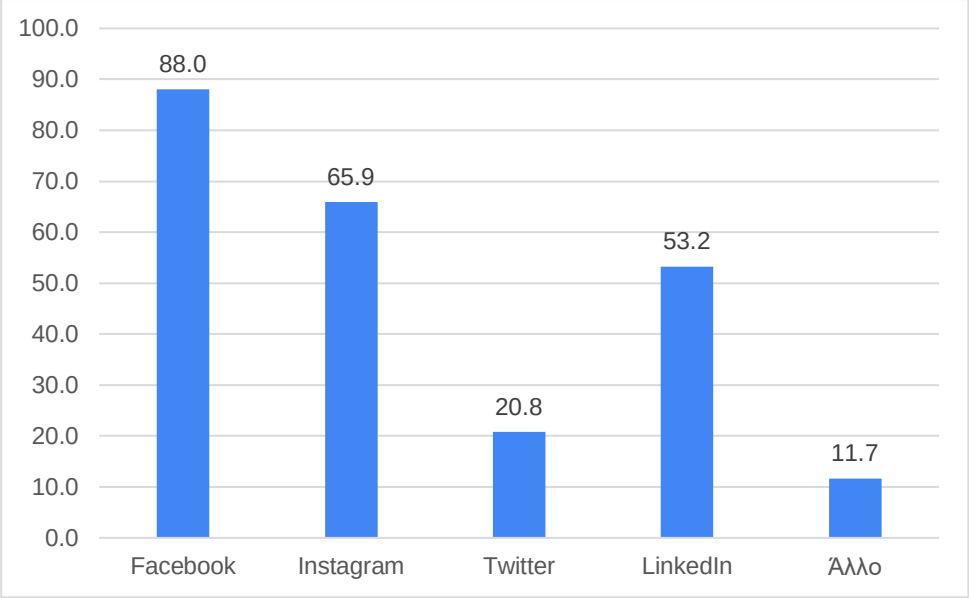
Διάγραμμα 9: Εγκατάσταση εφαρμογών

Στο παρακάτω γράφημα φαίνεται πως οι περισσότεροι από τους συμμετέχοντες έχουν τουλάχιστον έναν λογαριασμό στο Facebook, Twitter, Instagram ή Twitter.



Διάγραμμα 10: Χρήση Social Media

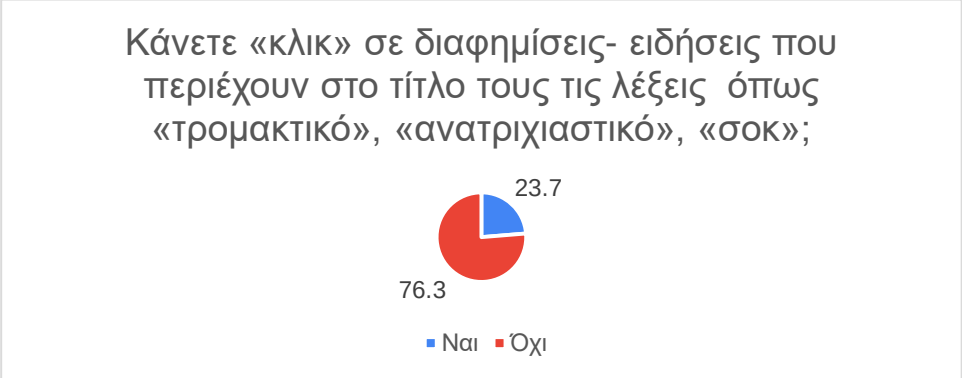
Το πιο δημοφιλές μεταξύ των κοινωνικών δικτύων είναι το Facebook με τα Instagram και LinkedIn να ακολουθούν με σημαντικό μερίδιο.



Διάγραμμα 11: Δημοφιλέστερα Social Networks

Από τις παραπάνω παρατηρήσεις συνάγεται το συμπέρασμα ότι οι χρήστες στην συντριπτική τους πλειοψηφία συνηθίζουν να εγκαθιστούν εφαρμογές στις συσκευές τους αλλά και διατηρούν λογαριασμούς σε κοινωνικά δίκτυα. Είναι δηλαδή εκτεθειμένοι σε δυνητικές προσπάθειες παράνομης κτήσης και επεξεργασίας των προσωπικών τους δεδομένων.

Σημαντικό ποσοστό φαίνεται να παρασύρεται από βαρύγδουπους τίτλους σε διαφημίσεις και να ακολουθεί επικίνδυνους συνδέσμους, όπως φαίνεται στο παρακάτω σχήμα.



Διάγραμμα 12: Ερώτηση 11

Μεγάλο ποσοστό επίσης δείχνει μια προτίμηση στο να συμπληρώνει ερωτηματολόγια καταγραφής του προφίλ δίνοντας την ευκαιρία σε ενδιαφερομένους να σκιαγραφήσουν εύκολα το προφίλ τους.

Διάγραμμα 13: Ερώτηση 20

Γενικότερα φαίνεται ότι οι περισσότεροι χρήστες χρησιμοποιούν τα κοινωνικά δίκτυα και έτσι δίνουν έμμεσα πληροφορίες για το προφίλ τους. Επίσης υπάρχει ένα σημαντικό ποσοστό αφελών ανθρώπων που παρέχουν προσωπικές τους πληροφορίες μόνο μετά από προτροπή προς τούτο. Οι χρήστες φαίνονται ενημερωμένοι για την πιθανότητα διαρροής των προσωπικών τους δεδομένων ως συνέπεια χρήσης διαδικτυακών εφαρμογών ενώ σε γενικές γραμμές γνωρίζουν για τον GDPR. Ωστόσο υπάρχει και ένα σημαντικό ποσοστό χρηστών που ή αγνοεί την ύπαρξη των κινδύνων, ή/και αγνοεί τις συνέπειες τους. Ακόμα υπάρχουν πολλοί χρήστες που δεν γνωρίζουν με ποιους τρόπους μπορούν να εξασφαλιστούν έναντι των κινδύνων αυτών.

Κεφάλαιο 5
Συμπεράσματα

Τα προσωπικά δεδομένα του πληθυσμού διαχρονικά ήταν πολύτιμα, ως στενά συνυφασμένα με το θεμελιώδες ατομικό δικαίωμα της προστασίας τους. Στην σύγχρονη εποχή που χαρακτηρίζεται από την ραγδαία εξέλιξη των τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών αλλά και τον έντονο ανταγωνισμό για επικράτηση σε κάθε τομέα της ανθρώπινης δραστηριότητας, αποκτούν μεγαλύτερη αξία. Αποτελούν βασική παράμετρο για την λήψη αποφάσεων σε στρατηγικό και τακτικό επίπεδο της σχεδίασης δραστηριοποίησης των οργανισμών. Στους κερδοσκοπικούς οργανισμούς συλλέγονται για να προσδιορίσουν τα χαρακτηριστικά, τις τάσεις και την συμπεριφορά του καταναλωτικού κοινού. Με βάση αυτά τίθενται οι επιχειρησιακοί στόχοι. Στην συνέχεια χρησιμοποιούνται για να εκτιμάται ο βαθμός επίτευξη των στόχων αυτών. Σε επίπεδο διακυβέρνησης χρησιμοποιούνται για να προσδιορίζονται οι τάσεις και η συμπεριφορά της κοινής γνώμης.

Οι έξυπνες κινητές συσκευές αποτελούν μέρος της ζωής του σύγχρονου ανθρώπου σε βαθμό τέτοιο που να είναι σε θέση να τον προσδιορίζουν. Είναι χαρακτηριστικό ότι χρησιμοποιούνται σε ορισμένες περιπτώσεις ακόμα και για την ταυτοποίηση τους. Ο τρόπος με τον οποίο χρησιμοποιούνται μπορεί να παρέχει με έμμεσο ή άμεσο τρόπο πληροφορίες σχετικά με το προφίλ του χρήστη τους στις οντότητες που διαχειρίζονται την λειτουργία των εφαρμογών που χρησιμοποιούν. Κατά συνέπεια γενικότερα οι έξυπνες κινητές συσκευές είναι πολύ σημαντικές για την ασφάλεια των προσωπικών δεδομένων των σύγχρονων ανθρώπων. Κατ΄ επέκταση οι εφαρμογές που είναι εγκατεστημένες και χρησιμοποιούνται ρυθμίζουν το πώς θα χρησιμοποιηθούν τα δεδομένα αυτά.

Η χρήση των εφαρμογών αυτών θα πρέπει να γίνεται με προσοχή προκειμένου να μην παρατηρείται διαρροή προσωπικών δεδομένων σε αναρμόδιες οντότητες.

Ο όρος προσοχή αναλύεται σε δύο βασικές συνιστώσες: την νομική και την τεχνική. Η κάθε μορφή διακυβέρνηση, είτε σε διεθνές είτε σε εθνικό επίπεδο, είναι ανάγκη να διασφαλίζει σε επαρκή βαθμό νομικά. Οι πολίτες, καθώς χρησιμοποιούν διάφορες διαδικτυακές εφαρμογές είναι συχνά υποχρεωμένοι να μεταδίδουν μέσω διαφορετικών καναλιών επικοινωνίας τα προσωπικά τους δεδομένα σε οντότητες με ποικίλους προσανατολισμούς. Παράλληλα με τις εμφανείς μεταδόσεις των στοιχείων, πολλές εφαρμογές επιχειρούν πλήθος αποστολών προσωπικών δεδομένων στο παρασκήνιο χωρίς να το γνωρίζει ο χρήστης.

Η νομική προστασία των δεδομένων που συλλέγονται με ή χωρίς την συγκατάθεση του χρήστη, άργησε να αποκατασταθεί καθώς οι εξελίξεις στους κλάδους της πληροφορικής και των τηλεπικοινωνιών υπήρξαν ραγδαίες και αιφνιδίασαν τις οντότητες εκείνες που αποστολή τους είναι η νομική θωράκιση των πολιτών. Ο GDPR αποτελεί μία στέρεη βάση για την ανάπτυξη νομικής ασπίδας προστασίας των χρηστών των διαδικτυακών εφαρμογών γενικότερα. Εξασφαλίζει σε επίπεδο πρόληψης τα υποκείμενο των προσωπικών δεδομένων καθώς θέτει συγκεκριμένες προϋποθέσεις για τη νόμιμη συλλογή και περαιτέρω επεξεργασία προσωπικών δεδομένων, όπως η συλλογή και επεξεργασία για σαφείς, ρητούς και διαφανείς σκοπούς, ενώ επίσης σε πολλές περιπτώσεις μπορεί να θεωρηθεί νόμιμη η συλλογή, διατήρηση και περαιτέρω επεξεργασία προσωπικών δεδομένων, μόνο αν αυτή από σαφή ελεύθερη συναίνεση, εν πλήρει επιγνώσει Οι κυβερνήσεις των κρατών κλήθηκαν να υιοθετήσουν στην νομοθεσία τους, τους κανόνες του GDPR. Αυτό σταδιακά συνέβη και μάλιστα στις περισσότερες περιπτώσεις προβλέπονται μεγάλες ποινές για την παραβίαση τους. Η εξέλιξη αυτή συνδράμει στην ισχυροποίηση της προστασίας των ευαίσθητων δεδομένων σε δύο επίπεδα. Σε επίπεδο πρόληψης αυξάνοντας το ρίσκο παραβίασης των κανόνων, αλλά και σε επίπεδο καταστολής καθώς

προβλέπονται τόσο η παραδειγματική τιμωρία των παραβατών όσο και η αποκατάσταση της ζημιάς που υφίσταται το θύμα. Σε κάθε περίπτωση χρειάζεται συνεχής έλεγχος και αξιολόγηση των εξελίξεων στις τεχνολογίες του διαδικτύου ώστε τόσο οι κανόνες του GDPR όσο και οι κοινοτικές, διεθνείς και εθνικές νομοθεσίες να επικαιριοποιούνται και να προσαρμόζονται στις νέες απαιτήσεις.

Ο σημαντικότερος παράγοντας που επηρεάζει την ασφάλεια των προσωπικών δεδομένων είναι ο βαθμός κατά τον οποίο ο χρήστης γνωρίζει σε τεχνικό επίπεδο:

- Τρόπους με τους οποίους μπορεί να μεταδοθούν τα προσωπικά του δεδομένα μέσω των διαδικτυακών εφαρμογών
- Τρόπους που μπορεί να χρησιμοποιηθούν τα δεδομένα και – κυρίως – πως μπορεί να χρησιμοποιηθούν εναντίον του
- Τρόπους με τους οποίους θα μπορεί να ελέγχει πότε, που και με ποιον τρόπο μεταδίδονται τα δεδομένα του
- Τρόπους για την αποτροπή μετάδοσης των προσωπικών του δεδομένων.
- Τρόπους ελέγχου της λειτουργίας των εγκατεστημένων εφαρμογών ώστε να είναι σε θέση να γνωρίζει πότε κάθε εφαρμογή πραγματοποιεί μεταδόσεις και που.

Με δεδομένο ότι οι χρήστες κατέχουν την στοιχειώδη απαραίτητη τεχνική γνώση, είναι καλή πρακτική για αυτούς να:

- Διατηρούν σε λειτουργία και να αξιοποιούν έμπιστο λογισμικό (π.χ. Lumen) το οποίο έχει την δυνατότητα σε φιλικές διεπαφές να παρουσιάζει την διαδικτυακή κίνηση που περνάει από την συσκευή τους και να τους δίνει την δυνατότητα να την διακόπτουν όταν θεωρούν ότι δεν ανταποκρίνεται στην χρήση που κάνουν.
- Να εγκαθιστούν και να χρησιμοποιούν μόνο έμπιστες εφαρμογές.

- Να δίνουν προσοχή στα δικαιώματα που απαιτεί κάθε εφαρμογή που εγκαθιστούν στην συσκευή τους προκειμένου να λειτουργήσει. Επίσης είναι προς όφελος τους να δίνουν προσοχή στις σημειώσεις που παρουσιάζουν οι κατασκευαστές εφαρμογών και που αφορούν στην διαχείριση των προσωπικών δεδομένων.

Οι σύγχρονοι χρήστες στην πλειοψηφία τους δείχνουν να είναι ενημερωμένοι για το πώς τα προσωπικά τους δεδομένα διαχειρίζονται από τις εφαρμογές. Οι περισσότεροι επίσης γνωρίζουν τους κινδύνους που εγκυμονεί η απόκτηση τους από κακόβουλους φορείς και ανθρώπους. Ωστόσο το ποσοστό των χρηστών που δηλώνει άγνοια για τους κινδύνους και την νομοθεσία που διέπει τα προσωπικά δεδομένα που διαχειρίζονται οι διαδικτυακές εφαρμογές είναι μεγάλο ιδιαίτερα αν - αναλογιζόμενοι ότι σχεδόν όλοι οι άνθρωποι στον πλανήτη έχουν πρόσβαση στο διαδίκτυο μέσω έξυπνης κινητής συσκευής – γίνει αναγωγή σε απόλυτους αριθμούς. Η κατάσταση είναι πιο δύσκολη στις μεγαλύτερες ηλικίες. Εκτιμάται ότι με τις συνεχείς προσπάθειες ευαισθητοποίησης των χρηστών, στο μέλλον το σύνολο τους θα γνωρίζει την αξία της προστασίας των προσωπικών τους δεδομένων. Αυτό θα είναι και το σημαντικότερο βήμα για την γενικότερη εξασφάλιση τους.

Οι τεχνικές γνώσεις των χρηστών σε ζητήματα που άπτονται της ασφάλειας των δεδομένων τους είναι επίσης περιορισμένες. Ωστόσο είναι τόσο μεγάλη η διείσδυση της χρήσης των διαδικτυακών εφαρμογών τόσο ποσοτικά όσο και ως προς την ποικιλία των προσανατολισμών τους, που θα αναγκάσει τους χρήστες να αναζητήσουν την απόκτηση επιπλέον τεχνικών γνώσεων για να ανταποκρίνονται στις απαιτήσεις τους. Αυτό θα τους κάνει πιο υποψιασμένους στο πως οι διαδικτυακές εφαρμογές θα μπορούσαν να χρησιμοποιήσουν τα προσωπικά τους δεδομένα και πιο ευέλικτους όταν διαπιστώνουν ότι χρησιμοποιούνται με τρόπο που δεν εγκρίνουν. Όταν το σύνολο των χρηστών θα έχει φθάσει σε τέτοιο επίπεδο, μεγάλο ποσοστό των κακόβουλων φορέων και ατόμων αναμένεται ότι θα αναγκαστεί να απομακρυνθεί από τέτοιες δραστηριότητες, καθώς η δεξαμενή των δυνητικών τους θυμάτων θα είναι μικρή.

Πρέπει επίσης να σημειωθεί ότι είναι εξαιρετικά σημαντικό η τεχνολογία να μπορέσει να υποβοηθήσει τους χρήστες στο να προστατεύονται από τους κινδύνους που εγείρονται από την επεξεργασία προσωπικών τους δεδομένων. Αυτό μπορεί να είναι ιδιαίτερα αποτελεσματικό σε περιπτώσεις όπου οι κίνδυνοι οφείλονται σε 'εσφαλμένες' ενέργειες των χρηστών, λόγω της άγνοιάς τους (π.χ. ανάρτηση προσωπικών πληροφοριών οι οποίες είναι 'ευαίσθητου' χαρακτήρα). Προς αυτήν την κατεύθυνση, αξίζει ενδεικτικά να αναφερθεί μια πρόσφατη ερευνητική προσπάθεια (εφαρμογή PrivacyBot), που αποσκοπεί στην έγκαιρη ανίχνευση 'επικίνδυνων' κειμένων που πρόκειται να αναρτήσει ένας χρήστης, προκειμένου να λάβει ειδοποίηση και να επανεξετάσει την ανάρτηση που πρόκειται να κάνει. (Welderufael B. Tesfay & Kai Rannenberg, 2019)

Παράρτημα Α
Ερωτήσεις στις οποίες απάντησαν οι συμμετέχοντες στην έρευνα

1. Φύλο

2. Ηλικία

3. Μορφωτικό επίπεδο

4. Επάγγελμα

5. Εγκαθιστάτε εφαρμογές στο Smartphone;

6. Εάν εγκαθιστάτε, διαβάζετε τους όρους χρήσης/πολιτική προστασίας δεδομένων αυτών;

7. Κατά την χρήση εφαρμογών εμφανίζονται διαφημίσεις σχετικές με τις προηγούμενες αναζητήσεις σας στο διαδίκτυο;

8. Αξιοποιεί το Smartphone την τοποθεσία σας;

9. Χρησιμοποιείτε μέσα- εφαρμογές κοινωνικής δικτύωσης και ποιες;

10. Χρησιμοποιείτε κάποιες από τις παρακάτω δημοφιλείς εφαρμογές (επιλέξτε έως τέσσερις εφαρμογές);

11. Κάνετε «κλικ» σε διαφημίσεις- ειδήσεις που περιέχουν στο τίτλο τους τις λέξεις όπως «τρομακτικό», «ανατριχιαστικό», «σοκ»;

12. Παρατηρείτε προσεκτικά τις άδειες που ζητούν οι εφαρμογές στην συσκευή σας;

13. Γνωρίζετε για τον Ευρωπαϊκό Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR);

14. Πιστεύετε ότι οι επιλογές, οι πληροφορίες και η χρήση των εφαρμογών καταγράφονται από τους παρόχους των εφαρμογών

15. Πιστεύετε ότι οι επιλογές, οι πληροφορίες και η χρήση των εφαρμογών μοιράζονται σε τρίτους;

16. Ακόμα και μετά τη διαγραφή του ιστορικού περιήγησης, του λογαριασμού ή εφαρμογής, πιστεύετε διατηρούνται «κάπου» πληροφορίες για εσάς;

17. Πιστεύετε ότι παραβιάζεται η ιδιωτική σας ζωή στις ηλεκτρονικές επικοινωνίες μέσω των εφαρμογών;

18. Πιστεύετε τα δεδομένα σας πωλούνται ή αξιοποιούνται για σκοπούς από τρίτους;

19. Πιστεύετε ότι ο συγχρονισμός συσκευών οδηγεί στην μεγαλύτερη απόκτηση δεδομένων για τους χρήστες

20. Συμμετέχετε στην συμπλήρωση ερωτηματολογίων- quiz ή τεστ προσωπικότητας στο διαδίκτυο

21. Πιστεύετε ότι τα προσωπικά στοιχεία, οι προτιμήσεις και η κοινωνική σας ζωή διαμορφώνουν την εξέλιξη των μελλοντικών τάσεων; (μελλοντικές τάσεις π.χ. μουσική βιομηχανία, παραγωγή και προώθηση προϊόντων, προσφορά υπηρεσιών κ.α).

22. Πιστεύετε ότι η ελεύθερη βούληση επηρεάζεται μέσω των διαφημίσεων του ίντερνετ και των εφαρμογών;

23. Πιστεύετε ότι η δυνατότητα φωνητικής γραφής θα μπορούσε μελλοντικά να συλλέγει επιπλέον δεδομένα για την προσωπική σας ζωή;

24. Ποια εφαρμογή πιστεύετε ότι συλλέγει παραπάνω δεδομένα για την προσωπική σας ζωή;

25. Πιστεύετε ότι το δαχτυλικό σας αποτύπωμα που εισάγετε για το ξεκλείδωμα του κινητού βρίσκεται καταχωρημένο και κάπου αλλού;

26. Πιστεύετε ότι οι συνομιλίες σας θα μπορούσαν να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων για εσάς;

27. Πιστεύετε ότι ο μόνιμος εντοπισμός της συσκευής σας συμβάλει στην:

Βιβλιογραφικές αναφορές

Amatya, S. (2013, 10 19). *Cross-Platform Mobile Development: An Alternative to Native Mobile Development.* Ανάκτηση από diva-portal: https://www.diva-portal.org/smash/get/diva2:664680/fulltext01.pdf

apptentive. (2015, 1 1). *15 Mobile App Development Trends To Look Out For In 2015*. Ανάκτηση από apptentive: https://www.apptentive.com/blog/2015/02/23/15-mobile-app-development-trends-look-2015/

COMMISSION, E. (2017, 1 10). Ανάκτηση από REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0368

Commission, E. (2019). *Special Eurobarometer 487a.*

Commission, E. (2019). Special Eurobarometer 487a. 26.

dataprivacymanager. (2020, 8 20). *100 Data Privacy and Data Security statistics for 2020.* Ανάκτηση από dataprivacymanager: https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/

enisa. (2017, 11 1). *Privacy and data protection in mobile applications.* enisa. Ανάκτηση από enisa.

Europa. (2020, 3 3). *GDPR in numbers.* Ανάκτηση από europa: https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf

eurostat. (2020, 8 1). *Statistical Confidentiality and PersonalL Data Protection.* Ανάκτηση από europa: https://ec.europa.eu/eurostat/web/microdata/statistical-confidentiality-and-personal-data-protection

Exploring Agile Mobile App Development in Industrial Contexts. (2019, 2 1). Ανάκτηση από researchgate: https://www.researchgate.net/profile/Samer_Zein/publication/329569528_Ex

ploring_Agile_Mobile_App_Development_in_Industrial_Contexts_A_Qualitative_Study/links/5c23b509a6fdccfc706b0d80/Exploring-Agile-Mobile-App-Development-in-Industrial-Contexts-A-Qualitat

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

Google. (2020, 10 10). *Upload an app.* Ανάκτηση από Google: https://support.google.com/googleplay/android-developer/answer/113469?hl=en

Hindi, D. (2020, 1 1). *15 Mobile App Development Trends of 2020*. Ανάκτηση από buildfire: https://buildfire.com/mobile-app-development-trends/

Hubbard, A. (2015, 1 1). *Mobile App Marketing – Ultimate Guide To Free Techniques.* Ανάκτηση από smartappmarketer: http://www.smartappmarketer.com/mobile-app-marketing-free/

Joseph, J., & K, S. K. (2013, 10 10). *Mobile OS – Comparative Study.* Ανάκτηση από citeseerx: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.7255&rep=rep1&type=pdf

Kaspersky. (2020, 1 1). *The dangers of phishing.* Ανάκτηση από Kaspersky: https://go.kaspersky.com/rs/802-IJN-240/images/Dangers_Phishing_Avoid_Lure_Cybercrime_ebook.pdf

Khanna, N. (2020, 6 2). *What is Lumen Privacy Monitor? How does it work?* Ανάκτηση από candid.technology: https://candid.technology/lumen-privacy-monitor-review/

Kim, H., & Song, J. H. (2010, 1 1). *The quality of word-of-mouth in the online shopping mall.* Ανάκτηση από researchgate: https://www.researchgate.net/publication/235299815_The_quality_of_word-of-mouth_in_the_online_shopping_mall

Kim, J. P. (2013). *Mobile application service networks: Apple's App Store.* Service Business.

Kristijan, L. (2015, 1 1). *App Marketing Strategies: 11 Ways To Help Your App Succeed.* Ανάκτηση από androidheadlines: http://www.androidheadlines.com/2015/03/app-marketing-strategies-11-ways-to-help-your-app-succeed.html

lawspot. (2018, 8 30). *GDPR: Δημοσιεύθηκε ο νόμος 4624/2019 για την προστασία προσωπικών δεδομένων*. Ανάκτηση από lawspot: https://www.lawspot.gr/nomika-nea/gdpr-dimosieythike-o-nomos-4624-2019-gia-tin-prostasia-prosopikon-dedomenon

Lucic, K. (2015, 1 1). *App Marketing Strategies: 11 Ways To Help Your App Succeed.* Ανάκτηση από androidheadlines: http://www.androidheadlines.com/2015/03/app-marketing-strategies-11-ways-to-help-your-app-succeed.html

Octeau, D., McDaniel, P., Jha, S., Bartel, A., Bodden, E., Klein, J., & Traon, Y. L. (2013, 4 1). *Effective Inter-Component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis.* Ανάκτηση από usenix: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_octeau.pdf

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). *Apps, Trackers, Privacy, and Regulators, A Global Study of the Mobile Tracking Ecosystem.*

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

Special Eurobarometer. (2019). *The General Data Protection Regulation*. Βρυξέλλες: EC.

statista. (2020, 6 1). *statista.* Ανάκτηση από statista: https://www.statista.com/statistics/270291/popular-categories-in-the-app-store/

Statista. (2020, 6 1). *Statista.* Ανάκτηση από Statista: https://www.statista.com/

Taylor, V. F., Beresford, A., & Martinovic, I. (2017). *Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones.*

Welderufael B. Tesfay, J. S., & Kai Rannenberg. (2019). PrivacyBot: Detecting Privacy Sensitive Information in Unstructured Texts», . *Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS).*

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

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης . (2016, 4 27). *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ*. Ανάκτηση από Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης : https://gdprteam.gr/wp-content/uploads/2018/03/kanonismos_EL_TXT.pdf

Ευρωπαϊκή Επιτροπή. (2020, 1 1). *Τι αποτελεί επεξεργασία δεδομένων;*. Ανάκτηση από europa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_el

Ευρωπαϊκή Επιτροπή. (2020, 1 1). *Τι είναι τα δεδομένα προσωπικού χαρακτήρα;*. Ανάκτηση από europa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_el

Εφημερίδα της Κυβερνήσεως. (2019, 8 29). *Νόμος 4624/2019.* Ανάκτηση από gdprteam: https://gdprteam.gr/wp-content/uploads/2019/09/n_4624_2019.pdf