ΠΑΝΕΠΙΣΤΗΜΙΟ
ΠΕΛΟΠΟΝΝΗΣΟΥ

Τμήμα Οικονομικών Επιστημών

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Επιχειρηματικότητα και Διακυβέρνηση»

Κατεύθυνση: «Επιχειρηματικότητα και Ανάπτυξη»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

"Η ασφάλεια των προσωπικών δεδομένων στα κοινωνικά δίκτυα στην Ελλάδα"

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Γρηγόριος Σπυράκης

Φοιτήτρια:

Μαρία Κωνσταντινίδου

Α.Μ.: 4042201503023

ΤΡΙΠΟΛΗ,

ΦΕΒΡΟΥΑΡΙΟΣ 2017

Η έγκριση της παρούσας εργασίας από το Πανεπιστήμιο Πελοποννήσου δεν συνεπάγεται και την υιοθέτηση των απόψεων της συγγραφέα.

Ευχαριστίες

Ευχαριστώ θερμά τον επιβλέπον καθηγητή μου κ. Σπυράκη για την αμέριστη υποστήριξη και καθοδήγηση του καθ' όλη την διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας, καθώς και όλους τους καθηγητές μου οι οποίοι με βοήθησαν στη επίτευξη του στόχου μου, με τις πολύτιμες γνώσεις και συμβουλές τους. Επιπλέον θα ήθελα να ευχαριστήσω τον κ. Αλέξανδρο Κουράκο, του Τμήματος Παροχής Στατιστικής Πληροφόρησης της Ελληνικής Στατιστικής Αρχής, όπως και την κα. Όλγα Γαλάνη, Αστυνομικό Β΄ Ειδικών Καθηκόντων της Διεύθυνσης Διώξεως Ηλεκτρονικού Εγκλήματος, για την συνεργασία τους, με σκοπό την παραχώρηση των απαραίτητων πληροφοριών. Οφείλω να ευχαριστήσω ακόμα όλους εκείνους που στάθηκαν δίπλα μου και με ενθαρρύναν στην ολοκλήρωση αυτού του «κύκλου».

Τέλος θα ήθελα να ευχαριστήσω ιδιαίτερα την οικογένεια μου για την αμέριστη ηθική και υλική υποστήριξη και συμπαράσταση της σε όλη την διάρκεια της προσπάθειας μου, όπως και την αδελφή μου για την πολύτιμη βοήθεια και ενθάρρυνση της.

ΠΕΡΙΛΗΨΗ- ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ

Η διαχείριση των προσωπικών δεδομένων στο διαδίκτυο είναι ένα θέμα που απασχολεί τους χρήστες του, καθώς η ραγδαία ανάπτυξη της τεχνολογίας έχει αφήσει το διαδίκτυο να εισβάλει στην καθημερινότητα τους. Πέρα από τις διευκολύνσεις που παρέχει, δεν παύει να αποτελεί έναν μεγάλο κίνδυνο για την ιδιωτικότητα και τα προσωπικά δεδομένα των χρηστών.

Η παρούσα διπλωματική εργασία αποσκοπεί στην απόκτηση γνώσης σχετικά με την χρήση των προσωπικών δεδομένων, μετά την καταγραφή τους στο διαδίκτυο και κυρίως στα μέσα κοινωνικής δικτύωσης. Επιπλέον, διερευνάται ο τρόπος με τον οποίο τα κοινωνικά δίκτυα συλλέγουν τις προσωπικές πληροφορίες των χρηστών, και το νομικό πλαίσιο προστασίας της ιδιωτικότητας. Μέσα από γενικές πληροφορίες σχετικά με το διαδίκτυο και τα κοινωνικά δίκτυα δίνεται ιδιαίτερη έμφαση σε θέματα ιδιωτικότητας και ασφάλειας. Στο πρώτο μέρος αναλύονται ορισμένες βασικές έννοιες σχετικά με το διαδίκτυο, τις διαδικτυακές κοινότητες και την ασφάλεια των πληροφοριών εντός αυτών. Έπειτα πραγματοποιείτε εκτενής αναφορά σε ορισμένες ιστοσελίδες κοινωνικής δικτύωσης όπου αναλύονται οι πολίτικες απορρήτου και οι οροί χρήσης των ιστοσελίδων. Αναφέρονται οι κίνδυνοι που αντιμετωπίζει ο χρήστης από την συλλογή των προσωπικών του δεδομένων, οι τρόποι περιορισμού του φαινομένου, και οι τρόποι με τους οποίους ο χρήστης προστατεύεται από την συλλογή τους. Αμέσως μετά, ακολουθούν τα σπουδαιότερα ζητήματα του ισχύοντος ελληνικού και ευρωπαϊκού νομικού πλαισίου για την προστασία της ιδιωτικότητας. Βασικές έννοιες και δικαιώματα των χρηστών αναλύονται με σκοπό την καθολική ενημέρωση τους. Τέλος, παρουσιάζεται μια πρωτογενής έρευνα σε 87 άτομα, σχετικά με την χρήση των μέσων κοινωνικής δικτύωσης. Τα ευρήματα οδηγούν στο συμπέρασμα ότι οι χρήστες επιθυμούν να κατέχουν τον απολυτό έλεγχο των προσωπικών τους δεδομένων χωρίς όμως να προβαίνουν στις απαραίτητες ενέργειες. Το χάσμα μεταξύ «επιθυμίας» και «πράξης» δημιουργεί ένα έντονο αίσθημα διαδικτυακής ανασφάλειας και καχυποψίας. Τα αποτελέσματα της έρευνας μπορούν να χρησιμοποιηθούν μελλοντικά με σκοπό την διερεύνηση των αιτιών αυτού του φαινομένου.

Λέξεις κλειδιά: Προσωπικά Δεδομένα, Κοινωνική Δικτύωση, Μέσα Κοινωνικής Δικτύωσης, Διαδικτυακή Ιδιωτικότητα, Διαδικτυακή Ασφάλεια

ABSTRACT- KEYWORDS

The processing of personal data on the Internet raises serious concerns to its users, as the rapid development of technology has allowed the Internet to invade their daily lives. Apart from the its positive side, it still endangers both the privacy and the personal data of the users.

This thesis aims at deepening our knowledge about the use of personal data, after being shared on the internet and especially on social media. Furthermore, the way in which social networks collect and store the personal information of their users is explored, as well as the legal framework for privacy protection. Through general information on the internet and social networks, particular emphasis is given on privacy and security issues. The first part analyzes some basic concepts of the internet, such as the online communities and social networks and the security of information therein. Then, extensive reference is made in certain social networking sites analyzing their privacy policy and terms of use. The risks faced by the user due to the collection of their personal data, ways of limiting this phenomenon and ways in which the user could be protected from such practices are also examined. Moreover, the most important issues of the current Greek and European legal framework for the protection of privacy are presented. Basic concepts and the rights of users are analyzed with a view to raise their awareness. Finally, a primary research questionnaire, with 87 participants, on the use of social media is presented. The research findings suggest that users want to possess the absolute control of their personal data, but without taking the necessary steps. As a result, the gap between "desire" and "action" creates a strong sense of insecurity and mistrust online. These results could be used in the future to investigate the causes of this phenomenon.

Keywords: Personal Data, Social Networking, Social Media, Internet Privacy, Online Security

Πίνακας περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Γραφημάτων

Κατάλογος Εικόνων

Συντομογραφίες

ΑΣΠΑΙΤΕ : Ανωτάτη Σχολή Παιδαγωγικής Και Τεχνολογικής Εκπαίδευσης

ΑΤΕΙ : Ανώτατο Τεχνολογικό Εκπαιδευτικό Υδρία

Ε.Ε : Ευρωπαϊκή Ένωση

Ε.Κ : Ευρωπαϊκή Κοινότητα

ΕΛΣΤΑΤ : Ελληνική Στατιστική Αρχή

ΗΠΑ : Ηνωμένες Πολιτείες Αμερικής

Η/Υ : Ηλεκτρονικός Υπολογιστής

ΚΑΤΕΕ : Κέντρο Ανωτάτης Τεχνικής Επαγγελματικής Εκπαιδεύσεως

Ν. : Νόμος

Ο.Π. : Όπου Προηγουμένως

Παρ. : Παράγραφος

Π.Κ. : Ποινικός Κώδικας

ΤΕΙ : Τεχνολογικό Εκπαιδευτικό Ίδρυμα

ALS : Amyotrophic Lateral sclerosis

EMPACT : European Multidisciplinary Platform Against Criminal Threats

Europol : European Police Office

FTC : Federal Trade Commission

Interpol : International Criminal Police Organization

IP : Internet Protocol

SPSS : Statistical Package For The Social Sciences

Εισαγωγή

Τα μέσα κοινωνικής δικτύωσης αποτελούν ένα πρόσφατο επιστημονικό επίτευγμα το οποίο με το πέρασμα του χρόνου εισέρχεται όλο και περισσότερο στις ζωές μας. Με την εξάπλωση του διαδικτύου οι διαδικτυακές κοινότητες έκαναν την εμφάνιση τους αρχικά με σκοπό την επικοινωνία με γνωστούς και αγνώστους, και έπειτα για την ταχεία και άμεση ενημέρωση των χρηστών από τα online συνδεδεμένα άτομα χωρίς την διαμεσολάβηση τρίτων (πχ. δημοσιογράφων). Το ερώτημα, από που προέρχονται οι πόροι των μέσων κοινωνικής δικτύωσης, δεν άργησε να έρθει στην επιφάνεια. Η απάντηση περιλάμβανε τα προσωπικά δεδομένα των χρηστών. Τα δεδομένα που οι χρήστες καλούνταν να υποβάλουν στις ιστοσελίδες για να επιτευχθεί η εγγραφή τους, χρησιμοποιούνταν για μεταπώληση με σκοπό την εύρεση των τάσεων της αγοράς, καθώς και των γενικότερων προτιμήσεων των χρηστών. Η άγνοια των χρηστών για την μετέπειτα χρήση των προσωπικών τους δεδομένων δημιουργεί κλίμα διαδικτυακής ανασφάλειας. Ωστόσο, πολλοί είναι και οι χρήστες οι οποίοι παρασυρόμενοι από τον φαινομενικά αθώο κόσμο και το «κλειστό» περιβάλλον των ιστοσελίδων κοινωνικής δικτύωσης, καταθέτουν προσωπικές πληροφορίες και ευαίσθητα προσωπικά δεδομένα αγνοώντας τους κίνδυνους που ελλοχεύουν. Οικονομικές απάτες, πλαστοπροσωπία, εξαπάτηση, διακίνηση παράνομου υλικού, κακόβουλου λογισμικού και υποκλοπή αρχείων, αποτελούν μόνο λίγους από τους κίνδυνους του διαδικτύου.

Για τον περιορισμό τέτοιων φαινομένων απαιτήθηκε μια ενιαία και καθολική πολιτική, προληπτικού κυρίως χαρακτήρα, που να μπορεί να κατευνάσει και να περιορίσει τέτοιου είδους φαινόμενα. Η Ελλάδα κλήθηκε να διαμορφώσει την διαδικτυακή της πολιτική πάνω στις Ευρωπαϊκές Οδηγίες. Ο νόμος 2472/1997 αποτελεί τον πυλώνα της ελληνικής διαδικτυακής πολιτικής. Η σύστασή του έγινε σύμφωνα με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την «προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Το νομοθετικό πλαίσιο ωστόσο παρά τις ποινές που περιλαμβάνει για την συμμόρφωση των χρηστών στο νομοθετικό πλαίσιο, δεν διασφαλίζει την ορθή λειτουργία της νομοθεσίας και την τήρηση της. Το κενό που δημιουργείται καλείται να καλύψει η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στην Ελλάδα όπου μέσα από καταγγελίες και έρευνες οδηγείται στην αποτροπή και εξιχνίαση διαδικτυακών εγκλημάτων.

Η παρούσα διπλωματική εργασία συνδυάζει την βιβλιογραφική ανασκόπηση και την εμπειρική έρευνα, με σκοπό να παρουσιάσει μια ολοκληρωμένη «εικόνα» για τους πραγματικούς κινδύνους των μέσων κοινωνικής δικτύωσης αλλά και για το πώς οι χρήστες αντιλαμβάνονται και ενδιαφέρονται για την προστασία των προσωπικών τους δεδομένων. Αναλυτικότερα, στο πρώτο κεφάλαιο επιχειρείται η εισαγωγή του αναγνώστη στην «σφαίρα» του διαδικτύου και παρουσιάζονται οι βασικές έννοιες οι οποίες κρίνονται απαραίτητες για την περαιτέρω ανάπτυξη του θέματος. Οι διαδικτυακές κοινότητες αναλύονται με σκοπό την παρουσίαση διαφόρων μορφών που μπορούν να λάβουν αλλά και για την επισήμανση των κινδύνων που ελλοχεύουν. Η ασφάλεια των πληροφοριών αποτελεί ένα άλλο σημαντικό σημείο. Οι διαδικτυακές απάτες και το κακόβουλο λογισμικό που μπορεί να μεταβεί στον ηλεκτρονικό υπολογιστή του χρήστη παρουσιάζονται αναλυτικά συνδυαστικά με τα μέτρα ασφάλειας που μπορούν να ληφθούν για την προστασία της ιδιωτικής ζωής αλλά και των ανήλικων χρηστών. Έπειτα παρουσιάζονται μερικές από τις δημοφιλέστερες ιστοσελίδες κοινωνικής δικτύωσης στην Ελλάδα. Σε αυτό το σημείο πρέπει να αναφερθεί πως προτιμήθηκαν οι δημοφιλέστερες ιστοσελίδες, οι οποίες όμως περιέχουν διαφορετική δομή και στόχο χρήσης. Το Facebook, το Twitter, το LinkedIn, το Pinterest, το YouTube, και το Patientslikeme είναι ιστοσελίδες που προτιμούν οι χρήστες δίνοντας τους παροχές διαφορετικών ενδιαφερόντων.

Στην συνέχεια, περνώντας στο δεύτερο κεφάλαιο της εργασίας, αναλύεται το νομικό πλαίσιο που προστατεύει τους χρήστες. Όπως είδαμε προηγουμένως πολλές ιστοσελίδες ζητούν ευαίσθητα προσωπικά δεδομένα. Χαρακτηριστικό είναι το παράδειγμα του Patientslikeme όπου οι χρήστες- ασθενείς καλούνται να καταθέτου σε τακτά χρονικά διαστήματα την πορεία της υγείας τους, με σκοπό την σύγκριση των δεδομένων τους με άλλων χρηστών. Όλα αυτά δημιουργούν δαιδαλώδεις συζητήσεις για τα όρια της ιδιωτικότητας και της παγκόσμιας διαδικτυακής κοινότητας. Οι απαντήσεις ζητήθηκαν μέσα στην ελληνική και ευρωπαϊκή νομοθεσία. Με αυτόν τον τρόπο κατοχυρώνονται τα (ευαίσθητα ή μη) προσωπικά δεδομένα των χρηστών αναφέροντας πλήρως και με ακρίβεια τα δικαιώματα του καθώς και την έννομη πορεία των προσωπικών του δεδομένων. Η νομοθεσία είναι συντονισμένη και εφαρμόζεται έχοντας ως βάση την Ευρωπαϊκή Οδηγία 95/46/ΕΚ και τους μετέπειτα Κανονισμούς.

Τέλος, παρουσιάζεται η ερευνά σε δείγμα 87 ατόμων. Η έρευνα καλείται να δώσει την πραγματική εικόνα που επικρατεί στην κοινωνία, πέρα από την βιβλιογραφία και το νομικό πλαίσιο, που συμβουλεύουν και προστατεύουν τους χρήστες. Τα αποτελέσματα της έρευνας φανέρωσαν κλίμα ανασφάλειας και ανησυχίας των χρηστών για το περιεχόμενο

των πληροφοριών τους στο διαδίκτυο και στις ιστοσελίδες κοινωνικής δικτύωσης. Έκπληξη προκαλεί το γεγονός πως οι ίδιοι οι χρήστες που εκφράζουν την ανησυχία τους και τους φόβους τους δεν έχουν προβεί σε ενέργειες προστασίας και επίβλεψης επεξεργασίας και συλλογής των πληροφοριών τους. Ιδιαίτερο ενδιαφέρον θα αποτελούσε η μετέπειτα μελέτη των αιτιών της αντίφασης που παρουσιάζεται στην κοινωνία. Θα πρέπει ωστόσο να αναφερθεί η δυσκολία συλλογής του δείγματος για τον λόγο ότι η ερευνά διανεμήθηκε και μέσω ηλεκτρονικού ταχυδρομείου όσο και μέσω ιστοσελίδων κοινωνικής δικτύωσης, όπου τα κίνητρα συμμετοχής είναι χαμηλά και δεν δίνεται η δυνατότητα στον ερευνητή να ελέγξει τη ορθότητα των απαντήσεων διασφαλίζοντας την συμμετοχή μιας και μόνο φοράς σε κάθε ερωτώμενο. Ο σκοπός της έρευνας ήταν να συνδυάσει το θεωρητικό πλαίσιο που παρουσιάστηκε στα κεφάλαια 1 και 2 με τις απόψεις των χρηστών. Επιπλέον αναδείχθηκαν ιστοσελίδες κοινωνικής δικτύωσης με σειρά δημοτικότητας των χρηστών, φανερωθήκαν τα πιο συνήθεις μετρά προστασίας των χρηστών, προσδιοριστήκαν οι πιο ενεργές διαδικτυακά ηλικιακές ομάδες και μέσα από το στατιστικό πακέτο SPSS κατάφεραν να αναδειχθούν ορισμένα συμπεράσματα βασιζόμενα σε διασταυρώσεις και συσχετίσεις δεδομένων.

Κεφάλαιο 1 : ΤΟ ΔΙΑΔΙΚΤΥΟ

1.1 Το Internet

Ο παγκόσμιος ιστός έχει εισχωρήσει στις ζωές των ατόμων σε όλα τα επίπεδα της καθημερινότητας τους και φαίνεται να έχει ξεπεράσει το αρχικό όραμα του δημιουργού του Tim Barnes- Lee. Η εκτεταμένη χρήση του μαζί με την εύκολη πρόσβαση που προσφέρεται στους χρήστες, αποτελούν σημαντικό κομμάτι επαγγελματικών και προσωπικών συνδιαλλαγών εκμηδενίζοντας τον χρόνο και τις αποστάσεις.[1] Η μεγάλη αύξηση των χρηστών σε συνδυασμό με την είσοδο νέων υπηρεσιών και επιχειρήσεων στο διαδίκτυο έφερε πληθώρα αλλαγών. Η χρήση του διαδικτύου σταματάει πλέον να έχει καθαρά επαγγελματικό και πληροφοριακό χαρακτήρα και μετατρέπεται σε πολυμήχανά. Το εύρος χρήσης του διαδικτύου επεκτείνεται σε νέα πεδία ηλεκτρονικού εμπορίου, δημοπρασιών, μάρκετινγκ, εκπαίδευσης, ηλεκτρονικών μουσείων, χρηματικών συναλλαγών, υγείας και επικοινωνίας των χρηστών.[2]

Το Internet, ως ένα διαδίκτυο που ενώνει πάνω από 100 εκατομμύρια υπολογιστές, ορίζεται ως ένα μεγάλο παγκόσμιο δίκτυο συνδεδεμένων διακομιστών και δικτυών. Η σύνδεση των υπολογιστών επιτυγχάνεται με την χρήση του πρωτόκολλου IP (Internet Protocol).[3] Παράλληλα ο Ιστός αποτελεί ένα μέρος του δικτύου που αποτελεί το Internet, και συγκεκριμένα των εγγράφων, ή σύμφωνα με την ορολογία του διαδικτύου τις «σελίδες».[4]

1.2 Διαδικτυακές κοινότητες

Μέσα από την φυσική έλξη των ανθρώπων προς την δημιουργία κοινοτήτων φανερώνεται η βαθύτατη ανάγκη για επικοινωνία και συντροφικότητα. Το ίδιο συμβαίνει και στο διαδίκτυο. Η ραγδαία ανάπτυξη των μέσων τεχνολογίας δίνει τη δυνατότητα στα υποκείμενα να κοινωνικοποιηθούν σε πραγματικό χρόνο με άτομα από όλο τον κόσμο κάνοντας πράξη την έννοια της παγκοσμιοποίησης. Σύνορα και αποστάσεις καταργούνται μέσα από την οθόνη του ηλεκτρονικού υπολογιστή και η γνώση διαμοιράζεται. Σημαντική είναι η συμβολή των εικονικών κοινοτήτων σε άτομα με ειδικές ικανότητες στους οποίους παρέχεται ευκολότερα η ευκαιρία στην γνώση και στην διασκέδαση.

---

[1] Simson Garfinkel with Gene Spafford, Web Security, Privacy & Commerce, O'REILLY, 2002, 2nd Edition, pp. 400

[2] Jo Anne Woodcock, Εισαγωγή στα δίκτυα Υπολογιστών, Κλειδάριθμος 2003, σελ.243

[3] Αθηνά Α. Λαζακίδου, Σύγχρονες Τεχνολογίες και Υπηρεσίες Πληροφορικής και Τηλεπικοινωνιών, σελ. 39

[4] Jo Anne Woodcock, Εισαγωγή στα δίκτυα Υπολογιστών, Κλειδάριθμος 2003, σελ.244

Στην πραγματικότητα πρόκειται για μια δεύτερη κοινότητα, πλασματική, που παρέχεται μέσα από το παγκόσμιο τηλεπικοινωνιακό δίκτυο. Η εν λόγο κοινότητα είναι καθαρά προσωπική αφού ο χρήστης μπορεί εξ ολοκλήρου να ελέγξει το περιβάλλον μέσα στο οποίο θα κινείται. Πάρα όμως την αληθοφάνεια και την τέρψη της επικοινωνίας που παρέχεται μέσω των δικτυών, η διαδικτυακή επαφή δεν αντικαθιστά την πραγματική.[5]

1.2.1 Τύποι εικονικών κοινοτήτων

Οι εικονικές κοινότητες (virtual communities) αποτελούν διαδικτυακούς χώρους συνομιλίων, όπου οι χρήστες μπορούν να ανταλλάξουν πληροφορίες σε δημόσιες ή ιδιωτικές συζητήσεις. Ο χώρος οπού αυτές ο συνομιλίες εξελίσσονται ονομάστηκε για πρώτη φορά από τον συγγραφέα William Gibson στο έργο του με τίτλο "Neuromancer"ως «κυβερνοχώρος» (cyberspace). Ο κυβερνοχώρος δημιουργείται μέσα από υπολογιστικά συστήματα και δίνουν την δυνατότητα στους χρήστες να επικοινωνούν και να εκτελούν πληθώρα δραστηριοτήτων, όπως συμμετοχή σε ηλεκτρονική δημοπρασία, εξ αποστάσεως εκπαίδευση, οικονομικές συναλλαγές, ηλεκτρονικές χρηματικές συναλλαγές ηλεκτρονικό εμπόριο κ.α.

Οι εικονικές κοινότητες διαχωρίζονται σε έξι μορφές: Το Mailing List όπου πρόκειται για τον πιο απλό και διαδεδομένο συνάμα τρόπο επικοινωνίας των χρηστών. Το άτομο μέσα από την δημιουργία λίστας email μπορεί να επικοινωνήσει μέσω της εικονικής κοινότητας. Το Newsgroup- UseNet, όπου οι χρήστες επικοινωνούν μεταξύ τους για ένα συγκεκριμένο θέμα ανταλλάσσοντας απόψεις και σχόλια, τα Chats που πρόκειται για διάλογους που συμβαίνουν σε πραγματικό χρόνο δίνοντας την δυνατότητα στους χρήστες να ανταποκριθούν άμεσα στην συνομιλία. Το περιβάλλον που εξελίσσεται η συνομιλία ονομάζεται "chat room". Τα Web-based discussion groups, των οποίων η φιλοσοφία είναι παρεμφερή με την φιλοσοφία των emails μόνο που σε αυτή την περίπτωση δίνεται η δυνατότητα στον χρήστη να συμμετάσχει σε ομάδες διαλόγου και να δημιουργήσει μια καινούργια ομάδα συζήτησης. Το Messenger, που είναι η πιο δημοφιλής μορφή εικονικής κοινότητας και δίνει την δυνατότητα στον χρήστη να μπορεί να δει αν ο συνομιλητής του είναι συνδεδεμένος και να συνομιλήσει μαζί του γραπτά, προφορικά ακόμα και με εικόνα μέσω κάμερας, και τέλος οι τρισδιάστατοι εικονικοί κόσμοι.[6]

[5] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 62

[6] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, ό.π., σελ. 64

1.2.2 Θετικά των μέσων κοινωνικής δικτύωσης

Η χρήση των μέσων κοινωνικής δικτύωση απαριθμεί πολλά οφέλη για τον χρήστη και την κοινωνία εν γένει. Αρχικά συμβάλλει στην αύξηση της κοινωνικότητας του ατόμου μέσα από την επαφή του με άτομα από κάθε γωνιά της γης, και την ανταλλαγή πληροφοριών και απόψεων. Επιπλέον, βελτιώνει τις δεξιότητες του χρήστη και διευρύνει τους ορίζοντες του απασχολώντας τον με ευχάριστες δεξιότητες που δεν απαιτούν ιδιαίτερες γνώσεις και ικανότητες. Σημαντικές είναι και οι συναισθηματικές ανάγκες του ατόμου για επικοινωνία και αποδοχή που καλύπτονται μέσα από τις συνομιλίες με άτομα κοινών ενδιαφερόντων. Η αμεσότητα που παρέχεται δίνει την αίσθηση ικανοποίησης στους χρήστες.

Σε κοινωνικό επίπεδο τα οφέλη διαχέονται στους επιστημονικούς χώρους. Νέες τεχνολογίες και νέες ανάγκες αναδύονται δημιουργώντας καινούργιες θέσης εργασίας και νέες ειδικότητες. Επιπλέον προωθείται η οικονομία μέσα από ηλεκτρονικές πωλήσεις και το παγκόσμιο εμπόριο θέτοντας υψηλότερες προδιαγραφές για τις τοπικές παροχές.[7]

1..2.3 Οι κίνδυνοι των μέσων κοινωνικής δικτύωσης

Η μη προσωπική επαφή των χρηστών του διαδικτύου και ο παγκόσμιος χαρακτήρας του δημιουργεί ορισμένους κίνδυνους για τους χρήστες. Η πλαστοπροσωπία, η εμφάνιση δηλαδή του ατόμου με άλλη ταυτότητα (φύλο, όνομα, φυλή, τόπο διαμονής, επάγγελμα κα) δημιουργεί κλίμα καχυποψίας στους χρήστες.[8] Επιπλέον η ελεύθερη διακίνηση ιδεών χωρίς να υπάγονται σε κανέναν έλεγχο αφήνει «ανεξέλεγκτη» την παράνομη διακίνηση υλικού (πχ. προσωπικών στοιχείων), το ενδεχόμενο εξαπατήσεως, εκβιασμών, καθώς και την διακίνηση πορνογραφίας, αλλά και λοιπών ψευδών υλικών ποικίλου περιεχομένου.[9] Για τον περιορισμό αυτών των φαινομένων και την απαλοιφή τέτοιων κρουσμάτων δημιουργήθηκαν ειδικές ομάδες στην αστυνομία και στον δικηγορικό σύλλογο, με εξειδίκευση στο ηλεκτρονικό έγκλημα.[10]

Μέσα από την χρήση των δικτυών το άτομο έρχεται αντιμέτωπο με μια νέα πραγματικότητα. Ο αυτοπροσδιορισμός και η αυτοπροβολή είναι τα κεντρικά στοιχεία των μέσων κοινωνικής δικτύωσης. Σε αυτά ο κάθε χρήστης επιλέγει πως θέλει να προβάλει τον

[7] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 71

[8] Jan L. Harrington, Network Security: A Practical Approach, Morgan Kaufmann Publishers, 2005, pp.12

[9] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 4th Edition, 2007, pp. 407

[10] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, ό.π., σελ. 72

εαυτό του και ποια οπτική της ζωής του θέλει να παρουσιάσει ως επικρατέστερη. Πρόκειται για μια «ψεύτικη πραγματικότητα» όπου η αλήθεια και το «φαίνεται», αν και δυο καθόλα αντίθετες εννοείς, έχουν ίσο μερίδιο και δείχνουν να συνυπάρχουν αρμονικά.

Η ιδιά αντίθεση επικρατεί και στην ιδιωτικότητα των χρηστών. Κάνοντας λόγο για παγκόσμιο ιστό και κοινωνική δικτύωση η έννοια της ιδιωτικότητας φαίνεται να περιορίζεται μέσα στην δημοσιά έκθεση προσωπικών, και μη, δεδομένων. Το μόνο που απομένει είναι η εύρεση της χρυσής τομής αναμεσά στο δημόσιο και το ιδιωτικό, καθώς επίσης και η εξέταση του ποσοστού που ο χρηστής μπορεί να επέμβει και να διαφυλάξει την ιδιωτικότητας του. Αξίζει όμως να αναφέρουμε πως σε αρκετούς ιστότοπους ο χρήστης μπορεί να διατηρήσει την ανωνυμία του ή ακόμα και να συνδεθεί χωρίς να φανερώσει την ταυτότητα του, είτε χωρίς σύνδεση σε προσωπικό του λογαριασμό είτε με την χρήση ψευδωνύμου.[11]

Επιπλέον η πολύωρη ενασχόληση του ατόμου με τα μέσα κοινωνικής δικτυώσεις φέρουν μια σειρά από αρνητικές συνέπειες. Η αποξένωση του από τους οικείους του, καθώς και η παντελής έλλειψη ενδιαφέροντος για τα κοινά, συμβάλει στην αύξηση του ατομικισμού και στην παραμέληση της πραγματικότητας. Οι εικονικές φιλίες αντικαθιστούν τις πραγματικές και ο χρήστης εγκλωβίζεται σε ένα ψεύτικο κόσμο. Πρέπει ωστόσο να επισημάνομε πως τέτοιου είδους κρούσματα είναι περιορισμένα και για την αντιμετώπιση τους συνίσταται ψυχολογική υποστήριξη του ατόμου.[12]

Τέλος, δεν πρέπει να παραβλέπουμε την τεράστια δύναμη που φέρουν τα μέσα κοινωνικής δικτύωσης όσο αφορά την κινητοποίηση των πολιτών. Το Facebook και το Twitter έχουν αποδειχτεί ως τα μέσα που είναι ικανά να συγκεντρώσουν το υψηλότερο αριθμό πολιτών σε κινητοποιήσεις.[13]

1.3 Ασφάλεια Πληροφοριών

1.3.1 Ασφάλεια πληροφοριών

Στην εποχή οπού η χρήση του διαδικτύου αυξάνεται συνεχώς, χρησιμοποιώντας το για επαγγελματικούς και προσωπικούς λόγους, δεν είναι εφικτό να παραληφθούν οι κίνδυνοι που φέρει. Ο βασικός κίνδυνος είναι πως όλες οι πληροφορίες έχουν λάβει

[11] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 4th Edition, 2007, pp. 614-616

[12] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 33

[13] Rick Smolan, Jennifer Erwitt, The Human Face Of Data, http://www.humanfaceofbigdata.com/, 20/9/2016

ψηφιακή μορφή γεγονός που τις κάνουν ευάλωτες σε διαρροές. Νέα συστήματα προστασίας κάνουν την εμφάνιση τους αλλά οι παραβιάσεις συστημάτων ασφάλειας συνεχίζουν να υφίστανται. Σημαντικό ρολό σε αυτό κατέχει η άγνοια και τα ελλιπή μέτρα ασφάλειας των χρηστών.

Η αναφορά στην ασφάλεια των υπολογιστών διαθέτει τρεις βασικούς πυλώνες· την εμπιστευτικότητα (συνώνυμο της ιδιωτικότητας και του απορρήτου στην διαδικτυακή περιήγηση), την ακεραιότητα , και την διαθεσιμότητα.[14] Σκοπός είναι η απόλυτη ισορροπία αναμεσά στις τρεις συνιστώσες για να επιτευχθεί η πλήρης ασφάλεια.[15]

Εικόνα 1: Information Security 16

Λόγω του παγκόσμιου και μη ελεγχόμενου χαρακτήρα του διαδικτύου έχουν επεκταθεί ορισμένες μορφές επιθέσεων που αποσκοπούν στην δημιουργία προβλημάτων και συχνά στην ικανοποίηση συμφερόντων. Στόχος τους είναι η μεταφορά ή αντιγραφή προσωπικών αρχείων με σκοπό την μετέπειτα χρήση τους, η αλλοίωση των δεδομένων, η εισβολή σε χρηματικές συναλλαγές με σκοπό το οικονομικό όφελος κ.α.[17] Οι συνηθέστεροι κίνδυνοι είναι οι εξής:

- Masquerade (Μη εξουσιοδοτημένη χρήση): πρόκειται για επιθέσεις από μη εξουσιοδοτημένο χρήστη ο οποίος προσπαθεί με παράνομο τρόπο να αποκτήσει πρόσβαση σε προστατευμένους ισόχωρους.

[14] Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Πληροφοριακών Συστημάτων, εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004, σελ. 24
[15] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 4th Edition, 2007, pp. 09-12
[16] http://informationsecurityadviser.co.uk/cia-triad/, 04/11/2016
[17] Simson Garfinkel with Gene Spafford, Web Security, Privacy & Commerce, O'REILLY, 2002, 2nd Edition, pp.5

- Passive Tapping (Παθητική παρακολούθηση): σε αυτή την περίπτωση ο εισβολέας απλώς παρακολουθεί τα αρχεία που ανταλλάσσουν οι συμμετέχοντες.
- Active Tapping (Ενεργός παρακολούθηση): Εκ διαμέτρου αντίθετη παρακολούθηση με την παθητική. Αυτή η μορφή παρακολούθησης περιλαμβάνει την αλλαγή των μηνυμάτων μεταξύ των συνομιλητών. Ο εντοπισμός όμως της εισβολής είναι ευκολότερος.
- Repudiation (Αποποίηση): πρόκειται για την άρνηση συμμέτοχης σε μια συνομιλία.
- Denial of Service (Άρνηση Παροχής Υπηρεσίας): αυτού του είδους οι επίθεσης εμπίπτουν στην άρνηση παροχής μιας υπηρεσίας, στην διαγραφή μηνυμάτων και στην καθυστέρηση εξυπηρέτησης.
- Replay (Επανεκπέμπω Μηνυμάτων): σε αυτή την περίπτωση ο χρήστης προσποιούμενος τον εξουσιοδοτημένο χρήστη αποθηκεύει υπάρχοντα μηνύματα και τα μεταδίδει σε μεταγενέστερο χρόνο με σκοπό να προετοιμάσει το έδαφος για την Άρνηση Παροχής Υπηρεσίας και να αποστείλει υστερόβουλα μηνύματα για την ικανοποίηση διάφορων συμφερόντων.
- Traffic Analysis (Ανάλυση Επικοινωνίας): μέσα από την παρακολούθηση μηνυμάτων ο εισβολέας επιτυγχάνει την ανάλυση της ταυτότητας των συμμετεχόντων καθώς και την συχνότητα και την ποσότητα δεδομένων που ανταλλάσσονται.
- Viruses, Trojan horses, Worms (Κακόβουλο Λογισμικό): το κακόβουλο λογισμικό εισβάλει στο διαδικτυακό περιβάλλον του χρήστη και υποκλέπτει αρχεία ή προετοιμάζει την Άρνηση Παροχής Υπηρεσιών.[18] Στην περίπτωση των Viruses το κακόβουλο λογισμικό ενδέχεται να αλλάζει μορφή όσο μεταδίδεται (Polymorphic Virus).[19]

Έχοντας ως στόχο την ενημέρωση των πολίτων και την αύξηση της εμπιστοσύνης του στις παροχές-υπηρεσίες του διαδίκτυο ιδρύθηκε η «Ομάδα Δράσης για την Ψηφιακή Ασφάλεια» (Digital Awareness & Response to Treats). Η δράση της στρέφεται προς την οργάνωση και τον συντονισμό των αρμοδίων φορέων για την επίσπευση και βελτίωση των αποτελεσμάτων που φέρουν. Τα αποτελέσματα της D.A.R.T. σε συνδυασμό με την

[18] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 91

[19] Jan L. Harrington, Network Security: A Practical Approach, Morgan Kaufmann Publishers, 2005, pp.182

περεταίρω εξοικείωση των χρηστών θα αυξήσει και θα βελτιώσει σε μεγάλο βαθμό τις ηλεκτρονικές υπηρεσίες που παρέχονται στην Ελλάδα.

Επιπλέον, θεσπίστηκαν τέσσερα (4) είδη κριτικών που αποσκοπούν στην προστασία και ενίσχυση της ιδιωτικής ζωής των χρηστών. Η θέσπιση πραγματοποιήθηκε από τον οργανισμό "Common Criteria"[20] η οποία ασχολείται με την ενίσχυση της ιδιωτικότητας. Τα κριτήρια αυτά αναφέρονται στην ανωνυμία (την αδυναμία προσδιορισμού του χρήστη), την ψευδωνυμία, η μη συνδεσιμότητα (όπου δηλαδή καθίσταται αδύνατον να προσδιοριστεί ο χρήστης που προκάλεσε βλάβες ή μετατροπές στο σύστημα), και τέλος η αδυναμία εντοπισμού λειτουργιών που εκτελούνται.[21]

1.3.2 Διαδικτυακές απάτες

Αν αναλογιστούμε την ραγδαία άνοδο της χρήσης των ηλεκτρονικών υπολογιστών από το 1981 όπου συμμετείχαν μόνο 231 ηλεκτρονικοί υπολογιστές στο Arpanet (προάγγελος του Internet), για ερευνητικούς λογούς, μπορούμε να καταλάβουμε πως η αύξηση χρήσης αυτών των 37 χρονών, καθώς και η επέκταση της χρήσεως, του επέφερε πληθώρα μεταβολών και χώρο για την δημιουργία κίνδυνων ενάντια στους χρήστες.[22] Οι συνηθέστεροι κίνδυνοι που αντιμετωπίζει ο χρήστης κατά την περιήγηση του στο διαδίκτυο συνοψίζονται στις παρακάτω περιπτώσεις:

- Ευκαιρίες απασχόλησης: Στην εποχή της τεχνολογίας η εργασία από το σπίτι είναι αρκετά διαδεδομένη. Ωστόσο αρκετοί επιτήδειοι προσπαθούν να εκμεταλλευτούν την γενικευμένη κρίση που βιώνει η χωρά και την μεγάλη ζήτηση εργασίας αποκομίζοντας χρηματικά οφέλη. Ο χρήστης θα πρέπει να ερευνήσει την υπόσταση και την φήμη της εταιρίας πριν προβεί σε οποιαδήποτε ενέργεια. Παρόμοιες απάτες εμφανίζονται με την μορφή εκπαιδευτικής ευκαιρίας.
- Υποκλοπή προσωπικών δεδομένων: πρόκειται για υποκλοπή προσωπικών δεδομένων με σκοπό την μεταβίβαση τους και την χρήση τους από τρίτα άτομα τα οποία προβαίνουν σε συναλλαγές με «κλεμμένα» προσωπικά δεδομένα. Οι συνηθέστερες μορφές αυτού είναι η κλοπή ταυτότητας και η υποκλοπή προσωπικών δεδομένων. Η υποκλοπή συνήθως εμφανίζεται σε τραπεζικές συναλλαγές όπου ο είσβαλες προσπαθεί να υποκλέψει τους ηλεκτρονικούς

[20] http://www.commoncriteria.org/, 13/09/2016
[21] Helena Lindskog and Stefan Lindskog, Web Site Privacy with P3P, Wiley Publishing, 2003, pp. 5-10
[22] Simson Garfinkel with Gene Spafford, Web Security, Privacy & Commerce, O'REILLY, 2002, 2nd Edition, pp.399

κωδικούς τραπέζης μέσα από ένα ψεύτικο «παράθυρο» που παρακινεί τον χρήση να αποστείλει τους κωδικούς μέσω ηλεκτρονικού ταχυδρομικού.

- Υπόσχεση παροχής υπηρεσιών: αναφέρεται σε προπληρωμένες υπηρεσίες οι οποίες μετά την πληρωμή δεν παρέχονται στον χρήστη.
- Ψευδή επιχειρηματικά σχέδια και χειραγώγηση της αγοράς: συνηθέστερη μορφή είναι η παραπληροφόρηση σχετικά με την χρηματιστηριακή αγορά και την αξία μέτοχων.[23]

Οι δράστες αυτών των υποθέσεων ποικίλουν ανάλογα με τα κίνητρα τους, ωστόσο μπορούν να χωριστούν σε τέσσερίς (4) βασικές κατηγορίες. Η πρώτη κατηγορία αναφέρεται στους ερασιτέχνες, οι οποίοι έχοντας βασικές γνώσεις διείσδυσης σε πληροφοριακά συστήματα κατά την διάρκεια της περιήγησης τους επιτυγχάνουν την είσοδο σε συστήματα χαμηλής προστασίας- ασφάλειας. Έπειτα ο κακόβουλος εισβολέας, ο οποίος εισέρχεται με σκοπό να βλάψει και να υποκλέψει δεδομένα, οι εισβολείς που στοχεύουν αποκλειστικά σε εταιρίες (συνήθως πρόκειται για οργανωμένες επιθέσεις με οικονομικά ή αλλού είδους οφέλη) και τέλος, οι «τρομοκράτες», οι οποίοι έχοντας κυρίως στόχο τους πολίτικους οργανισμούς αποσκοπούν στην δημιουργία εντυπώσεων, στην ταχεία μεταφορά του μηνύματος που θέλουν να εκπέμψουν και στην προσβολή αρχείων στους ιστότοπους.[24]

1.3.3 Κακόβουλο Λογισμικό

I. Malware

Όπως φανερώνει και η ετυμηγορία των λέξεων από τις οποίες προσέρχεται ο ορός (malicious- software) πρόκειται για ένα βλαβερό λογισμικό που βάλει τον υπολογιστή και τον χρήστη του. Ο όρος περιλαμβάνει τους ιούς που προκαλούν ζημίες στον υπολογιστή, τα σκουλήκια δηλαδή τους ηλεκτρονικούς ιούς, τους Δούρειους Ίππους (Trojan horses) που εγκαθίστανται από τους χρήστες μέσα από φαινομενικά ακίνδυνα προγράμματα και καταγράφουν τη δραστηριότητα τους, τα Spyware, ένα ακόμα σύστημα παρακολούθησης του χρήστη που κατεβαίνει από το διαδίκτυο, και τέλος το Scum ware, το οποίο αλλάζει την εμφάνιση των ιστοσελίδων που επισκέπτεται ο χρήστης αλλάζοντας και τις διαφημίσεις προωθώντας δικούς του πωλητές.[25] Οι χρήστες για να προστατευτούν από την

[23] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 98

[24] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 4th Edition, 2007, pp. 21-23

[25] Βλαχόπουλος Κωνσταντίνος, Ηλεκτρονικό Έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, 2007, σελ. 39

απειλή μπορούν να εγκαταστήσουν Anti-Malware Software, αμυντικό λογισμικό που εμποδίζει την εισροή στον ηλεκτρονικό υπολογιστή του χρήστη.[26]

II. Phishing

Το εν λόγο λογισμικό επιχειρεί να αποσπάσει προσωπικές πληροφορίες των χρηστών, τραπεζικούς κωδικούς και κωδικούς πρόσβασης και να αποσπάσει χρηματικά ποσά. Καθημερινά συμβαίνουν περίπου 7 εκατομμύρια απόπειρες. Αξίζει να σημειωθεί πως το 46% των Phishing server βρίσκονται στις Η.Π.Α.

III. Dialers

Πρόκειται για ένα προγράμματα ο οποίο το εγκαθιστά στον υπολογιστή ο ίδιος ο χρήστης αφού φέρει την μορφή χρήσιμου προγράμματος. Αφού εγκατασταθεί μεταφέρει τις γραμμές σε γραμμές υψηλής χρεώσεις και πολλές φορές πραγματοποιεί κλήσεις εξωτερικού. Το ίδιο πρόγραμμα φέρουν και ορισμένα προγράμματα που εμφανίζονται ως χωρίς χρέωση. Ο χρήστης θα πρέπει να είναι ιδιαιτέρως προσεκτικός στην εγκατάσταση τυχαίων προγραμμάτων. Επιπλέων μπορούν να καταφύγουν στον ΟΤΕ κάνοντας φραγή κλήσεων εξωτερικού με σκοπό να αποτρέψουν την χρέωση. Παράλληλα στην αγορά υπάρχουν προγράμματα anti-Dialer, τα οποία προστατεύουν τον υπολογιστή από την εγκατάσταση Dialer και καθαρίζουν τον υπολογιστή σε περίπτωση υπάρχουσας εγκατάστασης.[27]

1.4 Ιστοσελίδες Κοινωνικής Δικτύωσης

Πρόκειται για ιστοσελίδες που η αρχική ιδέα της δημιουργίας τους ήταν η επαφή ατόμων με κοινά ενδιαφέροντα και η ανταλλαγή ιδεών.[28] Αργότερα δημιουργήθηκαν μονοθεματικες ιστοσελίδες, ιστοσελίδες δηλαδή όπου όλοι οι συμμετέχοντες συζητάνε πάνω σε ένα συγκεκριμένο θέμα. Χαρακτηριστικό παράδειγμα αποτελεί το Patientslikeme οπού ιατροί και ασθενείς μπορούν να έρθουν σε επικοινωνία. Στις ιστοσελίδες ο χρήστης διαμορφώνει έναν εικονικό χαρακτήρα που αλλάζει σύμφωνα με τα ενδιαφέροντά και την ψυχική του διάθεση μέσα από τις προσωπικές πληροφορίες που παραχωρεί, τις φωτογραφίες και βίντεο που αναρτεί. Οι ιστοσελίδες κοινωνικής δικτύωσης περιέχουν

[26] Helena Lindskog and Stefan Lindskog, Web Site Privacy with P3P, Wiley Publishing, 2003, pp.27
[27] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, εικονικός κόσμος και νέες τεχνολογίες, Κλειδάριθμος, σελ. 101-104
[28] Ι. Ιγγλεζάκη, Ελευθερία Έκφρασης Και Ανωνυμία Στο Διαδίκτυο: Το Παράδειγμα Των Ιστολογίων, ΔΙΜΕΕ τεύχος 3/2011, σελ. 317-319

chatrooms, ομάδες κοινών ενδιαφερόντων, δυνατότητα ανάρτησης αρχείων-φωτογραφιών- video κα.[29]

Το όφελος των χρηστών από την χρήση του κοινωνικού δικτύου εξαρτάται κυρίως από τον αριθμό των μελών που αυτό απαρτίζεται. Δίκτυα με περισσοτέρους χρήστες συμβάλουν περισσότερο στην πνευματική και κοινωνική εξέλιξη των χρηστών τους μέσα από την υιοθέτηση νέων ιδεών. Η επικοινωνία, τα κοινά ενδιαφέροντα των χρηστών, η πνευματική και μη προσφορά του διαδικτυακού τόπου, η δόμηση του, ο ρόλος του υπευθύνου δικτύου (σύμβολο της ασφάλειας των χρηστών) και οι ξεκάθαροι στόχοι δημιουργίας του δικτύου, είναι τα κυριότερα χαρακτηριστικά της επιτυχίας του.

Οι δημοφιλέστερες ιστοσελίδες κοινωνικής δικτύωσης αναλύονται παρακάτω:

1.5 Facebook

Το Facebook με πάνω από 1,43 δισεκατομμύρια χρήστες το 2015 είναι μια από τις δημοφιλέστερες υπηρεσίες κοινωνικής δικτύωσης, στην οποία το κάθε άτομο μπορεί να έχει πρόσβαση χωρίς συνδρομή. Η χρήση του είναι η επικοινωνία των μελών του μέσω μηνυμάτων, εικόνων, βίντεο και κοινοποιήσεων. Η λειτουργία του στηρίζεται πάνω στα προσωπικά δεδομένα που οι ίδιοι οι χρήστες παραχωρούν και στην μετέπειτα χρήση τους για διαφημιστικούς σκοπούς.[30]

Εικόνα 2: Το λογότυπο του Facebook

1.5.1 Συλλογή προσωπικών δεδομένων

Η πολιτική συλλογής δεδομένων που εφαρμόζει το Facebook στηρίζεται πάνω σε πολύπλευρα δεδομένα και πληροφορίες. Η απευθείας ανάκτηση προσωπικών πληροφορίων από τον χρήστη, όπως φωτογραφίες, διάρκεια συνομιλίων, sites που επισκέπτεται συχνά και τοποθεσίες, συνδυαστικά με τις πληροφορίες που συλλέγονται από

[29] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ.138-148

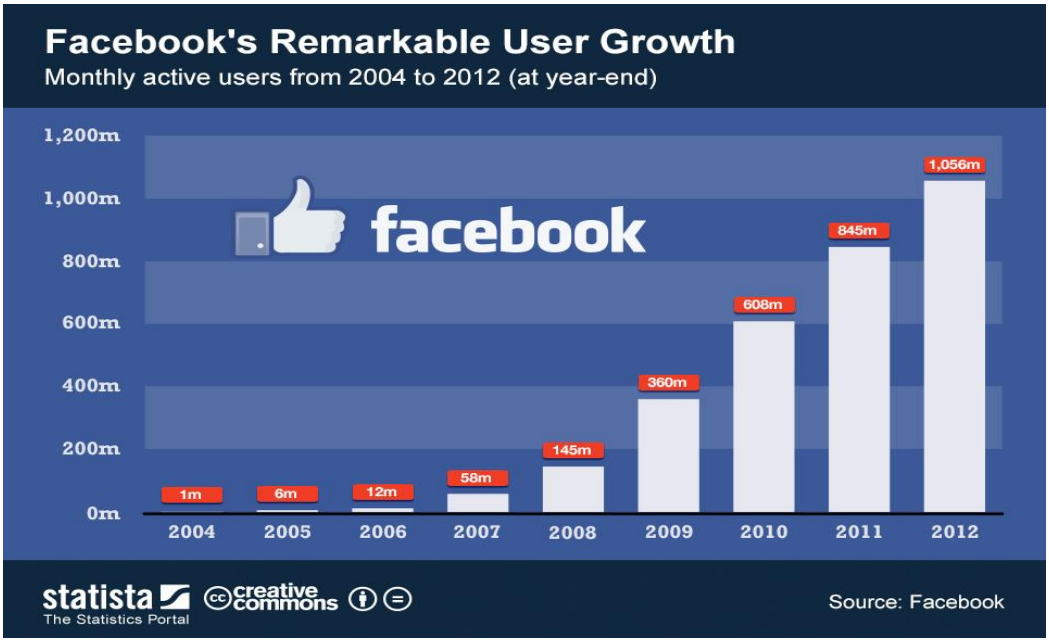
[30] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, ό.π., σελ.140

τα προφίλ τρίτων για τον χρήστη πχ. κοινοποιήσεις ή μηνύματα, συνθέτουν μια ολοκληρωμένη εικόνα του κοινωνικού προφίλ του χρήστη ως προς τα στοιχεία που συλλεγεί το Facebook. [31]

Η αποδοχή πρόσβασης της εφαρμογής στις επαφές των συσκευών αυτομάτως δίνει το δικαίωμα για καταγραφή των επαφών του χρήστη και την μετέπειτα χρήση τους. Το ίδιο ισχύει και για την χρήση οποιασδήποτε συσκευής που θα εγκατασταθεί το πρόγραμμα του Facebook. Με τη χρήση του Facebook για αγορές μέσω πιστωτικής κάρτας δίνεται το δικαίωμα στον κοινωνικό ιστότοπο να αποθηκεύσει πληροφορίες σχετικά με τις αγορές όπως η συχνότητα, το ποσό, τα στοιχεία της κάρτας κα. Χαρακτηριστικά όπως το λειτουργικό σύστημα, η έκδοση υλικού, οι ρυθμίσεις της συσκευής, τα ονόματα και οι τύποι αρχείων και εφαρμογών λογισμικού, οι τοποθεσίες συσκευής και οι πληροφορίες σύνδεσης, είναι μερικές μόνο από τις πληροφορίες που συλλέγονται. Τέλος συνεργάτες του Facebook (Facebook Payments Inc., Atlas, Instagram LLC, Onavo , Parse, Moves, Oculus, LiveRail, WhatsApp Inc., Masquerade) και διαφημιζόμενες εταιρίες παρέχουν στο Facebook οποιαδήποτε πληροφορία διαθέτουν για τους χρήστες.[32]

Σε περίπτωση που ο χρήστης θελήσει να διαγράψει την προσωπική του σελίδα στον ιστοχώρο απαιτείται χρόνος. Το αίτημα για διαγραφή του χρήστη γίνεται δεκτό και ο λογαριασμός διαγράφεται έπειτα από λίγα εικοσιτετράωρα με την προϋπόθεση ότι δεν έχει υπάρξει ενδιάμεση σύνδεση σε αυτόν. Τα προσωπικά δεδομένα σβήνονται με εξαίρεση συνομιλίες και κοινοποιήσεις από λογαριασμούς τρίτων προσώπων τα ποια εξακολουθούν να υπάρχουν. Τα προσωπικά δεδομένα παραμένουν έως 90 μέρες στα αντίγραφα ασφάλειας μέχρι να διαγράφουν, ενώ ορισμένα προσωπικά δεδομένα δεν διαγράφονται ποτέ και παραμένουν καταγεγραμμένα χωρίς όμως την άμεση σύνδεση με το άτομο που αντιστοιχούν.[33]

[31] https://www.facebook.com/privacy/explanation, 3/10/2016
[32] https://www.facebook.com/help/111814505650678, 3/10/2016
[33] https://www.facebook.com/help/125338004213029 , Ποια είναι η διαφορά μεταξύ απενεργοποίησης και διαγραφής του λογαριασμού μου;, 3/10/2016



Εικόνα 3: Αύξηση χρηστών του Facebook κατά τα έτη 2004-2012 34

1.5.2 Η χρήση των συλλεχθεντων πληροφοριών

Η χρήση των συλλεχθεντων πληροφοριών ποικίλει. Η ευκολία του χρήστη τίθεται σε πρωταρχική θέση με την επεξεργασία των πληροφοριών για εύκολη εύρεση δραστηριοτήτων που θα ενδιαφέρουν τον χρήστη, τις προτάσεις για εκδηλώσεις σε κοντινά μέρη, και την αυτοματοποίηση κάποιων εφαρμογών όπως η αυτόματη εισαγωγή πρόσθεσης με το προφίλ κάποιου αλλού χρήστη σε φωτογραφίες. Όλα αυτά γίνονται μέσα από αυτοματοποιημένες διαδικασίες και την διασφάλιση της προστασίας μέσα από τον έλεγχο των χρηστών περί ψευδών στοιχείων και απάτης. [35]

Το Facebook παρέχει στοιχεία σε εταιρείες για διαφημιστικούς σκοπούς χωρίς ωστόσο να προβαίνει στην αποκάλυψη της ταυτότητας του χρήστη. Τα στοιχεία περιορίζονται στις βασικές πληροφορίες που θα βοηθήσουν στις στατιστικές έρευνες και στην τόνωση του ενδιαφέροντος του κοινού. Για να προβεί σε αποκάλυψη προσωπικών στοιχείων απαιτείται η άδεια του χρήστη, εκτός και αν αφορά αλλαγή ιδιοκτησίας καθεστώτος. Επιπλέον μεταβιβάζονται σε περίπτωση που θεωρηθεί πως το άτομο μπορεί να βλάψει τον εαυτό του ή να εξαπατήσει άλλους χρήστες (έπειτα από νομικό αίτημα ή την εντολή της δίωξης ηλεκτρονικού εγκλήματος), ή υπόκειται νομική παραβίασή.[36]

[34] https://www.statista.com/chart/870/facebooks-user-growth-since-, 17/12/2016
[35] https://www.facebook.com/privacy/explanation, 3/10/2016
[36] https://www.facebook.com/privacy/explanation, 3/10/2016

1.5.3 Η ασφάλεια των προσωπικών δεδομένων

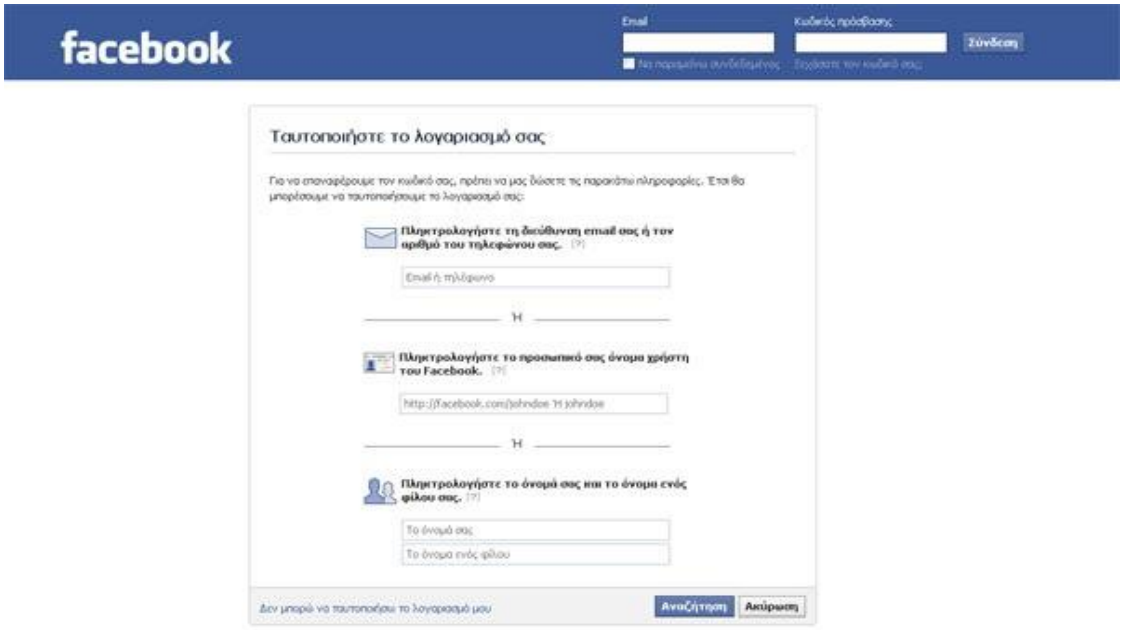
Το Facebook στην σελίδα που διαθέτει για την ενημέρωση των χρηστών σχετικά με τις βασικές ρυθμίσεις απορρήτου, αναφέρει, πως μέσα από τα ειδικά εργαλεία παρακολούθησης δικτύου και κρυπτογράφησης που διαθέτει εγγυάται την ασφάλεια των προσωπικών δεδομένων των χρηστών.[37]

Ο Έλεγχος Ασφάλειας είναι ένα πρόγραμμα το οποίο βοηθάει τον χρήστη να προστατέψει τις ήδη υπάρχουσες λειτουργίες ή να προσθέσει νέες. Μέσα από αυτόν ο χρήστης μπορεί να λάβει άμεσα ειδοποιητικό email όταν κάποιος προσπαθήσει να συνδεθεί με τον λογαριασμό του από νέα συσκευή, να αποσυνδεθεί από μη χρήσιμες προς αυτόν εφαρμογές και προγράμματα περιήγησης, και τέλος, να ενημερωθεί για την προστασία του κωδικού πρόσβασης που διαθέτει. Συγκεκριμένα σύμφωνα με τις οδηγίες συνίσταται προσοχή κατά την είσοδο του χρήστη από συσκευές που δεν ανήκουν στην ιδιοκτησία του, και προτρέπει την αποσύνδεση του αμέσως μετά την χρήση. Επιπλέον συνιστά ο κωδικός να είναι αρκετά πρωτότυπος και να μην κοινοποιείται. Η προστασία του υπολογιστή από ιούς και κακόβουλο λογισμικό είναι εξίσου σημαντική όπως και η σύνδεση με ένα αξιόπιστο- προσωπικό email. Οδηγίες που έχει κοινοποίηση συμβουλεύουν τους χρήστες για μη αποδοχή αγνώστων χρηστών και για αποφυγή επισκέψεων ύποπτων σελίδων και προφίλ.[38]

Σε μια προσπάθεια για μείωση του κίνδυνου των χρηστών έχουν δημιουργηθεί ειδικά τμήματα που ασχολούνται αποκλείστηκα με την ασφάλεια. Ο εντοπισμός κακόβουλου λογισμικού και η ενημέρωση των χρηστών για την ύπαρξή του, οι επιπρόσθετες πληροφορίες που ζητούνται καθώς και η χρήση του πραγματικού ονόματος του χρήστη είναι μερικές από τις τακτικές που χρησιμοποιεί. Επιπροσθέτως, ο κάθε χρήστης μπορεί να αναφέρει ύποπτη ή ανάρμοστη συμπεριφορά εντός της ιστοσελίδας και να καταγγείλει την υποψία παραβίασης του λογαριασμού του.

Το Facebook, θέλοντας να βοηθήσει τους χρήστες να ανακτήσουν τον έλεγχο των προφίλ τους σε περίπτωση απώλειας κωδίκων έχει ρυθμίσει ορισμένες δικλίδες ασφάλειας. Η ανάκτηση του ελέγχου γίνεται μέσω του email που έχει δηλώσει ο χρήστης, μιας ερώτησης ασφάλειας που έχει απαντηθεί κατά την δημιουργία του λογαριασμού, ή ακόμα και μέσω των έμπιστων επαφών.

[37] Τα προσωπικά δεδομένα σας, https://www.facebook.com/help/330229433729799/, 3/10/2016
[38] https://www.facebook.com/help/android-app/799880743466869?ref=related, 3/10/2016



Εικόνα 4: Ταυτοποίηση λογαριασμού χρήστη

1.7 Twitter

Το Twitter, με σήμα το καναρίνι, δημιουργήθηκε τον Μάρτιο του 2006 από τον Τζακ Ντορσει. Η δημοτικότητά του το κατατάσσει στα 10 πιο δημοφιλή site κοινωνικής δικτυώσεις αριθμώντας το 2015, 313 εκατομμύρια ενεργούς χρήστες. Το Twitter εντάσσεται στην κατηγορία microbrogging καθώς ο ιστοτοπος δίνει την δυνατότητα στους χρήστες να δημοσιεύουν μηνύματα μικρότερα των 140 χαρακτήρων. [39]

Η χρήση του παρουσιάζει ομοιότητες με του Facebook. Ο χρήστης για να μπορέσει να εισέλθει στο Twitter πρέπει να εγγραφεί στην σελίδα. Τα στοιχεία που απαιτούνται για την πραγματοποίηση την εγγραφής είναι πιο περιορισμένα από εκείνα που ζητάει το Facebook. Έπειτα ο χρήστης μπορεί να διαμορφώσει το προσωπικό του προφίλ κατά βούληση. Κάθε δημοσίευση ονομάζεται στον κόσμο του Twitter «tweet» (τιτίβισμα). Όλοι οι χρήστες του διαδικτύου μπορούν να δουν την δημοσίευση αλλά πρέπει να διαθέτουν λογαριασμό και να ακολουθούν (follow) τον χρήστη για να εμφανίζονται όλες οι δημοσιεύσεις του και να είναι δυνατός ο σχολιασμός τους. Το οροί των 140 λέξεων υπάρχει και στον σχολιασμό δημοσιεύσεων. Η βασική διαφορά με το Facebook τίθεται στην διαδικασία που συνδέονται οι χρήστες. Ενώ στο Facebook το αίτημα φίλιας πρέπει να αποδεχτεί από τον χρήστη , στο Twitter ο χρήστης μπορεί να ακολουθήσει ένα πρόσωπο χωρίς να δοθεί η έγκριση του δευτέρου. Επιπλέον δεν χρειάζεται ο δεύτερος χρήστης να ακολουθήσει με την σειρά του τον πρώτο.

[39] https://about.twitter.com/company, 3/10/2016

Το όριο χαρακτήρων και τα σύντομα μηνύματα (hashtag) που συνοδεύουν τις δημοσιεύσεις κάνουν το Twitter ένα από τα πιο εύκολα, και γρηγορά στην χρήση κοινωνικά δίκτυα. Η χρήση του δεν περιορίζεται μόνο στην διασκέδαση των χρηστών του αλλά έχει επεκταθεί. Πολλές εταιρίες χρησιμοποιούν το Twitter για την άμεση ενημέρωση των εργαζομένων τους, όπως και πολλά μέσα μαζικής ενημερώσεις για την γρήγορη μετάδοση των ειδήσεων.

Εικόνα 5: Το λογότυπο του Twitter

1.7.1 Η προστασία των προσωπικών δεδομένων

Το Twitter ως μέσο κοινωνικής δικτύωσης είναι εξ ορισμού ανοιχτό στην μετάδοση των πληροφοριών των χρηστών του. Ο χρήστης κατά την διάρκεια της εγγραφής του αμέσως ενημερώνεται από ένα παράθυρο στο πάνω μέρος της σελίδας πως τα δεδομένα του που θα συλλέγονται και θα μεταβιβάζονται σε άλλες χώρες της Ευρώπης. Με την χρήση του twitter ο χρήστης παραχωρεί στην ιστοσελίδα κάθε δικαίωμα για χρήση, αντιγραφή, αναπαραγωγή, επεξεργασία, προσαρμογή, τροποποίηση, δημοσίευση, μετάδοση , προβολή και διανομή των πληροφοριών του χρήστη.[40] Στην προστασία προσωπικών δεδομένων του site αναφέρεται πως με την χρήση της σελίδας ο χρήστης δίνει αυτόματη άδεια για την συλλογή και τη επεξεργασία των προσωπικών του δεδομένων και την μεταφορά τους στις ΗΠΑ και στην Ιρλανδία και σε άλλες χώρες για χρήση τους από το ίδιο το Twitter. Παρ' όλα αυτά, το άτομο μπορεί να επιλέξει ορισμένες δημοσιεύσεις του να είναι προστατευμένες ορίζοντας ο ίδιος το κοινό προβολής του το οποίο όμως μπορεί να επαναδημοσιεύσει την δημοσίευση καθιστώντας την δημόσια. [41]

Επιπλέον το Twitter δεν φέρει οποιαδήποτε ευθύνη σχετικά με το περιεχόμενο των δημοσιεύσεων διατηρώντας παράλληλα το δικαίωμα να αφαιρέσει περιεχόμενο το οποίο φέρεται να παρεκκλίνει. Το Twitter έχει το δικαίωμα απενεργοποίησης λογαριασμών χρηστών με παραβατική συμπεριφορά.

[40] https://twitter.com/tos?lang=en#privacy, 30/09/2016
[41] https://twitter.com/privacy?lang=en, 30/9/2016

Ο χρήστης μπορεί να διαγράψει τον λογαριασμό του απενεργοποιώντας τον και διακόπτοντας τη χρήση των Υπηρεσιών. Επίσης αν υπάρξει παύση χρήσης των Υπηρεσιών χωρίς απενεργοποίηση του λογαριασμού, ο λογαριασμός μπορεί να απενεργοποιηθεί λόγω της παρατεταμένης αδράνειας.[42]

Με την προτροπή για χρήση ισχυρών κωδικών πρόσβασης και την αλλαγή τους σε τακτά χρονικά διαστήματα επιχειρείται η αποτροπή κρουσμάτων παραβίασης. Σε περίπτωση που απευθυνθεί καταγγελία για πλαστοπροσωπία ή παραβίαση λογαριασμού το Twitter κινεί όλες τις νόμιμες διαδικασίες για να εξακριβώσει την εγκυρότητα των καταγγελιών και να λάβει τα απαραίτητα μέτρα.

1.6 LinkedIn

Το LinkedIn με 332 εκατομμύρια χρήστες το 2014 και 2,7 εκατομμύρια εταιρικά προφίλ, είναι ο πιο πετυχημένος ισόχωρος επαγγελματικής κοινωνικής δικτύωσης. Ιδρύθηκε τον Δεκέμβριο του 2002 από τον Ρεντ Χόφμαν ενώ η επίσημη έναρξη του έγινε στις 5 Μάιου 2003. Η χρήση του δικτύου είναι αμιγώς επαγγελματική. Κάθε χρήστης-εταιρία μπορεί να εγγραφεί στην σελίδα και να διαμορφώσει το προσωπικό του προφίλ. Εργασιακή εμπειρία, σπουδές, ξένες γλώσσες, εθελοντισμός είναι μερικά μόνο από τα στοιχεία που μπορούν να συμπεριληφθούν στο προσωπικό προφίλ. Έπειτα δίνεται η δυνατότητα σύνδεσης με άλλους χρήστες με σκοπό την αλληλεπίδραση και την εύρεση εργασίας. Σε πιο σπάνιες περιπτώσεις μαθητές εγγράφονται στο LinkedIn για να μπορέσουν να διαμορφώσουν μια γενική εικόνα ζήτησης και ευκαιριών του κλάδου προτίμησης τους.[43]

Στους επαγγελματίες δίνεται η δυνατότητα μέσα από την σύνδεση με το LinkedIn να δημιουργήσουν ένα δίκτυο επαφών με άλλους επαγγελματίες διευρύνοντας τον επαγγελματικό κύκλο, δημιουργώντας νέες συνεργασίες και καινοτόμες ιδέες. Μέσα από την δικτύωση με απλούς χρήστες, μπορούν να βρουν εύκολα και γρηγορά το κατάλληλο εργατικό δυναμικό μέσα από τα online βιογραφικά που έχουν αναρτήσει οι χρήστες. Επιπλέον μέσα από κοινές επαφές επαγγελματία-χρήστη είναι ευκολότερη η εύρεση συστάσεων.

[42] https://twitter.com/tos?lang=en#privacy, 30/09/2016
[43] https://ourstory.linkedin.com/#year-2014, 7/10/2016

Εικόνα 6: Το λογότυπο του LinkedIn

1.6.1 Δημιουργία λογαριασμού

Ο χρήστης που επιθυμεί να δημιουργήσει λογαριασμό μπορεί να επισκεφτεί την επίσημη ιστοσελίδα του και να καταχωρίσει τα στοιχεία που απαιτούνται όπως το όνομα, το επίθετο , το email και να δημιουργήσει ένα κωδικό 6 ψηφίων με τον οποίο θα μπορεί να πραγματοποιεί σύνδεση από οποιονδήποτε υπολογιστή. Έπειτα ο χρήστης λαμβάνει ένα email στην δηλωμένη διεύθυνση ηλεκτρονικού ταχυδρομείου η οποία επιβεβαιώνει την σύνδεση και τα δοθέντα στοιχεία.

Στην συνέχεια η ιστοσελίδα βοηθάει στην δημιουργία του προφίλ. Αναλόγως αν ο χρήστης εργάζεται ή όχι ανοίγει η αντίστοιχη σελίδα οπού πρέπει να συμπληρωθούν όλα τα στοιχεία με σκοπό την δημιουργία μιας ολοκληρωμένης εικόνας στον υποψήφιο εργοδότη. Περνώντας στο επόμενο βήμα και προς ευκολία του χρήστη το LinkedIn δίνει την ευκαιρία της αυτόματης μεταφοράς των αποθηκευμένων επαφών του χρήστη από το ηλεκτρονικό ταχυδρομείο του απευθείας στο LinkedIn. Έπειτα εμφανίζονται προτάσεις φίλιας ατόμων που ενδεχομένως να γνωρίζει ο χρήστης. Η εύρεση των προτάσεων γίνεται με τον συσχετισμό πληροφοριών του χρήστη. Τελευταίο βήμα για την ολοκλήρωση δημιουργίας προφίλ είναι η απάντηση σε ορισμένες ερωτήσεις. Λόγο του ότι η σελίδα του LinkedIn δεν παρέχεται στα ελληνικά, ο χρήστης που ζει στην Ελλάδα μπορεί να παραλείψει ορισμένες ερωτήσεις που δεν αντιστοιχούν στα δεδομένα της χωράς.[44]

1.6.2 Χρήση δεδομένων

Ο χρήστης κατά την εγγραφή του στο LinkedIn αποδέχεται εκούσια τους όρους χρήσης των προσωπικών του δεδομένων που ορίζει η εφαρμοστέα Πολιτική Προστασίας Προσωπικών Δεδομένων και η Συμφωνία Χρήστη της ιστοσελίδας, και είναι υπεύθυνος για τις πληροφορίες που δημοσιεύει εντός της πλατφόρμας. Η αποκάλυψή προσωπικών στοιχείων εντός ομάδων ή σε δημόσια χρήση δεν υπόκεινται στην πολιτική προστασίας προσωπικών δεδομένων και ως εκ τούτου δεν προστατεύονται.

[44] https://www.linkedin.com/uas/login, 7/10/2016

Πιο συγκεκριμένα τα δεδομένα που παρέχονται στο σύστημα μπορούν να συλλεχθούν, να επεξεργαστούν και να μεταβιβαστούν σε τρίτους. Η χρήση των προσωπικών πληροφοριών του μέλους γίνεται με γνώμονα την διευκόλυνση και την πλήρη αξιοποίηση την πλατφόρμας. Μηχανές αναζήτησης που κατέχουν τα προσωπικά στοιχεία του μέλος βοηθάνε στην ευκολότερη και ταχύτερη εύρεση του κατάλληλου υποψήφιου για τους εργοδότες, αλλά βοηθούν και τους υποψήφιους εργαζομένους να ανακαλύψουν την κατάλληλη για αυτούς θέση μέσα σε ένα δίκτυο προσφοράς και ζήτησης. Σε περίπτωση που κατά την χρήση της ιστοσελίδας επιθυμείτε η τροποποίηση των όρων χρήσης, υπάρχει η δυνατότητα αλλαγής τους από τις ρυθμίσεις του λογαριασμού. Το LinkedIn είναι σε συνεχή επικοινωνία με τον χρήστη μέσω email και μηνυμάτων στην πλατφόρμα του ιστοτοπου με σκοπό την ενημέρωσή τους για τυχών αλλαγές απορρήτου, διαθέσιμες υπηρεσίες αλλά και διαφημίσεις συνεργαζόμενων εταιριών.

Το LinkedIn μοιράζεται όλα τα δεδομένα που συλλεγεί με τις θυγατρικές της εταιρίες. Επιπλέον τα προσωπικά δεδομένα διανέμονται και σε αλλά μέσα κοινωνικής δικτυώσεις που δεν υπόκεινται στην δικαιοδοσία του σε περίπτωση που ο χρήστης επιλέξει να συνδέσει τον λογαριασμό του. Επιπλέον δεσμεύεται πως δεν διανέμει τις προσωπικές πληροφορίες του χρήστη εκτός κι αν τίθεται νομικό ζήτημα, παράβαση δεδομένων τρίτων, ή προστασία της ασφάλειας του LinkedIn. Αντιθέτως οι δημοσιές πληροφορίες είναι ευκολοπροσβάσημες από κάθε μέλος ή και μη, της διαδικτυακής κοινότητας.

Το LinkedIn διεξάγει σε τακτά χρονικά διαστήματα έρευνες και δημοσκοπήσεις στις οποίες ο χρήστης καλείτε να συμμετάσχει. Η συμμετοχή των χρηστών δεν είναι απαραίτητη αν δεν το επιθυμούν καθώς μερικές από τις οποίες είναι ονοματικές. Τα δεδομένα που συλλέγονται ενδέχεται να περιλαμβάνουν και περαιτέρω προσωπικές πληροφορίες με την συναίνεση του χρήστη. Παρ'όλα αυτά έρευνες πραγματοποιούνται και χωρίς την συμμετοχή των χρηστών στις οποίες οι πληροφορίες που παρέχει ο χρήστης συλλέγοντα και επεξεργάζονται στα πλαίσια ερευνάς και ανάπτυξης για την παροχή καλυτέρων υπηρεσιών.

Τέλος, το LinkedIn χρησιμοποιεί τεχνολογία αυτόματης σάρωσης με σκοπό τον εντοπισμό κακόβουλων λογισμικών και spam για την ενίσχυση της ασφάλειας των χρηστών.[45]

[45] https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv, 03/09//2016

1.6.3 Προστασία προσωπικών δεδομένων

Το πρόβλημα των προσωπικών δεδομένων παρουσιάζεται και στην περίπτωση του LinkedIn. Πληθώρα προσωπικών δεδομένων που αναρτούν οι χρήστες τους κοινοποιείται σε όλους τους χρήστες της ιστοσελίδας. Το ίδιο το site δίνει την δυνατότητα να προστατευθούν τα προσωπικά δεδομένα μέσα από μια σειρά ενεργειών. Ο χρήστης μέσα από της ρυθμίσεις του προφίλ του μπορεί να αλλάξει το κοινό δημοσιεύσεων των αλλαγών του προσωπικού του προφίλ, των δημοσιεύσεων του και των επαφών , επιλέγοντας τα άτομα που επιθυμεί να ενημερώνονται για τις αλλαγές. Το LinkedIn ενημερώνει τον χρήστη για κάθε επισκευή στο προφίλ τους παρέχοντας τα στοιχεία του ατόμου που το επισκέφτηκε. Και ο επισκέπτης όμως έχει την δυνατότητα μερικής ή ολικής κάλυψης των στοιχείων του. Τέλος σε αντίθεση με αλλά site, ο χρήστης μπορεί να επιλέξει το κοινό που επιθυμεί να εμφανίζεται η φωτογραφία του.[46]

Μια ακόμα σημαντική δυνατότητα που δίνει το site στους χρήστες του είναι να επιλέξουν οι ίδιοι μέσα από την κατηγορία “Manage Advertising Preference” αν δίνουν την έγκρισή τους στο site να χρησιμοποιήσει την φωτογραφία και το όνομα του χρήστη για διαφημιστικούς σκοπούς σε αλλά κοινωνικά δίκτυα. Επιπλέον συλλέγοντας προσωπικά δεδομένα εμφανίζει διαφημίσεις που ενδιαφέρουν τον χρήστη μέσα από τις ενέργειες του . Και αυτή η υπηρεσία είναι απενεργοποιεί σιμή από τον χρήστη.

Συνοψίζοντας η πολιτική απορρήτου το LinkedIn είναι πολύ φιλική προς τον χρήστη. Το ίδιο το άτομα είναι σε θέση να ελέγχει που θα εμφανίζονται τα προσωπικά του δεδομένα και ποιοι μπορούν να κάνουν χρήση τους. Σε αυτό ενδεχομένως να οφείλεται και ο καθαρά επαγγελματικός χαρακτήρας του δικτύου που απαιτεί απόλυτη διασφάλιση του μεγάλου όγκου των προσωπικών στοιχείων.

Παρ’όλα αυτά τον Μάϊο του 2016 το LinkedIn ζήτησε από χιλιάδες χρήστες του να αλλάξουν τους κωδικούς τους αντικαθιστώντας τους με πιο ισχυρούς και να διασφαλίσουν τα στοιχεία τους. Ο λόγος ήταν οι υποκλοπές που σημειωθήκαν στα προφίλ χιλιάδων χρηστών. Όπως αναφέρει το RT[47] ο χάκερ “PEACE” πούλησε email και password, 117 εκατομμύριων λογαριασμών, μέσα στους οποίους βρίσκονταν και ελληνικοί. Την Πέμπτη 19 Μαΐου 2016 το LinkedIn έστειλε μήνυμα ηλεκτρονικού ταχυδρομείου σε όλους τους Έλληνες χρήστες του να αλλάξουν τους κωδικούς τους (CNN Greece).

[46] https://www.linkedin.com/help/linkedin?lang=en
[47] http://www.cnn.gr/money/tech/story/32746/logariasmoi-toy-linkedin-poloyntai-sto-darknet , 30/9/2016

1.8 Pinterest

Το Pinterest, είναι ένα νέος δημοφιλής κοινωνικός ιστοτοπος που ιδρύθηκε τον Μάρτιο του 2010 και απευθύνεται σε ενήλικους και παιδιά άνω των 13 ετών. Η φιλοσοφία του Pinterest διαφέρει από του Facebook. Πρόκειται για μια νέα ιδέα στον χώρο των ιστοσελίδων που συνδυάζει την κοινωνική δικτύωση με τα προσωπικά ενδιαφέροντα του κάθε χρήστη. Οι θεματικές ενότητες που αναλύονται ποικίλουν και καλύπτουν σχεδόν κάθε πτυχή της καθημερινής ζωής. Χειροτεχνίες, κηπουρική, μαγειρική, ζαχαροπλαστική, μόδα, μακιγιάζ, έξυπνες λύσεις, εικόνες από δυσπρόσιτα μέρη, δώρα, εκπαίδευση, μουσική , τεχνολογία, μηχανικά, περίεργα, χιούμορ, ιστορία είναι λίγα μόνο από τα θέματα που μπορεί να ανακαλύψει ο χρήστης. Κατά την εγγραφή του στο Pinterest ο χρήστης μπορεί να επιλέξει τα ενδιαφέροντα του μέσα από ένα πολύ μεγάλο πεδίο κατηγοριών. Έπειτα στην κεντρική σελίδα εμφανίζονται διάφορες εικόνες και βίντεο που στηρίζονται πάνω στις επιλεγμένες θεματικές ενότητες. Όλο το Pinterest στηρίζεται πάνω σε εικόνες, σύντομα βίντεο και άρθρα. Επίσης επιτρέπει στους χρήστες του να δημιουργήσουν ένα "σελιδοδείκτη" ("bookmark") από ιστοσελίδες που βρίσκουν ενδιαφέρουσες, να τις "καρφιτσώσουν" στο προσωπικό τους πίνακα εικόνες και να τις τοποθετήσουν σε θεματικές κατηγορίες της επιλογής τους, να δηλώσουν επικρότηση (like), να ακολουθήσουν χρήστες με ενδιαφέρουσα θεματολογία, και να αναδημοσιεύσουν δημοσιεύσεις.

Το Pinterest γνώρισε ταχεία ανάπτυξη. Μέσα σε 6 χρονιά λειτουργίας αριθμεί πάνω από 70 εκατομμύρια χρήστες. Σε έρευνα που έλαβε χώρα διαπιστώθηκε πως η πλειοψηφία των χρηστών του παγκοσμίως (83%) είναι γυναίκες μεταξύ 25- 54, και πως όλοι οι χρήστες μένουν συνδεδεμένοι για μεγάλο χρονικό διάστημα.[48]

Εικόνα 7: Το λογότυπο του Pinterest

[48] http://www.engauge.com/assets/pdf/Engauge-Pinterest.pdf, 30/09/2016

1.8.1 Συλλογή προσωπικών δεδομένων

Τα στοιχεία που συλλέγει το Pinterest είναι τα στοιχεία τα οποία ο ίδιος ο χρήστης παρέχει κατά την εγγραφή του στη ιστοσελίδα. Όνομα φωτογραφία προφίλ, σχόλια, like, ενδιαφέροντα διεύθυνση ηλεκτρονικού ταχυδρομείου και αριθμό τηλεφώνου είναι ορισμένα από τα στοιχεία που παρέχονται στο site από την πλειοψηφία των χρηστών. Οι πληροφορίες συλλέγονται με τέτοιο τρόπο που να ανταποκρίνονται στον σκοπό της χρήσης τους, αναλόγως με τα πεδία που ερευνώνται.[49]

Εάν ο χρήστης προβεί στην εγκατάσταση της εφαρμογής του Pinterest από το κινητό, με την αποδοχή των ορών δίνεται αυτομάτως άδεια παραχωρήσεις στην εφαρμογή των επαφών της συσκευής. Εάν η σύνδεση γίνει μέσω άλλης εφαρμογής το Pinterest μπορεί να συλλέξει και τα στοιχεία που έχουν καταχωρηθεί στην εφαρμογή μέσω της οποίας πραγματοποιείται η σύνδεση. Κάθε φορά που χρησιμοποιείτε το Pinterest υπάρχει αυτόματη συλλογή πληροφοριών όπως:

- Τα δεδομένα: Οι διακομιστές καταγράφουν πληροφορίες συμπεριλαμβανομένων των πληροφοριών του browser. Τα δεδομένα καταγραφής μπορεί να περιλαμβάνουν τη διεύθυνση πρωτοκόλλου του Internet, τη διεύθυνση των ιστοσελίδων που χρησιμοποιήθηκαν, τον τύπο του προγράμματος περιήγησης και τις ρυθμίσεις, την ημερομηνία και την ώρα, και τα δεδομένα cookie.
- Πληροφορίες συσκευής: πληροφορίες της συσκευής που χρησιμοποιείται για την σύνδεση στο Pinterest συλλέγονται αυτομάτως. Αυτού του είδους οι πληροφορίες περιλαμβάνουν το είδος της συσκευής, του λειτουργικού συστήματος, και τις ρυθμίσεις της συσκευής. Οι πληροφορίες που θα συλλεχθούν εξαρτώνται και από το τύπο της συσκευής που χρησιμοποιεί ο χρήστης.[50]

1.8.2 Χρήση συλλεχθεντων πληροφοριών

Α) Κοινή χρήση δεδομένων.

Συνεργαζόμενες εταιρίες και διαφημιστές αποδέχονται τις πληροφορίες που συλλέγει το Pinterest. Αυτό φέρει βελτίωση των υπηρεσιών για τον χρήστη καθώς του απευθύνονται διαφημίσεις που τον ενδιαφέρουν, αυξάνοντας τις πωλήσεις των διαφημιζομένων προϊόντων.[51]

Β) Αποθήκευση πληροφοριών αγοράς.

[49] https://about.pinterest.com/en/privacy-policy, 30/09/2016
[50] https://about.pinterest.com/el/privacy-policy, 30/09/2016
[51] https://about.pinterest.com/el/privacy-policy , 30/09/2016

Αν πραγματοποιηθεί μια αγορά μέσω Pinterest ο ιστότοπος κρατάει τα στοιχεία του χρήστη με σκοπό την επόμενη φορά η αγορά να γίνει πιο εύκολη και γρήγορη.

Γ) Προσαρμοσμένες πληροφορίες.

Μετά την υποδήλωση ότι ο χρήστης ενδιαφέρεται για ένα pin το Pinterest κρατάει τα δεδομένα και συνεχίζει να εμφανίζει σχετικά άρθρα και διαφημίσεις για να κάνει την περιήγηση πιο ενδιαφέρουσα. Επιπλέον οι χρήστες λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου με pins που σύμφωνα με τις πιο πρόσφατες αναζητήσεις τους ενδιαφέρουν. Με αυτό τον τρόπο το site κρατάει τους χρήστες διαρκώς ενημερωμένους και ενεργούς.

Δ) Σύνδεση με γνωστές επαφές.

Το Pinterest μέσα από την συλλογή πληροφοριών επαφών και διευθύνσεων ηλεκτρονικού ταχυδρομείου βοηθάει τους χρήστες του να συνδεθούν με τους πίνακες φιλικών προσώπων.[52]

1.8.3 Οι επιλογές του χρήστη

Ο χρήστης ως διαχειριστής της σελίδας έχει απολυτή πρόσβαση σε όλες τις τροποποιήσεις που του παρέχονται. Συγκεκριμένα έχει πρόσβαση σε κάθε αλλαγή των πληροφοριών στη σελίδα του προφίλ του όποτε το θελήσει, καθώς και επιλογής του κοινού που μπορεί να εντοπίσει το λογαριασμό του στο Pinterest χρησιμοποιώντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου. Η δημιουργία ιδιωτικών ενοτήτων ανάμεσα σε χρήστες του Pinterest προωθούν τον ιδιωτικό χαρακτήρα τις ιστοσελίδας. Πρόκειται για ιδιωτικές ενότητες στις οποίες έχουν πρόσβαση μόνο τα μέλη τους και δεν είναι ορατές από τους υπολοίπους χρήστες. Επιπλέον δίνεται η δυνατότητα αποσύνδεσης του λογαριασμού από άλλους λογαριασμούς που έχει πραγματοποιηθεί σύνδεση (π.χ. το ή το Twitter) και επιλογής αν επιτρέπεται η δημοσίευση των δραστηριοτήτων από το Pinterest σε άλλες υπηρεσίες.

Ο λογαριασμός στο Pinterest μπορεί να τεθεί εκτός λειτουργίας οπότε ο χρήστης το αποφασίσει. Με την απενεργοποίηση του λογαριασμού διαγράφονται αυτόματα πίνακες και δημοσιεύσεις από την ορατότητα των χρηστών. Ωστόσο το ίδιο το Pinterest διατηρεί αρχειοθετημένα αντίγραφα των στοιχείων, όπως απαιτείται από το νόμο και για επιχειρηματικούς σκοπούς. [53]

[52] https://about.pinterest.com/en/privacy-policy, 30/09/2016
[53] https://about.pinterest.com/el/privacy-policy , 30/09/2016

1.9 YouTube

Το YouTube δημιουργήθηκε τον Φεβρουάριο του 2005. Τον Οκτώβριο του 2006 αγοραστικέ από την Google για 1,65 δισεκατομμύρια δολάρια, ενώ ένα μηνά αργότερα τον Νοέμβριο του 2006 ονομάστηκε από το περιοδικό TIM "Invention of the Year 2006" (Η Εφεύρεση του 2006). Η χρήση του γίνεται μέσω του Adobe Flash Video (λογισμικό προσωπικών υπολογιστών) που επιτρέπει την άνοδο μεγάλου αριθμού βίντεο.

Κάθε χρήστης του διαδικτύου είναι σε θέση να παρακολουθήσει τα βίντεο που έχουν αναρτηθεί στο YouTube και να δηλώσει αν του αρέσουν ή όχι. Τα εγγεγραμμένα μέλη έχουν πιο πολλά δικαιώματα χρήσης. Είναι σε θέση να αναρτούν βίντεο, να τα βαθμολογούν, να τα αποθηκεύουν, να δηλώσουν ότι τους αρέσουν μέσα από το ειδικό κουμπί «μου αρέσει» που βρίσκεται στο κάτω μέρος των βίντεο αλλά και να απαντούν σε σχόλια άλλων χρηστών. Κάθε προβολή καταγράφεται με σκοπό να φανερωθούν τα πιο δημοφιλή βίντεο. Οι εγγεγραμμένοι χρήστες έχουν δικαίωμα να αναρτήσουν βίντεο διάρκειας μικρότερης των δέκα λεπτών. Το όριο τέθηκε τον Μάρτιο του 2006 όταν το YouTube διαπίστωσε πως τα βίντεο που υπερβαίναν αυτό το χρονικό όριο συνήθως περιείχαν παράνομη αναπαραγωγή οπτικοακουστικού υλικού. Εξαίρεση αποτελούν εταιρικοί λογαριασμοί οι οποίοι για την ανάρτηση μεγαλύτερου μεγέθους βίντεο απαιτούν έγκριση από το YouTube.

Σύμφωνα με την SimilarWeb το YouTube με περισσότερους από 15 δισεκατομμύρια επισκέπτες ανά μήνα κατακτά την πρώτη θέση ως η δημοφιλέστερη σε επισκεψημοτητα ιστοσελίδα για την αναπαραγωγή βίντεο παγκόσμιος (στην κατηγορία Arts And Entertainment > TV And Video).[54]

Εικόνα 8: Το λογότυπο του YouTube

[54] https://www.similarweb.com/top-websites/category/arts-and-entertainment/tv-and-video, SimilarWeb, «Top 50 sites in the world for Arts And Entertainment > TV And Video», 30/9/2016

1.9.1 Συλλεχθέντα δεδομένα

Το YouTube ως προϊόν της Google ακολουθεί κοινό κανονισμό με τα υπόλοιπο προϊόντα της. Συλλεγεί στοιχεία από την περιήγηση των χρηστών του με σκοπό να κάνει πιο ενδιαφέρουσα την περιήγηση στον ιστότοπο. Τα στοιχεία που συλλέγονται προέρχονται από τους εξής τόπους:

- Τις πληροφορίες εγγραφής του χρήστη: Σε περίπτωση που κάποιος χρήστης θέλει να εγγραφεί στο YouTube για έχει το δικαίωμα να αναρτά και να σχολιάζει βίντεο, τα στοιχεία του καταχωρούνται αυτομάτως, συλλέγονται και επεξεργάζονται από την Google.
- Τις πληροφορίες χρήσης: Κάθε κίνηση του χρήστη εντός των υπηρεσιών της Google καταγράφεται και επεξεργάζεται.. Πιο συγκεκριμένα, οι πληροφορίες που συλλέγονται συνοψίζονται στις εξής κατηγορίες:
    1. Στοιχεία συσκευής : μοντέλο συσκευής, έκδοση λειτουργικού συστήματος, δίκτυο κινητής τηλεφωνίας αριθμό τηλεφώνου
    2. Στοιχεία καταγραφής: στοιχεία αναζήτησης, τηλεφωνικά στοιχεία καταγραφής (όπως τον αριθμό του κινητού σας τηλεφώνου, τον αριθμό του καλούμενου, αριθμούς προώθησης, την ώρα και την ημερομηνία κλήσεων, τη διάρκεια των κλήσεων, τις πληροφορίες δρομολόγησης SMS και τους τύπους κλήσεων), διεύθυνση πρωτοκόλλου δικτύου(γνωστό ως IP), στοιχεία συμβάντων της συσκευής (όπως τυχόν διακοπές λειτουργία), τη δραστηριότητα του συστήματος, τις ρυθμίσεις της συσκευής, τον τύπο του προγράμματος περιήγησης, τη γλώσσα του προγράμματος περιήγησης, την ημερομηνία και την ώρα του αιτήματος σας και τη διεύθυνση URL αναφοράς, cookie.
    3. Στοιχεία τοποθεσίας
    4. Χώρος αποθήκευσης: Το YouTube ενδέχεται να συλλέξει και να αποθηκεύσει πληροφορίες στην συσκευή με την οποία εισέρχεται ο χρήστης στο σύστημα.
    5. Cookie

Η συλλογή δεδομένων των χρηστών διευκολύνει την Google στην ανάλυση της επισκεψιμότητα των σελίδων και των εφαρμογών της. Επιπλέον μέσα από αυτό βελτιώνει τις παροχές τις εστιάζοντας στα κομμάτια που φέρουν μεγαλύτερη επισκεψιμότητα. Οι

πληροφορίες που συλλέγονται συσχετίζονται με τον λογαριασμό Google του χρήστη και αντιμετωπίζονται ως προσωπικά στοιχεία.[55]

1.9.2 Χρήση πληροφοριών από την Google

Οι πληροφορίες που συλλέγονται έχουν ως στόχο την βελτίωση των παροχών, την προστασία τους, την ανάπτυξη νέων παροχών καθώς και την προστασία των χρηστών. Ένα από τα προϊόντα που χρησιμοποιεί η Google για να επιτύχει αυτόν το στόχο είναι το Google Analytics. Απώτερος στόχος είναι η εξατομίκευση του YouTube όπως και τις κάθε υπηρεσίας που προσφέρει η Google για τον χρήστη και η ευκολότερη περιήγηση. Κάθε υπηρεσία της Google συσχετίζεται με τις υπόλοιπες και δημιουργείται ένα κοινό προσωπικό προφίλ του κάθε χρήστη. Όνομα, ενέργειες, φωτογραφίες, διεύθυνση ηλεκτρονικού ταχυδρομείου, κριτικές και δημοφιλής διαφημίσεις είναι μερικά μόνο από τα στοιχεία που συλλέγονται. Αξίζει να σημειωθεί πως τα προσωπικά στοιχεία των χρηστών μεταφέρονται σε διακομιστές εκτός της χωράς στην οποία συλλέχθηκαν[56] χωρίς να μεταπωλούνται σε τρίτους.[57]

1.9.3 Ασφάλεια πληροφοριών χρήστη

Η Google διασφαλίζει την ασφάλεια των χρηστών της για κάθε μια από τις πληροφορίες που συλλεγεί μέσα από μια σειρά ενεργειών που αποτρέπει κακόβουλες ενεργείς και επεμβάσεις.

- Κρυπτογράφηση υπηρεσιών με την χρήση του SSL, το οποίο προσφέρει ασφάλεια και ιδιωτικότητα.
- Λειτουργία ασφαλούς περιήγησης.
- Συχνοί έλεγχοι των στοιχείων και των πρακτικών συλλογής και αποθήκευσης για προστασία από μη εξουσιοδοτημένη είσοδο στο σύστημα.
- Περιορισμένη πρόσβαση: Η πρόσβαση στα προσωπικά στοιχεία περιορίζεται μόνο σε υπαλλήλους, αναδόχους και αντιπροσώπους της Google που πρέπει να γνωρίζουν αυτά τα στοιχεία για την επεξεργασία τους και οι οποίοι υπόκεινται σε αυστηρές συμβατικές υποχρεώσεις εμπιστευτικότητας και ενδέχεται να υπόκεινται

[55] https://www.google.com/intl/el/policies/privacy/#infocollect, 03/09/2016
[56] https://www.google.com/intl/el/policies/privacy/#infouse, 03/09/2016
[57] https://privacy.google.com/intl/el/how-ads-work.html, 03/09/2016

σε πειθαρχικές διαδικασίες ή σε απόλυση εάν δεν ανταποκριθούν σε αυτές τις υποχρεώσεις.[58]

1.9.4 Ανήλικοι και YouTube

Το YouTube απευθύνεται σε παιδιά ηλικίας άνω των 13 ετών. Ο ιστοτοπος παρέχει τις απαραίτητες οδηγίες και μνήματα οπού ο χρήστης θα πρέπει να επιβεβαιώσει την ηλικία του πριν την είσοδο σε ακατάλληλο περιεχόμενο. Αν τα στοιχεία που δηλωθούν είναι ψευδή ο λογαριασμός καταργείται. Η δημιουργία play list καθώς και η χρήση των παραπομπών από ένα κατάλληλο για την ηλικία του παιδιού βίντεο σε μετάβαση σε παρόμοιο περιεχομένου ενδείκνυται για την χρήση του YouTube από ανήλικους. Η λειτουργία περιορισμένης πρόσβασης και οι ρυθμίσεις απορρήτου και ασφαλείας μπορούν να προστατέψουν το παΐδι από κίνδυνους και πρόσβαση σε μη κατάλληλο περιεχόμενο.[59]

1.10 Γενικά Μετρά Ασφάλειας Στις Διαδικτυακές Κοινότητες

Πέρα από την τέρψη που προσφέρει η κοινωνικοποίηση μέσω του διαδικτύου επιτακτική είναι η ανάγκη απροσπέλαστων κωδίκων που εμποδίζουν την είσοδο από μη εξουσιοδοτημένους χρήστες καθώς και η ανάγκη καθορισμού του περιεχομένου που μπορεί κοινοποιηθεί δημοσιά- περιορισμένα ή και καθόλου.[60] Ο ηλεκτρονικός αυτοκαθορισμό του ατόμου ωστόσο, δεν μπορεί να περιοριστεί από τα μετρά ασφάλειας που προτείνουν οι ιστοτοπου καθώς το υποκείμενο έχει την ευθύνη των αποφάσεων του και του βαθμού που επιθυμεί να εκθέσει τον εαυτό του.[61]

Κατά την εγγραφή στις διαδικτυακές κοινότητες ο χρήστης καλείτε να υποβάλει ορισμένα προσωπικά στοιχεία. Τα πιο διαδεδομένα είναι το ονοματεπώνυμο του, διεύθυνση ηλεκτρονικού ταχυδρομείου και ένας κωδικός με τον οποίο θα εισέρχεται στην σελίδα. Ορισμένες επιπρόσθετες πληροφορίες όπως τηλέφωνο, τόπος κατοικίας, εκπαίδευση, επάγγελμα ημερομηνία γέννησης, φύλο κα. ζητούνται είτε ως προαιρετικά πεδία είτε ως υποχρεωτικά με σκοπό την χρήση τους για την επέκταση τις σελίδας και για διαφημιστικούς λόγους. Τα προσωπικά στοιχεία που κατατίθενται είναι ορατά σε όλους τους χρήστες και αυτομάτως νομιμοποίητε η χρήση τους για σκοπούς της εταιρίας που

[58] https://www.google.com/intl/el/policies/privacy/, 03/09/2016
[59] https://support.google.com/youtube/answer/2802244, 03/09/2016
[60] Εισαγωγή στα Δίκτυα Υπολογιστών, JoAnne Woodcock, Κλειδάριθμος, σελ. 257
[61] Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 88-90

ανήκει η ιστοσελίδα. Πολλοί είναι οι χρήστες που με το πέρασμα του χρόνου δημιουργούν μέσα από το εικονικό προφίλ τους προσωπική σχέση με τους διαδικτυακούς φίλους και αποφασίζουν να κοινοποιήσουν περισσότερες πληροφορίες για το άτομο τους. Η ψευδής αίσθηση ασφάλειας και οικειότητας ωστόσο μπορεί να αποβεί μοιραία για τον χρήστη. Το ηλεκτρονικό «ψάρεμα» ως η πιο κοινή μορφή απάτης στηρίζεται σε αυτή την πρακτική της αίσθησης εμπιστοσύνης των μελών της διαδικτυακής κοινότητας. Έρευνα της Ομοσπονδιακής Επιτροπής Εμπορίου των Ηνωμένων Πολιτείων (FTC) φανέρωσε πως το συντριπτικό ποσοστό (86%) των διευθύνσεων ηλεκτρονικού ταχυδρομείου που παρέχονται στις ηλεκτρονικές τοποθεσίες και σε ομάδες ενημέρωσης λαμβάνουν ανεπιθύμητα μηνύματα.[62]

Προς αντιμετωπίσει φαινομένων παρενόχλησης των χρηστών οι ηλεκτρονικές κοινότητες παρέχουν στους χρήστες τους ορισμένους τρόπους προστασίας των προσωπικών τους δεδομένων από κακόβουλη χρήση:

- Κώδικας συμπεριφοράς χρηστών: πρόκειται για αναφορά σε επιτρεπτές και μη ενέργειες εντός το ιστότοπου όπως και σε πιθανές κυρώσεις των παραβατών
- Οδηγίες για γονείς και παιδιά: οπού αναφέρονται οι ρυθμίσεις στις οποίες μπορεί να προβεί ο γονέας για να προφυλάξει τα παιδιά του και να διασφαλίσει την ορθή χρήση του διαδικτύου.
- Κωδικοί πρόσβασης: κατά την εγγραφή ο χρήστης καλείτε να δημιουργήσει ένα προσωπικό κωδικό πρόσβασης. Ο κωδικός σύμφωνα με τις οδηγίες δεν είναι κοινωποιήσιμος. Δικλείδα ασφάλειας για πιθανή απώλεια του κωδικού είναι ορισμένες προσωπικές ερώτησης που αναρτώνται κατά την εγγραφή στο δίκτυο.
- Πολίτικες απορρήτου: τα στοιχεία δηλαδή που συλλέγονται από το προφίλ του χρήστη και πως αυτά χρησιμοποιούνται από την εταιρία και τις συνεργαζόμενες εταιρίες.
- Διεύθυνση ηλεκτρονικού ταχυδρομείου: ο χρήστης μπορεί να αποκρύψει μέρος ή και ολόκληρη την διεύθυνση ηλεκτρονικού ταχυδρομείου, ώστε να μην είναι ορατή από τους υπολοίπους χρήστες.
- Φίλτρα που καθορίζουν το κοινό των δημοσιεύσεων.

[62] Αθηνά Α. Λαζακίδου, Σύγχρονες Τεχνολογίες και Υπηρεσίες Πληροφορικής και Τηλεπικοινωνιών, σελ.154

- Φραγή ανώνυμων ανακοινώσεων στις ιστοσελίδες. Αύτη η ενέργεια αίρει την ανωνυμία από τους κακόβολους χρήστες και προστατεύει τον χρήστη από ανώνυμες απαντήσεις στο ιστολόγοι του.
- Σύνδεση με διεύθυνση IP: η οποία μπορεί να εντοπίσει όλους τους υπολογιστές που εισέρχονται στις ιστοσελίδες ώστε να επιβληθούν κυρώσεις οπού είναι απαραίτητο.
- Απόρρητες κοινότητες όπου διασφαλίζεται το μυστικό περιεχόμενο των συνομιλίων και η πρόσθεση νέου μέλους πρέπει να εγκριθεί από τα ήδη υπάρχοντα μέλη.
- Επιλογές να μην λαμβάνει ο χρήστης ηλεκτρονικά μηνύματα ή κλήσεις με σκοπό προώθηση προϊόντων.
- Μαρκάρισμα διευθύνσεων ηλεκτρονικού ταχυδρομείου. Πρόκειται για μια λέξη ή φράση (πχ. nospam) μέσα στο email του χρήστη που εμποδίζει τα μηνύματα αυτόματης συλλογής διευθύνσεων. Αυτή η μέθοδος δεν είναι πολύ αξιόπιστη.
- Δεύτερη διεύθυνση ηλεκτρονικού ταχυδρομείου. Ο χρήστης μπορεί να δώσει μια δεύτερη διεύθυνση ηλεκτρονικού ταχυδρομείου προκειμένου να αποφύγει ενοχλητικά email.[63]

Τα μετρά ασφάλειας χρηστών διαφοροποιούνται ανάλογα με την ιστοσελίδα.

1.10.1 Διαδίκτυο και παιδιά

Το διαδίκτυο αποτελεί μέρος της καθημερινότητας των παιδιών, εν αντιθέσει με τους ενήλικες οι οποίοι παρουσιάζουν μεγάλα ποσοστά ψηφιακής αναλφαβητικότητας. Η απειρία όμως και η αγνοία κίνδυνου τα καθιστούν ευάλωτα. Η αποστολή φωτογραφιών και video σε αγνώστους καθώς και οι κοινοποίηση προσωπικών πληροφοριών τα κάνουν εύκολα θύματα σε εκβιασμούς και παιδόφιλους. Ωστόσο στις περισσότερες ηλεκτρονικές σελίδες υπάρχει η ένδειξη για είσοδο μόνο σε παιδιά άνω των 13 ετών, αυτό δεν διασφαλίζει την ορθή χρήση και την αλήθεια των αποδοχών πάρα μόνο την νομική κάλυψη της ιστοσελίδας.[64]

Ακόμα και στους έφηβους παρουσιάζονται κρούσματα λανθασμένης χρήσης του διαδικτύου, βρίσκοντας στο ανοικτό του περιβάλλον την ευκαιρία να εκφράσουν την παραβατικότητα τους. Ιδιαίτερες φωτογραφίες συμμαθητών τους, βίντεο, ακραίες απόψεις,

[63] Αθηνά Α. Λαζακίδου, Σύγχρονες Τεχνολογίες και Υπηρεσίες Πληροφορικής και Τηλεπικοινωνιών, σελ.156

[64] Jan L. Harrington, Network Security: A Practical Approach, Morgan Kaufmann Publishers, 2005, pp. 14-15

πορνογραφία, τυχερά παιχνίδια είναι μόνο λίγες από τις μορφές εκδήλωσης της παραβατικότητας των εφήβων.

Η ορθή χρήση του διαδικτύου απαιτεί παιδιά και επιτήρηση. Οι γονείς ήδη από μικρή ηλικία απαιτείται να κατευθύνουν τα παιδεία στην σωστή χρήση του διαδικτύου χωρίς να την απαγορεύουν. Η απαγόρευση βάλει την προσωπικότητα του παιδιού και ενδεχομένων να φέρει αντίθετα αποτελέσματα από τα επιθυμητά. Επιπλέον ο γονέας ,μπορεί να ακολουθήσει μια σειρά από απλές κινήσεις για να προστατέψει το παιδί· η χρήση φίλτρου για τις μη κατάλληλες ιστοσελίδες και η μεταφορά του ηλεκτρονικού υπολογιστή σε σημείο του σπιτιού οπού ο γονέας θα μπορεί να παρακολουθεί τις δικτυακές κινήσεις του παιδιού είναι βασικοί κανόνες. Η χρήση του διαδικτύου από τον γονέα μαζί με το παιδί μπορεί να του διδάξει την ορθή διαδικτυακή συμπεριφορά μέσα από την διαδικασία της μίμησης.

Το παιδί πέρα από την καθοδήγηση του γονέα χρειάζεται ορισμένα εναύσματα και από το σχολείο καθώς η αντιδραστικότητα ορισμένων παιδιών μπορεί να αμφισβητήσει τα λεγόμενα και τις υποδείξεις. Γι' αυτόν τον λόγο είναι αναγκαία η διαμόρφωση μιας κοινής πορείας προς την ασφαλή διαδικτυακή συμπεριφορά. Η ένταξη ενός μαθήματος για την ασφαλή χρήση του διαδικτύου καθώς και η συνεχής επιμόρφωση των παιδιών όλων των ηλικιών και η ενημέρωση τους σχετικά με τους κινδύνους του διαδικτύου θα βελτίωνε μακροπρόθεσμα την χρήση του διαδικτύου. [65]

1.10.2 Κοινωνικά δίκτυα και εργασία

Ιδιαίτερη σημασία φαίνεται να δίνουν οι εργοδότες στα κοινωνικά προφίλ των εργαζομένων τους. Σύμφωνα με την εφημερίδα Times η εταιρία Badenoch & Clark (εταιρία εύρεσης προσωπικού) το 62% των υψηλόβαθμων στελεχών διατηρεί προσωπικό προφίλ στα μέσα κοινωνικής δικτύωσης για να μπορεί να συλλεγεί πληροφορίες για το ήδη υπάρχον αλλά και το μελλοντικό προσωπικό της εταιρίας. Περνώντας σε μια άλλη έρευνα που πραγματοποίησε το επαγγελματικό κοινωνικό δίκτυο Video φανερώνεται πως τα 2/3 των συμμετεχόντων στην ερευνά επηρεάζονται σε σημαντικό βαθμό από τα κοινωνικά προφίλ των υποψήφιων τους, ενώ ¼ από αυτούς δήλωσε πως δεν προέβει σε πρόσληψη λόγο του μη ικανοποιητικού προφίλ. Συγκεντρώνοντας τις πληροφορίες η εφημερίδα Times παρέχοντας οδηγίες μέσα από ερευνά στους μελλοντικούς εργαζομένους ανέφερε

[65] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, εικονικός κόσμος και νέες τεχνολογίες, Κλειδάριθμος, σελ. 100

συγκεντρωτικά τα στοιχεία που κάνουν την χείριστη εντύπωση στους εργοδότες και αναστέλλουν την πρόσληψη. Αυτά είναι η προκλητικές φωτογραφίες, οι πολύ προσωπικές φωτογραφίες και τα δημόσια παράπονα για προηγουμένη δουλεία του υποψήφιου.

Ιδιαίτερο ενδιαφέρον επίσης παρουσιάζει μια 6μηνη ερευνά στηριγμένη αποκλειστικά σε εφήβους που διεξήχθη στην Αμερική για το διδακτορικό της Danah Boyd από το πανεπιστήμιο του Berkeley. Η ερευνά διερευνούσε την πορεία των μαθητών αναμεσά στα κοινωνικά δίκτυα. Τα αποτελέσματα έδειξαν πως οι έφηβοι διαχωρίζονται στα κοινωνικά δίκτια ανάλογα με την πορεία των σπουδών τους. Έτσι προέκυψε πως οι χρήστες του Facebook είναι κυρίως λευκοί και επιθυμούν να συνεχίσουν τις σπουδές τους. Παρατηρούμε λοιπόν πως οι διάφορες έχουν βαθύτερα κοινωνικά αίτια.[66]

1.10.3 Κοινωνική δικτύωση στον τομέα της υγείας

Όπως έχει ήδη αναφερθεί ο κύριος λόγος για την δημιουργία των κοινωνικών δικτύων είναι η ανάγκη του ανθρώπου για επικοινωνία. Η επικοινωνία προσφέρει όχι μόνο στείρα πληροφόρηση, αλλά και δημιουργία δεσμών για τα μέλη. Με την προοπτική λοιπόν της επικοινωνίας, της συναισθηματικής υποστήριξης και κατανόησης αλλά πρωτίστως της πληροφόρησης για θεραπευτικές μεθόδους και νέες τεχνικές δημιουργήθηκαν τα πρώτα μέσα κοινωνικής δικτύωσης στον τομέα της υγειάς.

Σκοπός τους είναι η ψυχοκοινωνικής υποστήριξη και δικτύωση, καθώς και η ανταλλαγή πληροφοριών σχετικά με τις ασθένειες, τις θεραπείες και τα αποτελέσματά τους, τους επαγγελματίες υγείας και τις παρεχόμενες υπηρεσίες περίθαλψης. Μέσα από τα κοινωνά δίκτυα υγείας προσφέρονται πληθώρα θετικών επιπτώσεων σε ασθενείς κι ιατρούς. Η δημιουργία ομάδων που καλεί τους πάσχοντες να μιλήσουν για την ασθένεια τους με την ενεργή συμμετοχή ιατρών οι οποίοι μπορούν όχι μόνο να ενημερώσουν αλλά να πραγματοποιήσουν έρευνες για την ψυχολογία των ασθενών και για αντίστοιχες μεθόδους που χρησιμοποιούν συνάδελφοι, παρέχουν και στους επαγγελματίες υγείας τη δυνατότητα να παρατηρήσουν και να αναλύσουν τα δεδομένα που αναζητούν. Παρατηρούμε λοιπόν πως τα κοινωνικά δίκτυα μπορούν να ευνοήσουν το επίπεδο της υγείας του ατόμου και να τονώσουν την αυτοεκτίμηση του.[67]

Παρακάτω θα παρουσιαστεί ένα από τα πιο δημοφιλή κοινωνικά δίκτυα στον τομέα της υγείας του εξωτερικού:

[66] Αθηνά Α. Λαζακίδου, Διοφαντος Γ. Χατζημιτσης, Ιορδάνης Ε. Ευαγγέλου, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος, σελ. 150

[67] Ν. Φακιόλας, Επίδραση κοινωνικών δικτύων στην υγεία, epublishing, 2012, σελ. 220

1.11 Το παράδειγμα του Patientslikeme

Το Patientslikeme είναι μια δωρεάν ιστοσελίδα κοινωνικής δικτυώσεις που αριθμεί πάνω από 400.000 μέλη. Η ίδρυση της ιστοσελίδας έγινε το 2006 με στόχο την σύνδεση των ασθενών με προβλήματα υγείας, την προώθηση της επικοινωνίας, της ερευνάς και την αύξηση της αποτελεσματικότητας των ιατρικών μεθόδων. Εμπνευστής της ιδέας ήταν ο Stephen Heywood ο οποίος το 1998 σε ηλικία 29 ετών διαγνώστηκε με αμυοτροφική πλευρική σκλήρυνση (ALS).[68] Η πρώτη κοινότητα που ιδρύθηκε εντός της ιστοσελίδας περιλάμβανε την νόσο του εμπνευστή της, αμυοτροφική πλευρική σκλήρυνση. Έπειτα επεκτάθηκε σε όλες τις ασθένειες αλλά η πρωταρχική χρήση και εξειδίκευση της σελίδας είναι αυτή που την κατατάσσει ως την πρώτη ιστοσελίδα κοινωνικής δικτύωσης σε μέλη με ασθένεια ALS.

Το Patientslikeme παρέχει στους χρήστες πρόσβαση σε πληροφορίες που έχουν δοθεί από τα μέλη του σχετικά με την πορεία της ασθένειας, τις θεραπευτικές μεθόδους, τα αποτελέσματα τους, τις παρενέργειες και την ποιότητα ζωής. Οι ασθενείς μπορούν να συγκρίνουν το επίπεδο της ασθένειας τους με γραφήματα που έχουν δημιουργηθεί από τις απαντήσεις άλλων ασθενών με την ιδιά ασθένεια. Επιπλέον μπορούν να κρατούν και δικά τους προσωπικά στατιστικά και γραφήματα και μέσω των οποίων να βλέπουν την πορεία της νόσου. Πρέπει να τονιστεί πως το περιεχόμενο του Patientslikeme είναι καθαρά ενημερωτικό και δεν περιέχει συμβουλευτικό χαρακτήρα.[69] Επιπλέον η ιστοσελίδα δίνει την δυνατότητα στους χρήστες της να επικοινωνούν μεταξύ τους μέσω messenger, μηνυμάτων, και σχόλιων προφίλ.

Εικόνα 9: Το λογότυπο του Patientslikeme

[68] https://www.patientslikeme.com/about, 11/10/2016
[69] https://www.patientslikeme.com/about/user_agreement, 11/10/2016

1.11.1 Έρευνα και χρηματοδότηση

Σημαντική υπήρξε η συμβολή του Patientslikeme σε ερευνά που έγινε το 2013 σε συνεργασία με την UCB προκειμένου να διερευνηθούν παράγοντες που ευθύνονται για την ποιότητα ζωής στην επιληψία. Σε αυτή την ερευνά φανερώθηκαν ζητήματα έλλειψης συγκέντρωσης κατάθλιψής και παρενέργειες που είχαν οι ασθενείς. Φαίνεται πως το Patientslikeme διαφοροποιείτε σε μεγάλο βαθμό από τα συμβατικά μέσα κοινωνικής δικτύωσης αφού μέσα από άρτια δομημένες έρευνες εξάγονται στοιχεία που μπορούν να χρησιμοποιηθούν για ερευνητικούς σκοπούς.[70] Το Patientslikeme λοιπόν προάγει την επιστήμη βοηθώντας στην καλύτερη κατανόηση της νόσου, και στην βελτίωση των ιατροφαρμακευτικών προϊόντων. [71] Σε συνεργασίας με ακαδημαϊκούς και εμπορικούς συνεργάτες το Pantientlikeme δημοσίευσε σε έγκριτα επιστημονικά άρθρα σε ιατρικά-επιστημονικά περιοδικά όπως το BMJ, Nature Biotechnology κα.[72]

Το Patientslikeme δεν περιλαμβάνει διαφημίσεις ενώ η χρηματοδότηση της σελίδας γίνεται μέσω των πωλήσεων των ερευνών που πραγματοποιούνται από τα μέλη και την μεταπώληση τους στους εταίρους της, συμπεριλαμβανομένων των φαρμακευτικών και ιατρικών εταιρειών. Η εταιρεία προς ενίσχυση της διαφάνειας έχει κοινοποιήσει τις συνεργαζόμενες εταιρίες: University of Michigan Psoriasis Genetics Laboratory, UCB, η Novartis, Sanofi, Avanir Φαρμακευτικά και Acorda Therapeutics κα.[73] Αξίζει να σημειωθεί πως το 2007 η εταιρεία ονομάστηκε από το Business 2.0 και το CNN Money ως «"Next Disruptors: 15 Companies That Will Change The World».[74]

1.11.2 Προσωπικά δεδομένα

Η δημιουργίας της ιστοσελίδας βασίζεται σε ευαίσθητα προσωπικά δεδομένα των μελών και συγκεκριμένα σε δεδομένα υγείας τα οποία συλλέγονται, επεξεργάζονται και διανέμονται.. Σε αυτό στο σημείο δημιουργείτε μια αντίφαση σχετικά με την προστασία και την κοινοποίηση ευαίσθητων προσωπικών δεδομένων. Το ίδιο αναφέρει πως τα μέλη της συμμετέχουν αποκτώντας όφελος σε ψυχολογικό, σωματικό και επιστημονικό επίπεδο.

---

[70] http://jamanetwork.com/journals/jama/article-abstract/1883026, 11/10/2016
[71] http://patientslikeme_posters.s3.amazonaws.com/2013_PatientsLikeMe%20epilepsy%20community-%20factors%20affecting%20quality%20of%20life.pdf, 11/10/2016
[72] https://www.patientslikeme.com/research/publications, 11/10/2016
[73] https://www.patientslikeme.com/about/partners, 11/10/2016
[74] http://money.cnn.com/galleries/2007/biz2/0708/gallery.next_disruptors.biz2/7.html, 11/10/2016

Η φιλοσοφία του είναι βασισμένη στο γεγονός ότι το απαραβίαστο των προσωπικών δεδομένων σε θέμα υγείας δημιουργεί εμπόδια στην επιστήμη και καθυστερεί την μετάδοση και ανάπτυξη νεών πρακτικών. Αυτή η διαδικτυακή κοινότητα έχει δημιουργηθεί για να ανακάμψει όλα τα εμπόδια, με την θέληση των μελών, και να δημιουργήσει ένα καινούργιο πιο ανοιχτό τρόπο επικοινωνίας.[75]

Οι πληροφορίες που συλλέγοντες είναι εκείνες που παραχωρούν οι χρήστες κατά την εγγραφή του στην ιστοσελίδα όπως και οποιαδήποτε άλλη πληροφορία που παραχωρείται εντός της ιστοσελίδας (ιατρικού και μη περιεχομένου). Για την προστασία των μελών της η ιστοσελίδα δίνει την δυνατότητα ρύθμισης του απορρήτου. Η ρυθμίσεις απορρήτου περιλαμβάνουν δυο κατηγορίες. Το πρώτο αφορά αυστηρά τα μέλη της ομάδας τα οποία μπορούν να επικοινωνήσουν με άλλους χρήστες και να δουν τα προσωπικά τους στοιχεία. Το δεύτερο είναι δημόσιο οπού το προφίλ είναι ορατό από μέλη και μη της ομάδας αλλά η επικοινωνία περιορίζεται μόνο για τα μέλη του Pantientslikeme. Τα μέλη μπορούν να αλλάξουν το επίπεδο προστασίας της ιδιωτικότητας τους, ανά πάσα στιγμή.[76]

Επιπρόσθετη δικλείδα ασφάλειας αποτελεί ο διαχωρισμός των πληροφοριών σε περιορισμένης και κοινής χρήσεως. Τα περιορισμένα δεδομένα χρησιμοποιούνται μόνο με την έγκριση του κάτοχου και δεν παραχωρούνται σε τρίτους. Τα περιορισμένα δεδομένα αποτελούν το ονοματεπώνυμο, η διεύθυνση ηλεκτρονικού ταχυδρομείου, ο κωδικός πρόσβασης, η ταχυδρομική διεύθυνση, η ημερομηνία γεννήσεως, και τα προσωπικά μηνύματα.[77]

1.11.3 Κίνδυνοι του χρήστη

Πάρα το γεγονός πως η επίβλεψη στης υγείας του ασθενή φέρει θετικά αποτελέσματα η χρήση του Patientslikeme έχει αρκετούς κίνδυνους που σχετίζονται με την ιδιωτικότητας και τα προσωπικά δεδομένα του χρήστη. Η κοινοποίηση πληροφοριών υγείας που υπόκεινται στα ευαίσθητα προσωπικά δεδομένα μπορεί να θέσουν τον χρήστη σε άβολη θέση. Επιπλέον δεν αποκλείονται διακρίσεις εναντίον του από τρίτα πρόσωπα. Η εύκολη πρόσβαση σε προβλήματα υγείας του ατόμου μπορεί να χρησιμοποιηθεί βλάπτοντας τον ιδιαιτέρως σε θέματα εργασίας και ασφάλισης. [78]

[75] https://www.patientslikeme.com/about/openness, 13/10/2016
[76] https://www.patientslikeme.com/about/privacy, 13/10/2016
[77] https://www.patientslikeme.com/about/privacy, 13/10/2016
[78] https://www.patientslikeme.com/about/privacy, 13/10/2016

Εντούτοις η πολιτική προστασίας προσωπικών δεδομένων μπορεί να προφυλάξει το άτομο και να το ενημερώσει για τα στοιχεία που είναι εκτεθειμένα στο διαδίκτυο ενώ η εταιρία απαλλάσσεται από κάθε ευθύνη σύμφωνα με τους όρους χρήσης. Επιπλέον το Patientslikeme περιέχει συνδέσμους προς άλλους δικτυακούς τόπους που δεν είναι υπό τον έλεγχο της Patientslikeme και ως εκ τούτου δεν μπορεί να εγγυηθεί για την ορθή διαχείριση των προσωπικών δεδομένων. Ο χρήστης μπορεί να παρακάμψει ερωτήσεις και δεδομένα που δεν επιθυμεί να κοινοποιήσει ή ακόμα και να απενεργοποιήσει τον λογαριασμό του. Σε αυτή την περίπτωση όμως τα στοιχεία του μέλους θα παραμείνουν στο σύστημα για λόγους ελέγχου των έρευνών που διεξάχθηκαν πριν από την απενεργοποίηση του λογαριασμού.[79]

1.12 Συμπέρασμα

Συνοψίζοντας παρατηρούμε πως όλα τα μέσα κοινωνικής δικτύωσης ακολουθούν ορισμένες βασικές εφαρμογές προστασίας προσωπικών δεδομένων των χρηστών. Με την εγγραφή του χρήστη στις σελίδες κοινωνικής δικτύωσης αυτομάτως αποδέχεται την συλλογή και την επεξεργασία των προσωπικών δεδομένων από την σελίδα κοινωνικής δικτύωσης που εγγράφεται και δευτερευόντως από τις θυγατρικές και τις συνεργαζόμενες εταιρίες.

Ωστόσο ο ίδιος ο χρήστης είναι αυτός που καλείται να μεριμνήσει και να προστατέψει την ιδιωτικότητα του στον βαθμό που αυτό καθίσταται δυνατό. Η τροποποίηση των ρυθμίσεων βοηθά στον περιορισμό διοχέτευσης και μεταβίβασης των δεδομένων και ο διαχωρισμός των πληροφοριών σε περιορισμένες και κοινές είναι από τα βασικά εργαλεία στα χέρια του χρήστη.

Στο σύνολο των μέσων κοινωνικής δικτύωσης τα προσωπικά δεδομένα συλλέγονται με σκοπό την επεξεργασία είτε για μεταπώληση είτε για ιδιά χρήση, πάντοτε έχοντας σαν τελικό στόχο την χρηματοδότηση.

[79] https://www.patientslikeme.com/about/privacy, 13/10/2016

ΚΕΦΑΛΑΙΟ 2: ΙΔΙΩΤΙΚΟΤΗΤΑ

2.1 Εισαγωγή

Η τεχνολογική, κοινωνική, πολιτισμική και επιχειρηματική ανάπτυξη έχει στηριχθεί σε πολύ μεγάλο βαθμό στις ηλεκτρονικές επικοινωνίες.[80] Η κοινή πορεία της Ευρώπης προς την δημιουργία κοινής ανάπτυξης με στόχο την αύξηση της ανταγωνιστικότητας και των νέων ευκαιριών οδήγησε σε μια νέα μορφή της, στην «Κοινωνία Των Πληροφοριών». Η έκταση και η δύναμη που κατέχει απεικονίζεται καλυτέρα σε στοιχεία: το 40% της αύξησης της παραγωγικότητας της Ευρώπης, και το ένα τέταρτο της αύξησης του ακαθάριστου εθνικού προϊόντος, οφείλονται στις νέες μορφές τεχνολογιών και πληροφοριών, με την δυναμικότητα τους να εκτείνεται και σε άλλες μορφές επιχειρηματικών, κοινωνικών, οικονομικών αλλαγών.

Η ανάπτυξη και η πρόοδος των ηλεκτρονικών υπολογιστών δημιουργεί νέα δεδομένα τα οποία δεν μπορούν να παραληφθούν καθώς δημιουργούν πολλές μεταβολές και επιδρούν ποικιλοτρόπως στην κοινωνία. Το πιο ανησυχητικό είναι η ανάπτυξη παράνομων ενεργειών που ενδείκνυται σε ένα περιβάλλον οπού δεν υπάρχει έλεγχος και χρησιμοποιείται καθημερινά από την πλειονότητα των πολίτων.[81] Παράνομες ενέργειες, συμπεριλαμβανομένων εγκληματικών και τρομοκρατικών πράξεων, στοχεύουν σε βλάβη σε βάρος πολιτών και κοινωνίας[82]. Παράνομη πρόσβαση σε πληροφορίες, βλαβερό λογισμικό, υποκλοπή δεδομένων, είναι μόνο λίγες από τις μορφές των παραβάσεων. Η ίδια η δομή του διαδικτύου ωστόσο δεν ευνοεί τον απόλυτο έλεγχο και τον περιορισμό καθώς η ευελιξία και η πολυμορφικότητα των δομών, σε συνδυασμό με την καθολική χρονικά και χωρικά πρόσβαση των επιθέσεων[83] καθιστούν κάθε προσπάθεια πεπερασμένη. Η διασφάλιση ωστόσο του ατόμου έναντι της μη εξουσιοδοτημένης χρήσης των δεδομένων τους, άλλοτε με την αδιαφανή συλλογή τους,[84] και άλλοτε με τους περίπλοκους και

[80] Σπηλιοπούλου, Α.Σ., και Χοχλιούρος, Ι.Π.(2004).Σύγχρονες Προκλήσεις Από Την Παράλληλη Ανάπτυξη Κανονιστικών Παρεμβάσεων Και Μέτρων Αυτορρύθμισης Στους Τομείς Των Καινοτόμων Προηγμένων Εφαρμογών Και Υπηρεσιών Ηλεκτρονικής Επικοινωνίας Στο Διαδίκτυο, Νομικό Βήμα ΔΣΑ, Νοέμβριος 2004, σελ. 1866-1882

[81] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών Και Εφαρμογών, Διασφάλιση Του Απορρήτου Και Νόμιμη Παρακολούθηση Των Επικοινωνιών, Εκδόσεις Αντ. Ν. Σάκκουλα 2006, σελ. 15-17

[82] Συμβούλιο Της Ευρωπαϊκής Ένωσης: Απόφαση -Πλαίσιο 2005/222/ΔΕΥ Της 24ης Φεβρουάριου 2005, Για Τις Επιθέσεις Κατά Των Συστημάτων Πληροφοριών», Επίσημη Εφημερίδα (ΕΕ), σελ. 67

[83] Eloff, M.M., and von Solms, S.H., Information Security Management: An Approach to Combine Process Certification and Product Evaluation, Computers & Security, pp. 699

[84] Theodore Grossman and Aaron M. Grossman, Understanding Internet Privacy: the US perspective, IBL, 2001, pp.391

δυσνόητους όρους χρήσης, χρήζει άμεσης αντιμετώπισης καθώς η ανασφάλεια δημιουργεί επιφυλακτικότητα στους χρήστες.[85]

Η κίνηση για τον περιορισμό τέτοιου είδους κρουσμάτων πρέπει να υπάρξει συντονισμένα από όλα τα κράτη μέλη της Ένωσης με την ανάπτυξη πολιτικής ασφάλειας και άμυνας. Στόχος είναι η ύπαρξη ενός διαδικτύου που θα προάγει την εξέλιξη και τον υγιή ανταγωνισμό σε όλα τα επίπεδα, χωρίς όμως να θέτει σε κίνδυνο την ασφάλεια των χρηστών και την διακύβευση της δικαιοσύνης.[86] Χωρίς την ασφάλεια βάλλεται η χρήση του εμπορίου και των υπηρεσιών μέσω του διαδικτύου, καθώς η ανασφάλεια των χρηστών δρα ανασταλτικά στην χρήση του και κατ' επέκταση στην μη ομαλή ανάπτυξη τέτοιων εφαρμογών.[87] Παρατηρείται λοιπόν, η ανάγκη για ένα καθολικό και αυστηρό νομικό πλαίσιο για την προστασία των διαδικτυακών επαφών και συναλλαγών, που πρωτίστως θα προστατεύει το άτομο διασφαλίζοντας το απόρρητο και την ιδιωτικότητα των προσωπικών του δεδομένων. Αυτό επιτυγχάνεται μέσω του Ν.2472/1997 «περί προστασίας του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα» που αποτελεί τον θεμελιώδη λίθο του πληροφοριακού αυτοκαθορισμού του ατόμου.

2.2 Η έννοια της ιδιωτικής ζωής

Καθ' όλη την διάρκεια της ιστορίας υπήρξαν περίοδοί που η έννοια της ιδιωτικής ζωής κλονίζονταν, ενώ σε πολλές περιπτώσεις θεωρούνταν επικίνδυνη και αποτελούσε αφορμή κριτικής. Στις μέρες μας η ιδιωτικότητας αποτελεί υπέρτατο αγαθό. Το δικαίωμα του ιδιωτικού χώρου όπως και της διαφορετικότητας έχουν κατοχυρωθεί νομικά για τον κάθε άνθρωπο και αποτελούν κομμάτι της προσωπικότητας και της αξιοπρέπειάς του.

Με την ανάπτυξη της τεχνολογίας και την εκτεταμένη χρήση του διαδικτύου αυτά τα δικαιώματα βάλλονται. Η είσοδος σε προσωπικά δεδομένα επεκτάθηκε με την ανάγκη επεξεργασίας τους, είτε αυτή ονομάζεται βελτίωση παροχών είτε επιστημονικοί λόγοι. Παραβίαση ιδιωτικότητας δεν θεωρείται μόνο η είσοδος ή η έρευνα σε προσωπικό χώρο, αλλά η γενικότερη παρακολούθηση του υποκείμενου και η κατασκόπευση της ζωής του με οποιονδήποτε κρυφό ή φανερό τρόπο. Το δικαίωμα του ιδιωτικού βίου διακηρύχθηκε για

[85] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ.203

[86] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών Και Εφαρμογών, Διασφάλιση Του Απορρήτου Και Νόμιμη Παρακολούθηση Των Επικοινωνιών, Εκδόσεις Αντ. Ν. Σάκκουλα 2006, σελ. 20-23

[87] Ιωάννης Π. Χοχλιούρος, Ι.Π., Και Σπηλιοπούλου, Α.Σ., Δυναμικό Και Βασικές Προοπτικές Της Ευρωπαϊκής Οδηγίας Για Το Ηλεκτρονικό Εμπόριο Για Την Αποτελεσματική Προώθηση Συγχρόνων Επιχειρηματικών Εφαρμογών Στο Διαδίκτυο. Τηλεπικοινωνιακή Επιθεώρηση Και Δίκαιο Νέας Τεχνολογίας, Τεύχος Δ, Δεκέμβριος 2004, σελ. 502-535

πρώτη φορά στο Bill of Rights του 1776 της Βιργινίας και στην συνέχεια καταχωρήθηκε στο Σύνταγμα των ΗΠΑ.

Είναι αναμενόμενο λοιπόν πως μέσα από την ανεξέλεγκτή διάχυση της πληροφορίας στο διαδίκτυο και της ανασφάλειας για τα προσωπικά δεδομένα ξαναέρχονται στην επιφάνια απόψεις όπως του Polach περί «δικαιώματος πληροφοριακού αυτοκαθορισμού των πολίτων» και «δικαίωμα αυτοδιάθεσης των πληροφοριών».[88]

Αυτό το δικαίωμα καταχωρήθηκε στην Ελληνική νομοθεσία μέσω του νόμου 2472/1997 περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο βασικός σκοπός είναι η προστασία των δικαιωμάτων του ατόμου καθώς και η διασφάλιση θεμελιωδών ελευθέριων του.[89] Μπορούμε να συμπεράνουμε πως μέσα από αυτά το άτομο οδηγείται στην πλήρη προσωπική ελευθέρια, απαλλαγμένο από φόβους κατασκόπευσης την προσωπικής του ζωής. Στο πλαίσιο της επεξεργασίας περιλαμβάνεται η καταγραφή, η καταχώρηση και ο έλεγχος του ατόμου. Μέσα από αυτά φανερώνεται το δικαίωμα του ατόμου στην ιδιωτική ζωή τονίζοντας το απαραβίαστο της. (άρθρο 9 παρ.1). Σε αυτό το σημείο αξίζει να αναφερθεί το παράδειγμα της Βρετάνιας, η οποία σύμφωνα με ανακοίνωση του Βρετανικού Υπουργείου Οικονομικών θα παράσχει 2,32 δισεκατομμύρια δολάρια με σκοπό την ενίσχυση της διαδικτυακής άμυνας, ποσό διπλάσιο από αυτό που παρείχε για τα έτη 2011-2016. Παράλληλα θα δημιουργηθεί ένα νέο Ερευνητικό Ινστιτούτο Κυβερνητικής Ασφάλειας το οποίο θα λειτουργεί σε συνεργασία με το ήδη υπάρχον Εθνικό Κέντρο Διαδικτυακής Ασφάλειας.[90]

2.3 Ν. 2472/1997 περί Προστασίας Του Ατόμου Από Την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

2.3.1 Τα σπουδαιότερα ζητήματα

Η έννοια της ιδιωτικότητας τείνει να θυσιαστεί στον βωμό της πληροφορίας και της παγκοσμιοποίησης. Η ανάγκη προστασίας το ατόμου από την ελεύθερη διακίνηση των προσωπικών του δεδομένων παρουσιάστηκε ήδη από το 1970. Έως τα τέλη του 1980 οι προσωπικές πληροφορίες θεωρούνται άρρηκτα συνδεδεμένες με το άτομο που τις φέρει

[88] Ελληνική Εταιρία Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, σελ. 332

[89] Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία, Ζητήματα από το Δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή, 2002, σελ. 24

[90] http://www.skai.gr/news/technology/article/329415/vretania-ependuseis-232-dis-dolarion-gia-ti-diadiktuaki-asfaleia/, 06/11/2016

και προστατεύονται από το δίκαιο.[91] Πλέον τα όρια της ιδιωτικότητας ορίζονται σε ευρωπαϊκό και παγκόσμιο επίπεδο με σαφή διάκριση της συλλογής και της επεξεργασίας των πληροφοριών καθώς επίσης και των δημοσίων και ιδιωτικών πληροφοριών των υποκείμενων. Το κράτος για να μπορέσει να λειτουργήσει και να ελέγξει τόσο τις οικονομικές , κοινωνικές και νομικές δραστηριότητες πρέπει να εντάξει στην λειτουργία του όλο το εύρος των δραστηριοτήτων που λαμβάνουν χωρά στο διαδίκτυο, εκσυγχρονίζοντας την λειτουργία του.[92] Σε αυτό το πλαίσιο ο νομοθέτης προσπαθεί να ισορροπήσει τα ατομικά δικαιώματα και τα ιδιωτικά συμφέροντα με την αξιοποίηση τους, και τον κρατικό έλεγχο στον οποίο πρέπει να υπάγονται. [93]

Πιο συγκριμένα η Ευρωπαϊκή Οδηγία 95/46 και ο σχετικός νομός 2472/1997 οριοθετούν τις απαγορεύσεις επεξεργασίας των προσωπικών δεδομένων, ορίζοντας παράλληλα ορισμένες εξαιρέσεις με την πλήρη γνώση και γνωστοποίηση του αρχείου της επεξεργασίας στην αρμόδια Ανεξάρτητη Αρχή. Όσο αφορά τα ευαίσθητα προσωπικά δεδομένα απαιτείται άδεια της Ανεξάρτητης Αρχής. Παρ'όλα αυτά από το 2000 εισέρχονται στο υπάρχον νομικό πλαίσιο όλο και περισσότερες εξαιρέσεις οι οποίες καταχωρούνται ως «κοινωνικά πρόσφορες και αναγκαίες ενέργειες». Σύμφωνα με αυτά τα δεδομένα προσωπικού χαρακτήρα κρίνονται ως ιδιωτικά και προστατεύονται από τον νόμο. Σε περίπτωση που συλλεχθούν κατά παράβαση του και δεν υπόκεινται σε κάποια κατηγορία εξαίρεσης του νομικού πλαισίου, υποβάλλονται κυρώσεις.[94]

2.3.2 Δεδομένα προσωπικού χαρακτήρα

Στην εποχή της ηλεκτρονικής πληροφορίας έπρεπε να υπάρξει ένας τρόπος αρμονικής συνύπαρξης ανάμεσα στην ιδιωτικότητα, τον σεβασμό των προσωπικών πληροφοριών, και στην συλλογή τους. Η αναγκαιότητα αυτή πηγάζει από το δικαίωμα ελεύθερης έκφρασης και ερευνάς.[95] Αυτό επιτυγχάνεται με την θέσπιση των προσωπικών δεδομένων.

Με τον νομό 2471/1997 εισαχθεί για πρώτη φορά ένας αμιγώς πληροφοριακός ορός, ο ορός των προσωπικών δεδομένων, ή αλλιώς των προσωπικών στοιχείων. Ο ορός

---

[91] Ι.Ιγγλεζακη, Ευαίσθητα Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2003, σελ.47

[92] Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 24-26

[93] Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 90-93

[94] Γ. Νούσκαλης, Ποινική Προστασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα 2005, σελ.1-6

[95] Ιωάννης Κ. Καράκωστας, Δίκαιο & Internet, Νομικά ζητήματα του Διαδικτύου, εκδόσεις Σάκκουλα σελ.153

«δεδομένα» (data) είναι ευρέως διαδεδομένος στον κόσμο της πληροφορικής. Η χρήση του δανείστηκε για την κατηγορία των δεδομένων που αναφέρονται και είναι ικανά να προσδιορίσουν το άτομο που τα φέρει.[96]

Ως «προσωπικά δεδομένα» θεωρείται κάθε πληροφορία από την οποία μπορεί να φανερωθεί η ταυτότητά του υποκείμενου. Το όνομα, το φύλο, η καταγωγή, ο τόπος κατοικίας, η κατάσταση της υγειάς του, η ερωτική του ζωή, το επάγγελμα, η θρησκεία, οι πολιτικές απόψεις, η συνδικαλιστική δράση και οι ποινικές διώξεις αποτελούν προσωπικά δεδομένα.

Οι προσωπικές πληροφορίες λοιπόν διαχωριστήκαν σε δυο κατηγόριες. Στις ευαίσθητες προσωπικές πληροφορίες και τις απλές πληροφορίες. Οι ευαίσθητες πληροφορίες υπάγονταν σε πολιτική αυξημένης προστασίας και υποβάλλονται σε αυστηρότερες ποινές από τα απλά δεδομένα. Ως ευαίσθητα χαρακτηρίζονται προσωπικά δεδομένα που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων. Η καθιέρωση της άνωθεν διάκρισης έλαβε χωρά το από το συμβούλιο της Ευρώπης για την προστασία του υποκείμενου από την αυτοματοποιημένη συλλογή των προσωπικών του πληροφοριών στις 28 Ιανουάριου του 1981απο την Σύμβαση 108.

Ο διαχωρισμός των πληροφοριών σε ευαίσθητές και μη, προστατεύει πλήρως την προσωπική ζωή, που αποτελεί το ζητούμενο της δημιουργίας τους, αλλά και την ευρύτερη ιδέα της προστασίας των θεμελιωδών δικαιωμάτων και των ελευθέριων του ατόμου. Σύμφωνα με τα άνωθεν, διασφαλίζονται όχι μόνο οι πληροφορίες που αφορούν την ιδιωτική ζωή του ατόμου, αλλά και εκείνες που είναι ικανές να βλάψουν το υποκείμενο όπως ποινικές διώξεις και φυλετικές διακρίσεις. Επιπλέον η διάκριση των πληροφοριών είναι απαραίτητη για την χρήση τους ως βασική οδηγία στα χεριά της δικαιοσύνης για να μπορέσει να στηρίξει αποφάσεις, καλύπτοντας τυχών νομικά κενά.[97]

Ο όρος δεδομένα προσωπικού χαρακτήρα δεν χρησιμοποιείτε τυχαία στον πληθυντικό αριθμό. Η χρήση του πληθυντικού αριθμού σηματοδοτεί την ύπαρξη του

[96] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.19

[97] Ελληνική Εταιρία Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, σελ. 304-309

υποκειμένου ως πολυδιάστατη οντότητα και δεν βάλλει την προσωπικότητα του. Επιπλέον η χρήση του όρου «δεδομένων» έναντι της χρήσης της πληροφορίας προήλθε επειδή η πληροφορία έχει διαφορετική ερμηνεία από το δεδομένο. Η πληροφορία αναφέρεται σε ένα σύμβολο το οποίο στερείτε νοηματικής αξίας, και ως δεδομένο εμπεριέχεται η έννοια της πληροφορίας χωρίς όμως να περιλαμβάνεται κανένα στοιχείο σύνδεσης με το άτομο. Ως δεδομένη πληροφορία θεωρείται η πληροφορία που έχει ήδη παρασχεθεί από το υποκείμενο, έχει καταγραφεί και είναι διαθέσιμη να υποβληθεί σε οποιαδήποτε μορφή επεξεργασίας.

Προχωρώντας στην εμβάθυνση του νομού παρατηρούμε πως τα δεδομένα προσωπικού χαρακτήρα αφορούν πτυχές της προσωπικότητας του ατόμου οι οποίες είναι σε θέση να υποστούν επεξεργασία, ενώνοντας έτσι το υποκείμενο των στοιχείων και την επεξεργασία με μια αρίστη σχέση.[98] Κατά την Λ. Μήτρου, ως προσωπικά δεδομένα χρησιμοποιούνται και τα στοιχεία που προσδιορίζουν την ταυτότητα του υποκείμενου όπως το όνομά του αλλά και στοιχεία που επιλέγονται από τα ιδιά τα άτομα όπως κωδικοί πρόσβασης κα.[99]

Τα δεδομένα που δεν θεωρούνται προσωπικού χαρακτήρα καθορίζονται από τον Ν. 2690/1999. Σύμφωνα με αυτόν τα κοινά προσωπικά δεδομένα συνοψίζονται στις εξής κατηγορίες: στοιχεία αναγνώρισης (πχ. Υπηκοότητα), προσωπικά χαρακτηριστικά (πχ φυσικά χαρακτηριστικά), οικογενειακές συνήθειες, εκπαίδευση, οικονομική κατάσταση, εργασία.

2.3.3 Ευαίσθητα προσωπικά δεδομένα

Υπό τον τίτλο «Ειδικές Κατηγορίες Επεξεργασίας» της Οδηγίας αναφέρονται ορισμένες ειδικές κατηγορίες δεδομένων για τα οποία προβλέπεται αυξημένη προστασία. Αυτές οι κατηγορίες αφορούν την φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, την συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγειά και την σεξουαλική ζωή. Οι παραπάνω ομάδα αναφέρεται στο άρθρο 8 της Οδηγίας. Πρέπει ωστόσο να σημειώσουμε πως τα ευαίσθητα προσωπικά δεδομένα χωρίζονται σε κατηγορίες ανάλογα με τον βαθμό που μπορούν να στιγματίσουν το άτομο που τα φέρει. Μερικοί από τους παράγοντες που καθιστούν ευαίσθητα τα δεδομένα είναι τα εκ φύσεως ευαίσθητα δεδομένα, αυτά που έχει κατατάξει το ίδιο το

[98] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.19-23

[99] Λ. Μήτρου, Προστασία Προσωπικών Δεδομένων, εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004, σελ.452

υποκείμενο ως ευαίσθητα, δεδομένα ιδιαίτερων χαρακτηριστικών, αυτά που είναι δηλωμένα σε μητρώα, και αυτά που μπορούν να οδηγήσουν στον εντοπισμό άλλων ευαίσθητων προσωπικών δεδομένων. [100]

Στην Ελλάδα στα ευαίσθητα προσωπικά δεδομένα συγκαταλέγεται η κοινωνική πρόνοια, η συμμετοχή σε ενώσεις και σωματεία καθώς και οι ποινικές δίωξης και καταδίκες. Αυτό συμβαίνει επειδή η Οδηγία δίνει την δυνατότητα στα επιμέρους κράτη-μέλη να ρυθμίσουν προσθέτοντάς νέες απαραίτητες για αυτά ομάδες στα ευαίσθητα προσωπικά δεδομένα. Ο λόγος είναι οι διαφοροποιημένες κοινωνικές και νομικές αντιλήψεις του κάθε κράτους που οριοθετεί διαφορετικά την ιδιωτικότητα αλλά και η δυσχέρεια διατύπωσης καθολικών κριτήριων τα οποία δεν θα εκθέτουν τους κάτοχους τους. Ωστόσο πρέπει να επισημανθεί πως η εσωτερική νομοθετική ρύθμιση δεν εμποδίζει την διασυνοριακή κυκλοφορία των δεδομένων μεταξύ των μελών της Ευρωπαϊκής Ένωσης.[101]

2.3.4 Το υποκείμενο των δεδομένων

Ο νομός έχοντας στο επίκεντρο την προστασία των δικαιωμάτων και των ελευθέριων του ατόμου αποσαφηνίζει την έννοια του υποκείμενου. Ως υποκείμενο των δεδομένων λοιπόν, ορίζεται κάθε φυσικό πρόσωπο, (όχι όμως τους αποθανόντες για τους οποίους ισχύει η ειδική διάταξη του άρθρου 365Π.Κ. περί προσβολής της μνήμης νεκρού), στο οποίο αναφέρονται τα δεδομένα, και η ταυτότητα του μπορεί να εξακριβωθεί. Η αντιστοίχιση μπορεί να γίνεται άμεσα με τον ορισμό ταυτότητας, ή έμμεσα μέσα από το στοιχεία που το φωτογραφίζουν, δηλαδή μέσα από φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική και κοινωνική άποψη.[102] Το υποκείμενο έχει δικαίωμα να αρνηθεί την χρήση των προσωπικών του δεδομένων καθώς και να έχει πρόσβαση σε αυτά κατά την επεξεργασίας τους.[103]

2.3.5 Η έννοια του αρχείου

Η έννοια του αρχείου είναι άρρηκτα συνδεδεμένη με την έννοια της επεξεργασίας καθώς αποτελεί το αντικείμενο της. Για τον καθορισμό της έννοιας του αρχείου πρέπει να

[100] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 4th Edition, 2007, pp.335-337

[101] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.23-42

[102] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.45-47

[103] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 207-209

υπάρχουν τα εξής βασικά χαρακτηριστικά: α) η ύπαρξη ενός συνόλου δεδομένων προσωπικού χαρακτήρα, β) η ύπαρξη επεξεργασίας πάνω σε αυτά τα δεδομένα, και γ) η τήρησή τους από ένα φυσικό πρόσωπο, η μια ομάδα προσώπων ή ακόμα και από το δημόσιο. Επιπλέον απαιτείτε η ύπαρξη μιας στοιχειώδους ομαδοποίησης των δεδομένων.[104] Αρκεί η ύπαρξη ενός και μόνο ευαίσθητου προσωπικού δεδομένου στο αρχείο για να μπορεί να πάρει νομική υπόσταση, και να λειτουργήσει ως μονάδα μέτρησης του νομικού αυτοκαθορισμού του ατόμου.

Η συλλογή προσωπικών δεδομένων χωρίς την άδεια της Αρχής και χωρίς την υπαγωγή σε κάποια από τις εξαιρέσεις που αναγράφονται στις Ευρωπαϊκές Οδηγίες και στην εγχωρία νομοθεσία, όπως επίσης και η μη γνωστοποίηση συλλογής, να υπόκεινται στην παράνομη διατήρηση αρχείου. Αυτό συμβαίνει λόγο αδυναμίας της Αρχής και του υποκείμενου να ελέγχουν τόσο την νομιμότητα, όσο και την χρήση του αρχείου γεγονός που δεν διασφαλίζει την έννομη χρήση του. Ωστόσο ο Ν.2472/1997 και η Οδηγία 95/46 , η οποία θα μελετηθεί παρακάτω, δεν θεωρεί αξιόποινο παράπτωμα την επεξεργασίας προσωπικών δεδομένων χωρίς άδεια, εν αντιθέσει με τα δεδομένα που επεξεργάζονται οντάς αυτοματοποιημένα και αυτά που πρόκειται να συμπεριληφθούν σε αρχείο. Αξίζει να σημειωθεί πως η εκκρεμής ποινική δικογραφία, και τα στοιχεία του ανακριτικού και της προανάκρισης σύμφωνα με τον νομό 2472/1997, απόφαση 147/2001 δεν αποτελούν αρχείο αλλά φάκελο. Το ερώτημα που εγείρεται ωστόσο είναι πως από φάκελος μετά την εκδίκαση και ολοκλήρωση της υπόθεσης μετατρέπεται αυτομάτως σε αρχείο.

Επιπλέον, στον ελληνικό νομό γίνετε λόγος μόνο για το σύνολο των προσωπικών δεδομένων τα οποία αποτελούν ένα αρχείο και αντικείμενο επεξεργασίας, χωρίς όμως τον βασικό ορό «διαρθρωμένο» που τον συνόδευε στην αρχική μορφή της Ευρωπαϊκής Οδηγίας. Τα κριτήρια που ορίζει η Οδηγία αφορούν την ανά πασά στιγμή εύρεση τους και την μόνιμη διατήρηση τους, κριτήρια δηλαδή που παραπέμπουν στο αρχείο. Παρατηρούμε λοιπόν, τον διαχωρισμό, (θελημένο ή μη) δυο άρρηκτα συνδεδεμένων εννοιών, του αρχείου και της επεξεργασίας, ο οποίος προκαλεί πρόβλημα στην ερμηνεία των νομών και των Οδηγιών. Με αυτόν τον τρόπο αποκλείονται ευκολότερα μη αρχειοθετημένα αρχεία για τα οποία αμφισβητείτε η υπόσταση τους αρχείο ή φακέλου. (Ο όρος που χρησιμοποιείτε στην Ευρωπαϊκή Οδηγία είναι ο “personal data filing system”).[105]

[104] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π,, σελ. 69
[105] Γεώργιος Ντούσαλης, Ποινική Προστασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2005, σελ.63-82

Από την άλλη πλευρά υποστηρίζεται η άποψη πως μπορεί ο εγχώριος νομοθέτης να επιδίωξε την ελαφρά τροποποίηση της Οδηγίας αυξάνοντας παράλληλα την αποτελεσματικότητα και το εύρος της. Έτσι ο εγχώριος νόμος γίνεται πολύ πιο γενικός από εκείνον που υιοθετείτε στην Οδηγία καθώς ο νομοθέτης αποφεύγει την χρήση των ορών «διατήρηση» και «αποθήκευση» του συνόλου των δεδομένων τα οποία αποτελούν κατά πασά πιθανότητα αυτονόητα στοιχεία της νομοθεσίας. Επιπλέον, μπορούμε να συμπεραίνουμε πως η χρήση του πιο ευρύ όρου της νομοθεσίας βοηθάει στην ένταξη και στην νομική κάλυψη ενός συλλόγου φακέλων οι οποίοι δεν θα καλύπτονταν νομικά. Έτσι, τα μη αυτοματοποιημένης επεξεργασίας αρχεία τα οποία δεν είναι διορθωμένα με βάση τα ειδικά κριτήρια δεν θα υπόκειται στην νομοθεσία. Αποτέλεσμα θα ήταν το υποκείμενο να μην έχει πρόσβαση σε αυτά. Βάση αυτής της διαφοροποίησης λοιπόν προσαρμόζεται ο νομός πλήρως πάνω στον σκοπό ύπαρξης του.[106]

2.3.6 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Στις 10/11/1997 συστάθηκε μια ανεξάρτητη Αρχή, με σκοπό την προστασία των προσωπικών δεδομένων. Η Αρχή Προστασίας Προσωπικών Δεδομένων συγκροτείται και λειτουργεί σύμφωνα με τις επιταγές του νόμου. Η Οδηγία απαιτούσε την δημιουργία μιας ανεξάρτητης Αρχής σε κάθε κράτος της Ευρωπαϊκής Ένωσης η οποία θα απολάμβανε πλήρης ανεξαρτησίας και δεν θα επέτρεπε την τροποποίηση των κανονισμών της από οποιαδήποτε νομική φύση. Η αποστολή της είναι η λεπτομερής ρύθμιση ειδικών θεμάτων, η εποπτεία της εφαρμογής του νόμου περί επεξεργασίας προσωπικών δεδομένων, καθώς και η ενσωμάτωση νεών Οδηγιών. Η ανεξαρτησία της Αρχής πρακτικά ορίζεται ως ανεξαρτησία από οποιονδήποτε διοικητικό έλεγχο, ανεξαρτησία (προσωπική και λειτουργική) μελών, και την ύπαρξη ιδιαίτερης γραμματείας. Η λειτουργία του χρηματοδοτείται από ειδικά κονδύλια που αναγράφοντα στον ετήσιο προϋπολογισμό του Υπουργείου Δικαιοσύνης.[107]

[106] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ. 69-75

[107] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.387-392, Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 235-249

2.3.7 Στατιστικά Στοιχεία

Τα στατιστικά στοιχεία χωρίζονται σε δυο κατηγορίες ανάλογα με το αν χρίζουν ή όχι προστασίας. Μη προστατευόμενα στατιστικά στοιχεία ονομάζεται εκείνα τα οποία δεν μπορούν να φανερώσουν την ταυτότητα του ατόμου που τα φέρει. Αυτό συμβαίνει όταν τα στοιχεία έχουν συλλεγεί στα πλαίσια μια στατιστικής ερευνάς και παρουσιάζονται ως αποτέλεσμα επεξεργασίας, δηλαδή ως ομαδοποιημένα αριθμητικά μεγέθη, καθιστώντας παράλληλα ανέφικτο τον προσδιορισμό των συμμετεχόντων.

Εν αντίθεσίν, τα προστατευόμενα στατιστικά στοιχεία, αναφέρονται σε αυτά που μπορούν να αποκαλύψουν, ακόμα και σε ένα άτομο, τους συμμετέχοντες στην ερευνά. Αυτό συνήθως συμβαίνει σε αραιοκατοικημένες περιοχές όπου η ηλικία και το μορφωτικό επίπεδο είναι ικανά να φανερώσουν την ταυτότητα του υποκειμένου.[108]

2.3.8 Η επεξεργασία δεδομένων προσωπικού χαρακτήρα

Παρόλο που ο όρος της επεξεργασίας έχει συνδεθεί με την ασφάλεια των πληροφοριακών συστημάτων, στον Ν.2472/1997 επιχειρείτε η διεύρυνση του μέσα από την διάκριση σε αυτοματοποιημένη και μη επεξεργασία. Ως επεξεργασία λογίζεται κάθε μορφή εργασιών πάνω σε δεδομένα προσωπικού χαρακτήρα. Η επεξεργασία λαμβάνει χωρά είτε από τον υπεύθυνο επεξεργασίας, είτε από τον εκτελών της επεξεργασίας είτε από τρίτο. Τις παραπάνω θέσεις μπορεί να τις φέρουν φυσικά πρόσωπα, δημοσιές αρχές-υπηρεσίες ή οποιοσδήποτε οργανισμός. Εντός του νόμου αριθμείτε ένας κατάλογος εργασιών στις οποίες μπορούν να εφαρμοστούν τα προσωπικά δεδομένα. Οι βασικότερες μορφές επεξεργασίας είναι οι εξής:

I. Συλλογή: πρόκειται για την ενέργεια που προηγείται της επεξεργασίας, αλλά εμπεριέχεται στην ευρύτερη έννοια της και υπόκειται στο ίδιο νομικό καθεστώς. Είναι η διαδικασία αναζήτησης εύρεσης και λήψης πληροφοριών με σκοπό την μετέπειτα χρήση τους.
II. Καταχώρηση: πρόκειται για την ένταξη των δεδομένων με σκοπό την διατήρηση και την περεταίρω επεξεργασία τους. Η καταχώρηση λαμβάνει χώρα με την εγγραφή, την αντιγραφή, ή την αυτόματη καταχώρησης σε ένα πληροφοριακό σύστημα. Τέλος, η καταχώρηση είναι αναγκαίο να υπόκειται σε κριτήρια (χρονικά, σκοπού κ.α.)

[108] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ.24-25

III. Οργάνωση: εν αντιθέσει με την καταχώρηση, η οργάνωση στοιχειοθετεί τα δεδομένα με τέτοιο τρόπο ώστε να αποτελούν ένα ενιαίο σύνολο. Η ύπαρξη αρχείου είναι βασική προϋπόθεση της οργάνωσης, αλλά όχι απαραίτητη αφού η απλή διατήρηση των προσωπικών δεδομένων δεν απαιτεί ορισμένη δομή.

IV. Διατήρηση/Αποθήκευση: πρόκειται για την επεξεργασία που υφίστανται τα προσωπικά δεδομένα με σκοπό την καταχώρηση τους, που συντελεί την διάσωση τους σε βάθος χρόνου. Πολλές φορές συνοδεύεται με τη δέσμευση τους και την ύπαρξη αρχείου.

V. Τροποποίηση: πρόκειται για την επέμβαση στα δεδομένα με σκοπό την αλλαγή της διατύπωσης, είτε την εξαγωγή άλλων νέων πορισμάτων μέσα από τα ίδια δεδομένα. Συνήθως αυτό επιτυγχάνεται με την εισαγωγή ή αφαίρεση στοιχείων στα ήδη υπάρχοντα δεδομένα.

VI. Εξαγωγή: πρόκειται για την επανάκτηση χαμένων αρχείων, την άντληση, την συλλογή και την λήψη ήδη υπαρχόντων δεδομένων, όπως επίσης και την καταγραφή των στοιχείων που προκύπτουν ως συμπεράσματα (νέα δεδομένα).

VII. Χρήση: ο ορός της χρήσης των προσωπικών δεδομένων εντός του Ν. 2472/1997 έχει ευρεία έννοια και περιλαμβάνει το σύνολο των ενεργειών που δεν έχουν κατοχυρωθεί με τους ορούς συλλογή και επεξεργασία. Η χρήση της έχει ισχυρό προστατευτικό χαρακτήρα υπέρ της διαφύλαξης του υποκείμενου από πάσης φύσεως κινδύνους.

VIII. Διαβίβαση: πρόκειται για την γνωστοποίηση των δεδομένων σε τρίτα άτομα με μεταβίβαση ή απευθείας μετάδοση.

IX. Διάδοση/Διάθεση: εν αντίθεση με την διαβίβαση των δεδομένων που μεταδίδονται προς συγκεκριμένο αποδεκτή, η διάδοση αφορά την μεταβίβαση προς κάθε κατεύθυνση απροσδιορίστου/ων αποδεκτή/ων.

X. Συσχέτιση/Συνδυασμός: πρόκειται για τις μορφές της επεξεργασίας στην οποία υποβάλλονται τα δεδομένα με σκοπό την εξαγωγή νέων πορισματικών δεδομένων. Η συσχέτιση χρησιμοποιείτε επίσης για την επαλήθευση δεδομένων αλλά και την συσχέτιση διαφορετικών αρχείων.

XI. Διασύνδεση: οπού διασυνδέονται δύο ή περισσότερα αρχεία μεταξύ τους.

XII. Δέσμευση: πρόκειται για το κλείδωμα των αρχείων με σκοπό την προστασία του από κάθε μορφή επεξεργασίας. Σκοπός είναι η απλή αποθήκευση και διατήρησή των δεδομένων. Η συνηθέστερη μορφή δέσμευσης, ιδιαιτέρως στα μέσα κοινωνικής δικτύωσης, είναι η απόκρυψη. Οι πληροφορίες διατηρούνται αλλά

απαγορεύεται η πρόσβαση σε αυτές από τρίτα άτομα, τα οποία σε ορισμένες περιπτώσεις ειδοποιούνται μέσα από μια ειδική σήμανση για την ύπαρξη των κρυφών στοιχείων. Μια άλλη μορφή δέσμευσης αφορά εμφανίσιμα σε όλους δεδομένα τα οποία όμως δεν δέχονται συγκεκριμένες επεξεργασίες. Τέλος, η δέσμευση μπορεί να λαμβάνει χωρά με προθεσμία λήξης.

XIII. Διαγραφή: πρόκειται για τον αποκλεισμό των δεδομένων από κάθε μορφή επεξεργασίας, από την πρόσβαση σε αυτά καθώς και τη γενικότερη αλλοίωσή τους μέσω της διαγράφης. Πρέπει να τονιστεί ότι η διαγραφή αφορά την κατάσταση των δεδομένων σε μορφή μη αναγνώσιμη. Εντούτοις η ανωνυμοποίηση και ψευδονυμοποίηση αποτελούν μια μορφή διαγράφης αφού το δεδομένο απαλλάσσεται από το υποκείμενο στο οποίο αρχικά ανήκε και δεν μπορεί πλέον να οδηγήσει στην εύρεση της ταυτότητας του. Η διαγραφή των δεδομένων από μια τοποθεσία δεν αποκλείει την ύπαρξη αντιγράφων τα οποία ενδεχομένως να συνεχίσουν την επεξεργασία τους. Διαγραφή γίνετε και αποσπασματικά σε αρχεία χωρίς την αναγκαστική διαγραφή του συνόλου των δεδομένων.

XIV. Καταστροφή: πρόκειται για ολική καταστροφή των δεδομένων αφού καταστρέφεται μαζί με αυτά η βάση στην οποία είχαν καταχωρηθεί. Η μετέπειτα ανάκτηση τους είναι αδύνατη.[109]

2.3.9 Συγκατάθεση του υποκειμένου

Για να είναι έννομη η συλλογή και η επεξεργασία των δεδομένων προσωπικού χαρακτήρα επιβάλλεται το υποκείμενο να φέρει πλήρη γνώση για την συλλογή. Πιο συγκεκριμένα απαιτείται η ελεύθερή, ρητή, σαφής και ειδική άδεια του υποκείμενου για την συλλογή και τη χρήση των προσωπικών του δεδομένων. Πριν όμως προβεί στο στάδιο της συγκατάθεσης, πρέπει να έχει λάβει γνώση για τον σκοπό της χρήσης τους, ποια από τα προσωπικά του δεδομένα θα χρησιμοποιηθούν, τους αποδέκτες που θα έχει η επεξεργασία, καθώς και το όνομα/ επωνυμία και την διεύθυνση του υπευθύνου επεξεργασίας. Η έγκριση και η συνένωση του υποκείμενου είναι απαραίτητη και πρέπει κατά νομό να προηγείται της συλλογής και της επεξεργασίας των προσωπικών του δεδομένων καθώς η έγκριση δεν φέρει αναδρομική ισχύ (αρθρο2, 5 παρ.1). Επιπλέον του

[109] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.47-69

δίνεται το δικαίωμα να άρει την έγκριση του κατά βούληση χωρίς αυτό ωστόσο να επηρεάσει τα δεδομένα που έχουν ήδη υποστεί επεξεργασία και καταχώρηση.[110]

2.3.10 Ποιοτικά χαρακτηριστικά προσωπικών δεδομένων

Με σκοπό την εύρεση ισορροπίας μεταξύ των συμφερόντων των υποκείμενων και της επεξεργασίας προσωπικών δεδομένων υιοθετήθηκαν ορισμένα βασικά ποιοτικά χαρακτηριστικά (αρθρο4) τα οποία πρέπει να διέπουν τα δεδομένα για να χαρακτηριστεί έννομη η χρήση τους. Τα χαρακτηριστικά είναι τα εξής: α) Ο τρόπος και ο σκοπός συλλογής και επεξεργασίας των δεδομένων, β) το περιεχόμενο και η συνάφεια που αυτό φέρει ως προς το σκοπό, την ακρίβεια και την επικαιρότητα των δεδομένων, και τέλος γ) τον τρόπο, τον σκοπό, και τον χρόνο της διατήρησης τους. Η δεσμευτικότητα των προαναφέρονταν ποιοτικών χαρακτηριστικών είναι απολυτή και σε περίπτωση συλλογής, η καθυστερημένη συγκατάθεση δεν γίνεται δεκτή από το νομό.[111]

Οι εν λόγο αρχές αποτελούν τις θεμελιωδέστερες από τον νομό αρχές καθώς διασφαλίζουν τον έλεγχο του υποκείμενου πάνω στα προσωπικά του δεδομένα και τον έλεγχο της Αρχής, μειώνοντας παράλληλα τους κίνδυνους προσβολής των υποκείμενων.[112]

I. Αρχή του νόμιμου τρόπου συλλογής: για να είναι η συλλογή των δεδομένων έννομη πρέπει να διέπετε από τους παρακάτω κανόνες:
    - Το υποκείμενο των προσωπικών δεδομένων να έχει ενημερωθεί (άρθρο 11)
    - Να υπάρχει προγενέστερη της συλλογής και επεξεργασίας συγκατάθεση του υποκείμενου (άρθρο 5)
    - Να έχει γνωστοποιηθεί στο υποκείμενο η δημιουργία αρχείου και η έναρξη της επεξεργασίας (άρθρο 6)
    - Να υπάρχει άδεια της Αρχής για επεξεργασία ευαίσθητων προσωπικών δεδομένων (άρθρο 7)
    - Σε περίπτωση διασύνδεσης να έχει γνωστοποιηθεί στην Αρχή και να έχει ληφθεί (άρθρο 8)
    - Σε περίπτωση διαβίβασης των συλλεχθεντων δεδομένων εκτός Ε.Ε. να πληρούνται όλες οι προϋποθέσεις νομιμότητας (άρθρο 9)
    - Να διασφαλίζεται το απόρρητο και η ασφάλεια των δεδομένων (άρθρο 10).

[110] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ. 92-96
[111] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ.112-114
[112] Α.Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, 2002, σελ.188

II. Αρχή του σκοπού: κατά το άρθρο 4 (παρ. 1) τα δεδομένα σύμφωνα με την Αρχή του σκοπού πρέπει να συλλέγονται και να επεξεργάζονται με καθορισμένο, σαφή και νόμιμο τρόπο. Με σκοπό την περαιτέρω ανάλυση και διευκρίνιση των επιμέρους πτυχών η Αρχή του σκοπού μελετάται σε τρεις επιμέρους αρχές:

- Την Αρχή του εκ των προτέρων καθορισμένου σκοπού: στον οποίο ορίζεται η αναγκαιότητα ο σκοπός να είναι ρητά καθορισμένος πριν την έναρξη της συλλογής και της επεξεργασίας.
- Η Αρχή της σαφήνειας του σκοπού: για να μπορέσει να σταθεί ο σκοπός και να γίνει κατανοητός προϋποθέτει την Αρχή της σαφήνειας. Για να θεωρηθεί λοιπόν ο σκοπός νόμιμος πρέπει να είναι σαφώς καθορισμένος και διατυπωμένος για να μπορέσει να ενημερωθεί πλήρως το υποκείμενο της ερευνάς αλλά και να ελέγχεται ταυτόχρονα ο υπεύθυνος επεξεργασίας. Η πολλυλειτουργική συλλογή θεωρείτε παράνομη εκτός και αν έχει προβλεφθεί και ελεγχθεί εκ των πρότερων.
- Η Αρχή της νομιμότητας του σκοπού: ο σκοπός της επεξεργασίας επιβάλετε να είναι νόμιμος, δηλαδή να χειρίζεται τα δεδομένα ανάλογα με την φύση τους (κοινά ή ευαίσθητα), να σέβεται το απόρρητο της επεξεργασίας, και τα δικαιώματα του υποκείμενου, και σε περίπτωση που πρόκειται για ευαίσθητα προσωπικά δεδομένα να διαθέτει άδεια από την Αρχή.

III. Αρχή της αναγκαιότητας της επεξεργασίας: η Αρχή της αναγκαιότητας ορίζει πως τα δεδομένα δεν μπορούν να έχουν νόμιμη επεξεργασία αν δεν είναι συναφή, προσφορά και δεν διαθέτουν το κατάλληλο πλήθος για την ερευνά. Πιο συγκεκριμένα αναλύεται στην:

- Αρχή συνάφειας των δεδομένων προς τους σκοπούς της επεξεργασίας: στον ποιο επισημαίνεται ότι για να είναι νόμιμη η επεξεργασία τα δεδομένα πρέπει να σχετίζονται με τον σκοπό, ο οποίος επίσης πρέπει να είναι νόμιμος.
- Αρχή της προσφορότατα των δεδομένων προς τους σκοπούς της επεξεργασίας: όπου αναφέρεται πως τα δεδομένα πρέπει να είναι καταλληλά για τον σκοπό της επεξεργασίας. Σε αντίθετη περίπτωση η επεξεργασία δεν είναι νόμιμη. Επιπλέον το πλήθος των δεδομένων πρέπει να είναι αριθμητικά όσο απαιτείται για την διεξαγωγή της επεξεργασίας.

- Αρχή της ποσοτικής ισορροπίας των δεδομένων προς τους σκοπούς της επεξεργασίας: σε αυτή την Αρχή γίνεται εκτενέστερη αναφορά στην απαιτούμενη ποσότητα δεδομένων. Τα περισσότερα συλλεχθέντα δεδομένα, όπως και τα ελλείπει δεδομένα, οδηγούν σε άνομη επεξεργασία.

IV. Αρχή της ακρίβειας των δεδομένων: σύμφωνα με την εν λόγω Αρχή τα δεδομένα πρέπει να ανταποκρίνονται στην πραγματικότητα, δηλαδή να είναι ακριβή, και σε περίπτωση που μεταβάλλονται μέσα στον χρόνο να είναι συνεχώς ενημερωμένα (επικαιροποίηση).

V. Αρχή της χρονικά πεπερασμένης διατήρησης: τα δεδομένα που μπορούν να οδηγήσουν σε προσδιορισμό του υποκείμενου που τα φέρει υπόκεινται σε χρονικό προσδιορισμό της διατήρησης τους. Ο χρόνος αυτός ορίζεται ως συνδυασμός του σκοπού της επεξεργασίας και της χρονικής διάρκειας που επιτρέπει η Αρχή. Τα δεδομένα ωστόσο που δεν οδηγούν στο υποκείμενο που τα φέρει είναι απαλλαγμένα χρονικής διάρκειας και επιτρέπετε η επ' αόριστο διατήρηση τους («ανωνυμοποίηση). Εξαίρεση στα παραπάνω αποτελούν δεδομένα που συλλέχθηκαν για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς.

Σε περίπτωση μη συμμόρφωσης στις προαναφερθείσες αρχές ο υπεύθυνος επεξεργασίας φέρει βαριές διοικητικές, ποινικές και αστικές ευθύνες και κυρώσεις, ενώ τα δεδομένα καταστρέφονται από την Αρχή.[113]

2.3.11 Περιορισμός πληροφοριακού αυτοκαθορισμού

Σύμφωνα με τον Ν.2472/1997 το άτομο μπορεί να τεθεί υπό επεξεργασία των προσωπικών του δεδομένων χωρίς την συγκατάθεση του ή ακόμα και παρά την ρητή αντίρρηση του. Οι περιπτώσεις οπού δεν απαιτείται η συγκατάθεση του υποκείμενου ορίζονται ρητά από τον νομό και αφορούν περιπτώσεις οπού βάλλεται κάποιο ζωτικό συμφέρον του υποκείμενου (πχ. η ζωή του υποκειμένου). Σε αυτή την περίπτωση η επεξεργασία κρίνεται αναγκαία αλλά υποβάλλεται στις Αρχές Προστασίας με καθορισμένη χρονική διάρκεια και περιορισμένα προσωπικά δεδομένα του υποκείμενου. Τέλος, ο περιορισμός τίθεται σε περίπτωση που το υποκείμενο αδυνατεί νομικά να συγκαταθέσει, ως εμπλεκόμενο σε δικαστικά ζητήματα.[114]

---

[113] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ. 115-140

[114] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ. 166-168

2.3.12 Η απαγόρευση επεξεργασίας ευαίσθητων προσωπικών δεδομένων

Στο άρθρο 7 παρ. 1 του Ν.2472/1997 προβλέπεται τη απαγόρευση της επεξεργασίας ευαίσθητων προσωπικών δεδομένων, ενώ παράλληλα αναφέρονται ορισμένες εξαιρέσεις (παρ. 2) καθώς και ο τρόπος που αυτές λαμβάνουν χώρα. Πιο συγκεκριμένα για κάθε μορφή εξαίρεσης απαιτείτε προηγούμενη άδεια της Αρχής για συλλογή και επεξεργασία. Οι εξαιρέσει συμπεριλαμβάνονται στις επτά παρακάτω περιπτώσεις:

- Η ύπαρξη γραπτής συγκατάθεσης του υποκείμενου: πρόκειται για την εγγράφως εγγύηση του φορέα των προσωπικών δεδομένων ως εκδήλωση ελεύθερης βούλησης την επεξεργασίας των ευαίσθητων δεδομένων του.
- Η διαφύλαξη ζωτικού συμφέροντος του υποκείμενου.
- Η δημοσιοποίηση από το ίδιο το υποκείμενο: σε αυτό συμβάλει η δυνατότητα αυτοκαθορισμού που έχει το άτομο. Με την δημόσια κοινοποίηση ευαίσθητων προσωπικών του δεδομένων θεωρείται από τον νόμο ότι το άτομο με πλήρη γνώση των συνέπειων επιθυμεί να προβεί σε αυτή την ενέργεια.[115] Εντούτοις δεν μπορεί να παραληφθεί σύμφωνα με την Ι.Ιγγλεζάκη ο κίνδυνος που ελλοχεύει καθώς η κοινοποίηση πληροφοριών από το υποκείμενο δεν προϋποθέτει την «ρητή, ελεύθερη, γραπτή και σαφή» έγκριση που προβλέπει ο νομός. Αντιθέτως μπορεί το άτομο να επέλεξε την δημοσιοποίηση εντός ορισμένων «συνόρων» τα οποία καταλύονται.
- Άσκηση δικαιώματος ενώπιον δικαστηρίου
- Υπηρεσίες υγείας: οπού τα ευαίσθητα προσωπικά δεδομένα υπόκεινται σε καθεστώς επαγγελματική εχεμυθείας.
- Αρμοδιότητες ενάσκησης δημόσιας εξουσίας για λογούς : εθνικής ασφάλειας, εγκληματικής- σωφρονιστικής πολιτικής, προστασίας δημοσίας υγείας, φορολογικού ελέγχου, κοινωνικών παροχών.
- Ερευνητικοί και επιστημονικοί σκοποί: όπου απαραίτητη προϋπόθεση είναι η ανωνυμία κατά την μετάδοση της ερευνάς. Δυστυχώς, έχει παρατηρηθεί, πως η πλήρης ανωνυμοποίηση των υποκείμενων δεν υφίσταται καθώς μέσα από ορισμένες ενέργειες είναι δυνατός ο επαναπροσδιορισμός του υποκείμενου.[116]

[115] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ. 223-230
[116] Ι.Ιγγλεζάκης, Ευαίσθητα Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2003, σελ. 226-242, Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 218-220

2.3.13 Η άδεια της Αρχής

Η άδεια της Αρχής εκδίδετε έπειτα από αίτηση του υπευθύνου επεξεργασίας για να προβεί στην συλλογή και στην έννομη επεξεργασία ευαίσθητων δεδομένων. Πρέπει να σημειωθεί πως η άδεια της Αρχής δεν φέρει αναδρομικό χαρακτήρα.

Ο ενδιαφερόμενος πρέπει να καταθέσει σχετική αίτηση στην Αρχή εκθέτοντας με σαφήνεια τους σκοπούς της επεξεργασίας και τα απαιτούμενα δικαιολογητικά. Έπειτα η Αρχή μπορεί να επιβάλει ορούς και προϋποθέσεις πάνω στην επεξεργασία. Η άδεια αφορά ορισμένο χρονικό διάστημα το οποίο μπορεί και να παραταθεί σε περίπτωση που ο ενδιαφερόμενος το ζητήσει.

Εντούτοις με το άρθρο 8 παρ.4 του Ν.2819/2000 (προστέθηκε το άρθρο $7^{Α}$ στο Ν.2472/1997) οριστήκαν πεδία στα οποία ο υπεύθυνος επεξεργασίας απαλλάσσεται από την υποχρέωση να γνωστοποιήσει την συλλογή και επεξεργασία και ως εκ τούτου να λάβει άδεια από την Αρχή. Αυτές οι κατηγορίες αναφερόντανε σε: επεξεργασία των δεδομένων στον εργασιακό χώρο, επεξεργασία που αφορά πελάτες ή προμηθευτές, δεδομένα μελών σωματείων, εταιριών, ενώσεων και πολίτικων κομμάτων, επεξεργασία ιατρικών δεδομένων από αρμόδιους, συλλειτουργούς της δικαιοσύνης, επεξεργασίας από την δικαστική λειτουργία.[117]

2.3.14 Διασύνδεση δεδομένων προσωπικού χαρακτήρα

Η διασύνδεση (άρθρο 8) είναι μια μορφή επεξεργασίας των δεδομένων και διακρίνεται σε απλή και ιδιαίτερη διασύνδεση. Και στις δύο περιπτώσεις βασική προϋπόθεση για να χαρακτηριστούν ως έννομες είναι η γνωστοποίηση τους στην Αρχή. Στην περίπτωση της ιδιαίτερης διασύνδεσης ωστόσο απαιτείται και λήψη άδειας από την Αρχή.

Αναλυτικότερα, στην απλή διασύνδεση η δήλωση στην Αρχή πρέπει να είναι η εγγραφή και να υποβάλλετε από κοινού για τους συμμετέχοντες στην διασύνδεση. Επιπλέον πρέπει να προηγείται της διασύνδεσης. Στην περίπτωση της ιδιαίτερης διασύνδεσης περιλαμβάνονται οι περιπτώσεις στις οποίες περιέχονται ευαίσθητα δεδομένα, ή πρόκειται να εξαχθούν κατά την διασύνδεση. Σε αυτή την περίπτωση οι υπεύθυνοι επεξεργασίας θα πρέπει να έχουν προβλέψει για την πρότερη έκδοση της σχετικής αδείας. Για την έκδοση της απαιτείτε η συμπλήρωση και η κατάθεση της ειδικής

[117] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ. 248-272

φόρμας καθώς και οι αναλυτικοί λόγοι για τους οποίους ζητείται η άδεια. Πρέπει να αναφερθεί επίσης πως η άδεια είναι πεπερασμένου χρόνου αλλά μπορεί να ανανεωθεί σε περίπτωση που αυτό συμβάλει στην προστασία των υποκειμένων ή για λόγους εξυπηρέτησης των υποκειμένων.

Όλα τα έγγραφα καθώς και τα αντίγραφα των αδειών διασύνδεσης των ιδιαίτερων διασυνδέσεων καταχωρούνται στο Μητρώο Διασυνδέσεων που διατηρεί η Αρχή και είναι προσβάσιμα σε κάθε πολίτη. Εξαίρεση αποτελούν οι διασυνδέσεις που υπόκεινται στο απόρρητο οι οποίες καταχωρούνται στο Μητρώο Απορρήτου και είναι μη προσιτές.[118]

2.3.15 Ελεύθερη ροή προσωπικών δεδομένων εκτός Ελλάδας

Η Ευρωπαϊκή Ένωση με σκοπό την ελεύθερη μεταφορά εμπορευμάτων, προσώπων, υπηρεσιών και κεφαλαίων έχει προβεί σε ένα κοινό θεσμικό πλαίσιο προστασίας προσωπικών δεδομένων. Η διασυνοριακή ροή παίρνει την μορφή διαβίβασης των πληροφοριών χωρίς να υπόκεινται σε κανένα περιορισμό πέρα από τις Αρχές και τους κανόνες που διέπουν την επεξεργασία των προσωπικών δεδομένων λόγο της εναρμόνισης των νομοθεσιών των κρατών-μελών και των ρυθμιστικών Κοινοτικών Οδηγιών. Ωστόσο τα δεδομένα δεν μεταβιβάζονται μόνο εντός Ευρωπαϊκής Ένωσης. Για να εξασφαλιστεί η προστασία τους έχει υπάρξει διαχωρισμός των χωρών σε δυο κατηγορίες. Στην μια κατατάσσονται οι χώρες που εξασφαλίζουν επαρκές επίπεδο προστασίας των προσωπικών δεδομένων (εδώ κατατάσσονται όλες οι χώρες την Ε.Ε.) και η άλλη που δεν παρέχει στα δεδομένα τον επιθυμητό βαθμό ασφαλείας. Για την μεταφορά των δεδομένων σε χώρες που διασφαλίζουν την ασφάλεια απαιτείτε η λήψη αδείας από την Αρχή ενώ μη τήρηση των απαραίτητων μέτρων ασφάλεια οδηγεί στην μη παραχώρηση αδειών (άρθρο 9). [119] Ωστόσο η μεταφορά δεδομένων μπορεί να γίνει με ιδιωτική υπογεγραμμένη συμφωνία αναμεσά στις χώρες που εξάγουν και εισάγου τα δεδομένα και χωρίς την χορήγηση άδειας. (Απόφαση 2001/497/ΕΚ της Ευρωπαϊκής Ένωσης «σχετικά με τις τυποποιημένες συμβατικές ρήτρες για την διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες βάση του άρθρου 26 παρ. 4 της Οδηγίας 95/46/ΕΚ»).

Επιπλέον, σε αυτό το σημείο θα πρέπει να τονίσουμε πως οι ΗΠΑ υπάγονται σε δικό τους καθεστώς σχετικά με την ροή δεδομένων. Οι ιδιοκτήτες των ιστοσελίδων έχουν

[118] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ. 274-281

[119] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ. 286-298

το δικαίωμα να αυτορυθμίσου θέτοντας οι ίδιοι τα όρια και τους περιορισμούς χρήσης τους. Σε μια προσπάθεια συνεργασίας με το Υπουργείο Εμπορίου των ΗΠΑ η Ευρωπαϊκή Επιτροπή δημιούργησε μια λίστα στην οποία μπορούν να συμπεριληφθούν οι εταιρίες που επιθυμούν να ανταλλάζουν δεδομένα με την Ευρώπη. Η συμμετοχή στην λίστα προϋποθέτει την ακολουθήσει των Οδηγιών και των Αποφάσεων της ΕΕ περί ορθής μετάδοσης δεδομένων, αναβαθμίζοντας παράλληλα και το περιβάλλον ροής των συμμετεχόντων εταιριών των ΗΠΑ. Σε περίπτωση που παραβιαστούν οι Κανονισμοί η εταιρία αποβάλλεται από την λίστα με απόφαση της Αρχής.[120]

2.3.16 Το απόρρητο της επεξεργασίας

Η νομιμότητα της επεξεργασίας των προσωπικών δεδομένων (άρθρο 10) βασίζεται στην ασφάλεια και το απόρρητο. Αυτές οι δυο αρχές αποτελούν τους θεμελιώδης λίθους για οποιαδήποτε περεταίρω επεξεργασία. Το απόρρητο φαινομενικά μπορεί να θεωρηθεί ότι έρχεται σε ρήξη με την Αρχή της διαφάνειας.[121] Ωστόσο κάτι τέτοιο δεν υφίσταται. Η Αρχή της διαφάνειας αναφέρεται αποκλειστικά και μόνο στην πρόσβαση που έχει το υποκείμενο των δεδομένων, και η Αρχή στην επεξεργασία, και στην δυνατότητα επέμβασης και τροποποίησης που τους παρέχει ο νομός. Καταλαβαίνουμε λοιπόν πως η Αρχή του απορρήτου αναφέρεται σε οποιονδήποτε τρίτο προσπαθήσει να έχει πρόσβαση σε προσωπικές πληροφορίες.

Ως εκ τούτου μεγάλη βαρύτητα πρέπει να δοθεί στα απαραίτητα μέτρα ασφάλειας. Η ασφάλεια των δεδομένων από τυχαία ή θεμιτή επεξεργασία και αλλοίωση τίθεται στις αρμοδιότητες του υπευθύνου επεξεργασίας. Για την καλύτερη διαφύλαξη των δεδομένων συνιστάτε η τροποποίηση των μεθόδων ασφάλειας ανάλογα με την τεχνολογική πρόοδο και εξέλιξη, καθώς και με τις απειλές που εμφανίζονται κατά τακτά χρονικά διαστήματα στο διαδίκτυο.[122]

---

[120] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 209-211, Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 217-221

[121] Λ.Μήτρου, Προστασία Προσωπικών Δεδομένων, 2004, σελ. 465

[122] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, ό.π., σελ. 306-312, Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 223

2.4 Τα δικαιώματα του υποκειμένου

2.4.1 Δικαίωμα ενημέρωσης του υποκείμενου

Το δικαίωμα ενημέρωσης του υποκείμενου ορίζεται ρητά από το άρθρο 11 και αποτελεί μέρος των δικαιωμάτων αυτοπροστασίας του ατόμου. Πρόκειται για το ένα από τα τρία συστήματα προληπτικού ελέγχου που έχουν καταχωρηθεί από την νομοθεσία, (μαζί με το σύστημα προηγουμένης γνωστοποίησης στην Αρχή της συλλογής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και το σύστημα προηγουμένης αδείας της Αρχής για τη συλλογή και επεξεργασία δεδομένων προσωπικό χαρακτήρα.)[123] Συνδυαστικά με το δικαίωμα προσβάσεις στην επεξεργασία το υποκείμενο κατέχει τον πλήρη έλεγχο για τον αυτοκαθορισμό της πληροφοριακής μορφής του.

Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων για την μετέπειτα επεξεργασία. Ο χρόνος καθορίζεται κατά την συλλογή ώστε το άτομο να μπορεί να ασκήσει τα δικαιώματα του (αποδοχή ή άρνηση) πριν το στάδιο της επεξεργασίας τους. Η ενημέρωση περιλαμβάνει πληροφορίες για την φύση των δεδομένων, τον σκοπό χρήσης τους, τους αποδέκτες της επεξεργασίας, αλλά και το όνομα/επωνυμία του υπευθύνου επεξεργασίας, την διεύθυνση του και του εκπροσώπου του. Επιπλέον δικαίωμα ενημέρωσης έχει το υποκείμενο και πριν την ανακοίνωση των δεδομένων σε τρίτο. Η ενημέρωση πρέπει να είναι ρητή αλλά όχι απαραιτήτως έγγραφη.[124] Στην περίπτωση των μέσων κοινωνικής δικτύωσης που μελετάει η παρούσα εργασία η ενημέρωση γίνεται με ειδική, σαφή και ευδιάκριτη σήμανση στην αρχή της ιστοσελίδας κοινωνικής δικτύωσης[125] (οροί χρήσης).

Μοναδικές εξαιρέσεις του δικαιώματος ενημέρωσης του υποκειμένου είναι όταν συντρέχουν λόγοι εθνικής ασφάλειας και κίνδυνοι σοβαρών εγκλημάτων οπού και πάλι η Αρχή είναι αυτή που θα αίρει το δικαίωμα του με αντίστοιχη απόφαση της.[126]

2.4.2 Δικαίωμα πρόσβασης

Το δικαίωμα πρόσβασης μαζί με το προαναφερθέν δικαίωμα πληροφορήσεις συμβάλουν στην ενίσχυση του δικαιώματος του υποκείμενου για τον πλήρη έλεγχο των προσωπικών του δεδομένων, ενισχύοντας παράλληλα και την διαφάνεια. Από τις

---

[123] Μ. Σταθόπουλος, Η Χρήση Προσωπικών Δε Δομών Και Η Διαπάλη Μεταξύ Ελευθέριων Των Κατόχων Τους Και Ελευθέριων Των Υποκειμένων Τους, ΝοΒ 2000, σελ. 8

[124] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 224

[125] Γέροντας Απόστολος, Η προστασία του πολίτη από την ηλεκτρονική επεξεργασία προσωπικών δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 225

[126] Παναγιώτης Δ. Αρμαμέντος, Βασίλης Α. Σωτηρόπουλος, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005, σελ.315-330

παραγράφους 2-6 του αρθούν 12, προκύπτει το δικαίωμα του υποκείμενου να γνωρίζει αν τα προσωπικά του δεδομένα έχουν υποβληθεί σε επεξεργασία. Το άτομο μπορεί με την αντίστοιχη αίτηση στον υπεύθυνο επεξεργασίας να λάβει άμεσα γνώση των πληροφοριών που επεξεργάζονται. Οι πληροφορίες που λαμβάνει από τον υπεύθυνο επεξεργασίας είναι τα δεδομένα που επεξεργάζονται και την πηγή άντλησης τους, ώστε να μπορεί να ελέγχει παράλληλα και η νομιμότητα των πληροφοριών, ο σκοπός της επεξεργασίας, οι αποδέκτες, η εξέλιξη της επεξεργασίας από την προηγουμένη ενημέρωση του υποκείμενου, και τέλος τον τρόπο και τα κριτήρια που χρησιμοποιεί η αυτοματοποιημένη επεξεργασία.

Σε περίπτωση που το υποκείμενο θελήσει την διόρθωση ή διαγραφή δεδομένων θα πρέπει να υποβάλει το αντίστοιχο αίτημα. Αν η απόφαση της Αρχής τον δικαιώσει ο υπεύθυνος πρέπει άμεσα να προβεί μέσα σε δεκαπέντε (15) μέρες στη διόρθωση και στην κοινοποίηση του διορθωμένων δεδομένων στο υποκείμενο.[127]

Διαφορετικό χειρισμό αντιμετωπίζουν τα δεδομένα που αφορούν τον τομέα της υγείας. Λόγο της ιδιαίτερης φύσης τους έχει προβλεφθεί η ένταξη τους νομικά σε επιπρόσθετες εγγυήσεις για την θεμιτή επεξεργασία τους παρέχοντας τους την μεγαλύτερη δυνατή προστασία. Τα δεδομένα υγείας θεωρούνται ευαίσθητα προσωπικά δεδομένα και γι' αυτό το λόγο τα αρχεία που παρέχουν δεδομένα υγείας αναθέτετε η τήρησή τους από τον υπεύθυνο επεξεργασίας σε άτομο που δεσμεύεται από το ιατρικό απόρρητο. Σε αυτή την κατηγορία κατατάσσετε το Patient like me.

2.4.3 Το δικαίωμα αντίρρησης του υποκείμενου

Η ελεύθερη ανάπτυξη της προσωπικότητας προϋποθέτει την ελευθέρια αυτοδιαθέσεις ή μη των προσωπικών δεδομένων. Αυτό προϋποθέτει και την άρνηση επεξεργασίας προσωπικών δεδομένων (άρθρο 13), σε κάθε χρονική στιγμή της επεξεργασίας και όχι αποκλειστικά κατά την συλλογή τους, ασχέτως με τις βαθμίδες νομιμότητας που τηρεί ο υπεύθυνος επεξεργασίας. Η επέμβαση μπορεί να φέρει την μορφή διόρθωσης, προσωρινής χρήσης, δέσμευσης, μη μεταβίβασης ή ακόμα και διαγράφης. Ειδική κατηγορία αποτελούν οι προωθήσεις και διαφημίσεις πωλήσεων/υπηρεσιών εξ αποστάσεων. Εκεί ο χρήστης μπορεί να προβεί σε περιορισμό των στοιχειών που θα παραχωρήσει ή ακόμα και σε καθολική άρνηση της χρήσης τους.[128]

[127] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 225-226
[128] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 226

2.4.4 Δικαίωμα προσωρινής δικαστής προστασίας

Η προσωρινή δικαστική προστασία (άρθρο 14) υποβάλλεται σε περιπτώσεις οπού υπάρχει προσβολή των προσωπικών δεδομένων και μόνο. Στο άρθρο 15 παρ. 1 ορίζεται ότι τέτοιου είδους αποφάσεις αφορούν μόνο πτυχές της προσωπικότητας του ατόμου όπως εργασιακή απόδοση, διαγωγή, αξιοπιστία κα. Η δυνατότητα αυτή που παρέχεται στο υποκείμενο υπηρετεί την ιδέα ότι ο άνθρωπος είναι το κύριο κομμάτι της επεξεργασίας και τα πληροφοριακά συστήματα υπηρετούν τις ανάγκες του, δίνοντας έτσι ανθρωποκεντρικό χαρακτήρα στην επεξεργασίας προσωπικών δεδομένων.[129]

2.5 Παράβαση νομού

Στο άρθρο 22 προβλέπονται οι ποινικές κυρώσεις σε περίπτωση παράβαση του νομικού πλαισίου. Η εισαγωγή του νομού 22 ήταν αναγκαία καθώς σύμφωνα με την Ι.Ιγγλεζακη δεν επαρκούσαν για την επιβολή του νομού οι γενικές διατάξεις που ακολουθούνται στην ηλεκτρονική εγκληματικότητα.[130] Οι παραβάσεις διαχωρίζονται σε δύο κατηγορίες: α) για πράξεις και παραλήψεις για τις οποίες η Αρχή δεν έχει ακόμη αποφανθεί, και σε β) μη συμμόρφωση σε αποφάσεις της Αρχής.

Οι παραβάσεις συνοψίζονται στις παρακάτω μορφές:

- Παράληψή γνωστοποίησης.
- Διατήρηση αρχείων με ευαίσθητα προσωπικά δεδομένα χωρίς άδεια της Αρχής.
- Παράνομη διασύνδεση αρχείων.
- Παράνομη επέμβαση σε προσωπικά δεδομένα.
- Μη συμμόρφωση σε απόφαση της Αρχής.
- Μη συμμόρφωση σε δικαστική απόφαση προσωρινής προστασίας.

Οι παραπάνω παραβιάσεις φέρουν ποινές ανάλογες με το παράπτωμα. Ανάκληση αδείας, προειδοποίηση και καταστροφή των δεδομένων είναι μερικές από τις κυρώσεις. Σε πιο σοβαρές μορφές παραβάσεων παρατηρούμε τη πλήρη αποζημίωση λόγο περιουσιακής ζημίας και ηθικής βλάβης αλλά ακόμα και την στέρηση της ελευθέριας του υπευθύνου (άρθρα 21-22-23, Ν.2472/1997).[131] Ως υπεύθυνος θεωρείτε ο υπεύθυνος επεξεργασίας ή ο εκπρόσωπος του αν πρόκειται για νομικό πρόσωπο. Ως επιβαρυντικός παράγοντας στο πόρισμα είναι η απόκτηση παράνομου οικονομικού οφέλους από τις παραπάνω άνομες ενεργείς, η βλάβη τρίτου προσώπου, και ο κίνδυνος για την εθνική ασφάλεια.

---

[129] Λ.Μήτρου, προστασία προσωπικών δεδομένων, 2004, σελ. 487
[130] Ι.Ιγγλεζάκης, Ευαίσθητα Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα 2003, σελ. 276
[131] Θεόδωρος Σιδηρόπουλος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003, σελ. 211

2.6 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης λαμβάνοντας υπόψη το άρθρο 100 Α για την συνθήκη της ίδρυσης της Ευρωπαϊκής Ένωσης, και την γνώμη της οικονομικής και κοινωνικής επιτροπής προέβει στην έκδοση της Οδηγίας 95/46/ΕΚ. Σύμφωνα με αυτή εξασφαλίζεται στα κράτη μέλη η προστασία των θεμελιωδών ελευθέριων και δικαιωμάτων των φυσικών προσώπων από την επεξεργασία των προσωπικών τους δεδομένων. Στόχος της ήταν η θέσπιση μέτρων για την ασφάλεια και την προστασία των δικαιωμάτων και των ελευθέριων των πολίτων. Για την επίτευξη του στόχου εισήχθησαν μέτρα ενισχυμένης προστασίας για την πρόσβαση τρίτων, παραβίαση απορρήτου, αλλοίωση δεδομένων,[132] χωρίς όμως να εμποδίζεται η μεταφορά των δεδομένων στα υπόλοιπα κράτη μέλη. (άρθρο 1)

Η ιδέα της Ευρωπαϊκής Ένωσης στηρίχθηκε στην ελεύθερη διακίνηση προϊόντων, προσώπων, πληροφοριών. Η ανάγκη όμως που προέκυψε για την προστασία των προσωπικών δεδομένων οδήγησε στην δημιουργία αυστηρών νόμων. Η παρούσα Οδηγία επανάφερε την ισορροπία στην προστασία των χρηστών. Τα προσωπικά δεδομένα μπήκαν σε περιβάλλον προστασίας χωρίς να δημιουργείται πρόβλημα στην μετάδοση τους εντός Ευρωπαϊκής Ένωσης.[133] (συμβούλιο της Ευρώπης 2014 οργανισμός θεμελιωδών δικαιωμάτων της ευρωπαϊκής ένωσης εγχειρίδιο ευρωπαϊκής νομοθεσίας για την προστασία προσωπικών δεδομένων). Πεδίο εφαρμογής ορίζεται το σύνολο των αυτοματοποιημένων ή μη επεξεργασιών προσωπικών δεδομένων με σκοπό την καταχώρηση σε αρχεία (άρθρο 3, παρ. 1). Εξαίρεση αποτελούν οι οικιακές ή προσωπικές δραστηριότητες καθώς και δραστηριότητες που εκπίπτουν στο κοινοτικό δίκαιο όπως η δημόσια ασφάλεια, η εθνική άμυνα, το ποινικό δίκαιο και η ασφάλεια του κράτους (Άρθρο 3 παρ.2).

[132] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών, εκδόσεις Σάκκουλα, 2006, σελ. 39

[133] Συμβούλιο της Ευρώπης 2014, Εγχειρίδιο Ευρωπαϊκής Νομοθεσίας Για Την Προστασία Προσωπικών Δεδομένων, http://www.adae.gr/fileadmin/docs/Handbook_data_protection_ELL.pdf, 25/10/2016

Κατά το δεύτερο κεφάλαιο της ευρωπαϊκής Οδηγίας 95/46/ΕΚ αναφέρονται όλες οι προϋπόθεσης σχετικά με την θεμιτή επεξεργασία προσωπικών δεδομένων. Οι Αρχές είναι οι εξής:[134]

I. Αρχές ως προς την ποιότητα των δεδομένων: (άρθρο 6 παρ. 1)

Οι αρχές ποιότητας των προσωπικών δεδομένων που πρέπει να τηρούνται αποτυπώνονται με σαφήνεια στην Οδηγία. Τα στοιχεία πρέπει να είναι σαφή, και να συλλέγονται για καθορισμένους, σαφής και νόμιμους σκοπούς. Επιπλέον ο όγκος τους δεν πρέπει να ξεπερνάει το απαραίτητο πλήθος των στοιχείων. Σε περίπτωση που υπάρχουν ανακριβή η ελλιπή δεδομένα προς τους σκοπούς συλλογής τους, θα πρέπει να καταστρέφονται. Η παραμονή προσωπικών δεδομένων σε αρχεία για περίοδο μεγαλύτερη της θεμιτής απαγορεύεται ρητά με ορισμένες εξαιρέσει όπως οι ιστορικοί σκοποί, οι στατιστικοί λόγοι και ο επιστημονικός χαρακτήρας των αρχείων. Σε αύτη την περίπτωση όλα τα κράτη μέλη προβάλλουν τις κατάλληλες εγγυήσεις. (άρθρο 6 παρ. 1)

II. Αρχές της νόμιμης επεξεργασίας δεδομένων: (άρθρο 7)

Η έγκριση – συναίνεση του ατόμου που θα συλλέγουν τα προσωπικά του δεδομένα είναι βασική προϋπόθεση για την συνέχεια της διαδικασίας συλλογής και επεξεργασίας. Εξαιρέσεις αποτελούν περιπτώσεις στις οποίες η επεξεργασία κρίνεται απαραίτητη . Αυτές είναι:

- Η εκτέλεση συμβάσης της οποίας το υποκείμενο αποτελεί συμβαλλόμενο μέρος
- Η τήρηση της νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος εργασίας
- Η διαφύλαξη ζωτικού συμφέροντος του υποκείμενου
- Η εκτέλεση αποστολής δημοσίου συμφέροντος
- Η υλοποίηση θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο επεξεργασίας

III. Ειδικές κατηγορίες δεδομένων (άρθρο 8)

Στις ειδικές κατηγορίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα απαγορεύεται η αποκάλυψη και επεξεργασία οποιασδήποτε πληροφορίας που αφορά την φυλετική καταγωγή, της δημόσιες απόψεις, της φιλοσοφικές ή θρησκευτικές πεποιθήσεις, το συνδικαλισμό του ατόμου, την υγειά και την ερωτική του ζωή. Εξαιρέσεις αποτελούν περιπτώσεις που αφορούν την υπεράσπιση των ζωτικών συμφερόντων και ιατρικούς λογούς.

IV. Αρχές ενημέρωσης του ενδιαφερομένου προσώπου (άρθρο 10)

[134] http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC, 25/10/2016

Το υποκείμενο της ερευνάς είναι σε θέση να γνωρίζει ορισμένες βασικές πληροφορίες σχετικές με την έρευνα όπως την ταυτότητα του υπευθύνου επεξεργασίας , τον σκοπό της ερευνάς, και τους παραλήπτες της. Αρμόδιος για την πληροφόρηση του υποκείμενου είναι ο υπεύθυνος επεξεργασίας.

V. Δικαίωμα πρόσβασης του προσώπου στα δεδομένα (άρθρο 12)

Κάθε υποκείμενο έχει το δικαίωμα να ζητήσει από τον υπευθύνου επεξεργασίας την βεβαίωση χρήσης ή μη των δεδομένων του καθώς και το κοινό κοινοποίησης τους. Επιπλέον την διόρθωση την διαγραφή και τροποποίηση δεδομένων, στα οποία δεν επιθυμεί δημοσίευση ή έχουν ανακριβή χαρακτήρα.

VI. Εξαιρέσεις και περιορισμοί (άρθρο 13)

Τα κράτη μέλη είναι σε θέση να περιορίσουν την ασφάλεια και το απόρρητο των προσωπικών δεδομένων του υποκείμενου σε περίπτωση που απαιτείται για την διαφύλαξη της ασφάλειας του κράτους, της άμυνας, της δημοσίας ασφάλειας ,του ποινικού νομού σημαντικού οικονομικού συμφέροντος του κράτους ή της ευρωπαϊκής ένωσης, ασκήσεως δημοσίας εξουσίας ή λόγο προστασίας του προσώπου που αυτά υπόκεινται (παράγραφος 1).

VII. Δικαίωμα αντίρρησης προσώπου που αναφέρονται τα δεδομένα (άρθρο 14)

Το υποκείμενο θα πρέπει να έχει το δικαίωμα να αρνηθεί την επεξεργασία των προσωπικών του δεδομένων καθώς και να ενημερώνεται πριν την κοινοποίηση στοιχείων αλλά και να έχει το δικαίωμα αντίρρησης σε αυτή την κοινοποίηση.

VIII. Το απόρρητο και την ασφάλεια της επεξεργασίας (άρθρο 16)

Κάθε άτομο που έχει πρόσβαση σε προσωπικά στοιχεία απαγορεύεται ρητά να κάνει χρήση τους αν δεν λάβει σαφή εντολή από τον υπεύθυνο επεξεργασίας. Ο τελευταίος είναι υπεύθυνος για να ληφθούν όλα τα απαραίτητα μέτρα ώστε να εμποδίσει τέτοιου ιδίους ενέργειες.

IX. Κοινοποίηση (άρθρο 18-21)

Κάθε εκτέλεση επεξεργασίας δεδομένων προϋποθέτει την κοινοποίηση της από τον υπεύθυνο επεξεργασίας της αρμόδιας ελεγκτικής Αρχής. Η Αρχή θα πρέπει να εξετάσει τους ενδεχομένους κινδύνους δικαιωμάτων και ελευθέριων. Τα αποτελέσματα δημοσιεύονται και η ελεγκτική Αρχή τηρεί μητρώο των κοινοποιημένων αποτελεσμάτων επεξεργασίας.

Στο τρίτο κεφάλαιο της Οδηγίας προβλέπεται η καθολική δυνατότητα των προσώπων για νομική προσφυγή σε περίπτωση που παραβιαστούν οι εθνικές διατάξεις περί προσωπικών δεδομένων καθώς η ζήτηση αποκατάστασης της ζημίας που υπέστησαν

(άρθρο 22). Η μεταβίβαση δεδομένων σε τρίτες χώρες επιτρέπεται υπό την προϋπόθεση ότι αυτές διαθέσουν το κατάλληλο επίπεδο προστασίας. Σε αντίθετη περίπτωση οι μεταβιβάσει δεν πραγματοποιούνται εκτός από ορισμένες εξαιρέσεις οι οποίες απαριθμούνται περιοριστικά. Η Οδηγία 95/46/ΕΚ εφαρμόζεται σε όλα τα ευρωπαϊκά κράτη υπ' ευθύνη ανεξάρτητων κρατικών αρχών. (άρθρο 25)[135]

Στη παρούσα Οδηγία αναφέρεται και η δημιουργία ομάδας προστασίας των προσώπων από την επεξεργασία προσωπικών δεδομένων στην οποία λαμβάνουν μέρος εκπρόσωποι εκλεκτικών αρχών των κοινωνικών θεσμικών οργάνων κι οργανισμών, εκπρόσωποι των εθνικών αρχών ελέγχου, και ένας εκπρόσωπος της Επιτροπής (άρθρο 29).

Η νομοθεσία για την προστασία της πνευματικής ιδιοκτησίας εξελίσσεται συνεχώς για να καλύψει όλες τις πτυχές της ηλεκτρονικής πραγματικότητας αλλά για να είναι απολύτως αποτελεσματική απαιτείται συνεργασία τεχνικών και χρηστών, και ολοένα πιο ανεπτυγμένα μετρά ελέγχου και προστασίας. Λόγο της ραγδαίας τεχνολογικής εξέλιξης κρίνεται απαραίτητη η συνεχής ανανέωση της νομοθεσίας και η εφαρμογή νέων μέσων προστασίας των χρηστών.[136]

2.6.1 Η περίπτωση της Αγγλίας στην εφαρμογή της Οδηγίας 95/46

Με άφορη την υπόθεση Durant το αγγλικό δικαστήριο και η Αγγλική Αρχή Προστασίας Προσωπικών Δεδομένων αναγκαστήκαν να ορίσουν αυστηρώς και να εφαρμόσουν την Οδηγία 95/46. Σύμφωνα με την θεωρία τους και τον τρόπο που πέρασε η Οδηγία στην Αγγλική νομοθεσία για να υπάρξουν προσωπικά δεδομένα σε κάποιο έγγραφο δεν αρκεί απλά η αναφορά του ονόματος του υποκείμενου αλλά θα πρέπει να φέρει σοβαρό αντίκτυπο στην προσωπική, επαγγελματική, ή οικογενειακή ζωή του ατόμου, πως επίσης να αναφέρεται ως κύριο πρόσωπο του εγγράφου και όχι απλός ως τρίτο- επικαλούμενο μέλος, με πληροφορίες που να οδηγούν απευθείας στην αναγνώριση του υποκείμενου. Επιπλέον στην απόφαση τονίστηκε ότι η προστασία προσωπικών δεδομένων αφορά μόνο τις πληροφορίες του ατόμου και όχι ολόκληρο το έγγραφο που αυτές εμπεριέχονται. Σε περίπτωση αμφιβολιών περί προσωπικών ή μη δεδομένων το δικαστήριο όρισε ως προσωπικά δεδομένα μόνο τα δεδομένα που επηρεάζουν δυσμενώς το υποκείμενο που τα φέρει.

---

[135] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr/portal/page?_pageid=33,123482&_dad=portal, 25/10/2016

[136] Ελληνική Εταιρία Επιστημόνων Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995, σελ. 320

Τέλος, θα πρέπει να τονίσουμε ότι η χρήση της λέξης «έγγραφο» δεν είναι τυχαία καθώς σύμφωνα με τον αγγλικό νομό ένα μη αυτοματοποιημένο σύνολο εγγράφων πρέπει να παρουσιάζει δομή αντίστοιχη με της αυτοματοποιημένης οργάνωσης για να θεωρηθεί ως αρχείο.[137]

2.6.2 Η περίπτωση της εφαρμογής της Οδηγίας 95/46 στην επεξεργασία ευαίσθητων προσωπικών δεδομένων υγείας στην ιρλανδικά

Το 2003 η Ανεξάρτητη Ιρλανδική Αρχή ήρθε αντιμέτωπη με την περίπτωση συλλογής και κοινοποίησης προσωπικών δεδομένων ασθενών μέσα από το σύλλογο μαιευτήρων γυναικολόγων, από το τοπικό συμβούλιο υγείας στα πλαίσια εξακρίβωσης της χρήσης ή μη επικινδύνων μέθοδο από μαιευτήρες- γυναικολόγους. Η απόφαση βγήκε υπέρ του υπευθύνου επεξεργασίας αφού τέθηκε θέμα ερευνάς εγκλημάτων και μετέπειτα αποφυγής τους (άρθρο 8 περ.b και d του Ιρλανδικού νομό περί προστασίας δεδομένων).

Μια άλλη περίπτωση προσωπικών δεδομένων υγείας έλαβε χωρά το 2002 οπού ένας ιατρός κατέφυγε στην Ιρλανδική ανεξάρτητη Αρχή έπειτα από έτυμα την Διεύθυνσης Δημοσίας Υγείας της Ιρλανδίας για παράδοση προσωπικών στοιχείων πελατών που λάμβαναν αγωγή για μια μεταδοτική ασθένεια των πνευμόνων. Ο λόγος σύμφωνα με την Διεύθυνση Δημοσίας Υγείας ήταν η υπεράσπιση του δημοσίου συμφέρον τους. Το πόρισμα ήταν απαγορευτικό με την επεξήγηση πως η δημοσιοποίηση δεδομένων υγειά επιτρέπετε μόνο από τους ιατρούς, ως εξαίρεση του κανονισμού με την προϋπόθεση ότι τα δεδομένα βρίσκονται στο αρχείο τους και έχει προηγηθεί δικαστική απόφαση.[138]

2.7 Νόμιμη παρακολούθηση επικοινωνιών

Από την Ευρωπαϊκή Σύμβαση περί προστασίας των δικαιωμάτων του ανθρώπου και των θεμελιωδών ελευθέριων του, και κάτ. επέκταση από τα Συντάγματα των κρατών-μελών προκύπτουν οι βασικές εγγυήσεις της εμπιστευτικότητας και του απορρήτου των επικοινωνιών. Εξαιρέσεις αποτελούν οι παρεμβάσεις που στοχεύουν στην διατήρηση της νομιμότητας. Οι παρεμβάσεις αυτές ισοσταθμίζονται με το δικαίωμα του υποκείμενου για ιδιωτικότητα και γίνονται με πλήρη εχεμύθεια και πάντα σύμφωνα με το κοινοτικό δίκαιο. Ανάλογα με τον βαθμό της παράβασης ως αρχική πρόθεση της ενημέρωσης του

[137] Γεώργιος Ντούσαλης, Ποινική Προστασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2005, σελ.126-129
[138] Γεώργιος Ντούσαλης, ό.π., σελ. 136-137

υποκείμενου. Σε περιπτώσεις ωστόσο που αυτό μπορεί να βλάψει την πορεία των ερευνών δεν πραγματοποιείτε.

Η άρση του απορρήτου προσδιορίζετε από την μορφή που θα λάβει χωρά πχ. τηλεφωνική άρση απορρήτου, επικοινωνία δεδομένων μέσω δικτύου δεδομένων, ασύρματες επικοινωνίες, δορυφορικές επικοινωνείς , επικοινωνία μέσω μισθωμένων κυκλωμάτων, υπηρεσίες επιπρόσθετης αξίας, καθώς και τα στοιχεία στα οποία αναφέρονται οι διατάξει καθορίζονται από το είδος της επικοινωνίας που αφορούν.

Επιπροσθέτως η ανάπτυξη νέων τεχνολογιών και μέσων αποτελεί συνεχώς καινούριες προκλήσεις για την εύρεση νέων μέσων ελέγχου και καταστολής που δεν θα βάλουν τα υποκείμενα της επικοινωνίας. Νέες κανονιστικές τεχνικές και νομοθετικές διατάξεις απαιτούνται, ιδιαιτέρως πάνω στο κομμάτι της αυτόματης επεξεργασίας δεδομένων. Δίνεται λοιπόν ιδιαίτερη έμφαση στην πρόληψη των κρουσμάτων όχι μόνο για την διαφύλαξη των χρηστών αλλά και της αξιοπιστίας των ηλεκτρονικών επικοινωνών χωρίς να δημιουργούνται εμπόδια και ανασταλτικοί παράγοντες στην χρήση τους.[139]

Σύμφωνα με το άρθρο 8 της ΕΣΔΑ κάθε προσπάθεια παρακολούθησης θεωρείτε παράνομη ακόμα και αν πραγματοποιείται από δημοσιές αρχές. Για την ένταξη της παρακολούθησης στο πλαίσιο της νομιμότητας πρέπει να αφορά την προστασία της δημοσίας ασφάλεια/ ασφάλεια του κράτους, της εθνικής άμυνας, να υπόκεινται στο ποινικό δίκαιο, να αφορά τρομοκρατικών ενεργειών, και τέλος για την προστασία των υποκείμενων.

Για την επίτευξη του αποτελεσματικότερου σχεδίου τα κράτη μέλη συνεργάζονται σύμφωνα με το Συμβούλιο της Ευρωπαϊκής Ένωσης με απόφαση του συμβουλίου 2003/481/ΔΕΥ της 19ης Δεκέμβριου 2002, σχετικά με την εφαρμογή ειδικών μέτρων αστυνομικής και δικαστικής συνεργασίας για την καταπολέμηση της τρομοκρατίας (σύμφωνα με το άρθρο 4 της κοινωνικής θέσης 2001/931/ΚΕΠΠΑ, στην Επίσημη Εφημερίδα σελ. 68-70), για την εγκατάσταση τεχνολογικών μέσων που θα παρέχουν τις απαραίτητες εγγυήσεις για την ελαχιστοποίηση επεξεργασίας των προσωπικών δεδομένων.[140]

---

[139] Οδηγία 97/66/ΕΕ Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου , Της 15ης Δεκέμβριου 1997 περί Επεξεργασίας Των Δεδομένων Προσωπικού Χαρακτήρα Και Της Προστασίας Της Ιδιωτικής Ζωής Στον Τηλεπικοινωνιακό Τομές, Επίσημη Εφημερίδα, 30/01/1998, σελ. 1-8, Απόστολος Γέροντας, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002, σελ. 309-327

[140] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών, εκδόσεις Σάκκουλα, 2006, σελ. 45-60

2.8 Δράσεις και προοπτικές διατήρησης δεδομένων κίνησης

Η παροχή διαδικτυακών υπηρεσιών πολλές φορές συνάδει με την διατήρηση δεδομένων προσωπικού χαρακτήρα των χρηστών. Η Οδηγία 2002/58/ΕΚ[141] θέτει κανόνες στους υπεύθυνους επεξεργασίας για τα δεδομένα κίνησης και θέσης των χρηστών τα οποία πρέπει να διαγραφούν ή να διατηρηθούν ανώνυμα σε περίπτωση που δεν είναι απαραίτητα για τον σκοπό της επεξεργασίας. Επιπλέον η έκταση και η διάρκεια της επεξεργασίας πρέπει να περιορίζεται στον μικρότερο δυνατό βαθμό πάντα με την συγκατάθεση του υποκείμενου. Η ενημέρωση του υποκείμενου έγγυται στον σκοπό, την διάρκεια , τον τύπο των συλλεχθεντων δεδομένων καθώς και στην πιθανότητα μετάδοσης της επεξεργασίας. Το υποκείμενο έχει καθολικό και διαχρονικό δικαίωμα ανάκλησης. Όλα τα παραπάνω αποτελούν κομμάτια των νομοθεσιών όλων των κρατών μελών που έχουν ως σκοπό την πρόληψη, τον εντοπισμό και την ποινική δίωξη των παραβάσεων. [142]

Για την γεφύρωση των διαφορών που υπάρχουν αναμεσά στις αντίστοιχες διατάξεις και την προώθηση μιας κοινής πολιτικής θεσπίσθηκε η Οδηγία 2006/24/ΕΚ[143] περί «διατήρησης δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών», η οποία αφορά μόνο δεδομένα που καταχωρήθηκαν έπειτα από παροχή υπηρεσίας και όχι μέσα από την κοινοποίηση του ιδίου του υποκειμένου, εξειδικεύοντας έτσι ακόμα περισσότερο τις επιμέρους περιπτώσεις. Παρατηρούμε λοιπόν πως σε συνδυασμό με την Οδηγία 2002/58/ΕΚ δημιουργείτε ένα ισχυρό υπόβαθρο που προστατεύει το υποκείμενο κρατώντας διασφαλισμένα τα προσωπικά του δεδομένα σε κάθε μορφή χρήσης τους εντός του διαδικτύου.

2.9 Δράσεις και πολιτικές για την προστασία της ασφάλεια και του απορρήτου στο σύγχρονο Ευρωπαϊκό περιβάλλον

Η ενσωμάτωση των νέων τεχνολογιών και η πλήρη ένταξη τους στην καθημερινότητα των πολίτων αποτελεί το όραμα της «Ηλεκτρονικής Ευρώπης» που

---

[141] Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr/portal/page?_pageid=33,123482&_dad=portal&_schema=PORTAL, 26/10/2016

[142] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών, εκδόσεις Σάκκουλα, 2006, σελ. 63-71

[143] Οδηγία 2006/24/ΕΚ Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου Της 15ης Μάρτιου 2006 , Για Τη Διατήρηση Δεδομένων Που Παράγονται Ή Υποβάλλονται Σε Επεξεργασία Σε Συνάρτηση Με Την Παροχή Διαθεσίμων Στο Κοινό Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Ή Δημοσίων Δικτύων Επικοινωνιών Και Για Την Τροποποίηση Της Οδηγίας 2002/58/ΕΚ, Επίσημη Εφημερίδα, 13/04/2006, σελ. 54-63

εισάχθηκε από ανακοίνωση της ευρωπαϊκής επιτροπής.[144] Το όραμα της «Κοινωνίας των Πληροφοριών» ωστόσο προϋποθέτει την απολυτή ασφάλεια εντός του διαδικτύου με την καθολική καταπολέμηση των παράνομων δράσεων.

Οι απαιτήσεις της ασφάλειας δεν περιορίζονται μόνο σε τοπικό επίπεδο. Η ανάγκη μιας καθολικής πολιτικής είναι επιτακτική αλλά όχι εύκολη. Οι διαφορετικές νομοθεσίες και ιδιαιτερότητες της κάθε χώρας δεν αποτελούν πρόσφορο έδαφος. Ως εκ τούτου οι Οδηγίες της Ευρωπαϊκής Ενώσεις αφήνουν την δυνατότητα στα επιμέρους μέλη κράτη να προσαρμόσουν στα τοπικές απαιτήσεις χωρίς όμως να δέχονται καμία αλλοίωση ή «έκπτωση» στην ασφάλεια, καθώς κάτι τέτοιο θα έβλαπτε ολόκληρη την Ευρώπη και την ηλεκτρονική της αξιοπιστία. Τα μετρά προλήψεις είναι απαραίτητα. Σκοπός είναι η απαίτηση για κατασταλτικά μετρά να τεθεί σε δεύτερο επίπεδο καθώς αυτά σηματοδοτούν την εκ τον υστέρων αντίληψη του προβλήματος ενώ η ασφάλεια, και η προστασία της ιδιωτικότητας έχει ήδη καταπατηθεί. Η μονή λύση είναι η συνεργασία αναμεσά στα κράτη μέλη μέσα από αμοιβαία κατανόηση και διαδραστίκη δράση με σκοπό την διασφάλιση υψηλού επίπεδου προστασίας των χρηστών και της ακεραιότητας των δικτύων.

Στην Ελλάδα ο Ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών και άλλες διατάξεις, (ΦΕΚ 13, 03/02/1996, άρθρο 3) καθόρισε το πλαίσιο της διασφάλισης της ακεραιότητας και της ασφάλειας των δημόσιων δικτύων επικοινωνιών. Σε αυτό βασίζεται και η Αρχή διασφάλισης του απορρήτου των επικοινωνιών που εισήχθη με τον Ν. 3115/2003.

Επιπροσθέτως η επέμβαση στα προσωπικά δεδομένα αλλού ατόμου, η υποκλοπή και η παρακολούθηση τους συνιστά σοβαρό αδίκημα για τις ευρωπαϊκές αρχές και αποτελεί εκ διαμέτρου αντίθετη πράξη με τον σκοπό της «κοινωνίας των πολίτων» που αναφέρεται στον σεβασμό των δικαιωμάτων και την κάθετη προστασία του απορρήτου και των προσωπικών δεδομένων. Μέσα από τις διατάξεις των Ευρωπαϊκών Οδηγιών όλα τα κράτη μέλη της ευρωπαϊκής ένωσης έχουν δεσμευτεί να ελέγχουν του υπευθύνους επεξεργασίας ότι το υποκείμενο έλαβε γνώση της επικείμενης επεξεργασίας.[145]

Στην Οδηγία 2002/58/ΕΚ περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, γίνεται λόγος για ένα φορέα παροχής υπηρεσιών ηλεκτρονικής επικοινωνίας ο οποίος εγγυάται την ασφάλεια των πληροφοριών των χρηστών, την

[144] "eEurope 2005: κοινωνία της πληροφορίας για όλους -Σχέδιο δράσης που υποβάλλεται ενόψει του ευρωπαϊκού συμβουλίου της Σεβίλλης, 21/22 Ιουνίου 2002»

[145] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών, εκδόσεις Σάκκουλα, 2006, σελ. 25-38

ιδιωτικότητα της επικοινωνίας, καθώς και την κάθε μορφή δεδομένων που μπορούν να υποστούν επεξεργασία («δεδομένα κίνησης»). Αυτό επιτεύχθηκε με σύγχρονα τεχνητά και οργανωτικά μετρά διασφαλίζοντας την ασφάλεια για κάθε είδος δικτύου, ιδιαιτέρως σε διαδικτυακές και κινητές συσκευές. Επιπλέον προβλέφθηκε η ένταξη των δεδομένων θέσης και των cookies στο απόρρητο. Το 2009 υπήρξε τροποποίηση της Οδηγίας μέσα από την Οδηγία 2009/136/ΕΚ με εκτενή αναφορά στην καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και την συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των υποκειμένων.

Στις 03/05/2000 στην επίσημη εφημερίδα του Συμβουλίου της Ευρωπαϊκής Ένωσης συμπεριλήφθηκε το κείμενο περί: «πρόληψης και ελέγχου του οργανωμένου εγκλήματος: στρατηγική της Ευρωπαϊκής Ένωσης για την αρχή της νέας χιλιετίας» όπου αναφερόταν εκτενέστατα στην ανάγκη ύπαρξης ρυθμίσεων και δια κανονιστικών μέτρων σε πανευρωπαϊκό επίπεδο. Επιπλέον ο ενιαίος και συντονισμένος κατασταλτικός μηχανισμός σε στενή συνεργασία των αρμοδίων δικαστών και αστυνομικών υπηρεσιών θα επέφεραν άμεσα κατασταλτικά αποτελέσματα.

Στην Ελλάδα η Αρχή διασφάλισης του απορρήτου των επικοινωνιών έχει προβεί στον καθορισμό μια σειράς κανονισμών οι οποίοι ανάλογα με το είδος της υπηρεσία και την κατάλληλη πολιτική διασφαλίζουν την ιδιωτικότητα του υποκειμένου.[146]

Επιπλέον το 2016 θεσπίστηκε η Οδηγία 2016/680 περί προστασίας των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης, δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων, καθώς και η Οδηγία 2016/681[147] αναφορικά με τη χρήση των δεδομένων για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων.

[146] Ιωάννης Π. Χοχλιούρος, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών και Εφαρμογών, εκδόσεις Σάκκουλα, 2006, σελ. 38-43

[147] Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PROSOPIKA%20DEDOMENA/FILES/CELEX_32016L0681_EL_TXT.PDF

2.10 Κανονισμός (ΕΕ) 2016/679 Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Στις 4 Μαΐου του 2016 δημοσιεύτηκε στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης ο Κανονισμός 2016/679 ο οποίος αντικαθιστά το μέχρι πρότινος γενικό κανονισμό για την προστασία δεδομένων. Τρεις σημαντικές νομοθετικές ρυθμίσεις οριοθετούν θέματα που αφορούν την προστασία της ιδιωτικής ζωής, των προσωπικών δεδομένων, και την ελεύθερη κυκλοφορία αυτών. Σκοπός του, είναι η προστασία των υποκειμένων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία τους. Οι ρυθμίσεις αναμένεται να ενδυναμώσουν τα δικαιώματα των πολίτων προς την προστασία των προσωπικών τους δεδομένων και να εξομαλύνουν τις νομοθετικές διαφοροποιήσεις που υπήρχαν στα κράτη- μέλη στην εφαρμογή της μέχρι πρότινος γενικής Οδηγίας 95/46/ΕΚ. Ο Κανονισμός περιλαμβάνει λεπτομερή ρύθμιση του δημοσίου και ιδιωτικού τομέα σχετικά με τα δεδομένα, καθώς και ρύθμιση όλων των μορφών των δεδομένων των υποκειμένων (απλά ή ευαίσθητα). Ο εν λόγω κανονισμός τέθηκε σε ισχύ στις 24 Μάιου 2016, η εφαρμογή του όμως θα λάβει χώρα τον Μάϊο του 2018 μέσα από την εναρμόνιση των εγχώριων νόμων.

Πεδίο εφαρμογής ορίζεται η αυτοματοποιημένη ή μη επεξεργασία προσωπικών δεδομένων τα οποία υπόκεινται σε σύστημα αρχειοθέτησης. Εξαιρέσεις αποτελούν η προσωπική χρήση του υποκείμενου δεδομένων προσωπικού χαρακτήρα, τα δεδομένα που δεν υπόκεινται στο Ευρωπαϊκό δίκαιο και τα δεδομένα τα οποία αφορούν την πρόληψη και διερεύνηση εγκληματικών ή ποινικών ενεργειών.

Σημαντική προσθήκη του Κανονισμού 679/2016 αποτελεί η ρύθμιση για τα παιδιά-χρήστες (άρθρο 8). Στον κανονισμό προβλέπεται η παροχή πληροφοριών υπό την προϋπόθεση ότι το παιδί έχει ολοκληρώσει τα 16 έτη ζωής. Σε περίπτωση που οι γονείς συναινέσουν, χρήση μπορεί να γίνει και από μικρότερες ηλικίες με την προϋπόθεση πως δεν είναι κάτω από 13 ετών. Για να διασφαλιστεί ο υπεύθυνος επεξεργασίας πρέπει να προβεί στις κατάλληλες ενέργειες για την διερεύνηση του θέματος με όλα τα τεχνολογικά μέσα που κατέχει.

Επιπλέον πρέπει να επισημανθεί πως σύμφωνα με το άρθρο 96, τρίτες χώρες και οργανισμοί για τις οποίες υπήρχε ελεύθερη ροή δεδομένων πριν τις 24 Μάιου του 2016 εξακολουθούν να διατηρούν τα δικαιώματα τους.

Συμπερασματικά μπορούμε να πούμε πως ο Κανονισμός 679/2016 δημιουργήθηκε με στόχο να καλύψει τα κενά της Οδηγίας 95/46/ΕΚ και να δημιουργήσει ένα ενιαίο κανονιστικό πλαίσιο στην Ευρωπαϊκή Ένωση, χωρίς να δίνει το δικαίωμα όπως η πρότερη γενική Οδηγία για επιμέρους τροποποιήσεις. Με αυτόν τον τρόπο εξαλείφονται όλα τα περιθώρια παρερμηνείας των επιμέρους χωρών. Ενώ ο Κανονισμός 2016/679 παρουσιάζει πολλές ομοιότητες με την Οδηγία 95/46/ΕΚ, προστέθηκαν ορισμένα άρθρα (πχ. το άρθρο 8), τα οποία συμβαδίζουν με την εποχή της πληροφορίας και προστατεύουν τους χρήστες τονίζοντας έτσι το αίσθημα της ασφάλεια στο διαδίκτυο. Το μόνο που απομένει είναι να δούμε πως ο Κανονισμός θα ερμηνευθεί και θα εφαρμοστεί από τα κράτη- μέλη της Ευρωπαϊκής Ένωσης.[148]

2.11 Συμπεράσματα και παρατηρήσεις

Συνοψίζοντας παρατηρούμε την έντονη προσπάθεια της Ελληνικής Αρχής για εξειδίκευση και επίλυση των προβλημάτων που προέκυψαν από την εφαρμογή του Ν.2472/1997. Η βάση του νόμου στηρίχθηκε στην αποφυγή της ενεξέλεκτης επεξεργασίας προσωπικών δεδομένων θεσπίζοντας τα δικαιώματα και τις υποχρεώσεις των υπευθύνων επεξεργασίας, των υποκείμενων αλλά και των τρίτων. Μέσα από τον ορισμό μια σειράς κανόνων αλλά και εξαιρέσεων το υποκείμενο μπορεί να λάβει γνώση των δικαιωμάτων του σεβόμενος τον πληροφοριακό αυτοκαθορισμού και το δικαίωμα στην ιδιωτικότητας.

Παρ'όλα αυτά παρατηρείται μια σημαντική ασάφεια στο Ν.2472/1997. Ενώ βασική έννοια που διατρέχει όλο τον νομό και αποτελεί την βάση του είναι η έννοια του «αρχείου», δεν υπάρχει σαφής οριοθέτηση του. Η Αρχή θα πρέπει να αποσαφηνίσει τον όρο βάσει αυστηρά καθορισμένων κριτήριων τα οποία δεν θα αφήνουν το περιθώριο στις επιμέρους αρχές για παραποίηση του. Το βάρος της σημαντικότητας της αποσαφήνισης προέρχεται από το γεγονός ότι η έννοια του αρχείου αποτελεί τον βασικό λίθο εισαγωγής του υποκείμενου στον εν λόγω νόμο.[149]

[148] EUR-Lex, Access to European Union law, http://eur-lex.europa.eu/legal-content/EL/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ELL, 26/10/2016

[149] Γεώργιος Ντούσαλης, Ποινική Προστασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2005, σελ. 143

Επιπλέον παρατηρείται η ετοιμότητα και η αμεσότητα εφαρμογής της Οδηγίας 95/46 της Ε.Ε. Η αντιμετώπιση των προβλημάτων που προέκυψαν από την παραπάνω Οδηγία ήταν άμεση. Αυτό οφείλεται και στο ήδη υπάρχον νομικό πλαίσιο για την προφύλαξη των προσωπικών δεδομένων των χωρών της Ε.Ε., με βάση το οποίο προσπαθεί να ερμηνευτεί η Οδηγία.

Επιπρόσθετα αξίζει να επισημάνουμε ότι η Οδηγία 95/46 όσο και ο Ν. 2472/1997 εισήγαγαν στην Ελλάδα ένα πλήρες ρυθμιστικό πλαίσιο χωρίς αποσπασματικό χαρακτήρα, με κύριο στόχο την ουσιαστική και καθολική προστασία τον πολίτων από μια νέα μέχρι τότε μορφή κίνδυνου. Μέσα από αυτό ρυθμίστηκαν τα δικαιώματα- υποχρεώσεις του (υπευθύνου επεξεργασίας και τρίτων), προάγοντας την «κοινωνία της πληροφορίας» χωρίς την καταπάτηση ελευθέριων και θεμελιωδών ανθρωπίνων δικαιωμάτων.

Τέλος, από όλα τα παραπάνω γίνεται φανερό πως η ύπαρξη της κοινωνίας των πληροφοριών προϋποθέτει την κοινή χάραξη κανονισμού διασυνοριακών κανόνων. Αυτές στηρίζονται σε βασικές ελευθερίες και δικαιώματα των πολιτών. Η διαχείριση της ασφάλεια των ηλεκτρονικών δεδομένων είναι ένα δύσκολο εγχείρημα που απαιτεί πολύπλευρο έλεγχο και σεβασμό στην ιδιωτικότητας του ατόμου. Στόχος είναι η εύρεση του σημείου στο οποίο θα επιτευχθεί η άμεση διερεύνηση και καταστολή παράνομων κινήσεων χωρίς όμως την παραβίαση του απορρήτου των δεδομένων των υποκειμένων. Αυτό θα φέρει ως αποτέλεσμα την ανάπτυξη μιας ενιαίας κοινωνίας απαλλαγμένη από τον διαδικτυακό φόβο.

ΚΕΦΑΛΑΙΟ 3: ΕΡΕΥΝΑ

3.1 Παρουσίαση της ερευνάς

Η παρούσα ερευνά επιχειρεί την ανάλυση της διαδικτυακής συμπεριφοράς των Ελλήνων χρηστών. Πιο συγκεκριμένα στοχεύει στην διερεύνηση του βαθμού προστασίας και διαχείρισης των προσωπικών δεδομένων των χρηστών καθώς επίσης και στην ενημέρωση τους πάνω σε θέματα και πρακτικές αυτοπροστασίας. Ιδιαίτερη εμφάνιση δίνεται στην χρήση των κοινωνικών δικτυών.

Η εκποίηση της ερευνάς πραγματοποιήθηκε μέσω ερωτηματολογίου με στόχο την λήψη στατιστικών δεδομένων. Στον σχεδιασμό επιλέχθηκε η ποσοτική μέθοδος, με στόχο την εύρεση σχέσεων μεταξύ διαφόρων παραγόντων, μέσα από την συλλογή πρωτογενών στοιχείων με απλή τυχαία δειγματοληψία[150]. Το ερωτηματολόγιο συντάχθηκε μέσω της σελίδας δημιουργίας ερωτηματολογίων της Google Form, και μοιράστηκε μέσω φυλλαδίων αλλά και με την χρήση του διαδικτύου με τυχαία επιλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου και της σελίδας κοινωνικής δικτύωσης Facebook, χρησιμοποιώντας την δειγματοληψία ευκολίας (πρωτογενή ερευνά). Με αυτόν τον τρόπο επιτεύχθηκε η ερευνά να περιλαμβάνει ένα αντιπροσωπευτικό δείγμα του πληθυσμού χωρίς να στοχοποιεί αποκλειστικά στους χρήστες του διαδικτύου ή των μέσων κοινωνικής δικτύωσης, παρέχοντας παράλληλα μια αντικειμενική εικόνα για το ποσοστό των χρηστών του Η/Υ και την χρήση του διαδικτύου στην Ελλάδα. Πρόκειται λοιπόν, για μια απλή τυχαία δειγματοληψία, καθώς όλες οι μονάδες του δείγματος επιλέχθηκαν με τυχαίο τρόπο. Η χρήση του ερωτηματολογίου με αυτό-συμπλήρωση έγινε για να συλλεχθούν στοιχεία καθημερινών ενεργειών, σκέψεων, αισθημάτων και πεποιθήσεων των ερωτώμενων.[151]

Bryman (1989): *«Η δειγματοληπτική ερευνά καθιστά αναγκαία τη συλλογή δεδομένων από έναν αριθμό μονάδων και συνήθως σε μια μοναδική χρονική στιγμή, με την προϋπόθεση να συλλέξουμε συστηματικά ένα σώμα δεδομένων που μπορούν να προσδιοριστούν ποσοτικά σε σχέση προς έναν αριθμό μεταβλητών που στην συνέχεια εξετάζονται για να διακρίνουμε πρότυπα συσχέτισης»*[152]

[150] Colin Robson, Η Έρευνα Του Πραγματικού Κόσμου: Ένα Μέσον Για Κοινωνικούς Επιστήμονες Και Επαγγελματίες Ερευνητές, GUTENBERG, 2007, σελ. 310

[151] Colin Robson, Η Έρευνα Του Πραγματικού Κόσμου: Ένα Μέσον Για Κοινωνικούς Επιστήμονες Και Επαγγελματίες Ερευνητές, GUTENBERG, 2007, σελ.265

[152] Colin Robson, Η Έρευνα Του Πραγματικού Κόσμου: Ένα Μέσον Για Κοινωνικούς Επιστήμονες Και Επαγγελματίες Ερευνητές, GUTENBERG, 2007, σελ.271

3.2 Πλεονεκτήματα και μειονεκτήματα ποσοτικής ερευνάς

Η ποσοτική ερευνά παρουσιάζει πληθώρα πλεονεκτημάτων, αλλά και ορισμένα μειονεκτήματα, τα οποία θα ήτο σκόπιμο να αναφερθούν στην συνέχεια της παρουσίασης. Μέσα από την συμπλήρωση του ερωτηματολογίου το υποκείμενο έχει την κάλυψη της ανωνυμίας, δεδομένου ότι η παρούσα ερευνά διεξαχθεί ανώνυμα, γεγονός που δεν επηρεάζει την εγκυρότητα των απαντήσεων που λήφθηκαν. Επιπλέον μας δόθηκε η δυνατότητα πανελλαδικής κάλυψης μέσα από την μεταφορά του ερωτηματολογίου μέσω Internet και τη συμπλήρωση του ανά πάσα ώρα επιθυμούσε ο ερωτώμενος, αφού η ερωτήσεις είναι κατά το πλησίον κλειστού τύπου, καθιστώντας παράλληλα τα δεδομένα γνησιά, αληθή και ευκολά στην συλλογή (οικονομία χρόνου και μειωμένο κόστος έρευνας).

Από την άλλη πλευρά, τα μειονεκτήματα βρίσκονται στην αδυναμία του ερευνητή να ελέγξει τον τρόπο απάντησης των ερωτήσεων και την εγκυρότητα τους. Παραδείγματος χάριν, ο ερωτώμενος θα μπορούσε να απαντήσει το ερωτηματολόγιο πάνω από μια φορές βλάπτοντας έτσι την εγκυρότητα των αποτελεσμάτων. Επιπλέον, σε περίπτωση απορίων, ο ερευνητής δεν μπορεί να απαντήσει άμεσα ώστε να βοηθήσει τον ερωτώμενο στην καλύτερη διεξαγωγή της ερευνάς. Τέλος, δεν μπορούμε να παραβλέψουμε και τα χαμηλά κίνητρα των ερωτώμενων για συμπλήρωση του ερωτηματολογίου γεγονός που οδηγεί σε μικρό δείγμα δεδομένων.[153] [154]

3.3 Το ερωτηματολόγιο

Το ερωτηματολόγιο περιλάμβανε 3 ενότητες. Η πρώτη αφορούσε ορισμένα προσωπικά στοιχεία του ερωτωμένου, η δεύτερη αφορούσε την γενική χρήση του διαδίκτυού και η τρίτη τα μέσα κοινωνικής δικτύωσης. Σε σύνολο 390 ερωτήσεις. Αναλυτικότερα τα ερωτήματα που ζητήθηκαν να διερευνηθούν ανά ενότητα είναι τα εξής:

Ενότητα 1: Προσωπικά δεδομένα:

- Φύλο
- Ηλικία
- Οικογενειακή κατάσταση

[153] http://mscinaccounting.teipir.gr/uploads/0b7ced8314f51ffea03704122c399f32.pdf, 07/11/2016

[154] Colin Robson, Η Έρευνα Του Πραγματικού Κόσμου: Ένα Μέσον Για Κοινωνικούς Επιστήμονες Και Επαγγελματίες Ερευνητές, GUTENBERG, 2007, σελ. 270-275, 281

- Επίπεδο εκπαίδευσης
- Επάγγελμα

Μέσα από την πρώτη ενότητα επιχειρείτε η εξαγωγή συμπερασμάτων για την χρήση του διαδικτύου συγκριτικά με τα βασικά του χαρακτηριστικά του πληθυσμού.

Ενότητα 2: Διαδίκτυο:

- Ύπαρξη ηλεκτρονικού υπολογιστή στην οικία
- Ύπαρξη σύνδεση στο διαδίκτυο και επισκεψημοτητα
- Μέσον σύνδεσης στο διαδίκτυο
- Λόγοι σύνδεσης
- Παραχώρηση προσωπικών στοιχείων- ρυθμίσεις προσβάσεις σε αυτά
- Καταγραφή δραστηριοτήτων- αντιμετρά χρήστη

Σε αυτή την ενότητα διερευνάτε το ποσοστό χρήσης του διαδικτύου και ο ψηφιακός αναλφαβητισμός. Επιπλέον επιχειρείτε η διεξαγωγή πορισμάτων σχετικά με την χρήση του διαδικτύου των Ελλήνων, τις προφυλάξεις και την ενημέρωση τους. Τα δεδομένα που συλλέχθηκαν στην παρούσα ενότητα αφορούν την γενική χρήση του διαδικτύου.

Ενότητα 3: Κοινωνικά δίκτυα:

- Πια μέσα κοινωνικής δικτύωσης χρησιμοποιούν
- Ηλικία εισόδου σε ιστοσελίδες κοινωνικής δικτύωσης
- Συχνότητα και χρόνος σύνδεσης
- Τόπος σύνδεσης
- Προσωπικά δεδομένα
- Ενεργείς ασφάλειας
- Έλεγχος κοινοποίησης
- Ιστοσελίδες κοινωνικής δικτύωσης και συνδρομή
- Βαθμός ενημέρωση για τις «πολίτικες απορρήτου» και τους «ορούς χρήσης»
- Ασφάλεια των ιστοσελίδων κοινωνικής δικτύωσης.

Στην τρίτη ενότητα μελετάτε η χρήση των μεσών κοινωνικής δικτύωσης· την προτίμηση των χρηστών για ορισμένες ιστοσελίδες, την αίσθηση ασφάλεια ή μη κατά την περιήγηση τους, και την ιδιωτικότητα.

3.4 Τύποι ερωτήσεων

Οι τύποι των ερωτήσεων που χρησιμοποιήθηκαν ήταν κυρίως κλειστού τύπου: διχοτομικές ερωτήσεις και πολλαπλής επιλογής. Υπήρξε ωστόσο μια ερώτηση ανοιχτού τύπου όπου ο ερωτώμενος καλείτο να συμπληρώσει την ηλικία του. Η εν λόγο ερώτηση κατά την παρουσίαση των δεδομένων ομαδοποιήθηκε σε τρείς ηλικιακές κλάσεις.

Το μέγεθος του δείγματος ανέρχεται στα 87 άτομα. Η ερευνά έλαβε χώρα το χρονικό διάστημα 19/9/2016 έως 5/11/2016. Στην ανάλυση των συλλεχθεντων δεδομένων θα χρησιμοποιηθεί ποσοστιαία βάση επι τις εκατό, η οποία θα μας διευκολύνει στην ανάλυση και σύγκριση των αποτελεσμάτων, αλλά και οι συχνότητες του δείγματος. Η ανάλυση θα γίνει με την χρήση του στατιστικού πακέτου SPSS.

3.5 Αποτελέσματα

3.5.1 Ανάλυση δημογραφικών στοιχείων

Η περιγραφική στατιστική μελετά τις μεθόδους που χρησιμοποιούνται για να περιγράφουν τα δεδομένα και τα χαρακτηριστικά τους.[155] Σε αυτή την ενότητα θα αναλύσουμε την σύσταση του πληθυσμού του δείγματος προς το φύλο, την ηλικία, την οικογενειακή κατάσταση, το επίπεδο σπουδών και την κυριά ασχολία.

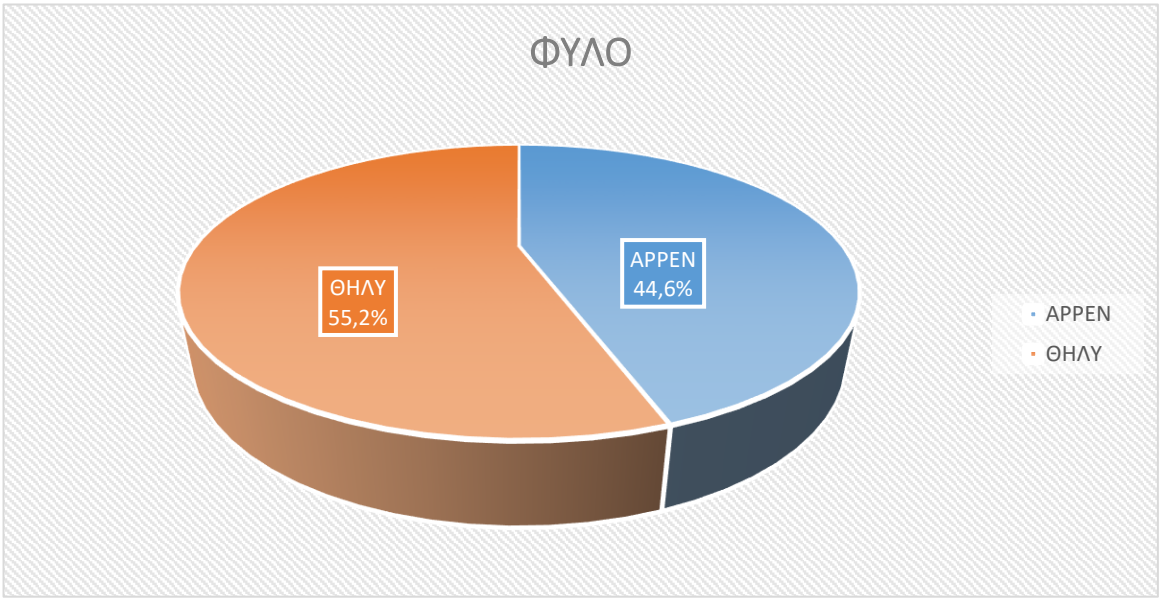
- **Φύλο**

Στην έρευνα συμμετείχαν συνολικά 87 άτομα, εκ των οποίων 39 άντρες και 48 γυναίκες. Οι γυναίκες παρατηρούμε πως αποτελούν την πλειοψηφία του δείγματος μας, με ποσοστό 55,2%, έναντι του ποσοστού των 44,8% των αντρών.

Φύλο

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
Άρρεν	*39*	*44,8*	*44,8*	*44,8*
Θήλυ	*48*	*55,2*	*55,2*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.1: Φύλο συμμετεχόντων



Γράφημα 3.1: Φύλο συμμετεχόντων

[155] Ian Diamond and Julie Jefferies, Αρχίζοντας Την Στατιστική: Μια Εισαγωγή Για Τους Κοινωνικούς Επιστήμονες, εκδόσεις Παπαζήση, 2006, σελ. 17

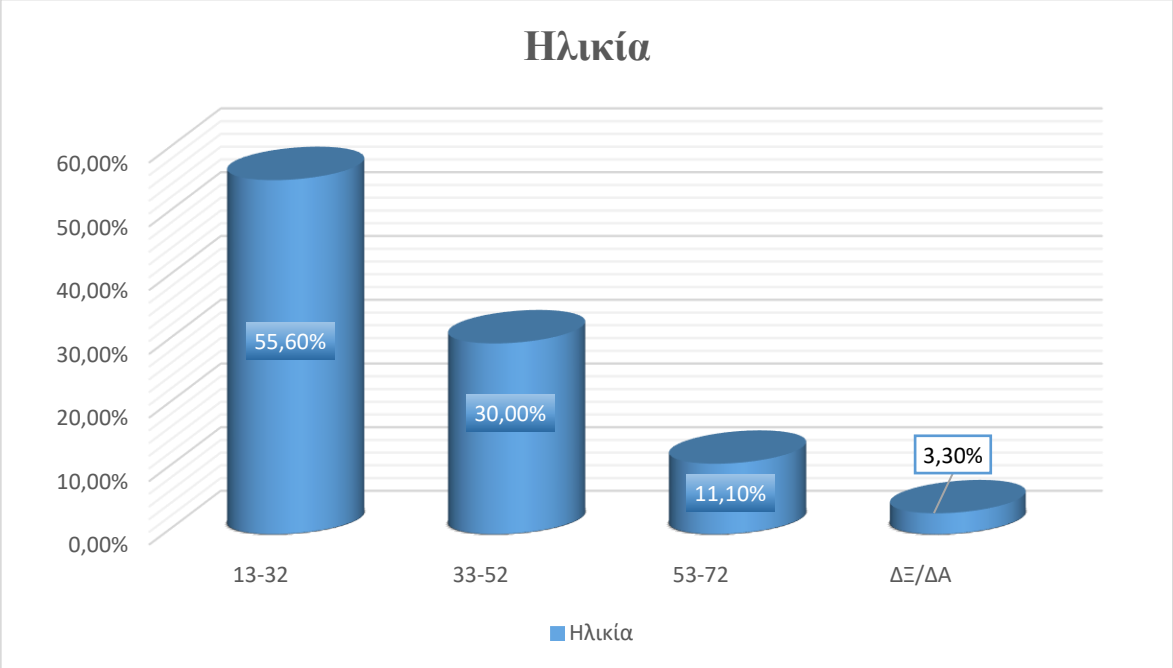
- **Ηλικία**

Για την ανάγκη της παρούσας ερευνάς δημιουργήθηκαν τρεις (3) ηλικιακές κλάσεις. Από τον πίνακα 3.2 και το παράρτημα 3.2 φανερώνεται πως η πλειοψηφία του δείγματος σε ποσοστό 55,6% ανήκει στην πιο νεαρή ηλικιακή ομάδα, η οποία περιλαμβάνει ηλικίες από 13 έως 32 ετών. Έπεται η μεσαία κλάση, 33 έως 52 ετών, με ποσοστό 31%. Τέλος οι ηλικίες άνω των 53 ετών έχουν την μικρότερη συμμετοχή στην παρούσα ερευνά με ποσοστό 11,1%. Παρατηρούμε επίσης, πως τρεις (3) ερωτώμενοι αρνήθηκαν να καταχωρήσουν την ηλικία τους.

Ηλικία

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
13-32	*50*	*55,6*	*57,5*	*57,5*
33-52	*27*	*30,0*	*31,0*	*88,5*
53-72	*10*	*11,1*	*11,5*	*100,0*
Σύνολο	*87*	*96,7*	*100,0*	
Missing System	*3*	*3,3*		
Σύνολο	*90*	*100,0*		

Πίνακας 3.2: Ηλικία συμμετεχόντων



Γράφημα 3.2: Ηλικία συμμετεχόντων

- **Οικογενειακή κατάσταση**

Το μεγαλύτερο ποσοστό του δείγματος αποτελείτε από άγαμα άτομα, σε ποσοστό 67,8%, (συχνότητα 59), ενώ έπονται οι έγγαμοι σε ποσοστό 27,6% (συχνότητα 24). Οι διαζευγμένοι και οι χήροι ακολουθούν με ποσοστά 3,4% και 1,1% αντίστοιχα.

Οικογενειακή Κατάσταση

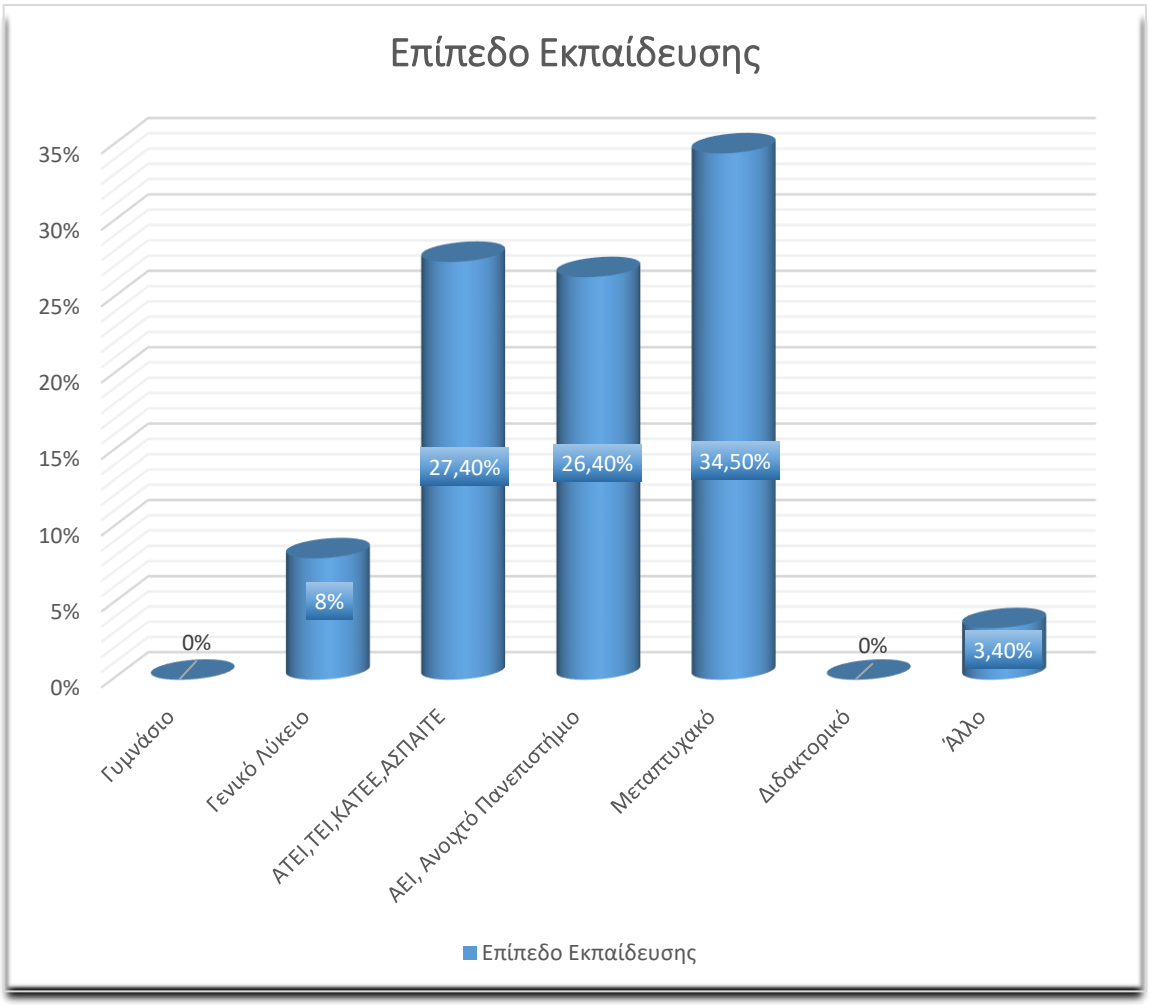
	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
Άγαμος/η	*59*	*67,8*	*67,8*	*67,8*
Διαζευγμένο	*3*	*3,4*	*3,4*	*71,3*
Έγγαμος/η	*24*	*27,6*	*27,6*	*98,9*
Χήρος/α	*1*	*1,1*	*1,1*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.3: Οικογενειακή κατάσταση συμμετεχόντων

Γράφημα 3.3: Οικογενειακή κατάσταση συμμετεχόντων

- **Επίπεδο εκπαίδευσης**

Αναφορικά με το επίπεδο εκπαίδευσης παρατηρούμε πως η πλειοψηφία του δείγματος μας (34,5%) είναι άτομα με υψηλό μορφωτικό επίπεδο. Έπονται οι κάτοχοι πτυχίου ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ ΚΑΙ ΑΣΠΑΙΤΕ σε ποσοστό 27,4% και οι απόφοιτη ΑΕΙ και Ανοιχτού πανεπιστήμιου με 26,4%. Αξίζει να αναφέρουμε τα μηδενικά ποσοστά σε αποφοίτους Γυμνάσιου και Διδακτορικού επιπέδου.



Γράφημα 3.4: Επίπεδο εκπαίδευσης συμμετεχόντων

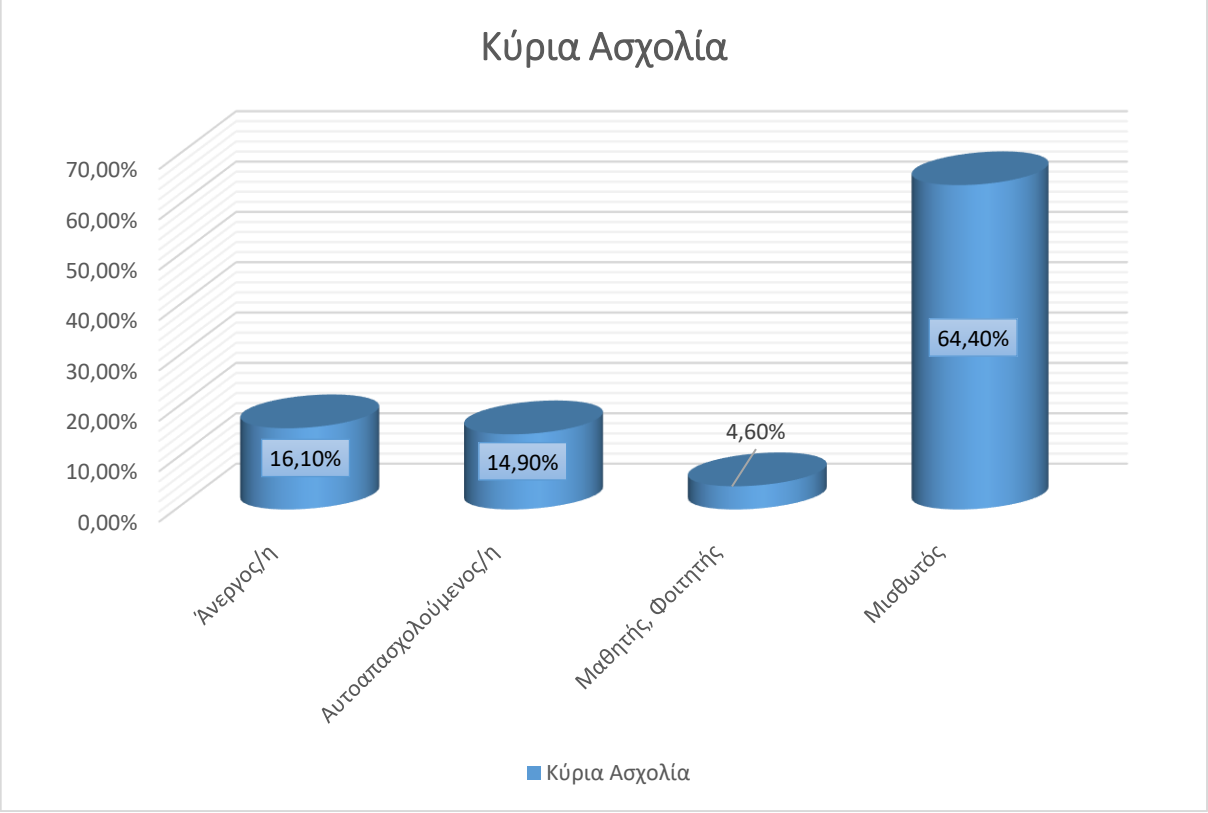
- **Κύρια ασχολία**

Η συντριπτική πλειοψηφία του δείγματος μας αποτελείτε από μισθωτούς (64,4%) ενώ έπονται οι άνεργη και οι αυτοαπασχολούμενοι με ποσοστά 16,1% και 14,9% αντίστοιχα.

Κύρια Ασχολία

	Συχνότητα	*Ποσοστά*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
Άνεργος/η	*14*	*16,1*	*16,1*	*16,1*
Αυτοαπασχολούμενος/η	*13*	*14,9*	*14,9*	*31,0*
Μαθητής, Φοιτητής	*4*	*4,6*	*4,6*	*35,6*
Μισθωτός/η	*56*	*64,4*	*64,4*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.4: Κύρια ασχολία συμμετεχόντων



Γράφημα 3.5: Κύρια ασχολία συμμετεχόντων

3.5.2 Διαδίκτυο

Περνώντας στην δεύτερη θεματική ενότητα του ερωτηματολογίου θα στοχεύει η διερεύνηση της χρήσης του διαδικτύου στο δείγμα. Παρακάτω παρουσιάζονται οι ερωτήσεις που κλήθηκαν να απαντήσουν οι ερωτώμενοι, καθώς και τα αναλυτικά ποσοστά των απαντήσεων τους.

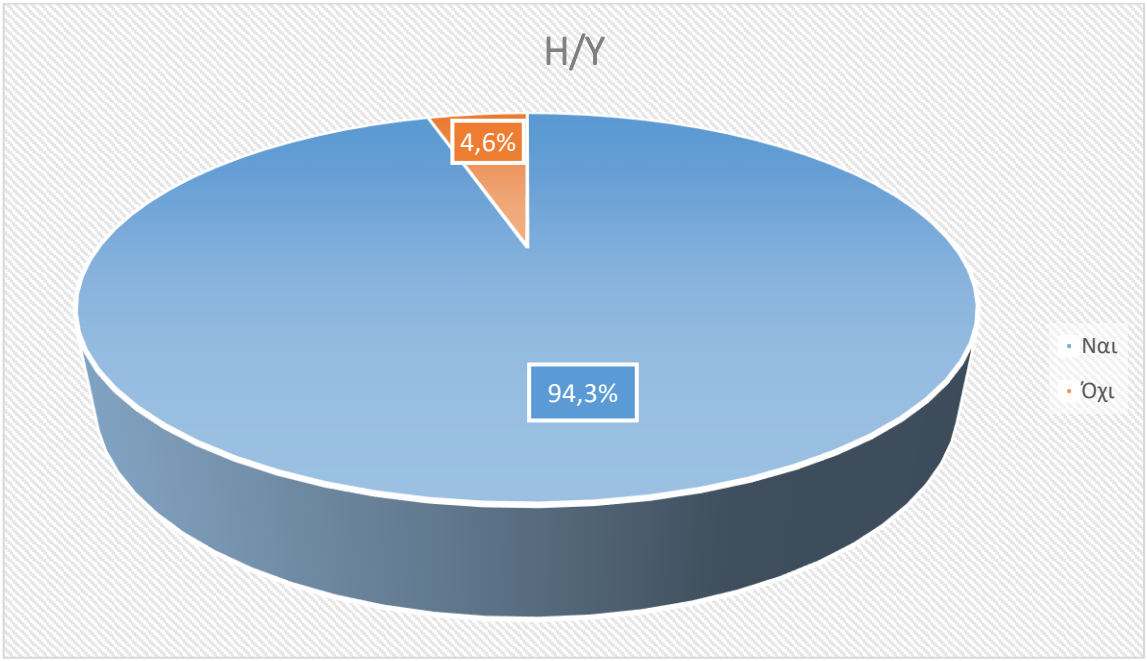
- **Έχετε ηλεκτρονικό υπολογιστή στην κατοικία σας;**

Η συντριπτική πλειοψηφία του δείγματος σε ποσοστό 94,3% και συχνότητα 82/87 αποκρίθηκε πως κατέχει ηλεκτρονικό υπολογιστή στην κατοικία του. Εν αντίθεσίν το πόστο που δεν διαθέτει ανέρχεται μόλις στο 4,6%. Σε αυτό το σημείο πρέπει να αναφέρουμε πως το ερωτηματολόγιο διανεμήθηκε τόσο μέσω του διαδικτύου και των μέσων κοινωνικής δικτύωσης όσο και από φυλλάδια. Η διττή διανομή μας εξασφάλισε ένα πιο ολοκληρωμένο δείγμα στον πληθυσμό.

Ηλεκτρονικός Υπολογιστής

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	1	*1,1*	*1,1*	*1,1*
Ναι	*82*	*94,3*	*94,3*	*95,4*
Όχι	*4*	*4,6*	*4,6*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.5: Ηλεκτρονικός Υπολογιστής



Γράφημα 3.6: Ηλεκτρονικός Υπολογιστής

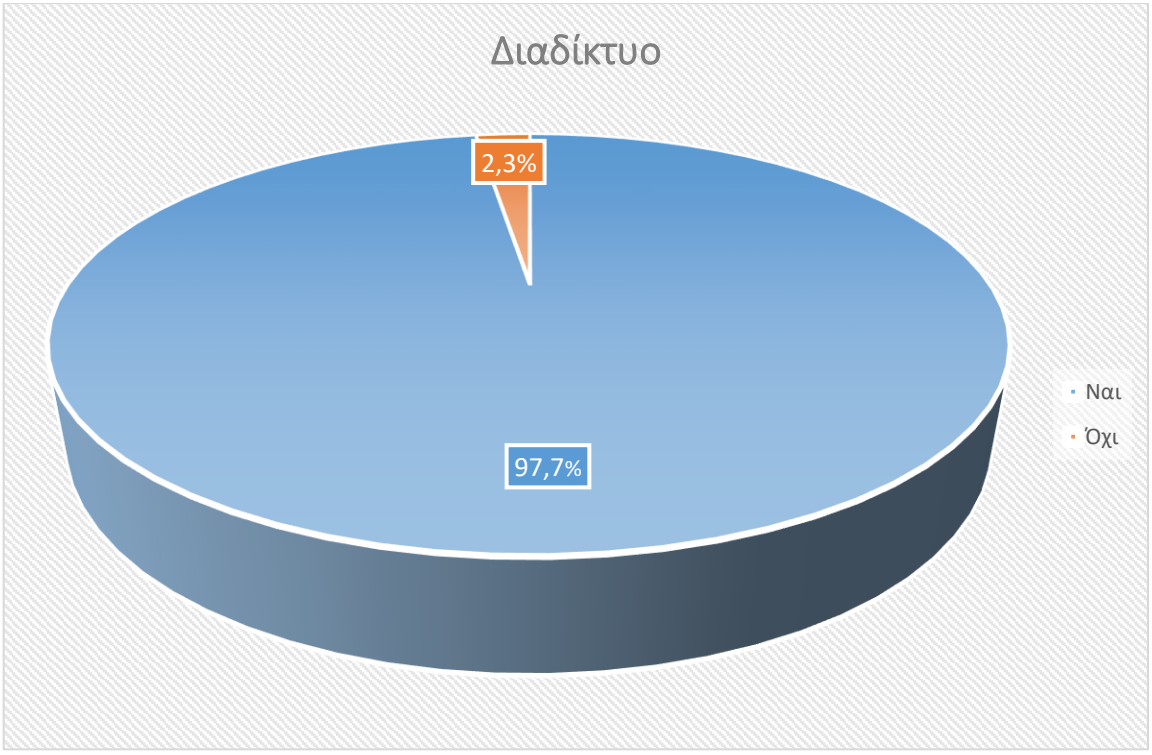
- **Έχετε πρόσβαση στο διαδίκτυο στην κατοικία σας;**

Εξίσου υψηλό εμφανίζεται και το ποσοστό που έχει σύνδεση στο Internet, 97,7% έναντι 2,3%.

Πρόσβαση στο Διαδίκτυο

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
Ναι	*85*	*97,7*	*97,7*	*97,7*
Όχι	*2*	*2,3*	*2,3*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.6: Πρόσβαση στο Διαδίκτυο



Γράφημα 3.7: Πρόσβαση στο Διαδίκτυο

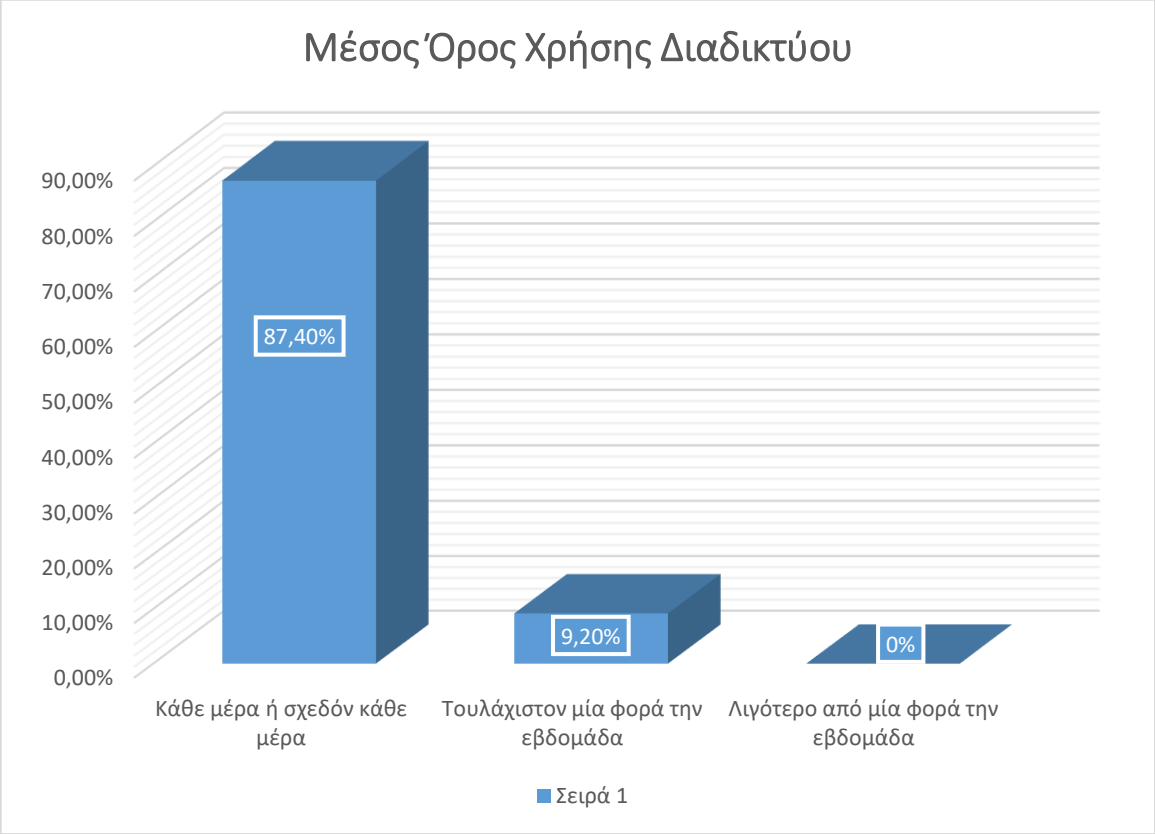
- **Πόσο συχνά χρησιμοποιείτε κατά μέσο ορό το διαδίκτυο;**

Η χρήση του διαδικτύου αποτελεί καθημερινή (ή σχεδόν καθημερινή) ενασχόληση για το 87,4% του δείγματος ενώ το 9,2% δηλώνει ως εισέρχεται τουλάχιστον μια φορά την εβδομάδα. Εδώ πρέπει να αναφέρουμε πως στις απαντήσεις συμπεριλαμβάνονταν και η χρήση του λιγότερο από 1 φορά την εβδομάδα. Η μη ένταξη της συγκεκριμένης απάντησης στον πίνακα του SPSS οφείλετε στην μηδενική επιλογή της από τους ερωτώμενους.

Μέσος Όρος Χρήσης Διαδικτύου

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	3	*3,4*	*3,4*	*3,4*
Κάθε μέρα ή σχεδόν κάθε μέρα	*76*	*87,4*	*87,4*	*90,8*
Τουλάχιστον μια φορά την εβδομάδα	*8*	*9,2*	*9,2*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.7: Μέσος Όρος Χρήσης Διαδικτύου



Γράφημα 3.8: Μέσος Όρος Χρήσης Διαδικτύου

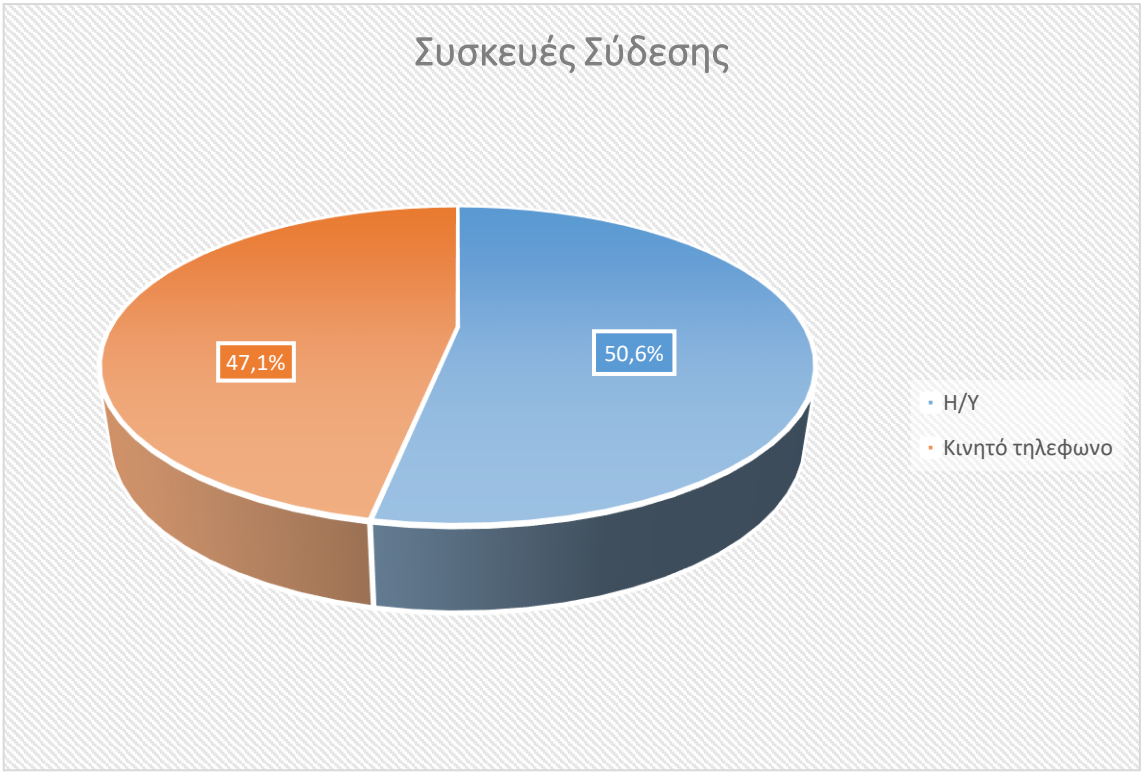
- **Ποια από τις παρακάτω συσκευές χρησιμοποιείτε *κυρίως* για την σύνδεσή σας στο διαδίκτυο;**

Θέλοντας να εξετάσουμε την συμπεριφορά των χρηστών και τις ανάγκες που ικανοποιεί η σύνδεση τους στο διαδίκτυο, κλήθηκαν να απαντήσουν για το μέσον σύνδεσης τους σε αυτό. Πρέπει να σημειωθεί πως έλαβα πολλά μηνύματα σχετικά με την παρούσα ερώτηση καθώς αρκετοί ήταν οι χρήστες που συνδέονται και από τα δυο μέσα. Παρ' όλα αυτά τα αποτελέσματα τις ερευνά έδειξαν πως το κινητό τηλέφωνο χρησιμοποιείτε όσο ο υπολογιστής από το δείγμα, με ένα ελαφρύ προβάδισμα στην χρήση του υπολογιστή.

Συσκευές

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	2	*2,3*	*2,3*	*2,3*
Κινητό τηλέφωνο	*41*	*47,1*	*47,1*	*49,4*
Υπολογιστή (σταθερό, φορητό, tube)	*44*	*50,6*	*50,6*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.8: Συσκευές Σύνδεσης



Γράφημα 3.9: Συσκευές Σύνδεσης

- **Για ποιους λογούς χρησιμοποιείτε κυρίως το διαδίκτυο;**

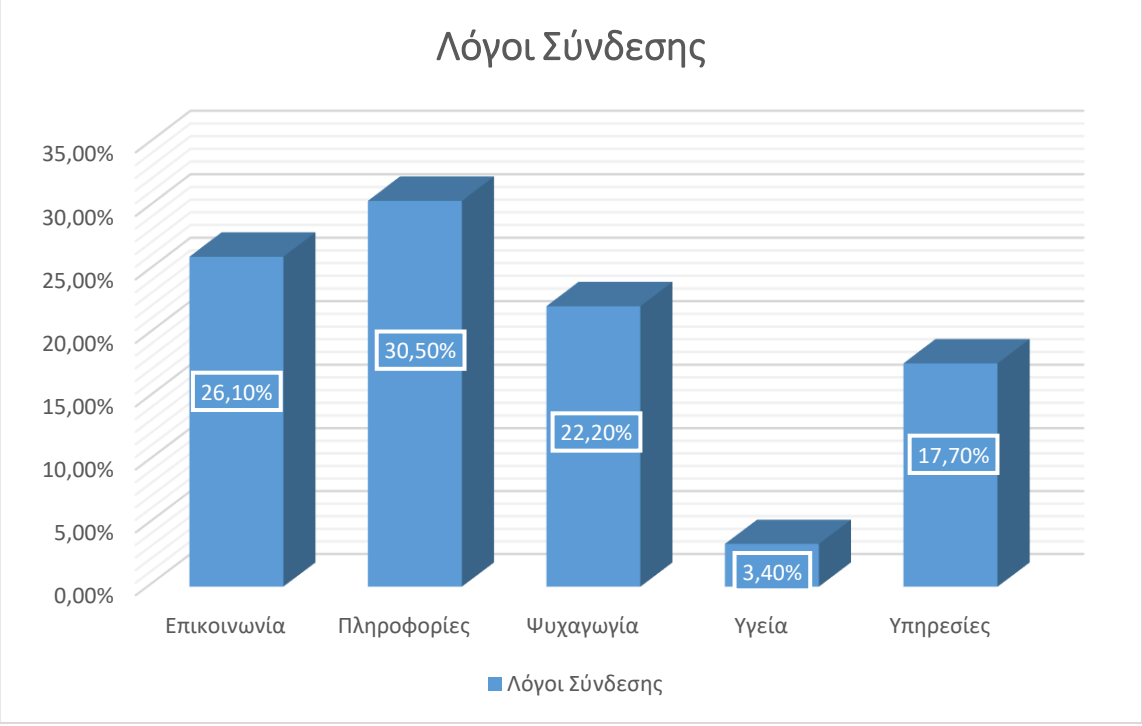
Όπως γίνεται αντιληπτό από τον πίνακα 3.9 και το ραβδόγραμμα 3.10, οι λόγοι χρήσης του διαδικτύου ποικίλουν. Η πλειοψηφία του δείγματος ανέφερε πως χρησιμοποιεί το διαδίκτυο για την εύρεση πληροφοριών (σε ποσοστό 30,5%), για να επικοινωνεί (26,1%). Έπεται η ψυχαγωγία με ποσοστό 22,2% και οι online υπηρεσίες (17,7%). Το ποσοστό της χρήσης του διαδικτύου για ζητήματα υγείας παρουσιάζεται αρκετά χαμηλό στο δείγμα, μόλις 3,4%.

$Λόγοι Frequencies

		Απαντήσεις		*Percent of Cases*
		N	*Ποσοστό*	
$Λόγοι[a]	*Επικοινωνία*	*53*	*26,1%*	*62,4%*
	Πληροφορίες	*62*	*30,5%*	*72,9%*
	Ψυχαγωγία	*45*	*22,2%*	*52,9%*
	Υγεία	*7*	*3,4%*	*8,2%*
	Υπηρεσίες	*36*	*17,7%*	*42,4%*
Σύνολο		*203*	*100,0%*	*238,8%*

a. Dichotomy group tabulated at value 1.

Πίνακας 3.9: Λόγοι Σύνδεσης



Γράφημα 3.10: Λόγοι Σύνδεσης

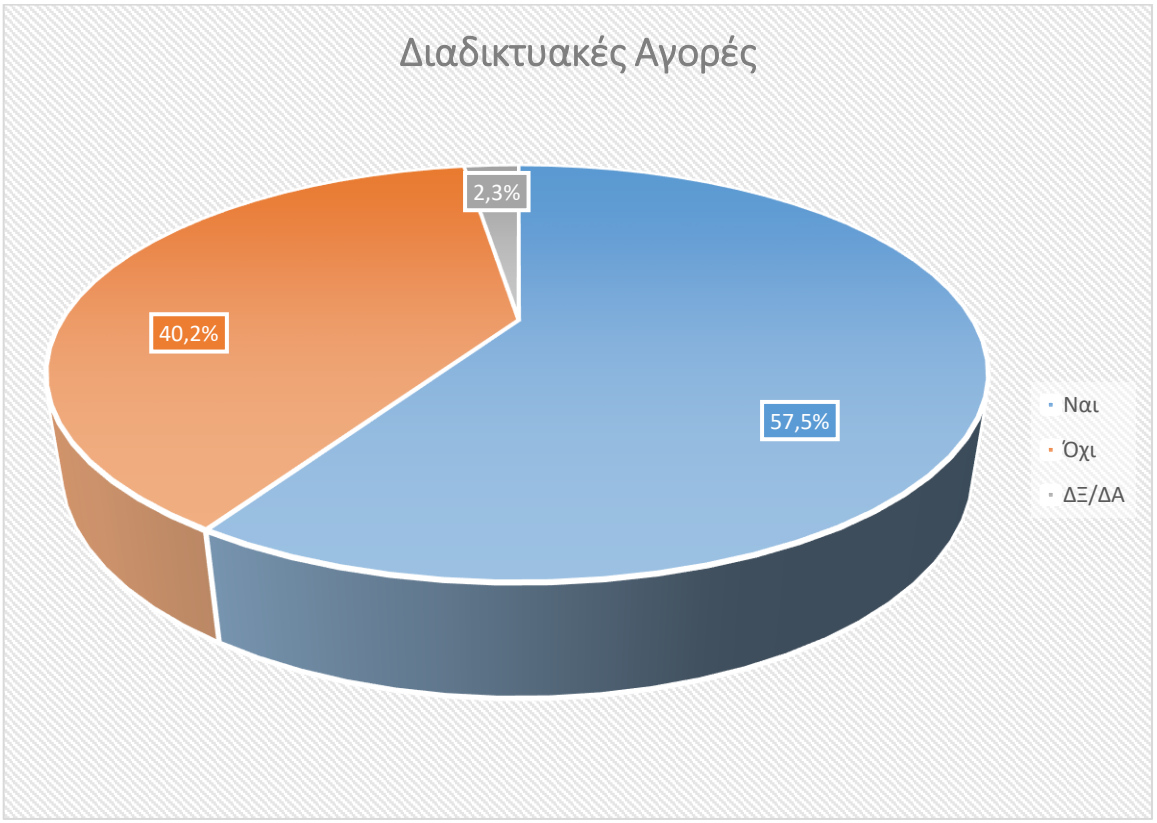
- **Χρησιμοποιείτε το διαδίκτυο για να πραγματοποιήσετε αγορές;**

Η αγορά μέσω διαδικτύου φαίνεται να αποτελεί μια προσφιλή συνήθεια για το 57,5% του δείγματος, σε αντίθεση με το 40,2% το οποίο δηλώνει πως δεν έχει χρησιμοποιήσει ποτέ αυτή την δυνατότητα του διαδικτύου.

Διαδικτυακές Αγορές

	Συχνότητα	*Ποσοστό*	*Εγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	2	*2,3*	*2,3*	*2,3*
Ναι	*50*	*57,5*	*57,5*	*59,8*
Όχι	*35*	*40,2*	*40,2*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.10: Διαδικτυακές Αγορές



Γράφημα 3.11: Διαδικτυακές Αγορές

- **Αν ναι, τα προϊόντα ή οι υπηρεσίες που αγοράσατε μέσω του διαδικτύου προέρχονταν από:**

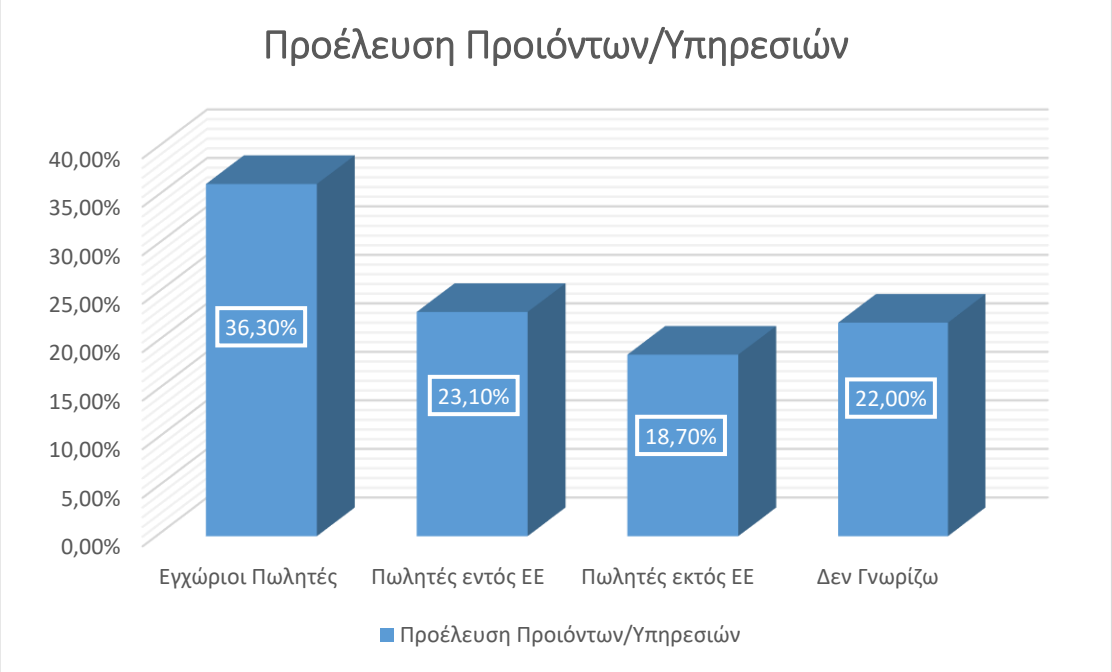
Το 57,5% του δείγματος που δήλωσε ότι πραγματοποιεί αγορές μέσω διαδικτύου ερωτήθηκε περί της προελεύσεως των προϊόντων ή των υπηρεσιών. Όπως φανερώνεται από τον πίνακα 3.11 το 36,3% προτιμούν εγχωρίους πωλητές. Έπονται οι πωλητές εντός της Ευρωπαϊκής Ένωσης 23,1%, ενώ χαμηλότερο είναι το ποσοστό αγορών που πραγματοποιούνται εκτός της Ευρωπαϊκής Ένωσης. Αξίζει να επισημάνουμε πως το 22,0% των ερωτηθέντων (ποσοστό διόλου ευκαταφρόνητο) δεν γνωρίζουν για την προέλευση των προϊόντων/υπηρεσιών.

$Προέλευση Frequencies

		Απαντήσεις		*Percent of Cases*
		N	*Ποσοστό*	
$Προέλευση[a]	*Εγχώριοι Πωλητές*	*33*	*36,3%*	*52,4%*
	Πωλητές Εντός ΕΕ	*21*	*23,1%*	*33,3%*
	Πωλητές Εκτός ΕΕ	*17*	*18,7%*	*27,0%*
	Δεν Γνωρίζω	*20*	*22,0%*	*31,7%*
Σύνολο		*91*	*100,0%*	*144,4%*

a. Dichotomy group tabulated at value 1.

Πίνακας 3.11: Προέλευση Προϊόντων/ Υπηρεσιών



Γράφημα 3.12: Προέλευση Προϊόντων/ Υπηρεσιών

- **Ποιο από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στο διαδίκτυο;**

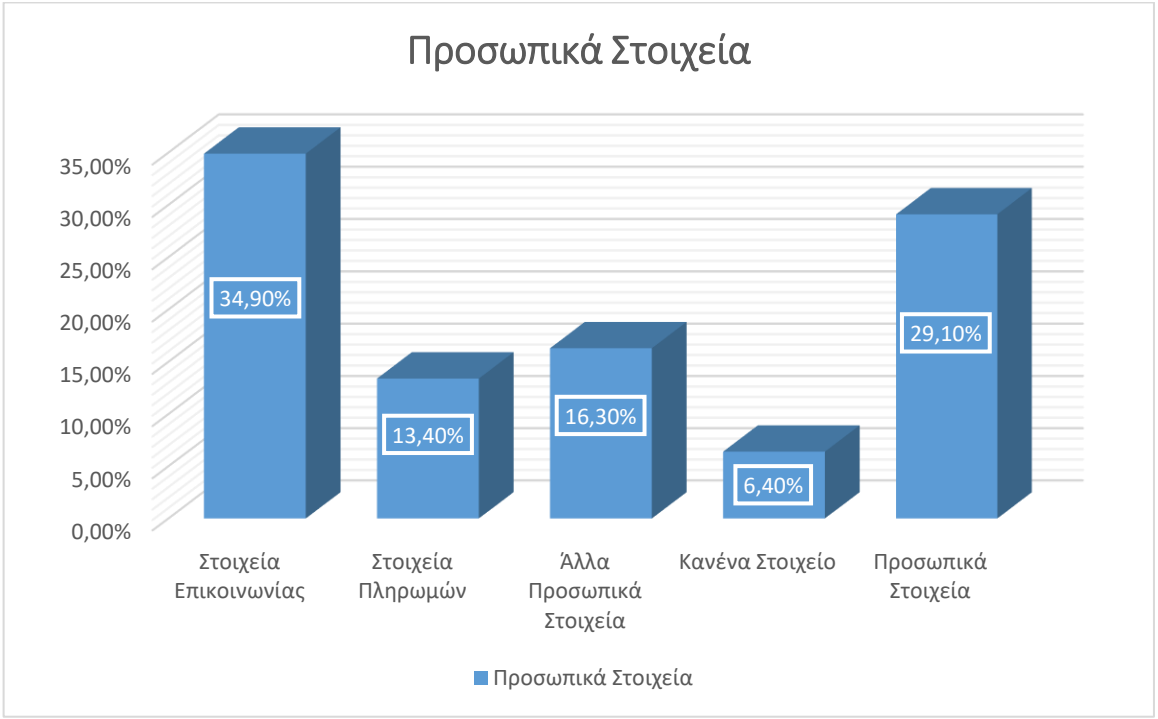
Η πλειονότητα του δείγματος ανέφερε πως έχει παραχωρήσει στοιχεία επικοινωνίας (34,9%) και προσωπικά στοιχεία στο διαδίκτυο (29,4%). Παρατηρείτε η τάση οι χρήστες του διαδικτύου να παραχωρούν σε μεγάλο ποσοστό προσωπικά τους στοιχεία. Το ποσοστό του δείγματος το οποίο δηλώνει πως δεν έχει παραχωρήσει κανένα στοιχεία ανέρχεται μόλις στο 6,4%.

$Προσωπικά Στοιχεία Frequencies

		Απαντήσεις		*Percent of Cases*
		N	*Ποσοστό*	
$Προσωπικά Στοιχεία[a]	*Στοιχεία επικοινωνίας*	*60*	*34,9%*	*70,6%*
	Στοιχεία πληρωμών	*23*	*13,4%*	*27,1%*
	Άλλα προσωπικά στοιχεία	*28*	*16,3%*	*32,9%*
	Κανένα στοιχείο	*11*	*6,4%*	*12,9%*
	Προσωπικά στοιχεία	*50*	*29,1%*	*58,8%*
	Σύνολο	*172*	*100,0%*	*202,4%*

a. Dichotomy group tabulated at value 1.

Πίνακας 3.12: Προσωπικά Στοιχεία



Γράφημα 3.13: Προσωπικά Στοιχεία

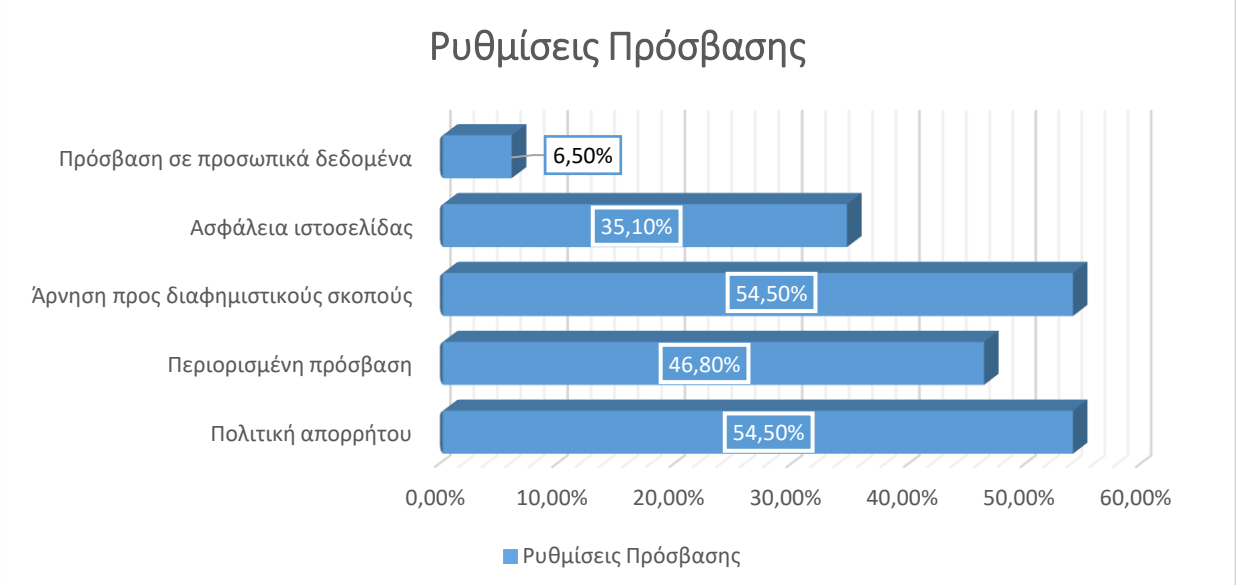
- **Έχετε προβεί σε κάποια από τις παρακάτω ενέργειες για να διαχειριστείτε τις ρυθμίσεις πρόσβασης σε προσωπικά σας δεδομένα;**

Οι χρήστες προκειμένου να διασφαλίσουν την ασφάλεια των προσωπικών τους δεδομένων καταφεύγουν σε διάφορες ενέργειες. Οι πιο συνήθεις ενέργειες είναι η ανάγνωση των πολιτικών απορρήτου προτού παραχωρηθούν προσωπικά στοιχεία και η άρνηση χρήσης των προσωπικών δεδομένων για διαφημιστικούς λόγους (με ποσοστό 54,5% έκαστο). Επίσης, μεγάλο ποσοστό του δείγματός (46,8%) επιλέγει την περιορισμένη πρόσβαση, για τους υπόλοιπους χρήστες, σε προσωπικά του στοιχεία.

$Ρυθμίσεις Πρόσβασης Frequencies

		Απαντήσεις		*Percent of Cases*
		N	*Ποσοστό*	
$Ρυθμίσεις πρόσβασης	*Διαβάσατε την πολιτική απορρήτου*	*42*	*27,6%*	*54,5%*
	Επιλέξατε την περιορισμένη πρόσβαση σε προσωπικά σας στοιχεία	*36*	*23,7%*	*46,8%*
	Αρνηθήκατε να χρησιμοποιηθούν τα προσωπικά σας δεδομένα για διαφημιστικούς λόγους	*42*	*27,6%*	*54,5%*
	Ελέγξατε την ασφάλεια της ιστοσελίδας προτού δώσετε τα προσωπικά σας στοιχεία	*27*	*17,8%*	*35,1%*
	Ζητήσατε να έχετε πρόσβαση σε τηρούνται προσωπικά δεδομένα (προς επικαιροποίηση ή διαγραφή)	*5*	*3,3%*	*6,5%*
	Σύνολο	*152*	*100,0%*	*197,4%*

Πίνακας 3.13: Ρυθμίσεις Πρόσβασης



Γράφημα 3.14: Ρυθμίσεις Πρόσβασης

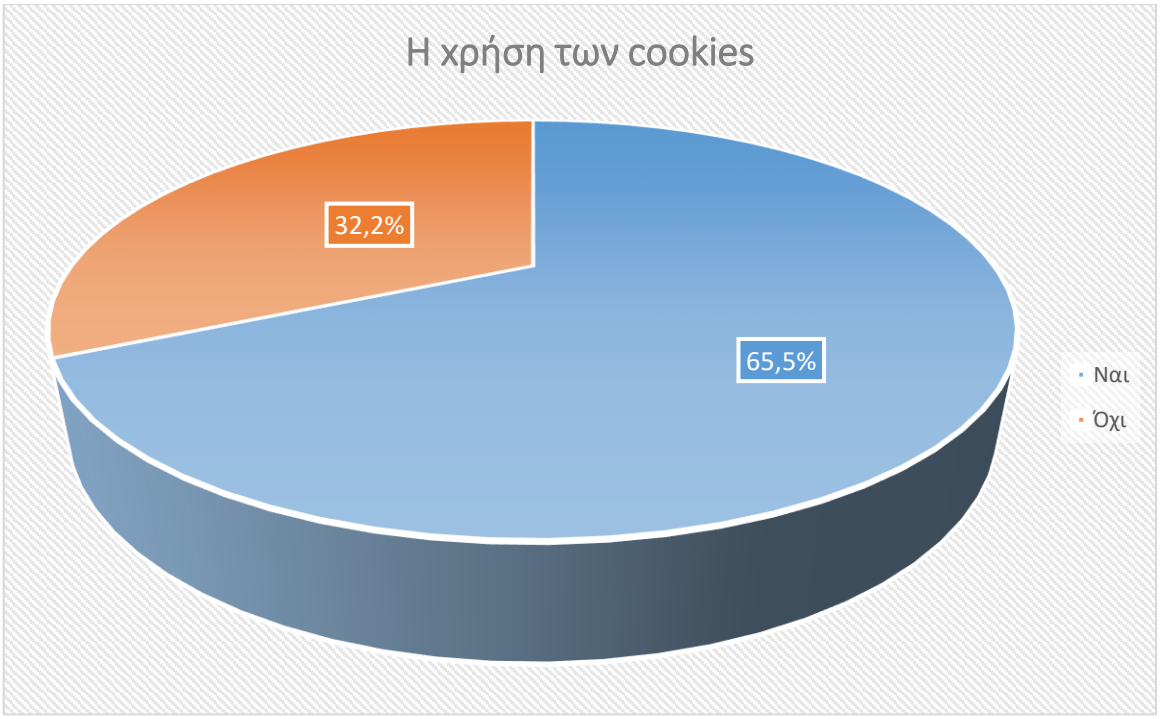
- **Γνωρίζετε ότι τα cookies μπορεί να χρησιμοποιηθούν για ανιχνευτή των κινήσεων στο διαδίκτυο και στην συνέχεια για τη δημιουργία προφίλ του κάθε χρήστη και την αποστολή διαφημίσεων για θέματα που τον ενδιαφέρουν;**

Στην ερώτηση αναφορικά με την χρήση των cookies το 65,5% απάντησαν πως είναι ενήμεροι για την χρήση τους, έχω το 32,2% πως όχι.

Cookies

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	2	*2,3*	*2,3*	*2,3*
Ναι	*57*	*65,5*	*65,5*	*67,8*
Όχι	*28*	*32,2*	*32,2*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.14: Cookies



Γράφημα 3.15: Cookies

- **Ποσό σας ενοχλεί το γεγονός ότι οι online δραστηριότητες σας στο διαδίκτυο καταγράφονται προκειμένου να χρησιμοποιηθούν για την αποστολή διαφημίσεων για θέματα που σας ενδιαφέρουν;**

Τα ποσοστά ενόχλησης των χρηστών δεν παρουσιάζουν καθαρή τάση. Το 42,5% δηλώνει αρκετά ενοχλημένο με την καταγραφή των δραστηριοτήτων του σε σχέση με τις διαφημίσεις. Πιο χαμηλά σε ποσοστό (28,7%) έρχεται η μηδαμινή ενόχληση των χρηστών, ενώ μόλις το 25,3% παρουσιάζεται πολύ ενοχλημένο.

Καταγραφή Online Δραστηριοτήτων

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	3	*3,4*	*3,4*	*3,4*
Αρκετά	*37*	*42,5*	*42,5*	*46,0*
Καθόλου	*25*	*28,7*	*28,7*	*74,7*
Πολύ	*22*	*25,3*	*25,3*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.15: Καταγραφή Online Δραστηριοτήτων

Γράφημα 3.16: Καταγραφή Online Δραστηριοτήτων

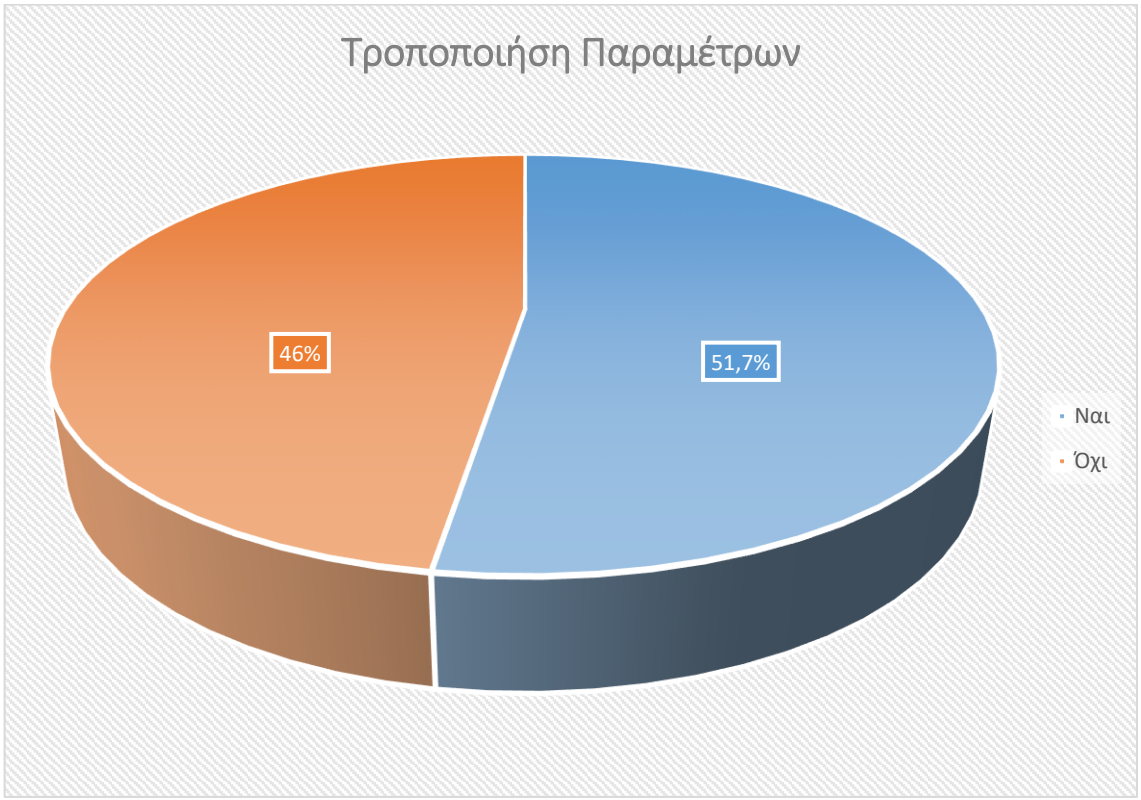
- **Έχετε ποτέ τροποποιήσει τις παραμέτρους των προγραμμάτων πλοήγησης προκειμένου να αποφύγετε ή να περιορίσετε την είσοδο των cookies στον υπολογιστή σας;**

Το 51,7% με συχνότητα ποσοστού 45 δηλώνει πως έχει προβεί σε τροποποίηση σε αντίθεση με το 46% συχνότητας 40 που δεν έχει προβεί σε αυτήν την ενέργεια.

Τροποποίηση

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	2	*2,3*	*2,3*	*2,3*
Ναι	*45*	*51,7*	*51,7*	*54,0*
Όχι	*40*	*46,0*	*46,0*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.16:Τροποποίηση



Γράφημα 3.17: Τροποποίηση

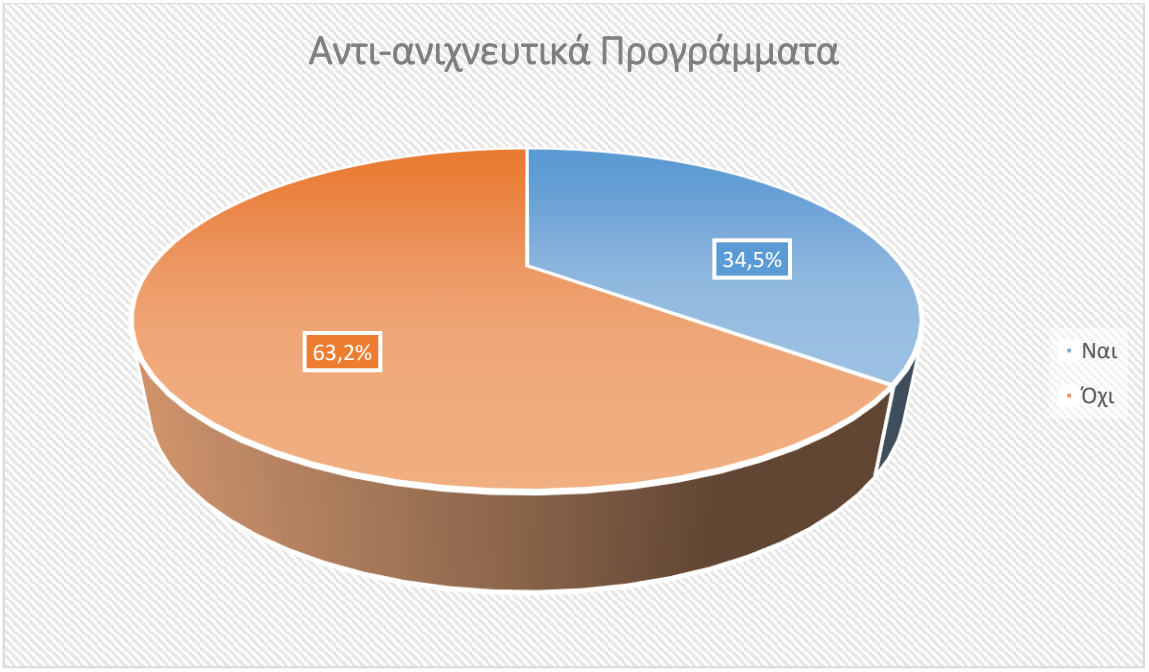
- **Χρησιμοποιείτε αντί-ανιχνευτικά προγράμματα προκειμένου να περιορίσετε τη δυνατότητα ανίχνευσης των δραστηριοτήτων σας στο διαδίκτυο;**

Η πλειοψηφία των χρηστών του δείγματος δεν διαθέτει αντι-ανιχνευτικα προγράμματα (63,2%).

Αντι-ανιχνευτικα

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	2	*2,3*	*2,3*	*2,3*
Ναι	*30*	*34,5*	*34,5*	*36,8*
Όχι	*55*	*63,2*	*63,2*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.17: Αντι-ανιχνευτικα



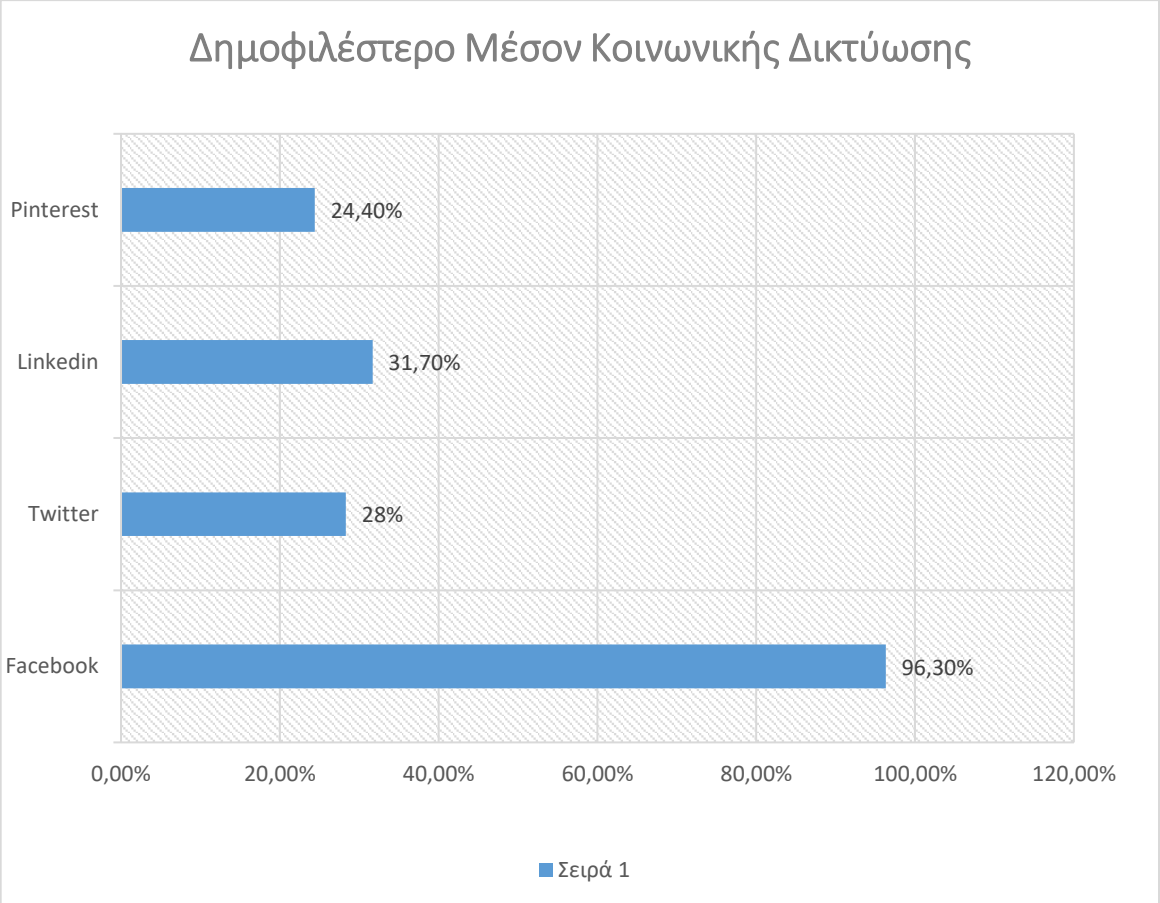
Γράφημα 3.18: Αντι-ανιχνευτικα

3.5.3 Μέσα Κοινωνικής Δικτύωσης

Στο τρίτο μέρος της ερευνάς παρουσιάζονται δεδομένα που στοχεύουν εξ' ολοκλήρου στην χρήση των ιστοσελίδων κοινωνικής δικτύωσης, στον τρόπου που χρησιμοποιούνται, καθώς και στον βαθμό ασφάλειας που νοιώθουν οι χρήστες τους. Παρακάτω παρουσιάζονται αναλυτικά οι απαντήσεις που συλλέχθηκαν:

- **Διατηρείτε λογαριασμό σε κάποιο από τις παρακάτω σελίδες κοινωνικής δικτύωσης;**

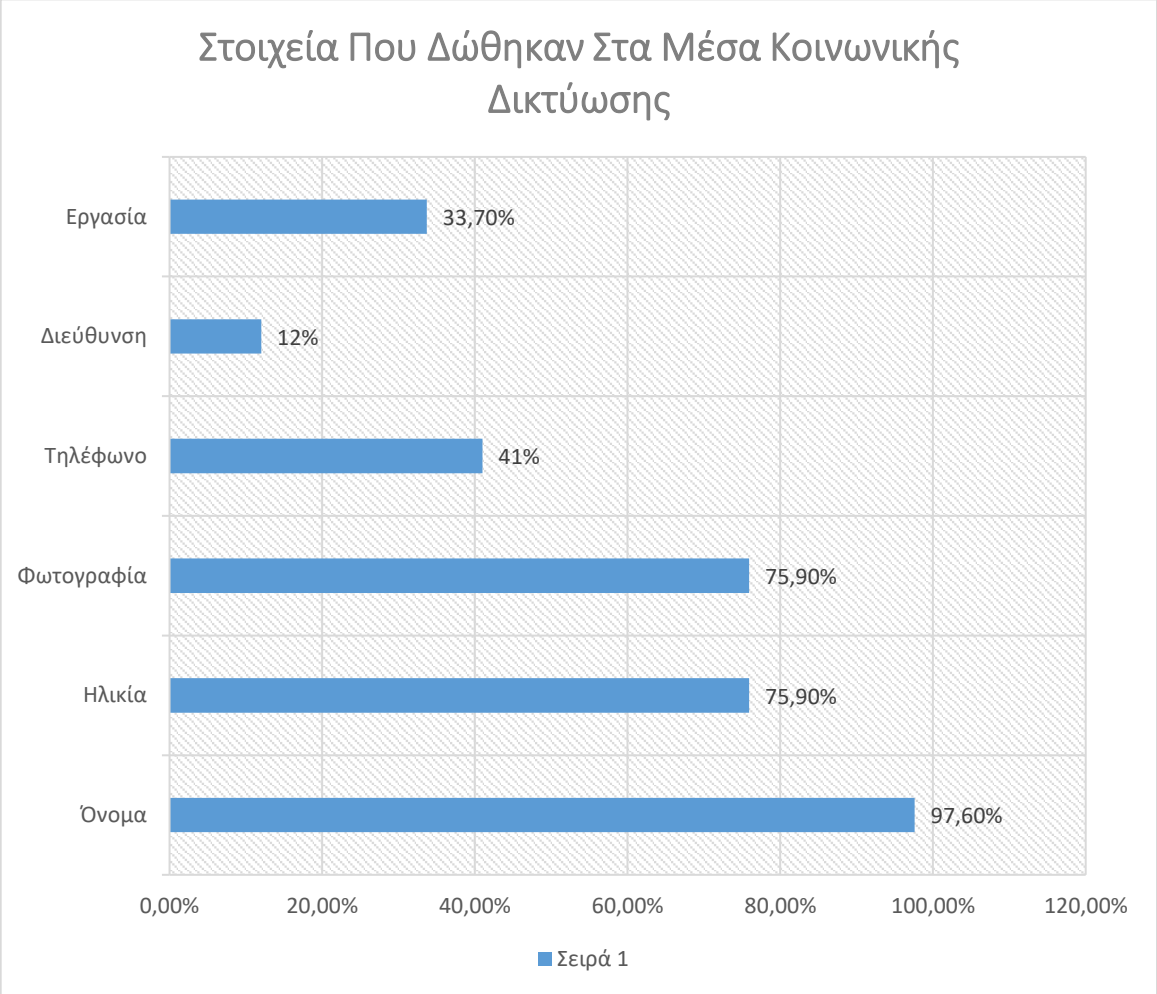
Η συντριπτική πλειοψηφία των χρηστών μέσον κοινωνικής δικτύωσης χρησιμοποιεί το facebook σε ποσοστό 96,3%. Αρκετά υψηλά ωστόσο παρουσιάζονται και τα ποσοστά του LinkedIn το οποίο χρησιμοποιείτε από το 31,7% του δείγματος.



Γράφημα 3.19: Δημοφιλέστερο Μέσον Κοινωνικής Δικτύωσης

- **Ποια από τα παρακάτω στοιχεία που έχετε δώσει στα δίκτυα κοινωνικής δικτύωσης είναι πραγματικά;**

Το όνομα (97,6%), η ηλικία (75,9%), και οι φωτογραφίες (75,9%) είναι από τα πιο συνήθης στοιχεία που παραχωρούν οι χρήστες στις ιστοσελίδες κοινωνικής δικτύωσης. Το πόρισμα δεν φαντάζει περίεργο καθώς η ιδιά η φύση των ιστοσελίδων επιταθεί την παραχωρήσει βασικών προσωπικών δεδομένων. Εντούτοις σημαντικό είναι και το ποσοστό το οποίο δεν διστάζει να παραχωρήσει στοιχεία επικοινωνίας με τους «διαδικτυακούς τους φίλους», όπως το τηλέφωνο που κατακτά ποσοστό 41%.



Γράφημα 3.20: Δοθέντα Στοιχεία

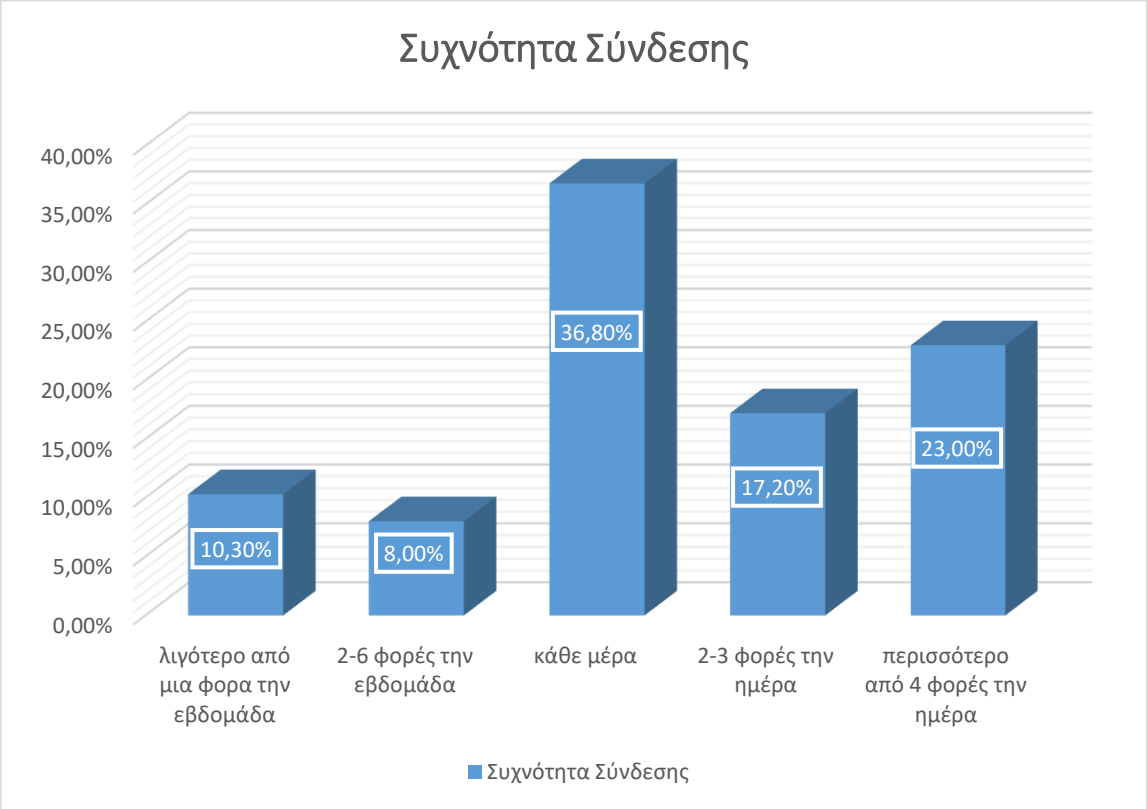
- **Ποσό συχνά επισκέπτεστε την σελίδα κοινωνικής δικτύωσης;**

Το μεγαλύτερο ποσοστό του δείγματος (36,8%) αναφέρει την καθημερινή χρήση των μέσων κοινωνικής δικτύωσης. Υψηλό είναι επίσης το ποσοστό που κάνει χρήση των μέσον περισσότερο από τέσσερίς (4) φορές την ημέρα (23,0%).

Συχνότητα Σύνδεσης

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	4	*4,6*	*4,6*	*4,6*
Λιγότερο από 1 φορά την εβδομάδα	*9*	*10,3*	*10,3*	*14,9*
Περισσότερο από 4 φορές την ημέρα	*20*	*23,0*	*23,0*	*37,9*
2-3 φορές την ημέρα	*15*	*17,2*	*17,2*	*55,2*
2-6 φορές την εβδομάδα	*7*	*8,0*	*8,0*	*63,2*
Κάθε μέρα	*32*	*36,8*	*36,8*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.18: Συχνότητα Σύνδεσης



Γράφημα 3.21: Συχνότητα Σύνδεσης

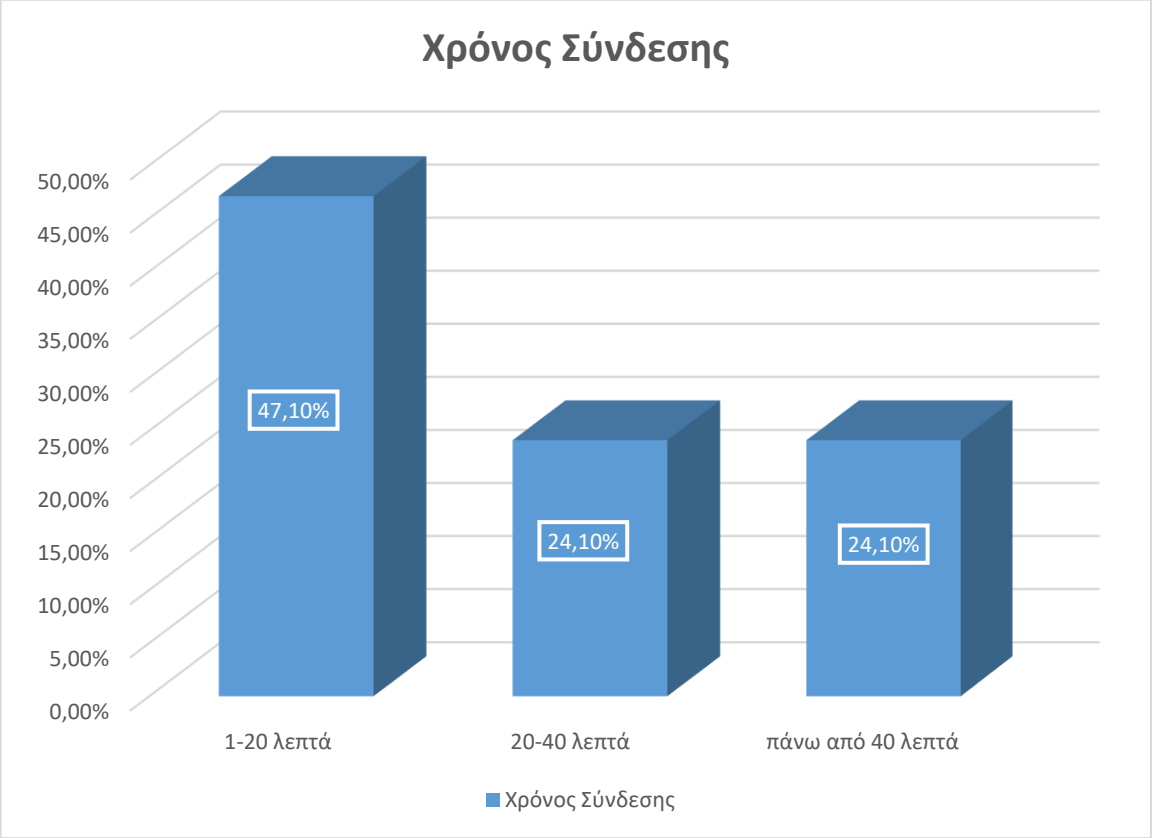
- **Ποσό χρόνο αφιερώνετε σε κάθε σας σύνδεση στην σελίδα κοινωνικής δικτύωσης;**

Ωστόσο παρατηρούμε πως η σύνδεση των χρηστών δεν διαρκεί περισσότερο από 20 λεπτά σύμφωνα με το 47,1% των ερωτηθέντων.

Χρόνος Σύνδεσης

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	4	*4,6*	*4,6*	*4,6*
>40 λεπτά	*21*	*24,1*	*24,1*	*28,7*
1-20 λεπτά	*41*	*47,1*	*47,1*	*75,9*
20-40 λεπτά	*21*	*24,1*	*24,1*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

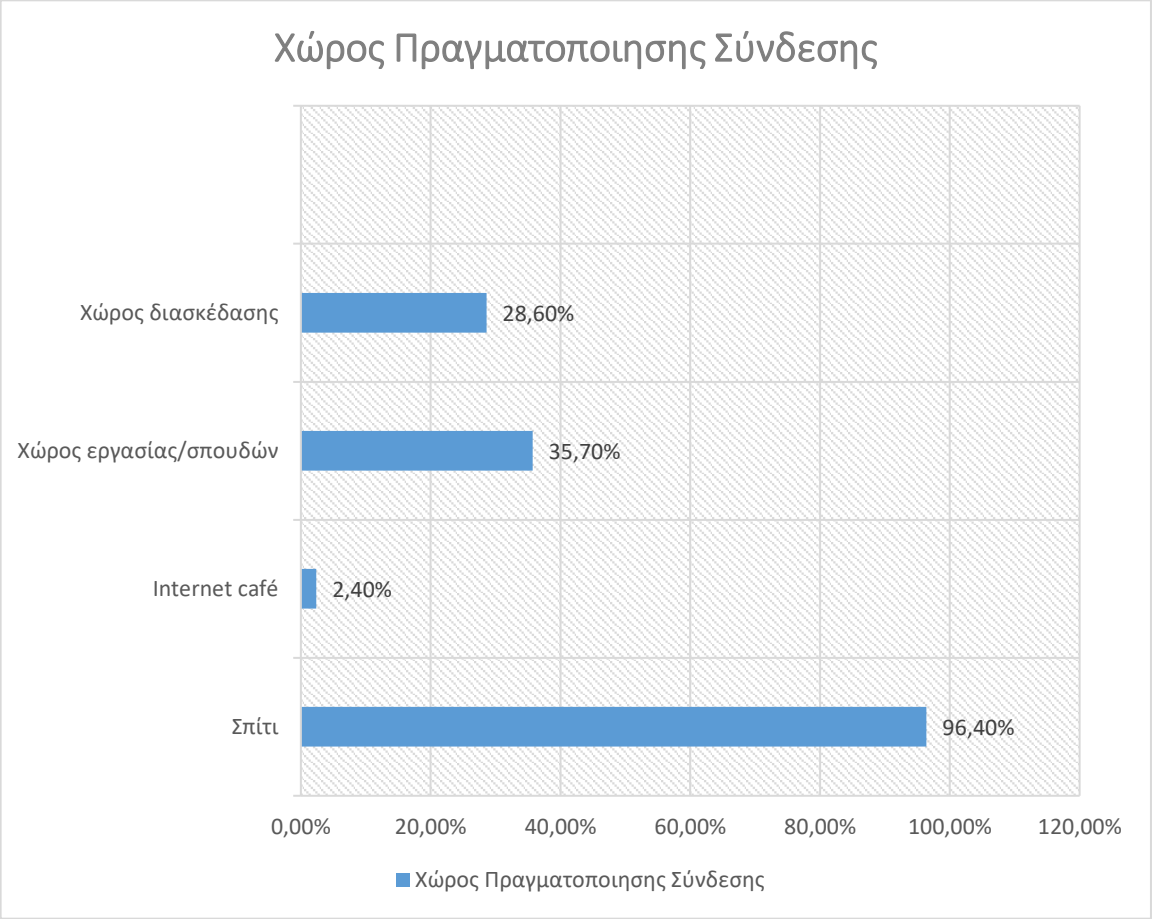
Πίνακας 3.19: Χρόνος Σύνδεσης



Γράφημα 3.22: Χρόνος Σύνδεσης

- **Η σύνδεση στον λογαριασμό σας πραγματοποιείτε από:**

Η σύνδεση στα μέσα κοινωνικής δικτύωσής γίνεται κυρίως από το σπίτι σε ποσοστό 96,4% αλλά και από των χώρο εργασίας και σπουδών (35,7%).



Γράφημα 3.23: Χώρος Σύνδεσης

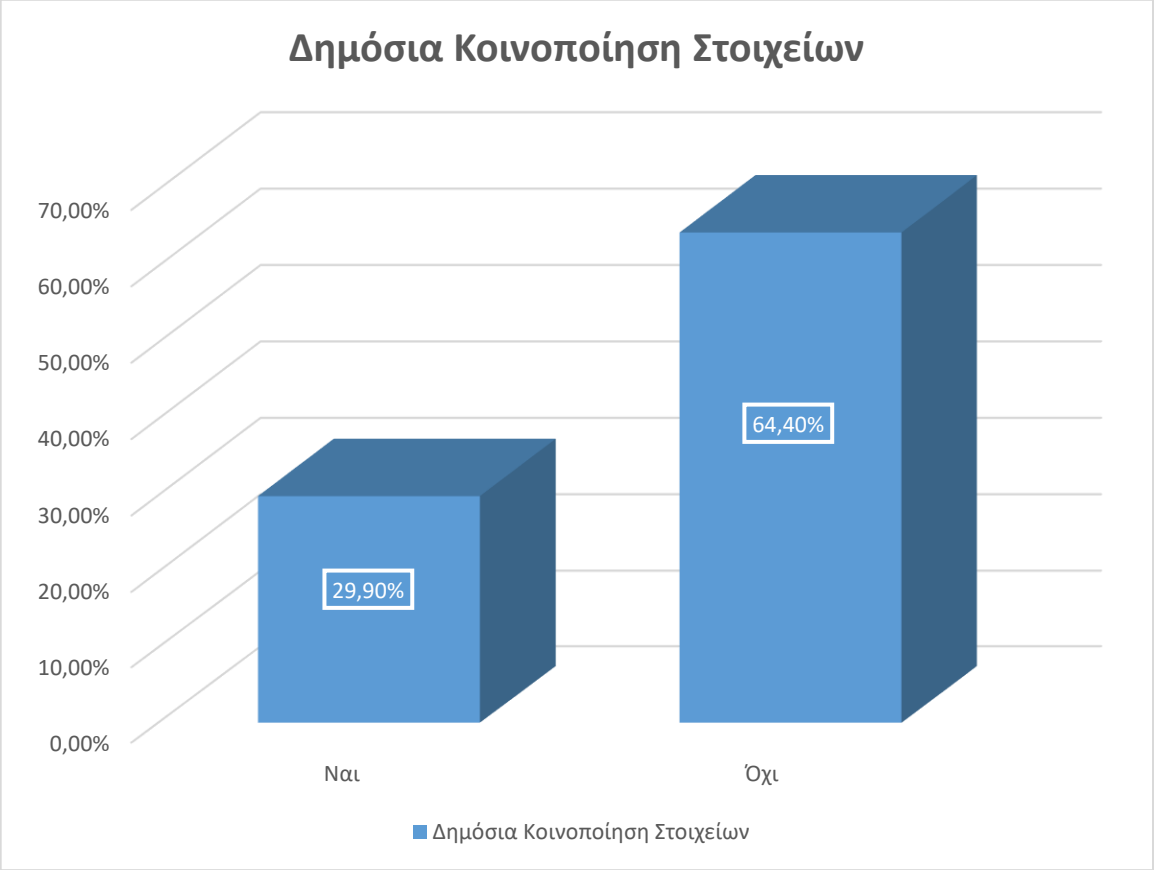
- **Τα προσωπικά σας στοιχεία είναι δημοσιά κοινοποιημένα στην σελίδα κοινωνικής δικτύωση σας;**

Περνώντας στην ασφάλεια των μέσων κοινωνικής δικτύωσης παρατηρούμε πως οι περισσότερο χρήστες επιλέγουν να μην εκθέτουν δημοσιά τα προσωπικά τους στοιχεία (64,4%) γεγονός που φανερώνει την επίγνωση των κίνδυνων που διατρέχουν στο διαδίκτυο.

Δημόσια Στοιχεία

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	5	*5,7*	*5,7*	*5,7*
Ναι	*26*	*29,9*	*29,9*	*35,6*
Όχι	*56*	*64,4*	*64,4*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.20: Δημόσια Κοινοποίηση Στοιχείων



Γράφημα 3.24: Δημόσια Κοινοποίηση Στοιχείων

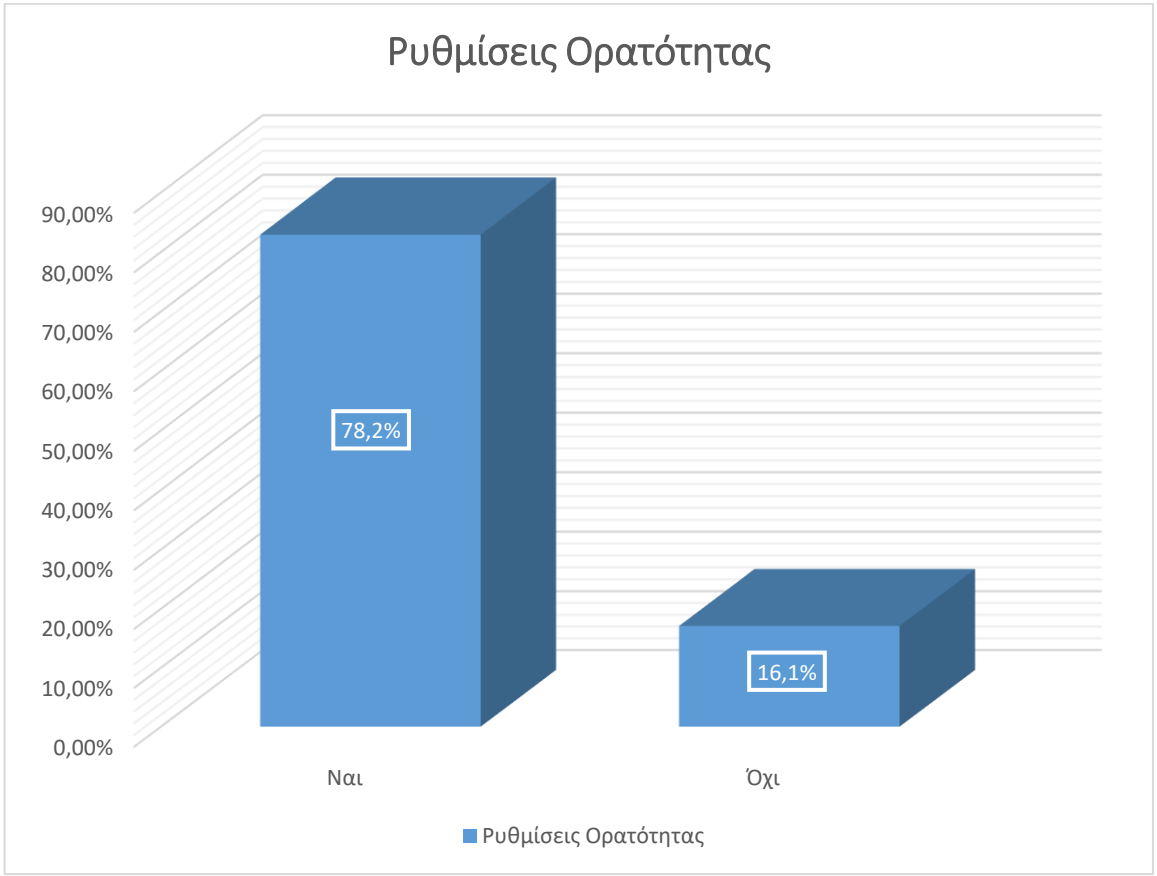
- **Έχετε κάνει τις απαραίτητες ρυθμίσεις ώστε να ελέγχεται σε ποιους είναι ορατά τα στοιχεία που αναρτάται;**

Επιπλέον έχουν πραγματοποιήσει τις ρυθμίσεις του λογαριασμού τους (78,2%) ώστε να αποφασίζουν οι ίδιοι την ορατότητα που θα έχουν στον υπόλοιπο ιστοτοπος.

Ορατότητα

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	5	*5,7*	*5,7*	*5,7*
Ναι	*68*	*78,2*	*78,2*	*83,9*
Όχι	*14*	*16,1*	*16,1*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 2.21: Ορατότητα



Γράφημα 3.25: Ορατότητα

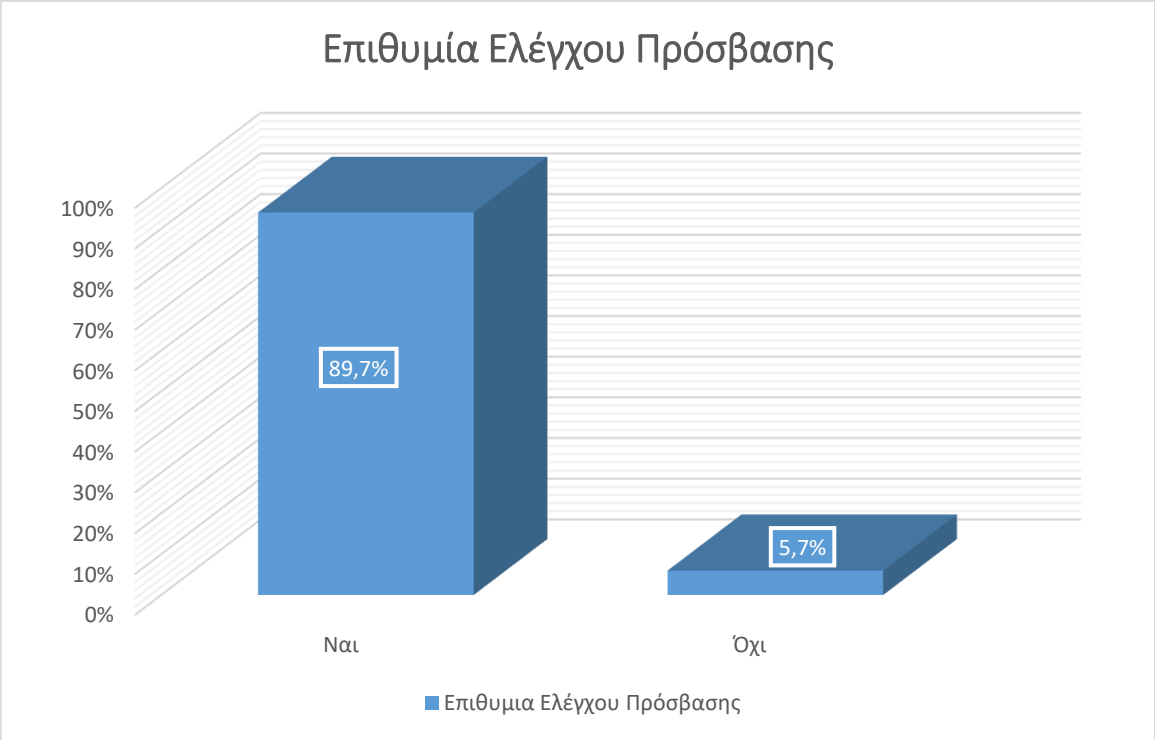
- **Θέλετε να μπορείτε να επιλέγατε ποιοι θα έχουν πρόσβαση στο περιεχόμενο που κοινοποιείται στο λογαριασμό σας;**

Σας συμπληρωματική ερώτηση, διερευνήθηκε πως οι χρήστες επιθυμούν να έχουν τον έλεγχο στην πρόσβαση και στην ορατότητα των δημοσιεύσεων τους σε ποσοστό 89,7%. Η απόκλιση που παρουσιάζεται από την προηγουμένη ερώτηση αναφορικά με τις ρυθμίσεις για να επιτευχθεί ο έλεγχος ενδεχομένως να οφείλετε στην ελλιπή πληροφόρηση των χρηστών για τα μετρά προφύλαξης που μπορούν να λάβουν.

Προσβασιμότητα

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	4	*4,6*	*4,6*	*4,6*
Ναι	*78*	*89,7*	*89,7*	*94,3*
Όχι	*5*	*5,7*	*5,7*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.22: Επιθυμία Ελέγχου Πρόσβασης



Γράφημα 3.26: Επιθυμία Ελέγχου Πρόσβασης

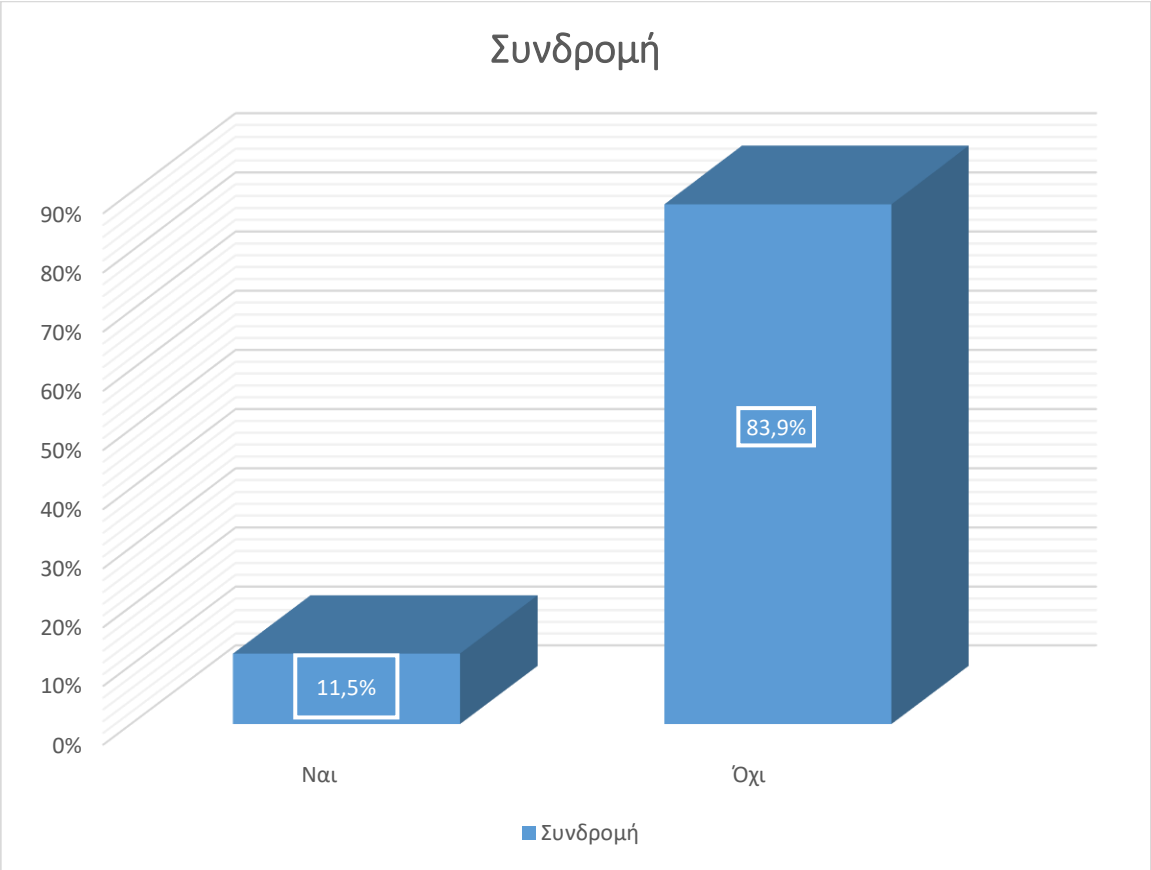
- **Θα συνεχίζατε να χρησιμοποιείτε τις σελίδες κοινωνικής δικτύωσης εάν απαιτούσαν συνδρομή;**

Η συνδρομή φαίνεται να αποτελεί ανασταλτικό παράγοντα στην χρήση των ιστοσελίδων κοινωνικής δικτύωσης με το 83,9% να δηλώνει πως θα διέκοπτε την χρήση τους σε περίπτωση που απαιτούνταν συνδρομή.

Συνδρομή

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	4	*4,6*	*4,6*	*4,6*
Ναι	*10*	*11,5*	*11,5*	*16,1*
Όχι	*73*	*83,9*	*83,9*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.23: Συνδρομή



Γράφημα 3.27: Συνδρομή

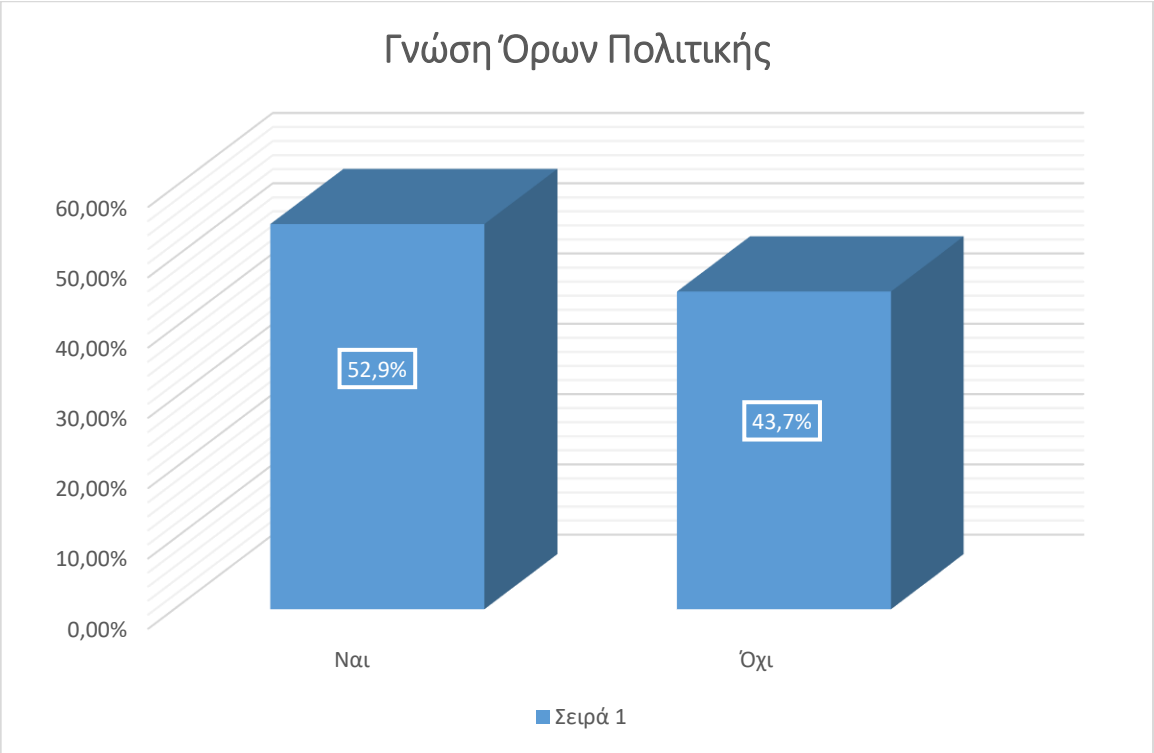
- **Έχετε διαβάσει τους «ορούς χρήσης» και την «πολίτικη απορρήτου» των σελίδων κοινωνικής δικτύωσης στις οποίες διαθέτετε λογαριασμούς;**

Οι οροί χρήσης των μέσων κοινωνικής δικτύωσης πάρα τον δεσμευτικό τους χαρακτήρα δεν επιτυγχάνουν την ενημέρωση του συνόλου των χρηστών, με το 43,7% να δηλώνει πως δεν έχει προβεί στην ανάγνωση των «ορών χρήσης» και «πολιτικής απορρήτου» των σελίδων.

Γνώση Όρων Πολιτικής

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	3	*3,4*	*3,4*	*3,4*
Ναι	*46*	*52,9*	*52,9*	*56,3*
Όχι	*38*	*43,7*	*43,7*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.24: Γνώση Όρων Πολιτικής



Γράφημα 3.28: Γνώση Όρων Πολιτικής

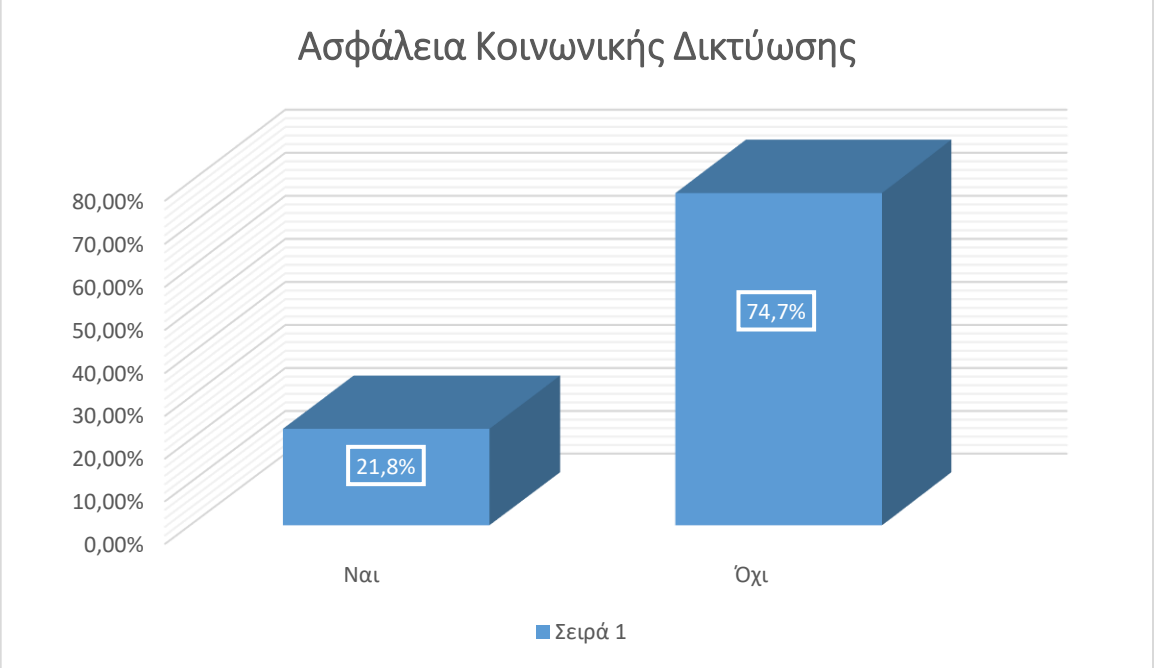
- **Θεωρείτε ότι οι σελίδες κοινωνικής δικτύωσης είναι ασφαλείς;**

Τέλος, ζητήσαμε από τους ερωτώμενους να απαντήσουν αν θεωρούν τα μέσα κοινωνικής δικτύωσης ασφαλή, μέσα από τα δικά τους βιώματα και ανάλογα με το ποσοστό που έχει θελήσει να ενημερωθεί ο καθένας επιλεγμένος χρήστης. Η γενική ανασφάλεια που αποτυπώθηκε στις παραπάνω ερωτήσεις εμφανίζεται και στην σύνοψη με το 74,7% να δηλώνουν πως νοιώθουν ανασφάλεια κατά την περιήγηση τους στα κοινωνικά μέσα.

Ασφάλεια

	Συχνότητα	*Ποσοστό*	*Έγκυρο ποσοστό*	*Αθροιστικό ποσοστό*
	3	*3,4*	*3,4*	*3,4*
Ναι	*19*	*21,8*	*21,8*	*25,3*
Όχι	*65*	*74,7*	*74,7*	*100,0*
Σύνολο	*87*	*100,0*	*100,0*	

Πίνακας 3.25: Ασφάλεια



Γράφημα 3.29: Ασφάλεια

3.6 Crosstabs

Με την χρήση του Στατιστικού Προγράμματος SPSS δημιουργήθηκαν οι παρακάτω διασταυρώσεις στο δείγμα της παρούσας έρευνας. Οι παρακάτω πίνακες και τα ραυδογράμματα βοηθούν στην περαιτέρω ανάλυση του δείγματος καθώς και στην άντληση ορθών συμπερασμάτων.[156] Παρακάτω παρατίθενται αναλυτικά τα πορίσματα:

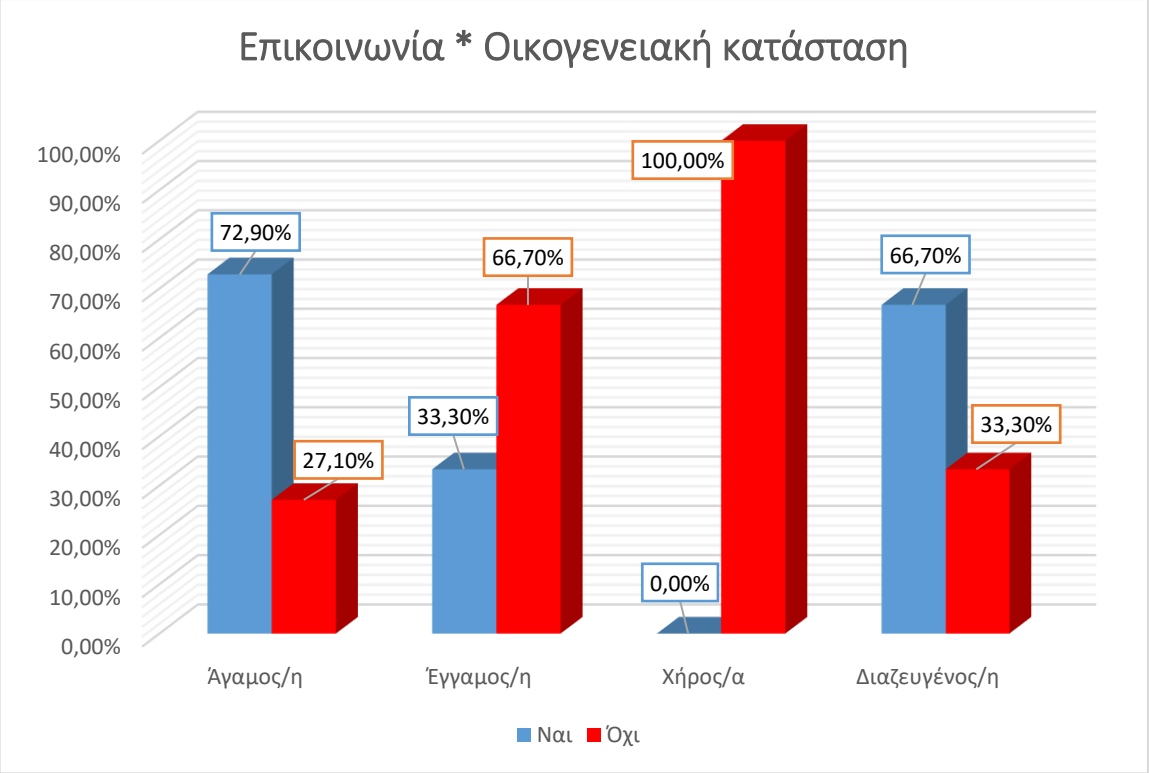
- *Οικογενειακή κατάσταση*Επικοινωνία*

Οικογενειακή κατάσταση*Επικοινωνία

			Επικοινωνία		**Σύνολο**
			Ναι	Όχι	
Οικογενειακή κατάσταση	Άγαμος	Συχνότητα	43	16	59
		Ποσοστό %	72,9%	27,1 %	100%
	Έγγαμος	Συχνότητα	8	16	24
		Ποσοστό %	33,3%	66,7 %	100%
	Χήρος	Συχνότητα	0	1	1
		Ποσοστό %	0%	100%	100%
	Διαζευγμένος	Συχνότητα	2	1	3
		Ποσοστό %	66,7%	33,3 %	100%

Πίνακας 3.26: Οικογενειακή κατάσταση*Επικοινωνία

[156] Η εικόνα των πινάκων που παρουσιάζονται δεν αντιστοιχεί στην αρχική εικόνα των outputs του στατιστικού προγράμματος SPSS. Τα δεδομένα που επιλέχθηκαν να παρουσιαστούν είναι τα απαραίτητα για την άντληση συμπερασμάτων. Τα αρχικά outputs παρατίθενται στην ενότητα «Παραρτήματα».



Γράφημα 3.30: Οικογενειακή κατάσταση*Επικοινωνία

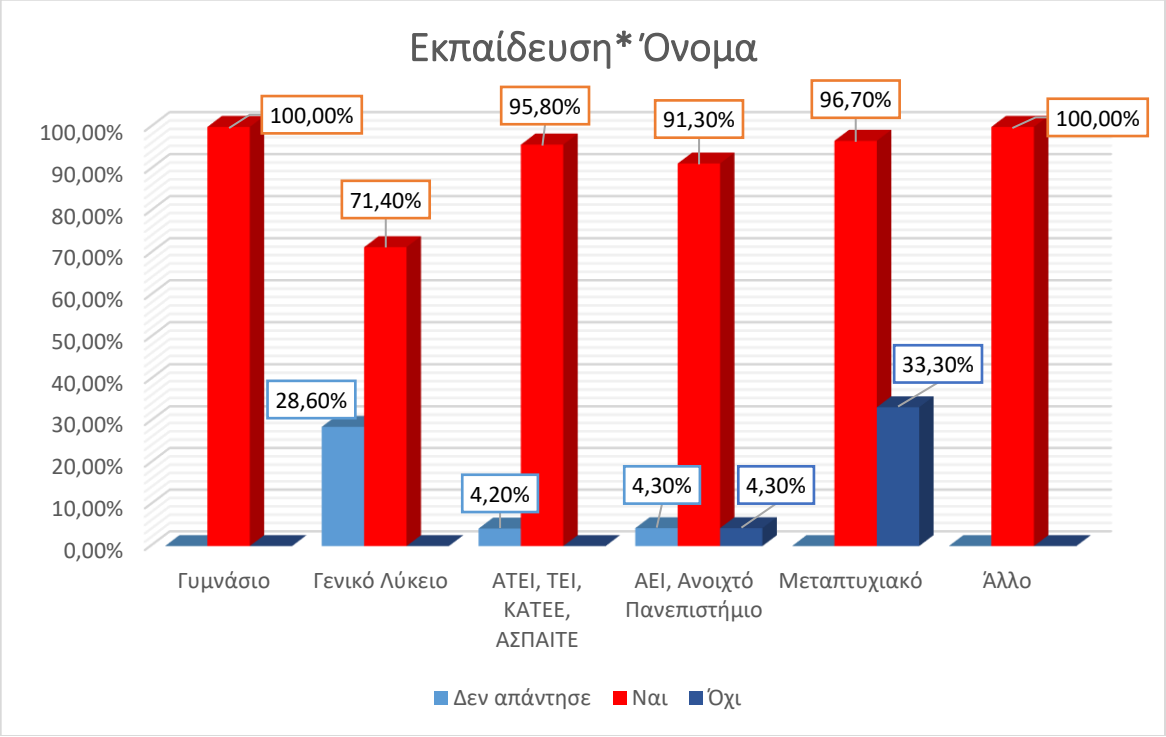
Το μεγαλύτερο ποσοστό των άγαμων ατόμων σε ποσοστό 72,9% χρησιμοποιεί το διαδίκτυο για λόγους επικοινωνίας. Εξίσου υψηλό είναι το ποσοστό και για τους διαζευγμένους. Εν αντιθέσει στους έγγαμους το ποσοστό είναι αρκετά χαμηλό, με το 33,3% να υποστηρίζουν πως η χρήση του διαδικτύου τους εξυπηρετεί στην επικοινωνία.

- *Εκπαίδευση* Όνομα*

Εκπαίδευση* Όνομα

			Όνομα			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	2	0	2
		Ποσοστό %	0,0%	100,0%	0,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	2	5	0	7
		Ποσοστό %	28,6%	71,4%	0,0%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	1	23	0	24
		Ποσοστό %	4,2%	95,8%	0,0%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	21	1	23
		Ποσοστό %	4,3%	91,3%	4,3%	100,0%
	Μεταπτυχιακό	Συχνότητα	0	29	1	30
		Ποσοστό %	0,0%	96,7%	33,3%	100,0%
	Άλλο	Συχνότητα	0	1	0	1
		Ποσοστό %	0,0%	100%	0,0%	100%

Πίνακας 3.27: Εκπαίδευση* Όνομα



Γράφημα 3.31 Εκπαίδευση* Όνομα

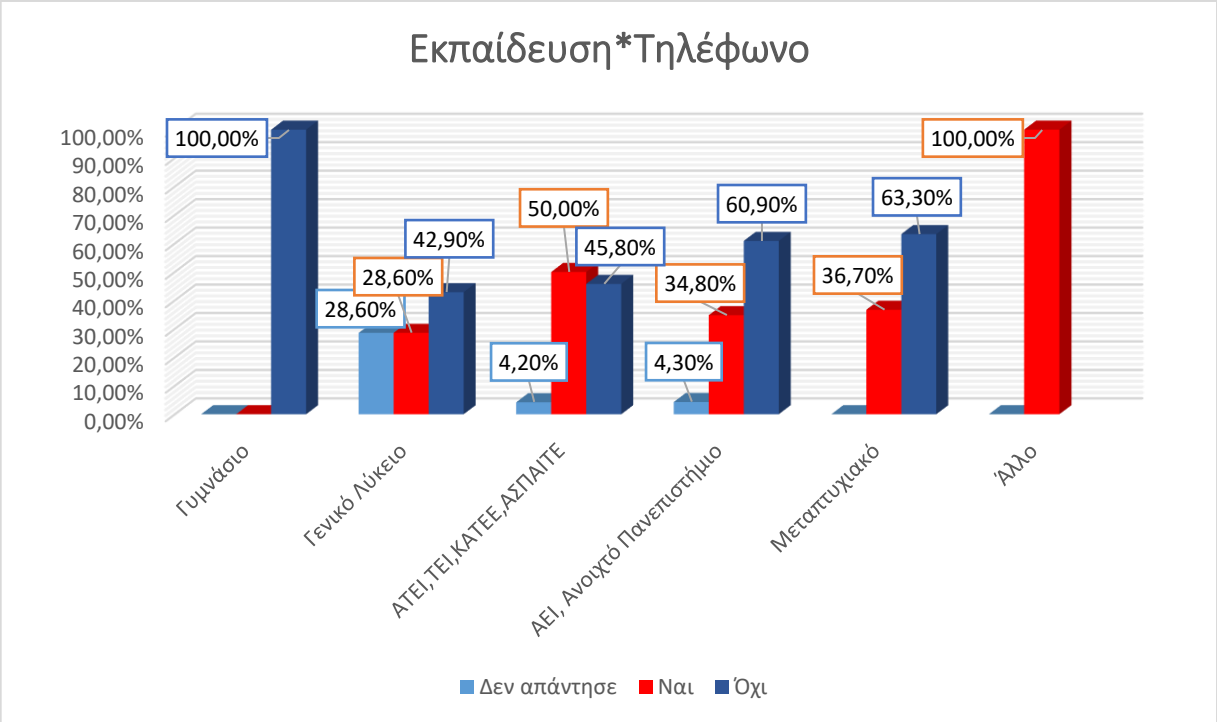
Η συντριπτική πλειοψηφία του δείγματος ανεξαρτήτως εκπαίδευσης υποστηρίζει πως έχει παραχωρήσει στα μέσα κοινωνικής δικτύωσης πραγματικό όνομα, σε ιδιαιτέρως υψηλά ποσοστά (από 71,4% έως 100% ανά κατηγορία επιπέδου εκπαίδευσης).

- *Εκπαίδευση* Τηλέφωνο*

Εκπαίδευση* Τηλέφωνο

			Τηλέφωνο			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	0	2	2
		Ποσοστό %	0,0%	0,0%	100,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	2	2	3	7
		Ποσοστό %	28,6%	28,6%	42,9%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	1	12	11	24
		Ποσοστό %	4,2%	50,0%	45,8%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	8	14	23
		Ποσοστό %	4,3&	34,8%	60,9%	100,0%
	Μεταπτυχιακό	Συχνότητα	0	11	19	30
		Ποσοστό %	0,0%	36,7%	63,3%	100,0%
	Άλλο	Συχνότητα	0	1	0	1
		Ποσοστό %	0,0%	100,0 %	0,0%	100,0%

Πίνακας 3.28: Εκπαίδευση* Τηλέφωνο



Γράφημα 3.32: Εκπαίδευση* Τηλέφωνο

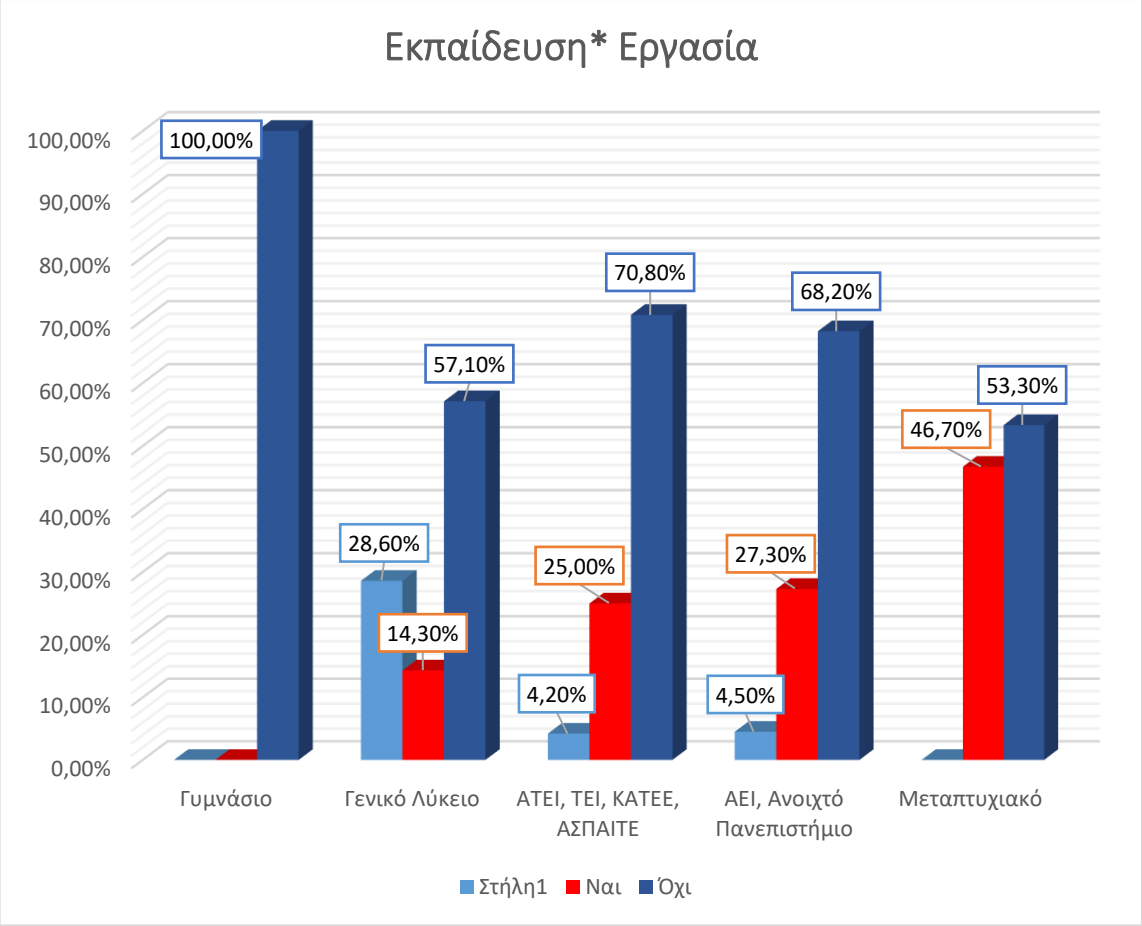
Αντιθέτως τα ποσοστά των ατόμων που παραχωρούν τον τηλεφωνικό τους αριθμό στα κοινωνικά δίκτυα είναι χαμηλά για όλες της βαθμίδες εκπαίδευσης. Ελαφριά αύξηση παρατηρείτε στην τριτοβάθμια εκπαίδευση, ενδεχομένως συνδυαστικά με την ενηλικίωση και την επαγγελματική καριέρα των ερωτώμενων.

- *Εκπαίδευση* Εργασία*

Εκπαίδευση* Εργασία

			Εργασία			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	0	2	2
		Ποσοστό %	0,0%	0,0%	100,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	2	1	4	7
		Ποσοστό %	28,6%	14,3%	57,1%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	1	6	17	24
		Ποσοστό %	4,2%	25,0%	70,8%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	6	15	22
		Ποσοστό %	4,5%	27,3%	68,2%	100,0%
	Μεταπτυχιακό	Συχνότητα	0	14	16	30
		Ποσοστό %	0,0%	46,7%	53,3%	100,0%
	Άλλο	Συχνότητα	0	1	0	1
		Ποσοστό %	0,0%	100,0%	0,0%	100,0%

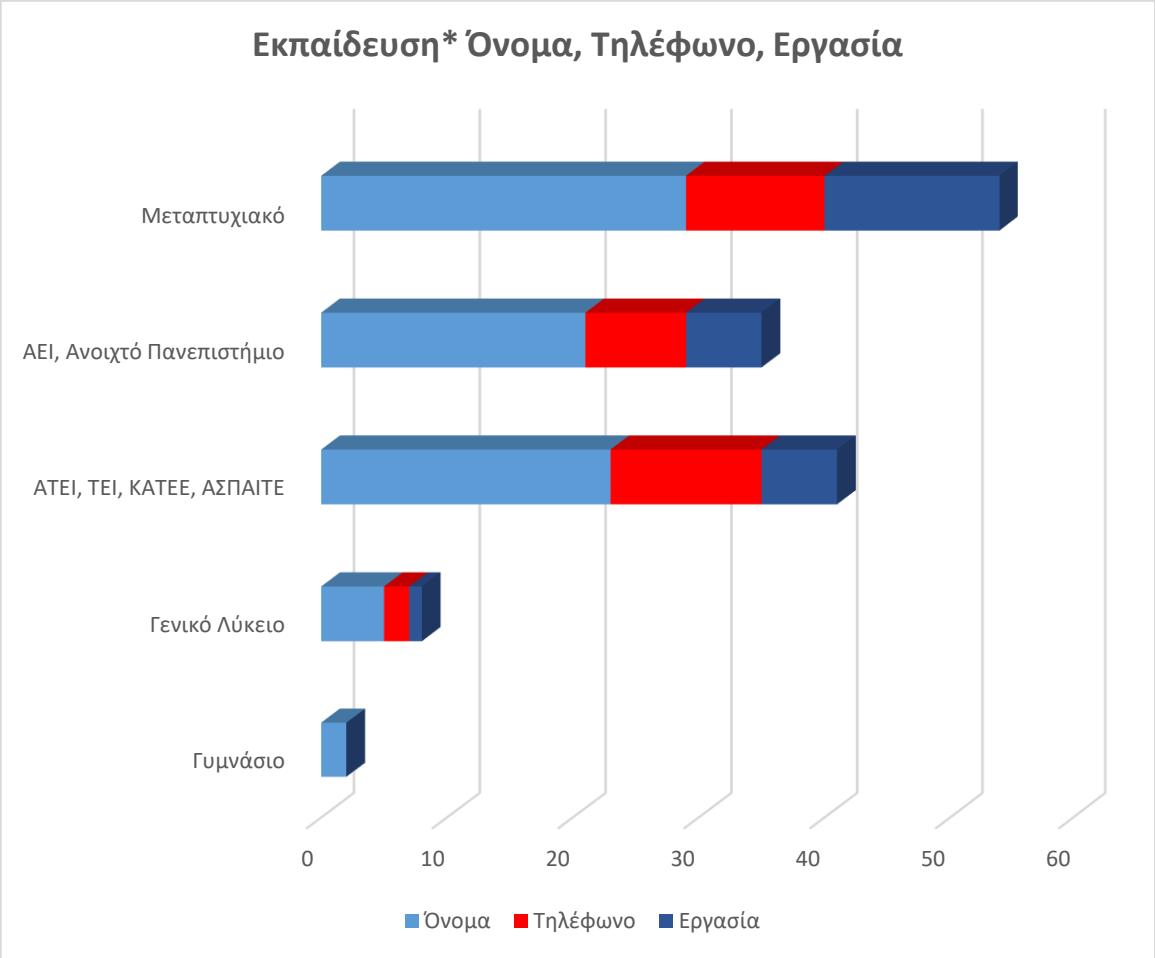
Πίνακας 3.29: Εκπαίδευση* Εργασία



Γράφημα 3.33: Εκπαίδευση* Εργασία

Το παραπάνω ενδεχόμενο επιβεβαιώνετε και από την σύνδεση της εκπαίδευσης με την αναφορά της εργασίας του υποκειμένου στις σελίδες κοινωνικής δικτύωσης. Παρατηρείτε αύξηση της καταγραφής της εργασιακής θέσης όσο αυξάνεται τι επίπεδο εκπαίδευσης. Πρέπει ωστόσο να επισημανθεί πως οι περισσότεροι ερωτώμενοι από όλες τις βαθμίδες εκπαίδευσης δεν επιθυμούν την καταγραφή της εργασιακής τους θέσης.

Συνοπτικά τα πορίσματα παρουσιάζονται στο παρακάτω γράφημα:



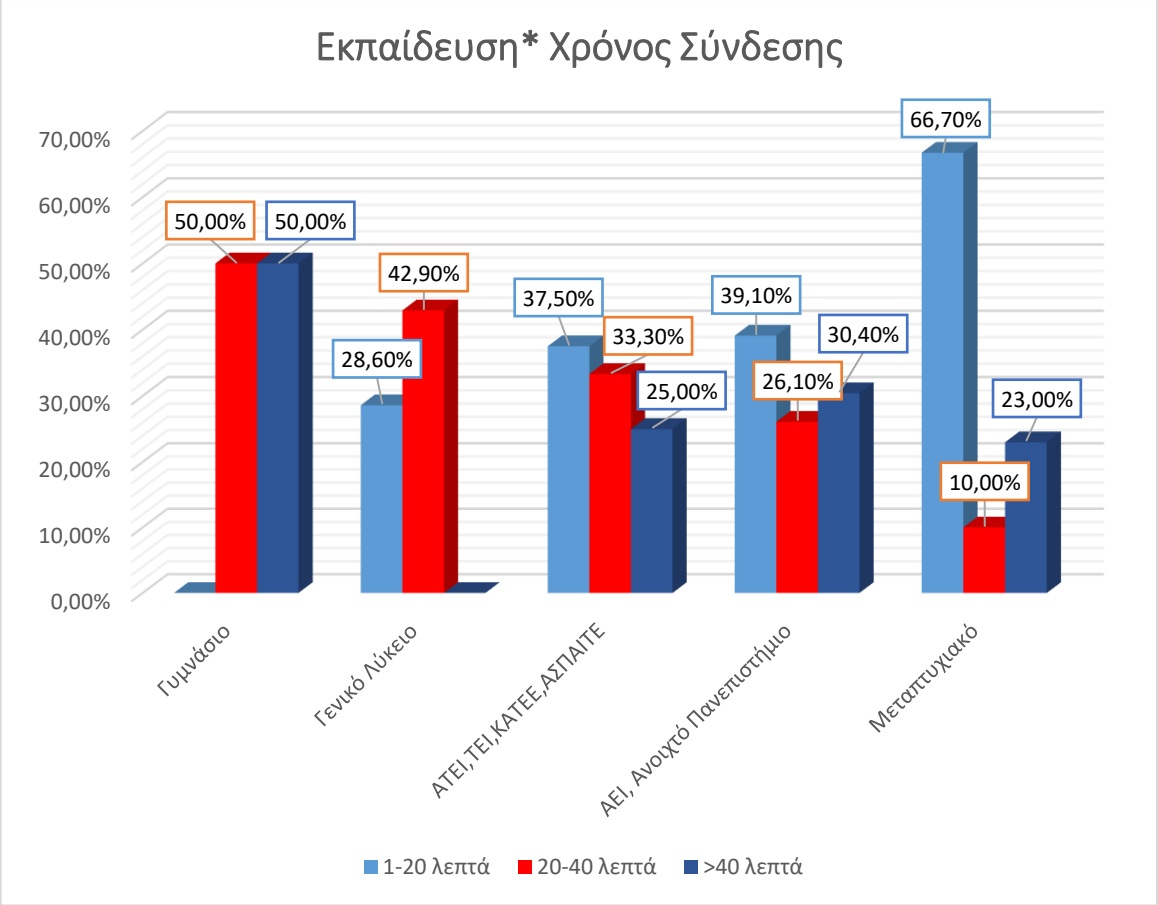
Γράφημα 3.34: Εκπαίδευση* Όνομα, Τηλέφωνο, Εργασία

- *Εκπαίδευση* Χρόνος Σύνδεσης*

Εκπαίδευση* Χρόνος Σύνδεσης

			Χρόνος Σύνδεσης				Σύνολο
			Δεν απάντησε	1-20 λεπτά	20-40 λεπτά	>40 λεπτά	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	0	1	1	2
		Ποσοστό %	0,0%	0,0%	50,0%	50,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	2	2	3	0	7
		Ποσοστό %	28,6%	28,6%	42,9%	0,0%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	1	9	8	6	24
		Ποσοστό %	4,2%	37,5%	33,3%	25,0%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	9	6	7	23
		Ποσοστό %	4,3%	39,1%	26,1%	30,4%	100,0%
	Μεταπτυχιακό	Συχνότητα	0	20	3	7	30
		Ποσοστό %	0,0%	66,7%	10,0%	23,0%	100,0%
	Άλλο	Συχνότητα	0	1	0	0	1
		Ποσοστό %	0,0%	100,0%	0,0%	0,0%	100,0%

Πίνακας 3.30: Εκπαίδευση* Χρόνος Σύνδεσης



Γράφημα 3.35: Εκπαίδευση* Χρόνος Σύνδεσης

Επιπλέον, η εκπαίδευση φαίνεται να κατέχει σημαντικό ρόλο στον χρόνο που παραμένει ο χρήστης της ιστοσελίδας συνδεδεμένος. Οι χρήστες της τριτοβάθμιας εκπαίδευσης τείνουν να παραμένουν για 1-20 λεπτά συνδεδεμένοι. Ιδιαιτέρως οι κάτοχοι μεταπτυχιακού τίτλου εμφανίζουν το υψηλότερο ποσοστό ολιγόλεπτης σύνδεσης με ποσοστό 66,7%. Οι χρήστες δευτεροβάθμιας εκπαίδευσης αφιερώνουν περισσότερο χρόνο στην κάθε σύνδεση τους. 20 έως 40 λεπτά σε ποσοστό 50% για τους χρήστες Γυμνασίου και 42,9% για τους χρήστες του Λυκείου. Το υψηλότερο ποσοστό για σύνδεση που υπερβαίνει τα 40 λεπτά παρουσιάζεται από χρήστες Γυμνασίου. Μπορούμε να συμπεράνουμε λοιπόν πως η ενασχόληση με τις ιστοσελίδες κοινωνικής δικτύωσης ελαττώνεται όσο αυξάνεται η ηλικία του χρήστη.

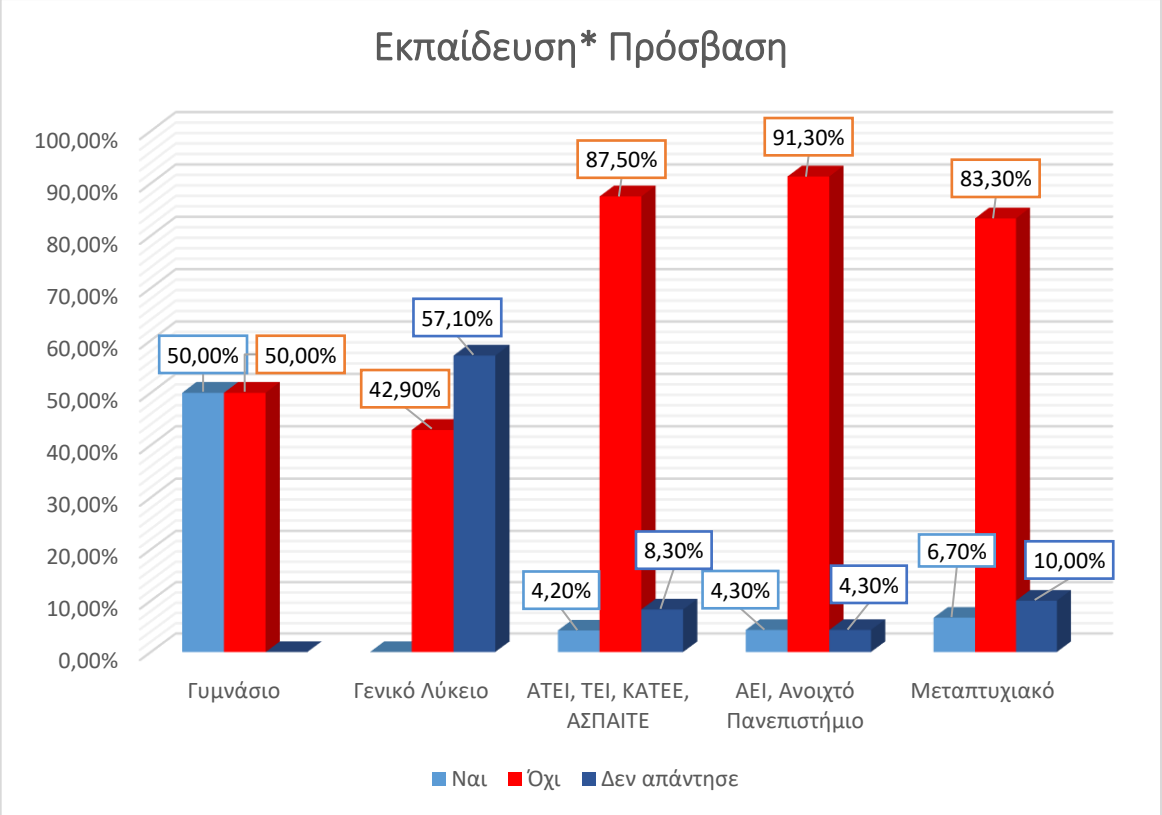
- *Εκπαίδευση*Πρόσβαση*

Παρακάτω εξετάστηκαν οι ενέργειες που έχουν κάνει τα υποκείμενα ως προς τις ιστοσελίδες που φυλάσουν τα προσωκά τους δεδομένα. Αναλυτικότερα, παρατηρούμε αν έχει ζητηθεί η πρόσβαση σε πληροφορίες που φυλάσονται με σκοπό την επικαιροποίηση ή την διαγραφή τους. Η διασταύρωση των στοιχείων έγινε με την χρήση του μορφωτικού επιπέδου, και βγήκαν τα παρακάτω πορίσματα:

Εκπαίδευση*Πρόσβαση

			Πρόσβαση			**Σύνολο**
			Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	1	1	2
		Ποσοστό %	0,0%	50,0%	50,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	4	0	3	7
		Ποσοστό %	57,1%	0,0%	42,9%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	2	1	21	24
		Ποσοστό %	8,3%	4,2%	87,5%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	1	21	23
		Ποσοστό %	4,3%	4,3%	91,3%	100,0%
	Μεταπτυχιακό	Συχνότητα	3	2	25	30
		Ποσοστό %	10,0%	6,7%	83,3%	100,0%
	Άλλο	Συχνότητα	0	0	1	1
		Ποσοστό %	0,0%	0,0%	100,0%	100%

Πίνακας 3.31: Εκπαίδευση*Πρόσβαση



Γράφημα 3.36: Εκπαίδευση*Πρόσβαση

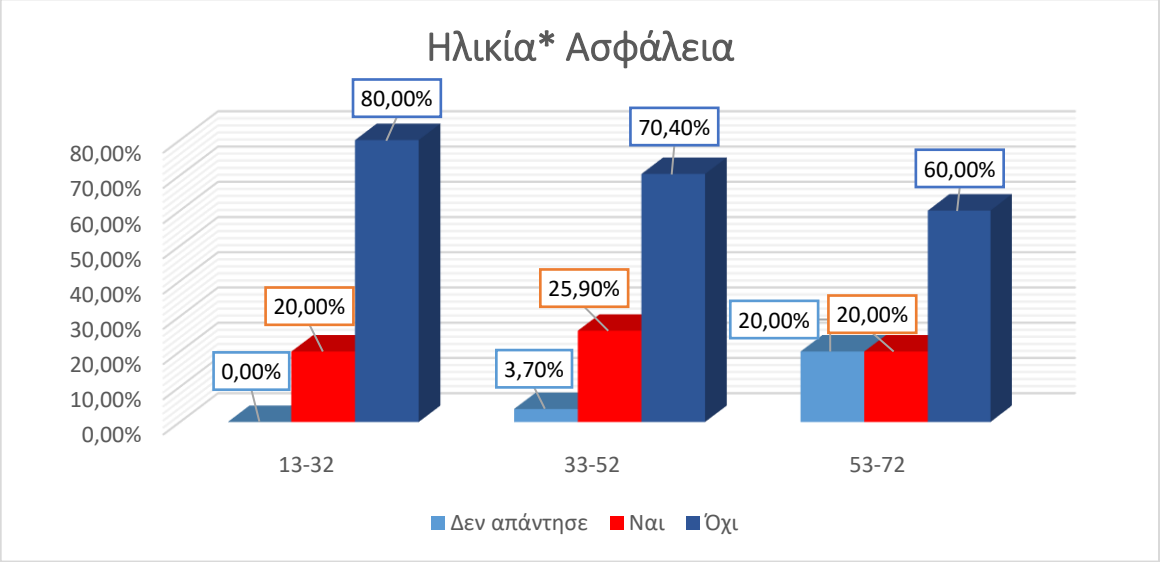
Τα άτομα που έχουν λάβει μόρφωση Γυμνασίου, τα οποία κατά πάσαν πιθανότητα πρόκειται για πιο νεαρά σε ηλικία άτομα, έχουν προβεί σε ενέργειες πιστοποίησης των προσωπικών τους στοιχείων, σε αντίθεση με τις υπόλοιπες βαθμίδες εκπαίδευσης στις οποίες τα ποσοστά είναι ιδιαιτέρως χαμηλά (0,0% για τα άτομα με Λυκειακή μόρφωση, 4,20% και 4,30% για την τριτοβάθμια εκπαίδευση, και 6,70% για τους κατόχους μεταπτυχιακού).

- *Ηλικία* Ασφάλεια*

Ηλικία* Ασφάλεια

			Ασφάλεια			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	0	10	40	50
		Ποσοστό %	0,0%	20,0%	80,0%	100,0%
	33-52	Συχνότητα	1	7	19	27
		Ποσοστό %	3,7%	25,9%	70,4%	100,0%
	53-72	Συχνότητα	2	2	6	10
		Ποσοστό %	20,0%	20,0%	60,0%	100,0%
	Σύνολο	Συχνότητα	3	19	65	87
		Ποσοστό %	3,4%	21,8%	74,7%	100,0%

Πίνακας 3.32: Ηλικία* Ασφάλεια



Γράφημα 3.37: Ηλικία* Ασφάλεια

Διασταυρώνοντας στις ηλικιακές ομάδες των ερωτώμενων με την αίσθηση ασφάλειας που τους προσφέρουν οι ιστοσελίδες κοινωνικής δικτύωσης παρατηρούμε πως η ανασφάλεια είναι έντονη και στις τρεις (3) ηλικιακές ομάδες. Πιο συγκεκριμένα, τα άτομα ηλικίας 13 με 32 ετών έχουν πιο έντονο το αίσθημα του φόβου για τα προσωπικά τους δεδομένα κατά την πλοήγηση τους με ποσοστό 80,0%. Έπεται η μεσαία ηλικιακή κλάση με 70,40%. Αξίζει να επισημάνουμε πως στη μεσαία ηλικιακή ομάδα παρατηρούνται τα υψηλότερα επίπεδα ασφάλειας, της τάξεως του 25,9%.

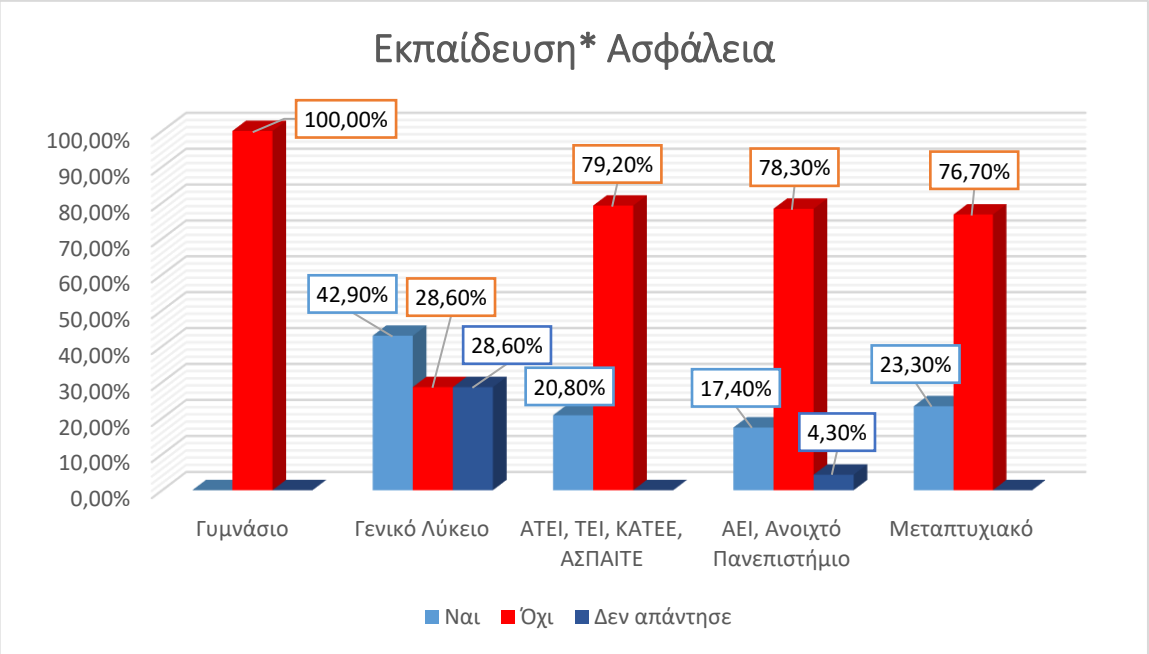
- *Εκπαίδευση* Ασφάλεια*

Θέλοντας να εντρυφήσουμε περισσότερο στα επίπεδα αίσθησης ασφάλειας των χρηστών αναλύθηκε η σχέση που μπορεί να φέρει η μόρφωση των ερωτώμενων με την αίσθηση ασφάλειας. Τα αποτελέσματα παρουσιάζονται στον πίνακα 3.33. Όλες οι εκπαιδευτικές βαθμίδες πέραν του Λυκείου παρουσιάζουν ιδιαιτέρως υψηλά ποσοστά ανασφάλειας.

Εκπαίδευση* Ασφάλεια

			Ασφάλεια			**Σύνολο**
			Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση	Γυμνάσιο	Συχνότητα	0	0	2	2
		Ποσοστό %	0,0%	0,0%	100,0%	100,0%
	Γενικό Λύκειο	Συχνότητα	2	3	2	7
		Ποσοστό %	28,6%	42,9%	28,6%	100,0%
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	Συχνότητα	0	5	19	24
		Ποσοστό %	0,0%	20,8%	79,2%	100,0%
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Συχνότητα	1	4	18	23
		Ποσοστό %	4,3%	17,4%	78,3%	100,0%
	Μεταπτυχιακό	Συχνότητα	0	7	23	30
		Ποσοστό %	0,0%	23,3%	76,7%	100,0%
	Άλλο	Συχνότητα	0	0	1	1
		Ποσοστό %	0,0%	0,0%	100,0%	100,0%
Σύνολο		Συχνότητα	3	19	65	87
		Ποσοστό%	3,4%	21,8%	74,7%	100,0%

Πίνακας 3.33: Εκπαίδευση* Ασφάλεια



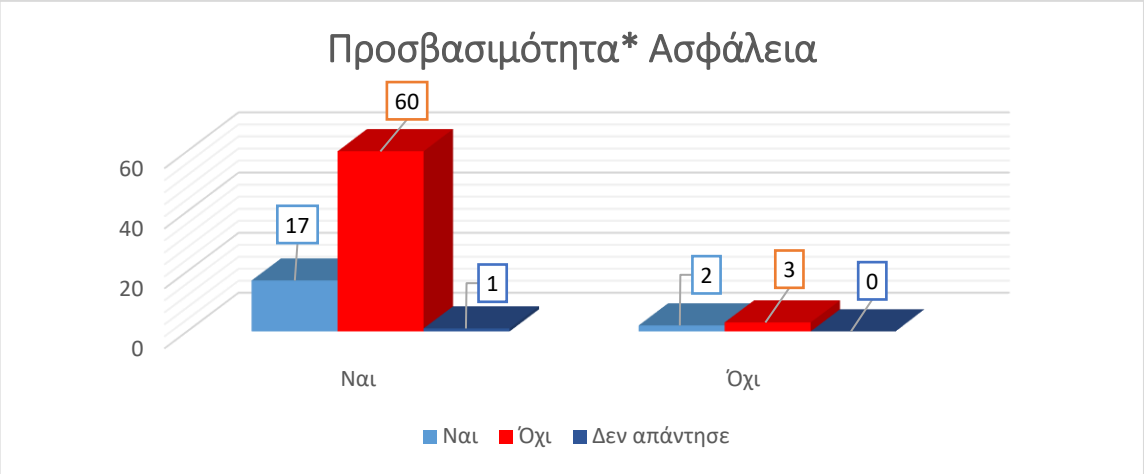
Γράφημα 3.38: Εκπαίδευση* Ασφάλεια

- *Προσβασιμότητα* Ασφάλεια*

Προσβασιμότητα* Ασφάλεια

			Ασφάλεια			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα	Δεν απάντησε	Συχνότητα	2	0	2	4
		Ποσοστό %	50,0%	0,0%	50,0%	100,0%
	Ναι	Συχνότητα	1	17	60	78
		Ποσοστό %	1,3%	21,8%	76,9%	100,0%
	Όχι	Συχνότητα	0	2	3	5
		Ποσοστό %	0,0%	40,0%	60,0%	100,0%
Σύνολο		Συχνότητα	3	19	65	87
		Ποσοστό %	3,4%	21,8%	74,7%	100,0%

Πίνακας 3.34: Προσβασιμότητα* Ασφάλεια



Γράφημα 3.39: Προσβασιμότητα* Ασφάλεια

Επιχειρώντας την κατανόηση της διαδικτυακής συμπεριφοράς των χρηστών εντός των ιστοσελίδων δικτύωσης συσχετίστηκαν οι απαντήσεις που δόθηκαν αναφορικά με την επιθυμία τους να επιλέγουν την πρόσβαση στις αναρτήσεις τους και την ασφάλεια που νιώθουν στις ίδιες ιστοσελίδες. Όπως φανερώνεται και από τον πίνακα3.34, τα υψηλότερα ποσοστά παρουσιάζονται στην επιθυμία των χρηστών να έχουν τον πλήρη έλεγχο πρόσβασης στις πληροφορίες που οι ίδιοι αναρτούν. Αυτή η απάντηση συνοδεύεται σε ποσοστό 76,9% με την ανασφάλεια που τους δημιουργούν οι ιστοσελίδες. Επιπλέον το 21,8% νιώθει ασφάλεια στα μέσα επιθυμεί τον έλεγχο της πρόσβασης σαν δικλείδα ασφαλείας. Το ραβδόγραμμα 3.38 φανερώνει τις συχνότητες των ερωτώμενων αναφορικά με την προσβασιμότητα και την ασφάλεια. Παρατηρείται επίσης αρκετά χαμηλή συχνότητα στα άτομα που δεν επιθυμούν να έχουν τον έλεγχο στις κοινοποιήσεις τους.[157]

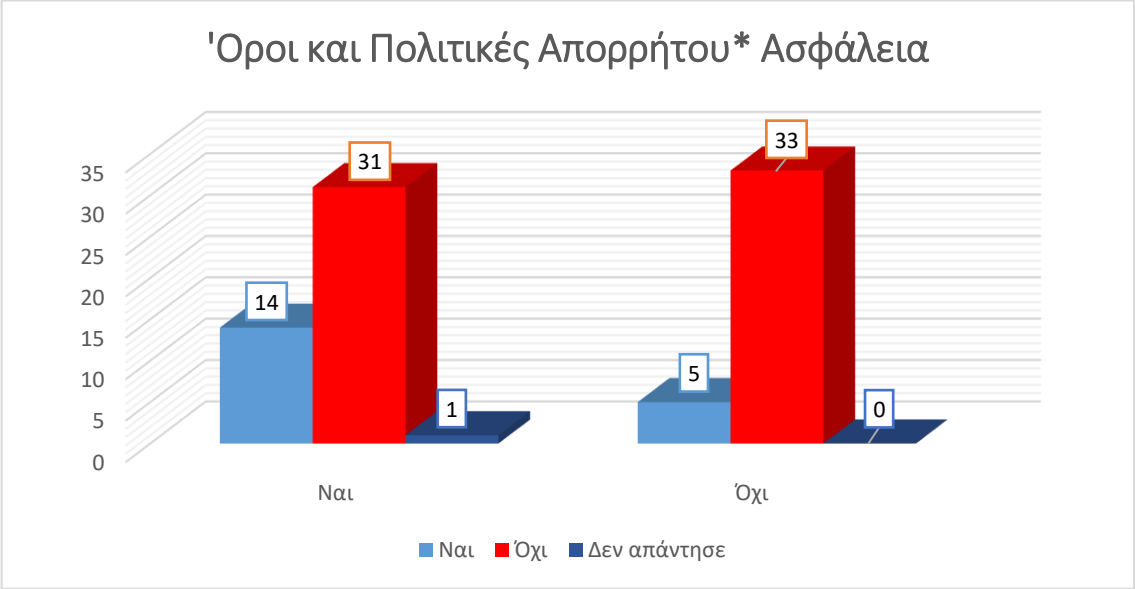
[157] Στο ραβδόγραμμα προτιμήθηκε η χρήση συχνοτήτων για να μπορέσει να φανερωθεί η αριθμητική υπεροχή των απαντήσεων και να εξαχθούν πιο ακριβή συμπεράσματα.

- *Όροι και πολιτικές απορρήτου* Ασφάλεια*

Όροι και πολιτικές απορρήτου* Ασφάλεια

			Ασφάλεια			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Όροι και πολιτικές απορρήτου	Δεν απάντησε	Συχνότητα	2	0	1	3
		Ποσοστό %	66,7%	0,0%	33,3%	100,0%
	Ναι	Συχνότητα	1	14	31	46
		Ποσοστό %	2,2%	30,4%	67,4%	100,0%
	Όχι	Συχνότητα	0	5	33	38
		Ποσοστό %	0,0%	13,2%	86,8%	100,0%
Σύνολο		Συχνότητα	3	19	65	87
		Ποσοστό %	3,4%	21,8%	74,7%	100,0%

Πίνακας 3.35: Όροι και πολιτικές απορρήτου* Ασφάλεια



Γράφημα 3.40: Όροι και πολιτικές απορρήτου* Ασφάλεια

Θέλοντας να διερευνηθούν όλες οι αιτίες που μπορεί να φέρουν την ανασφάλεια των χρηστών σε τόσο υψηλά επίπεδα διασταυρώθηκε με την ανάγνωση ή όχι των όρων χρήσης και της πολιτικής απορρήτου των εν λόγω ιστοσελίδων. Τα αποτελέσματα παρουσιάζονται αναλυτικά στον πίνακα3.35 όπου παρατηρείτε ένα υψηλό ποσοστό χρηστών (86,8%) που παραδέχεται πως ενώ δεν έχει διαβάσει τους όρους χρήσης και τις πολιτικές απορρήτου αισθάνεται ανασφάλεια. Αντίθετα, από τους χρήστες που έχουν προβεί σε ανάγνωση των όρων και των πολιτικών φαίνεται να αισθάνονται πιο ασφαλής σε ποσοστό 30,4%.

- *Ηλικία* Facebook, Twitter, LinkedIn, Pinterest, Άλλο*

Ηλικία* Facebook

			Facebook			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	1	48	1	50
		Ποσοστό %	2,0%	96,0%	2,0%	100,0%
	33-52	Συχνότητα	1	26	0	27
		Ποσοστό %	3,7%	96,3%	0,0%	100,0%
	53-72	Συχνότητα	3	5	2	10
		Ποσοστό %	30,0%	50,0%	20,0%	100,0%
	Σύνολο	Συχνότητα	5	79	3	87
		Ποσοστό %	5,7%	90,8%	3,4%	100,0%

Πίνακας 3.36: Ηλικία* Facebook

Ηλικία* Twitter

			Twitter			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	1	18	31	50
		Ποσοστό %	2,0%	36,0%	62,0%	100,0%
	33-52	Συχνότητα	1	5	21	27
		Ποσοστό %	3,7%	18,5%	77,8%	100,0%
	53-72	Συχνότητα	3	0	7	10
		Ποσοστό %	30,0%	0,0%	70,0%	100,0%
	Σύνολο	Συχνότητα	5	23	59	87
		Ποσοστό %	5,7%	26,4%	67,8%	100,0%

Πίνακας 3.37: Ηλικία* Twitter

Ηλικία* LinkedIn

			LinkedIn			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	1	14	35	50
		Ποσοστό %	2,0%	28,0%	70,0%	100,0%
	33-52	Συχνότητα	1	9	17	27
		Ποσοστό %	3,7%	33,3%	63,0%	100,0%
	53-72	Συχνότητα	3	3	4	10
		Ποσοστό %	30,0%	30,0%	40,0%	100,0%
	Σύνολο	Συχνότητα	5	26	56	87
		Ποσοστό %	5,7%	29,9%	64,4%	100,0%

Πίνακας3.38: Ηλικία* LinkedIn

Ηλικία* Pinterest

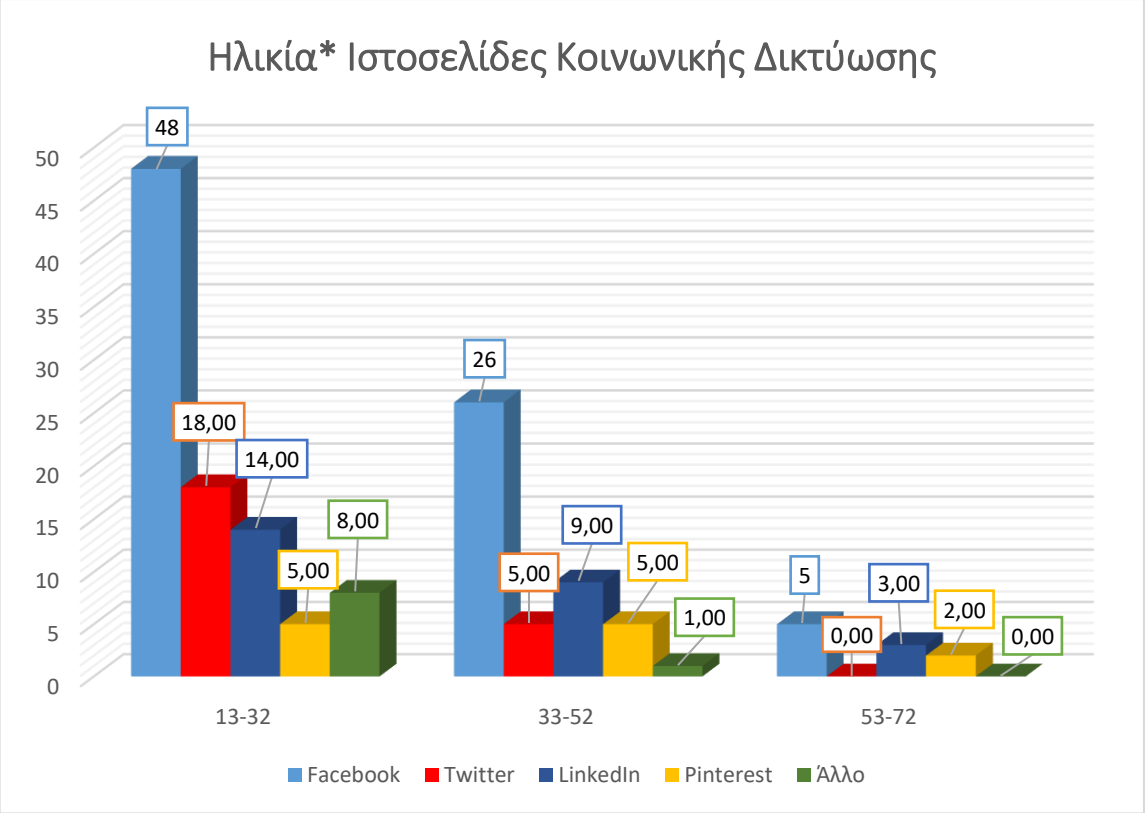
			Pinterest			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	1	5	44	50
		Ποσοστό %	2,0%	10,0%	88,0%	100,0%
	33-52	Συχνότητα	1	5	21	27
		Ποσοστό %	3,7%	18,5%	77,8%	100,0%
	53-72	Συχνότητα	3	2	5	10
		Ποσοστό %	30,0%	20,0%	50,0%	100,0%
	Σύνολο	Συχνότητα	5	12	70	87
		Ποσοστό %	5,7%	13,8%	80,5%	100,0%

Πίνακας 3.39: Ηλικία* Pinterest

Ηλικία* Άλλο

			Άλλο			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Ηλικία	13-32	Συχνότητα	1	8	41	50
		Ποσοστό %	2,0%	16,0%	82,0%	100,0%
	33-52	Συχνότητα	1	1	25	27
		Ποσοστό %	3,7%	3,7%	92,6%	100,0%
	53-72	Συχνότητα	3	0	7	10
		Ποσοστό %	30,0%	0,0%	70,0%	100,0%
	Σύνολο	Συχνότητα	5	9	73	87
		Ποσοστό %	5,7%	10,3%	83,9%	100,0%

Πίνακας 3.40: Ηλικία* Άλλο



Γράφημα 3.41: Ηλικία* Ιστοσελίδες Κοινωνικής Δικτύωσης

Στο γράφημα 3.40 παρατηρείται η συχνότητα χρήσης ορισμένων ιστοσελίδων κοινωνικής δικτύωσης ανά ηλικιακή ομάδα. Φανερή είναι η υπεροχή του Facebook έναντι των άλλων ιστοσελίδων με ιδιαιτέρως υψηλά ποσοστά (13-32 με 96,0%. 33-52 με 96,3%, 53-72 με 50,0%) κατατάσσοντας το ως την δημοφιλέστερη ιστοσελίδα κοινωνικής δικτύωσης (πίνακας 3.36). Ακολουθεί το Twitter για τους νεότερους χρήστες, ενώ για την ηλικιακή κλάση 33-52 ο διαδικτυακός ιστότοπος ευρέσεως εργασίας κατακτά την δεύτερη θέση στη προτίμηση των χρηστών.

- *Προσβασιμότητα* Facebook, Twitter, LinkedIn, Pinterest*

Προσβασιμότητα* Facebook

			Facebook			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα	Δεν απάντησε	Συχνότητα	4	0	0	4
		Ποσοστό %	100,0%	0,0%	0,0%	100,0%
	Ναι	Συχνότητα	1	74	3	78
		Ποσοστό %	1,3%	94,9%	3,8%	100,0%
	Όχι	Συχνότητα	0	5	0	5
		Ποσοστό %	0,0%	100,0%	0,0%	100,0%
Σύνολο		Συχνότητα	5	79	3	87
		Ποσοστό %	5,7%	90,8%	3,4%	100,0%

Πίνακας 3.41: Προσβασιμότητα* Facebook

Προσβασιμότητα* Twitter

			Twitter			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα	Δεν απάντησε	Συχνότητα	4	0	0	4
		Ποσοστό %	100,0%	0,0%	0,0%	100,0%
	Ναι	Συχνότητα	1	22	55	78
		Ποσοστό %	1,3%	28,2%	70,5%	100,0%
	Όχι	Συχνότητα	0	1	4	5
		Ποσοστό %	0,0%	20,0%	80,0%	100,0%
Σύνολο		Συχνότητα	5	23	59	87
		Ποσοστό %	5,7%	26,4%	67,8%	100,0%

Πίνακας 3.42: Προσβασιμότητα* Twitter

Προσβασιμότητα* LinkedIn

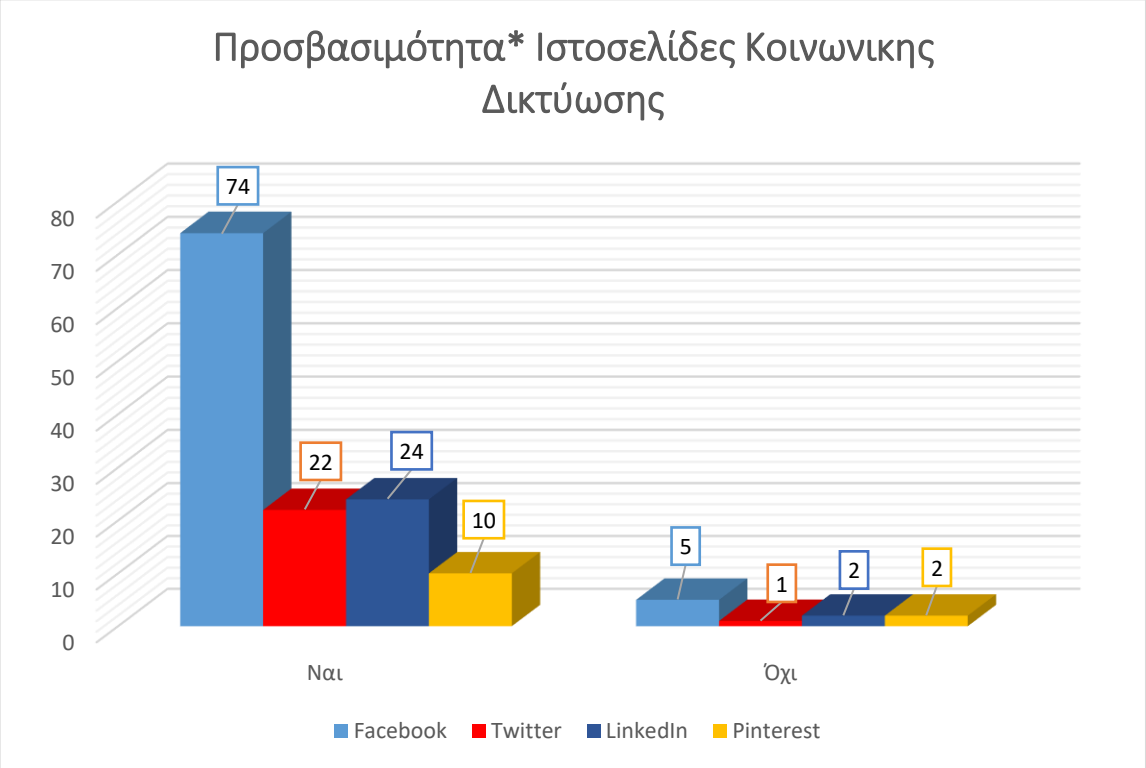
			LinkedIn			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα	Δεν απάντησε	Συχνότητα	4	0	0	4
		Ποσοστό %	100,0%	0,0%	0,0%	100,0%
	Ναι	Συχνότητα	1	24	53	78
		Ποσοστό %	1,3%	30,8%	67,9%	100,0%
	Όχι	Συχνότητα	0	2	3	5
		Ποσοστό %	0,0%	40,0%	60,0%	100,0%
Σύνολο		Συχνότητα	5	26	56	87
		Ποσοστό %	5,7%	29,9%	64,4%	100,0%

Πίνακας 3.43: Προσβασιμότητα* LinkedIn

Προσβασιμότητα* Pinterest

			Pinterest			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα	Δεν απάντησε	Συχνότητα	4	0	0	4
		Ποσοστό %	100,0%	0,0%	0,0%	100,0%
	Ναι	Συχνότητα	1	10	67	78
		Ποσοστό %	1,3%	12,8%	85,9%	100,0%
	Όχι	Συχνότητα	0	2	3	5
		Ποσοστό %	0,0%	40,0%	60,0%	100,0%
Σύνολο		Συχνότητα	5	12	70	87
		Ποσοστό %	5,7%	13,8%	80,5%	100,0%

Πίνακας 3.44: Προσβασιμότητα* Pinterest



Γράφημα 3.42: Προσβασιμότητα* Ιστοσελίδες Κοινωνικής Δικτύωσης

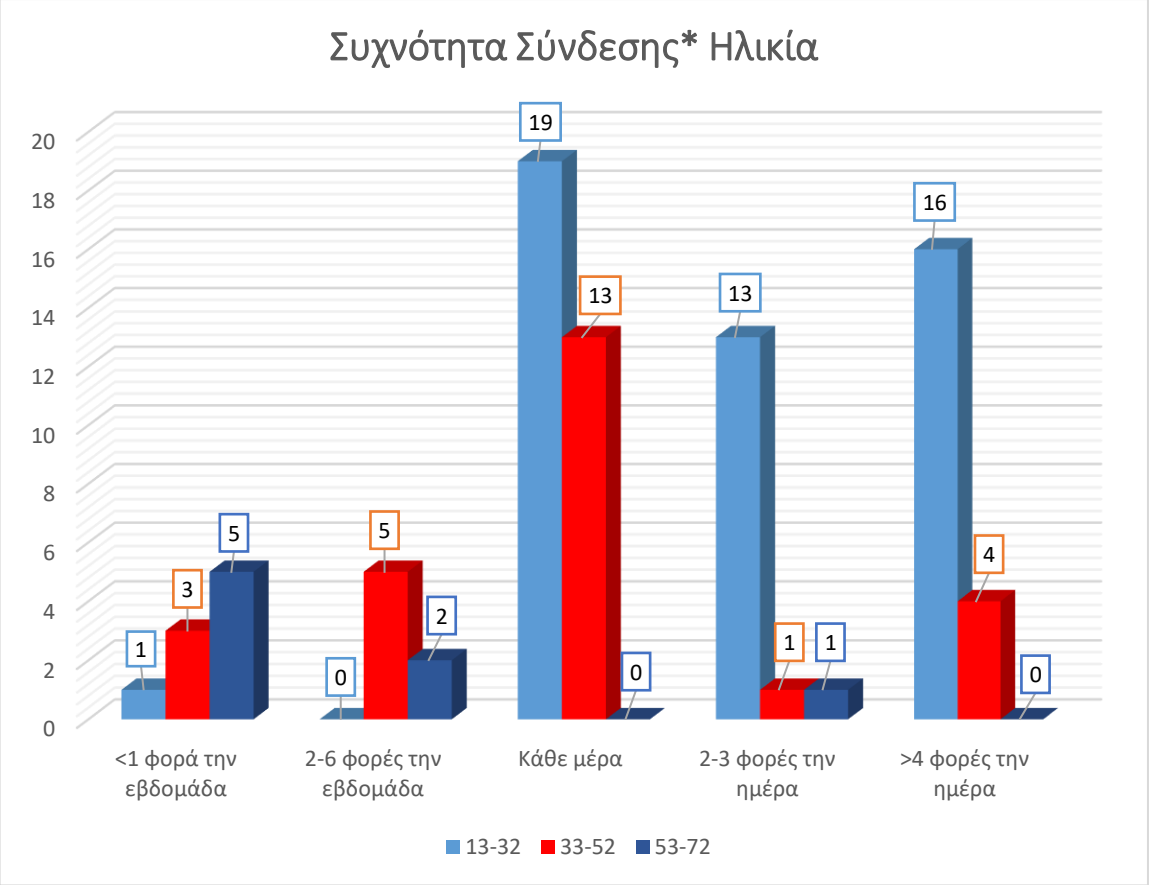
Κατά την διασταύρωση των ερωτήσεων περί επιθυμίας των χρηστών να επιλέγουν ποιοι θα βλέπουν το περιεχόμενο τω κοινοποιήσεων τους ανά σελίδα κοινωνικής δικτύωσης φανερώθηκε η καθολική επιθυμία για έλεγχο. Όπως αποδεικνύει το ραβδόγραμμα, η ιστοσελίδα δεν κατέχει κύριο ρόλο στην επιθυμία αυτή, αλλά είναι η γενική βούληση των χρηστών για έλεγχο της πρόσβασης σε κάθε είδους ιστοσελίδες.

- *Συχνότητα Σύνδεσης* Ηλικία*

Συχνότητα Σύνδεσης* Ηλικία

			Ηλικία			Σύνολο
			13-32	33-52	53-72	
Συχνότητα Σύνδεσης	Δεν απάντησε	Συχνότητα	1	1	2	4
		Ποσοστό %	25,0%	25,0%	50,0%	100,0%
	<1 φορά την εβδομάδα	Συχνότητα	1	3	5	9
		Ποσοστό %	11,1%	33,3%	55,6%	100,0%
	2-6 φορές την εβδομάδα	Συχνότητα	0	5	2	7
		Ποσοστό %	0,0%	71,4%	28,6%	100,0%
	Κάθε μέρα	Συχνότητα	19	13	0	32
		Ποσοστό %	59,4%	40,6%	0,0%	100,0%
	2-3 φορές την ημέρα	Συχνότητα	13	1	1	15
		Ποσοστό %	86,7%	6,7%	6,7%	100,0%
	>4 φορές την ημέρα	Συχνότητα	16	4	0	20
		Ποσοστό %	80,0%	20,0%	0,0%	100,0%
Σύνολο		Συχνότητα	50	27	10	87
		Ποσοστό %	57,5%	31,0%	11,5%	100,0%

Πίνακας 3.45: Συχνότητα Σύνδεσης* Ηλικία



Γράφημα 3.43: Συχνότητα Σύνδεσης* Ηλικία

Οι ηλικιακές ομάδες που δημιουργήθηκαν φαίνεται να διαφέρουν αισθητά μεταξύ τους ως προς την συχνότητα σύνδεσης στις ιστοσελίδες κοινωνικής δικτύωσης. Οι νεότεροι 13 έως 32 ετών έχουν την τάση να συνδέονται συχνότερα στις συγκεκριμένες ιστοσελίδες με το 38,0% της κλάσης να δηλώνει πως συνδέεται καθημερινά και το 32,0% περισσότερο από 4 φορές ημερησίως. Η ηλικιακή κατηγορία 33-52 ετών φαίνεται να εισέρχεται λιγότερο με το 48,1% να εισέρχεται καθημερινά και το 18,5% 2 έως 6 φορές την εβδομάδα. Στην τρίτη ηλικιακή κλάση το 50,0% δηλώνει πως εισέρχεται έως μια φορά την εβδομάδα.

Correlations

		Ηλικία	Συχνότητα_Σύνδεσης
Ηλικία	Pearson Correlation	1	-,579**
	Sig. (2-tailed)		,000
	N	87	87
Συχνότητα_ Σύνδεσης	Pearson Correlation	-,579**	1
	Sig. (2-tailed)	,000	
	N	87	87

**. Correlation is significant at the 0.01 level (2-tailed).

Πίνακας 3.46: Correlation Συχνότητα Σύνδεσης* Ηλικία

Δημιουργώντας έναν πίνακα συσχέτισης των μεταβλητών «ηλικία» και «συχνότητα σύνδεσης» παρατηρούμε πως η συσχέτιση τους είναι 0,579. Όπως παρατηρούμε από την μήτρα συσχέτισης ζητήθηκε η δημιουργία επιπέδου σημαντικότητας two-tailed. 87 ζεύγη τιμών (85 βαθμοί ελευθερίας) συντέλεσαν στον υπολογισμό της συσχέτισης του πίνακα 3.46. Η συσχέτιση είναι σημαντική σε επίπεδο σημαντικότητας 0.01 (1%)[158]. Συμπερασματικά βλέπουμε πως υπάρχει μια θετική συσχέτιση ανάμεσα στην ηλικία και την συχνότητα σύνδεσης ($r = 0{,}579$, $df = 85$, $p < 0.001$). Μέσα από την συσχέτιση φανερώνεται πως όσο αυξάνεται η ηλικία του ατόμου, τόσο μειώνεται η συχνότητα σύνδεσης στα μέσα κοινωνικής δικτύωσης.

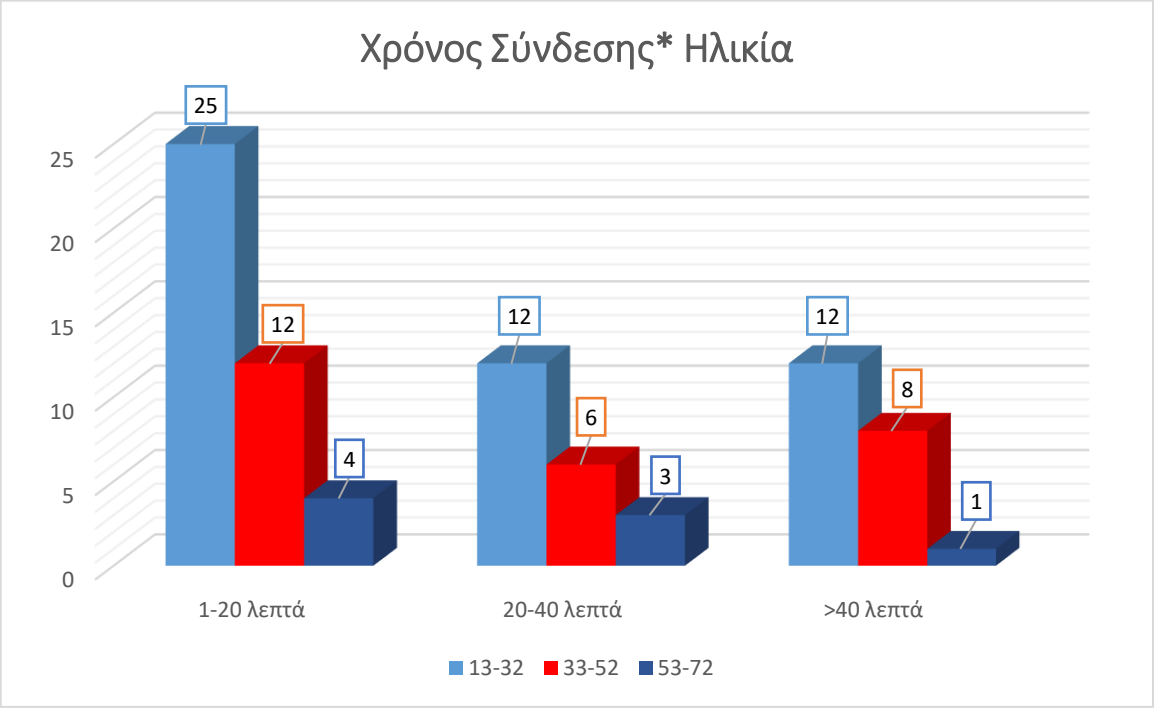
[158] Έχει επισημανθεί και από το στατιστικό πρόγραμμα που χρησιμοποιήθηκε (SPSS).

- *Χρόνος Σύνδεσης* Ηλικία*

Χρόνος Σύνδεσης* Ηλικία

			Ηλικία			Σύνολο
			13-32	33-52	53-72	
Χρόνος Σύνδεσης	Δεν απάντησε	Συχνότητα	1	1	2	4
		Ποσοστό %	25,0%	25,0%	50,0%	100,0%
	1-20 λεπτά	Συχνότητα	25	12	4	41
		Ποσοστό %	61,0%	29,3%	9,8%	100,0%
	20-40 λεπτά	Συχνότητα	12	6	3	21
		Ποσοστό %	57,1%	28,6%	14,3%	100,0%
	>40 λεπτά	Συχνότητα	12	8	1	21
		Ποσοστό %	57,1%	38,1%	4,8%	100,0%
Σύνολο		Συχνότητα	50	27	10	87
		Ποσοστό %	57,5%	31,0%	11,5%	100,0%

Πίνακας 3.47: Χρόνος Σύνδεσης* Ηλικία



Γράφημα 3.44: Χρόνος Σύνδεσης* Ηλικία

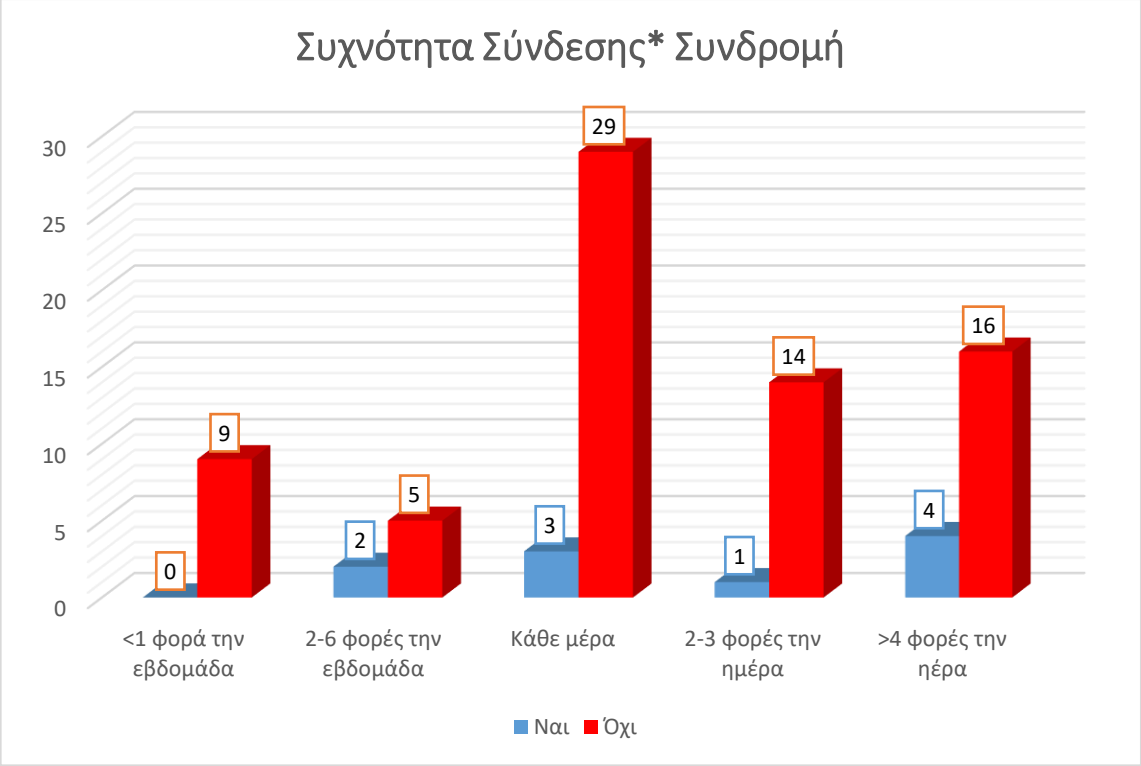
Όσον αφορά τον χρόνο σύνδεσης τα αποτελέσματα φαίνεται να είναι κοινά για όλες τις ηλικιακές κλάσης. Η πλειοψηφία των χρηστών των ηλικιακών ομάδων 13-32 και 53-72 φαίνεται να συνδέονται κατά κύριο λόγο για μικρό χρονικό διάστημα (1-20 λεπτά). Τα ποσοστά των χρηστών ακολουθούν φθίνουσα πορεία όσο ανεβαίνει ο χρόνος σύνδεσης. Το ίδιο όμως δεν φαίνεται να ισχύει και για την μεσαία ηλικιακή κλάση στην οποία παρ'όλο που τα υψηλότερα ποσοστά εμφανίσουν μικρή χρονική σύνδεση σε ποσοστό 44,4%,το 29,6% δηλώνει πως συνδέεται για περισσότερο από 40 λεπτά σε κάθε του σύνδεση.

- *Συχνότητα Σύνδεσης* Συνδρομή*

Συχνότητα Σύνδεσης* Συνδρομή

			Συνδρομή			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Συχνότητα Σύνδεσης	Δεν απάντησε	Συχνότητα	4	0	0	4
		Ποσοστό %	100,0%	0,0%	0,0%	100,0%
	<1 φορά την εβδομάδα	Συχνότητα	0	0	9	9
		Ποσοστό %	0,0%	0,0%	100,0%	100,0%
	2-6 φορές την εβδομάδα	Συχνότητα	0	2	5	7
		Ποσοστό %	0,0%	28,6%	71,4%	100,0%
	Κάθε μέρα	Συχνότητα	0	3	29	32
		Ποσοστό %	0,0%	9,4%	90,6%	100,0%
	2-3 φορές την ημέρα	Συχνότητα	0	1	14	15
		Ποσοστό %	0,0%	6,7%	93,3%	100,0%
	>4 φορές την ημέρα	Συχνότητα	0	4	16	20
		Ποσοστό %	0,0%	20,0%	80,0%	100,0%
Σύνολο		Συχνότητα	4	10	73	87
		Ποσοστό %	4,6%	11,5%	83,9%	100,0%

Πίνακας 3.48: Συχνότητα Σύνδεσης* Συνδρομή



Γράφημα 3.45: Συχνότητα Σύνδεσης* Συνδρομή

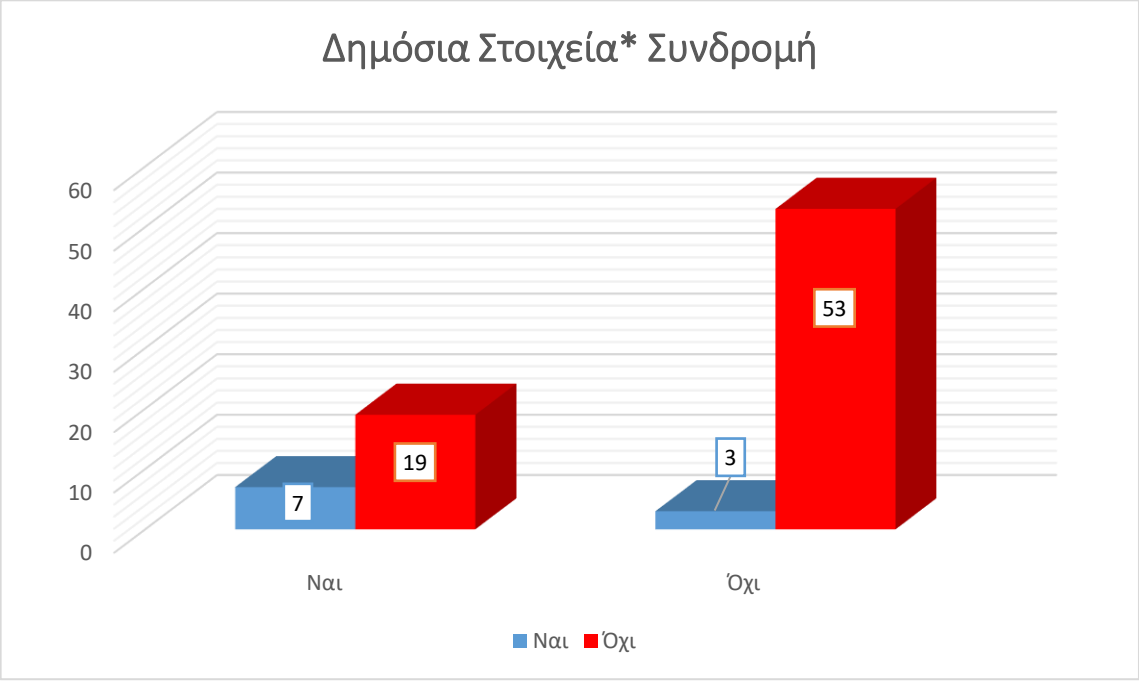
Αναφορικά με την συχνότητα σύνδεσης και την πιθανότητα καταβολής σύνδεσης για την παραμονή στις ιστοσελίδες κοινωνικής δικτυώσεις παρατηρείτε η τάση οι χρήστες που συνδέονται περισσότερες από 4 φορές ημερησίως να είναι θετικοί στην καταβολή συνδρομής περισσότερο από τις υπόλοιπες συχνότητες σύνδεσης. Αυτό ωστόσο δεν σημαίνει πως αποτελεί την πλειοψηφία καθώς το ποσοστό ανέρχεται στο 20,0%.

- *Συνδρομή * Δημόσια_Στοιχεία*

Δημόσια Στοιχεία* Συνδρομή

			Συνδρομή			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Δημόσια Στοιχεία	Δεν απάντησε	Συχνότητα	4	0	1	5
		Ποσοστό %	80,0%	0,0%	20,0%	100,0%
	Ναι	Συχνότητα	0	7	19	26
		Ποσοστό %	0,0%	26,9%	73,1%	100,0%
	Όχι	Συχνότητα	0	3	53	56
		Ποσοστό %	0,0%	5,4%	94,6%	100,0%
Σύνολο		Συχνότητα	4	10	73	87
		Ποσοστό %	4,6%	11,5%	83,9%	100,0%

Πίνακας 3.49: Δημόσια Στοιχεία* Συνδρομή



Γράφημα 3.46: Δημόσια Στοιχεία* Συνδρομή

Εξετάζοντας την πιθανή σχέση που μπορεί να φέρουν τα δημόσια κοινοποιημένα στοιχεία των χρηστών με την διάθεση καταβολής συνδρομής παρατηρείται η τάση οι χρήστες που έχουν δημόσια ανοιχτό το προσωπικό τους προφίλ να καταβάλουν σε μεγαλύτερο ποσοστό συνδρομή (70,0%) από εκείνους που έχουν κρυφά τα προσωπικά τους στοιχεία (30,0%).

Correlations

		Συνδρομή	Δημόσια_Στοιχεία
Συνδρομή1	Pearson Correlation	1	,591**
	Sig. (2-tailed)		,000
	N	87	87
Δημόσια_Στοιχεία	Pearson Correlation	,591**	1
	Sig. (2-tailed)	,000	
	N	87	87

**. Correlation is significant at the 0.01 level (2-tailed).

Πίνακας 3.50: Correlations Δημόσια Στοιχεία* Συνδρομή

Δημιουργώντας έναν πίνακα συσχέτισης των μεταβλητών «συνδρομή» και «δημόσια στοιχεία» παρατηρούμε πως η συσχέτιση τους είναι 0,591. Όπως παρατηρούμε από την μήτρα συσχέτισης ζητήθηκε η δημιουργία επιπέδου σημαντικότητας two-tailed. 87 ζεύγη τιμών (85 βαθμοί ελευθερίας) συντέλεσαν στον υπολογισμό της συσχέτισης του πίνακα 3.50. Η συσχέτιση είναι σημαντική σε επίπεδο σημαντικότητας 0.01 (1%)[159]. Συμπερασματικά, βλέπουμε πως υπάρχει μια θετική συσχέτιση ανάμεσα στην συνδρομή και στα στοιχεία που κοινοποιούνται δημόσια ($r = 0{,}591$, $df = 85$, $p < 0.001$). Μέσα από την συσχέτιση φανερώνεται πως τα άτομα που έχουν δημόσια τα στοιχεία τους στα μέσα κοινωνικής δικτύωσης είναι πιο θετικά προς την καταβολή συνδρομής για την παραμονή τους στο δίκτυο.

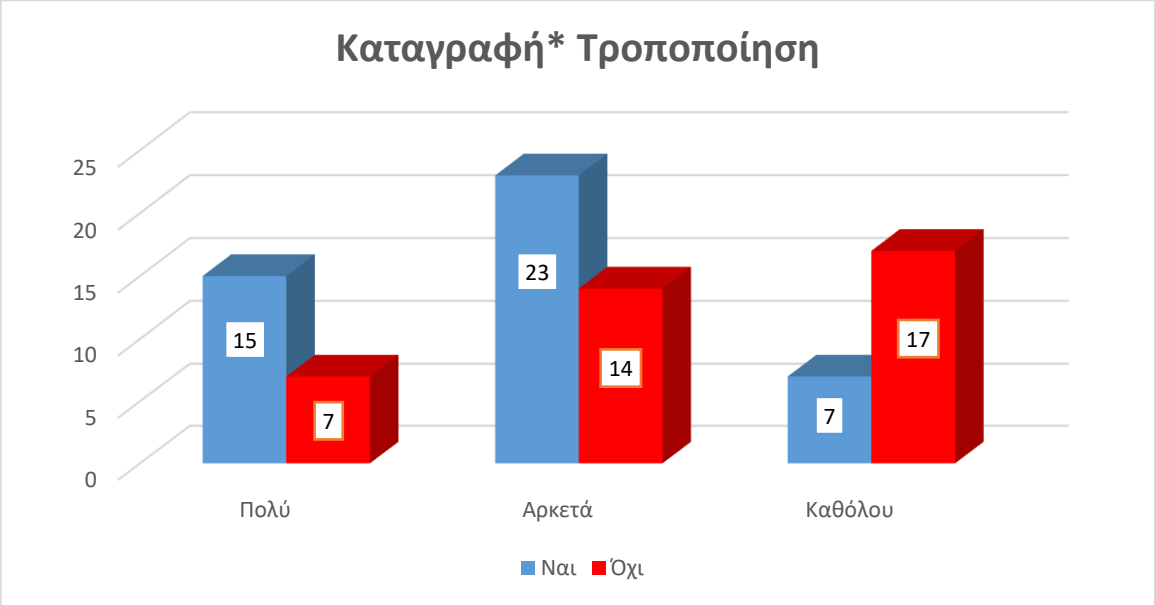
[159] Έχει επισημανθεί και από το στατιστικό πρόγραμμα που χρησιμοποιήθηκε (SPSS).

- *Καταγραφή* Τροποποίηση*

Καταγραφή* Τροποποίηση

			Τροποποίηση			Σύνολο
			Δεν απάντησε	Ναι	Όχι	
Καταγραφή	Δεν απάντησε	Συχνότητα	2	0	2	4
		Ποσοστό %	50,0%	0,0%	50,0%	100,0%
	Πολύ	Συχνότητα	0	15	7	22
		Ποσοστό %	0,0%	68,2%	31,8%	100,0%
	Αρκετά	Συχνότητα	0	23	14	37
		Ποσοστό %	0,0%	62,2%	37,8%	100,0%
	Καθόλου	Συχνότητα	0	7	17	24
		Ποσοστό %	0,0%	29,2%	70,8%	100,0%
Σύνολο		Συχνότητα	2	45	40	87
		Ποσοστό %	2,3%	51,7%	46,0%	100,0%

Πίνακας 3.51: Καταγραφή* Τροποποίηση



Γράφημα 3.47: Καταγραφή* Τροποποίηση

Η γενική εικόνα που θα μπορούσε να έχει ο μέσος άνθρωπος σχετικά με τον βαθμό που απασχολεί τον χρήστη η καταγραφή των στοιχείων του και η τροποποίηση των απαραίτητων ρυθμίσεων θα ήταν πως καθώς η επιθυμία για μην καταγραφή των κινήσεων μεγαλώνει οι τροποποιήσεις πρέπει να λάβουν χώρα. Αυτή η θεωρία επιβεβαιώνεται και από τον πίνακα 3.51 και το γράφημα 3.46, όπου παρατηρείται η τάση στους χρήστες που δεν ενδιαφέρονται για την καταγραφή των διαδικτυακών κινήσεων τους το 70,8% να δηλώνει πως δεν έχει προβεί σε καμία τροποποίηση. Ωστόσο το υπόλοιπο ποσοστό φαίνεται να ενδιαφέρεται παρά την δήλωση του, καθώς έχει ήδη προβεί σε τροποποιήσεις για περιορισμό των κινήσεων του. Εξίσου ενδιαφέρον παρουσιάζουν οι χρήστες που

δηλώνουν πως ενδιαφέρονται σε πολύ μεγάλο βαθμό. Σε αυτή την περίπτωση το 31,8% δεν έχει κάνει καμία ενέργεια να περιορίσει την καταγραφή. Παρατηρούμε λοιπόν, πως παρά την αρχική δήλωση των χρηστών οι πράξεις τους δεν υποστηρίζουν την συναισθηματική ανασφάλεια που τους δημιουργούν οι ιστοσελίδες κοινωνικής δικτύωσης.

3.7 Ελληνική Στατιστική Αρχή: «Χρήση Τεχνολογιών Πληροφόρησης Και Επικοινωνίας»

Η Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ) πραγματοποίει από το 2002 ερευνά για την «χρήση τεχνολογιών πληροφόρησης και επικοινωνίας». Σκοπός της ερευνάς είναι η διερεύνηση του βαθμού χρήσης νέων τεχνολογιών από κατοίκους όλης της Ελλάδας, και ειδικότερα την χρήση του ηλεκτρονικού υπολογιστή και την αίσθηση ασφάλειας των ατόμων εντός του δικτύου. Η παρούσα ερευνά βοήθησε στην καλύτερη κατανόηση και διερεύνηση της ένταξης των ηλεκτρονικών υπολογιστών στην ζωή των ατόμων σε βάθος χρόνου. Πρέπει ωστόσο να επισημάνουμε πως τα δοθέντα αποτελέσματα τις ΕΛΣΤΑΤ καλύπτουν μέχρι το έτος 2015, καθώς τα αντίστοιχα στοιχεία του 2016 δεν είναι ακόμα διαθέσιμα.

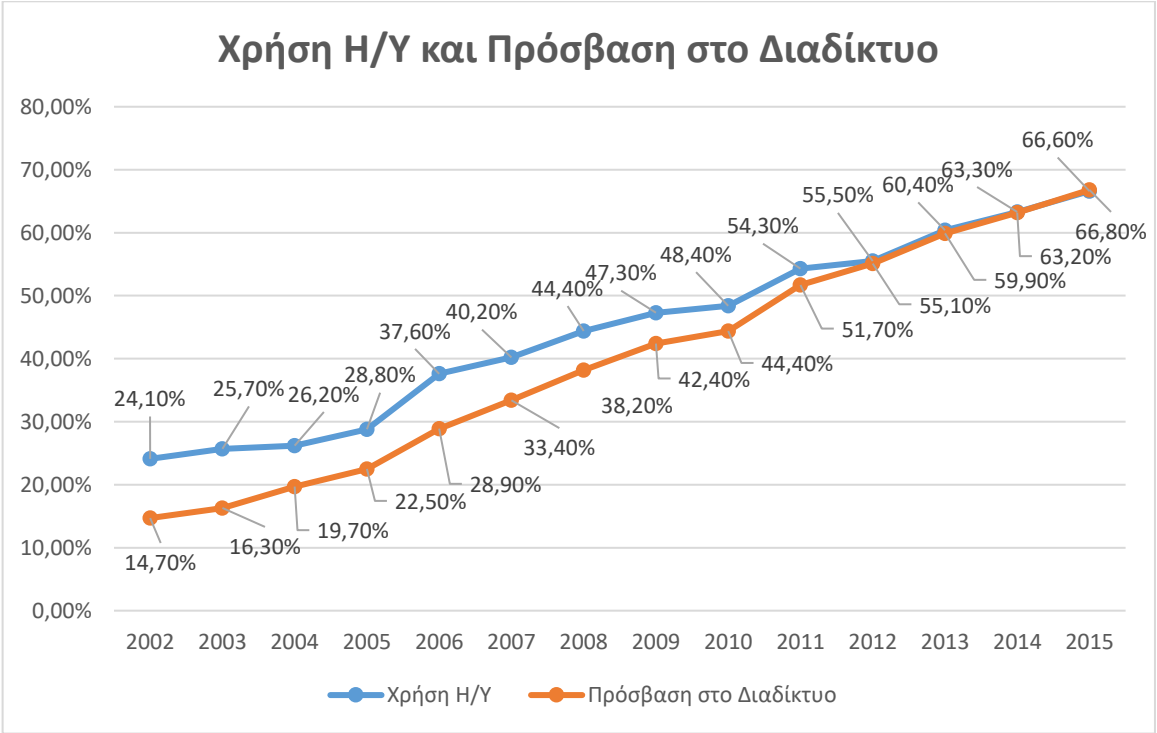
Η ερευνά πραγματοποιήθηκε σε 4.667 νοικοκυριά, σε άτομα 16-74 ετών. Ο ερωτώμενος καλείτο να απαντήσει ερωτήσεις σχετικές με όλα τα μέλη την κατοικίας, αλλά και ερωτήσεις που αφορούσαν τον ίδιο.

3.7.1 Έρευνα σε βάθος χρόνου

Σε αυτή την υποενότητα θα χρησιμοποιηθούν ορισμένα στατιστικά στοιχεία τα οποία έχουν δοθεί από την ΕΛΣΤΑΤ στην δημοσιότητα. Πρέπει να τονισθεί πως η Ελληνική Στατιστική Αρχή έχει λάβει γνώση για την χρήση των αποτελεσμάτων της ερευνάς και έχει παραχωρήσει τα δεδομένα.

Γράφημα 3.48: Πρόσβαση στο Διαδίκτυο 2010-2015

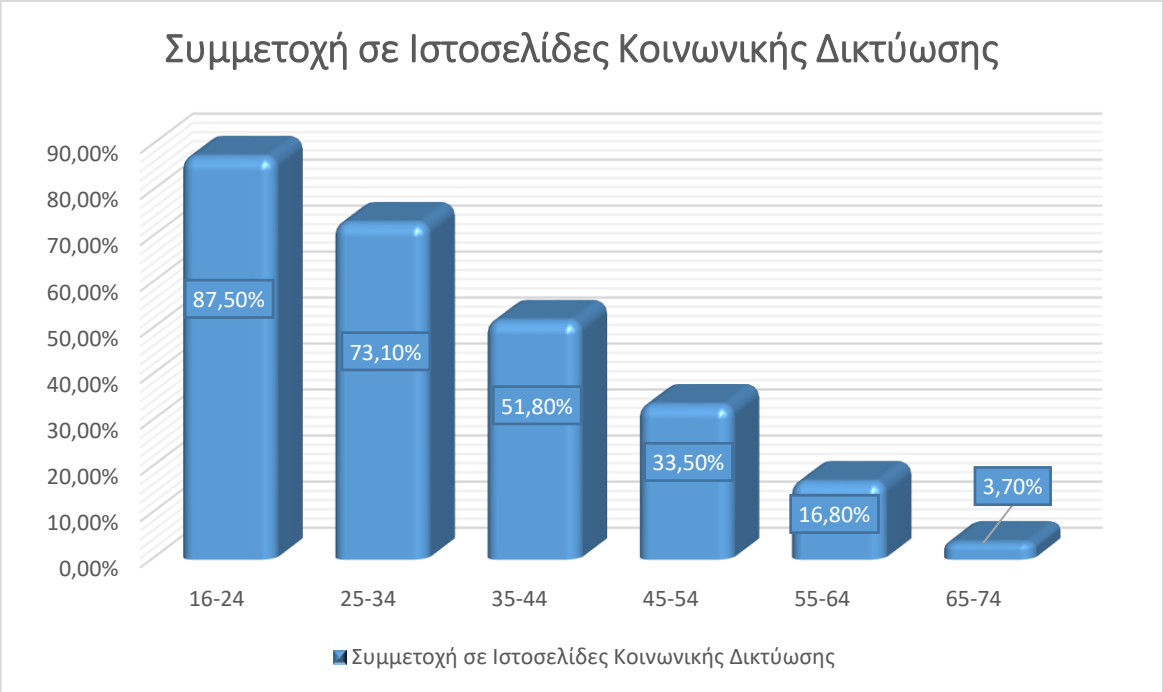
Από τον πίνακα παρατηρούμε την ραγδαία αύξηση στην χρήση του διαδικτύου, που έλαβε χωρά το χρονικό διάστημα 2010 έως 2015. Το έτος 2013-2014 η αύξηση διπλασιάστηκε σε σχέση με τα υπόλοιπα έτη με το ποσοστό να αγγίζει το 9,3%. Η συνολική αύξηση της υπό εξέταση πενταετίας ανέρχεται στο 46,8%.



Γράφημα 3.49: Χρήση Η/Υ και Πρόσβαση στο Διαδίκτυο

Ιδιαίτερο ενδιαφέρον παρουσιάζει η σύγκριση της χρήσης ηλεκτρονικού υπολογιστή με την πρόσβαση στο διαδίκτυο. Από το γράφημα 3.48 γίνετε αντιληπτό πως ενώ το 2002 ο Η/Υ αποτελούσε ένα σημαντικό εργαλείο για το 24,1% του πληθυσμού, δεν

ήταν άμεσα συνδεδεμένος με την χρήση του διαδικτύου, το ποσοστό χρήσης του οποίου έφτανε μόλις το 14,7%. Εντούτοις, από το 2012 και έπειτα, η χρήση των δυο μέσων τείνει να ακολουθεί κοινή πορεία με ποσοστά που δεν περνάνε το 0,5% στην επικράτηση του ενός έναντι του αλλού. Επιπλέον το 2014 η πορεία των δεδομένων αλλάζει θέτοντας το διαδίκτυο επικρατέστερο μέσο από τον Η/Υ και δηλώνοντας ξεκάθαρα την υπάρξει άλλων μέσων πρόσβασης σε αυτό. Γενικεύοντας παρατηρούμε πως η χρήση Η/Υ και του διαδικτύου ακολουθεί σταθερά ανοδική πορεία.



Γράφημα 3.50: Συμμετοχή σε Ιστοσελίδες Κοινωνικής Δικτύωσης

Το γράφημα 3.49 φανερώνει πως ένα μεγάλο μέρος του πληθυσμού είναι εγγεγραμμένο σε ιστοσελίδες κοινωνικής δικτύωσης. Στις νεότερες ηλικίες εμφανίζονται πολύ υψηλά ποσοστά της τάξεως του 87,5%, αλλά παρατηρούμε την τάση η ηλικία χρήσης να είναι αντίστροφος ανάλογη με την χρήση ιστοσελίδων κοινωνικής δικτύωσης. Ωστόσο φαίνεται οι ηλικίες μέχρι 44 ετών να χρησιμοποιούν στην πλειοψηφία τους τις εν λόγο ιστοσελίδες με πάνω από 1 στους 5 ερωτηθέντες να παραδέχεται την σύνδεση τους σε αυτές.

3.8.1 Διαδικτυακή εγκληματικότητα

Η διαδικτυακή εγκληματικότητα ή αλλιώς ηλεκτρονική εγκληματικότητα άργησε να φέρει έναν ορισμό που να μπορεί να καλύψει τόσο το εύρος της, όσο και τα μέσα, της μορφές και το νομικό πλαίσιο που απαιτούνταν ώστε να οδηγεί στην απόδοση ενός

εγκύρου και ορθού ορισμού. Ωστόσο, ο πλησιέστερος ορισμός που μπορεί να δοθεί περιλαμβάνει τρεις πτυχές- πυλώνες του φαινομένου. Πιο συγκεκριμένα ως ηλεκτρονικό έγκλημα θεωρείται κάθε νέα μορφή εγκλήματος το οποίο διαπράττεται με την χρήση: α) ηλεκτρονικού υπολογιστή ή/και β) την χρήση οποιουδήποτε άλλου μέσου που αντικαθιστά τον ηλεκτρονικό υπολογιστή, γ) και γενικότερα οποιαδήποτε άνομη πράξη που πράττεται με την βοήθεια ηλεκτρονικού υπολογιστή.[160]

Η διαδικτυακή εγκληματικότητα πάρα το γεγονός ότι έχει πάρει τεράστιες διαστάσεις ακολουθώντας την ραγδαία εξέλιξη της τεχνολογίας, αποτελεί ένα κομμάτι που δεν μπορεί ακόμα να εξαλειφθεί. Χαρακτηριστική είναι η αδυναμία διαχωρισμού των διαδικτυακών εγκληματικών πράξεων σε κατηγορίες και η αντικατάσταση της ονομασίας τους με τις βλάβες που προκαλούν στον χρήστη.

Η δυσκολία δίωξης της διαδικτυακής εγκληματικότητας οφείλεται σε μια σειρά παραγόντων οι οποίοι αποτελούνται από την δυσκολία κατανόησης της πράξεως, ιδιαιτέρως σε πιο πρώιμο στάδιο του φαινομένου, την έλλειψη αποδεικτικών στοιχείων, αφού η φύση της εγκληματικής ενέργειας δεν αφήνει ακράδαντες αποδείξεις για την ταυτότητα του εγκληματία και την έλλειψη αποδεικτικών των περιουσιακών στοιχείων του θύματος. Οι παραπάνω αίτιες αποτελούν προβλήματα στην διερεύνηση εγκληματικών ενεργειών. Ωστόσο δεν μπορούν να παραληφθούν και οι πολίτικες αίτιες βάση των ποιων δίνετε προτεραιότητα στην ανεξιχνίασης φυσικών εγκλημάτων και έπειτα των ενεργειών διαδικτυακής μορφής. . Η πολυπλοκότητα τέλος του φαινομένου σε συνδυασμό και με την εξιχνίαση της ηλικίας του χρήστη είναι μερικοί ακόμα παράγοντες. Αξίζει να σημειωθεί πως τα προηγούμενα χρονιά η πλειοψηφία την εγκληματικών ενεργειών γίνονταν από νεαρά άτομα τα οποία είχαν μεγαλύτερη εξοικείωση με το διαδίκτυο. Η επιβολή ποινών ωστόσο δεν ήταν πάντοτε εύκολη καθώς στις περιπτώσεις ανήλικων το νεαρό της ηλικίας και η αδυναμία συνειδητοποίησης των βλαβών που δημιουργούσαν αποτελούσαν υποστηρικτικούς για αυτούς παράγοντες.[161]

[160] Βλαχόπουλος Κωνσταντίνος, Ηλεκτρονικό Έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, 2007, σελ. 9
[161] Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, 2006, pp. 679-683

3.8 Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

Η Διεύθυνση Δίωξη Ηλεκτρονικού Εγκλήματος συνιστά τμήμα της Αστυνομίας. Η δράση του είναι συνδεδεμένη με εγκλήματα που διαπράττονται στο διαδίκτυο ή με την χρήση του διαδικτύου, καθώς και στην ενημέρωση των πολίτων έχοντας ως απώτερο στόχο την δημιουργία ευσυνείδητων και προσεκτικών χρηστών ως το καλύτερο μέσο πρόληψης. Κομμάτι της δίωξης ηλεκτρονικού εγκλήματος αποτελεί και το Cyberkid[162], ηλεκτρονική διεύθυνση που διδάσκει τα παιδιά και τους γονείς, μέσα από συμβουλευτικό υλικό, την ορθή συμπεριφορά στο διαδίκτυο μέσα από παιχνίδια και δραστηριότητες. Επιπλέον τα παιδιά έχουν την ευκαιρία να παίζουν σε ένα προστατευμένο διαδικτυακό περιβάλλον. Η επέκταση της στα αγγλικά δίνει την δυνατότητα χρήσης της από αγγλόφωνα παιδία. Σελίδα Cyberkid δημιουργήθηκε και στο Facebook.

Εικόνα 10: Δίωξη Ηλεκτρονικού Εγκλήματος

Η δράση της Δίωξης Ηλεκτρονικού Εγκλήματος όμως δεν περιορίζεται σε εθνικά σύνορα. Εκπαιδευτικά σεμινάρια της Ευρωπαϊκής Αστυνομικής Ακαδημίας (CEPOL), συνέδρια και συναντήσεις, τόσο στην Ελλάδα όσο και στο εξωτερικό, με ευρωπαϊκούς και διεθνής οργανισμούς, είναι λίγες μόνο από τις δράσεις της στην προσπάθεια συντονισμένου ελέγχου του διαδικτύου. Αξίζει να αναφερθεί και η δράση της Δίωξης Ηλεκτρονικού Εγκλήματος στην υλοποίηση του Cybercrime (Payment Card Fraud, Child Sexual Exploitation και Cyber Attacks) του European Multidisciplinary Platform against Criminal Threats (EMPACT).

Το « Cyberalert » (κέντρο διαχείρισης διαδικτυακού κίνδυνου) αποτελεί το κομμάτι το οποίο ερευνά τις καταγγελίες που δέχεται η δίωξη από τους πολίτες. Οι υποθέσεις που εξιχνιαστήκαν το 2015 ανέρχονται στις 1.822. Αναλυτικότερα τα ποσοστά παρουσιάζονται στο γράφημα 3.50.

[162] http://www.cyberkid.gov.gr/, 10/11/2016

Γράφημα 3.51:Υποθέσεις Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Στα πλαίσια της συνεργασίας της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος με την Interpol και Europol επιχειρήθηκε η από κοινού αντιμετώπιση για υποθέσεις ηλεκτρονικών εγκλημάτων, κακουργημάτων παιδικής πορνογραφίας, διαδικτυακών απατών, υποκλοπής κωδίκων και οικονομικών ποσών και παραεμπορίου.

Άλλες υποθέσεις που χειρίστηκε μέσα στο 2015 αφορούσαν το παραεμπόριο μέσω διαδικτύου, τον εντοπισμό και αποτροπή αποπείρων αυτοκτονιών, υποθέσεις για προστασία ζωών.

3.9 Συμπεράσματα

Η παρούσα έρευνα διεξήχθη σε δείγμα 87 υποκειμένων, με την πλειοψηφία τους να αποτελείται από νεαρές ηλικίες (13 έως 32 ετών), σε ποσοστό 55,6%. Λόγο του κλειστού τύπου των ερωτήσεων πραγματοποιήθηκαν διασταυρώσεις (Crosstabs) δεδομένων μέσω του Στατιστικού Προγράμματος SPSS. Από τους πίνακες και τα γραφήματα προκύπτουν τα εξής συμπεράσματα αναφορικά με το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης:

- Η πλειοψηφία των χρηστών τείνει να παραχωρεί προσωπικά δεδομένα, τόσο στις ιστοσελίδες κοινωνικής δικτύωσης, όσο και γενικότερα στο διαδίκτυο. Ιδιαιτέρως υψηλά εμφανίζονται τα ποσοστά παραχώρησης πραγματικού ονόματος, ηλικίας και φωτογραφιών του χρήστη.

- Το συντριπτικό ποσοστό του δείγματος κατέχει ηλεκτρονικό υπολογιστή στην οικία του (94,3%) και κάνει χρήση του διαδικτύου (97,7%). Ιδιαίτερη εντύπωση προκαλεί το γράφημα 3.49 που απεικονίζει την ραγδαία εξάπλωση της χρήσης Η/Υ και διαδικτύου.
- Οι ηλεκτρονικές αγορές έχουν μεγάλο μερίδιο της αγοράς καθώς το 57,5% πραγματοποιεί αγορές μέσω διαδικτύου κυρίως από εγχώριους 36,3% και ευρωπαίους (23,1%) πωλητές.
- Η άρνηση χρήσης των προσωπικών δεδομένων για διαφημιστικούς σκοπούς *54,5%* και η ανάγνωση των πολιτικών απορρήτου (54,5%) αποτελούν τα δημοφιλέστερα μέτρα προστασίας των χρηστών.
- Ενώ φαίνεται πως το 42,5% των ερωτώμενων ενοχλείται από την καταγραφή των διαδικτυακών του κινήσεων χαμηλά παρουσιάζονται τα ποσοστά των χρηστών που αντιδρούν εμπράκτως σε αυτό. Μόλις το 51,7% έχει τροποποιήσει τις παραμέτρους για να μην καταγράφονται οι κινήσεις του, ενώ το 63,2% παραδέχεται πως δεν χρησιμοποιεί αντί-ανιχνευτικά προγράμματα.
- Το 96,3% του δείγματος διατηρεί λογαριασμό στο Facebook κατατάσσοντας την ως την δημοφιλέστερη ιστοσελίδα κοινωνικής δικτύωσης της παρούσας έρευνας. Ακολουθεί με 31,7% το LinkedIn, ποσοστό ιδιαίτερα υψηλό για σελίδα εξειδικευμένης χρήσης. Εικάζουμε πως αυτό οφείλεται στην παρούσα οικονομική κρίση και στα υψηλά ποσοστά ανεργίας (23,5 % τον Αύγουστο του 2016)[163].
- Τα άτομα με εκπαίδευση Γυμνασίου και Λυκείου τείνουν να συνδέονται για περισσότερη ώρα στις ιστοσελίδες κοινωνικής δικτύωσης. Όσο αυξάνεται το μορφωτικό επίπεδο και η ηλικία του χρήστη ο χρόνος σύνδεσης μειώνεται.
- Η σύσταση των χρηστών του Facebook, το LinkedIn και toTwitter αποτελείται κυρίως από νέα άτομα 13-32 ετών. Αντίθετα το Pinterest το επισκέπτονται πιο μεγάλες ηλικιακές κλάσεις.
- Οι συντριπτική πλειοψηφία των χρηστών επιθυμεί να επιλέγει ποιοι θα βλέπουν το περιεχόμενο των κοινοποιήσεων τους ανά σελίδα κοινωνικής δικτύωσης φανερώνοντας με αυτόν τον τρόπο τη καθολική επιθυμία για έλεγχο.
- Οι ηλικίες 13-32 συνδέονται περισσότερο από μια φορά την ημέρα και για μεγαλύτερο χρονικό διάστημα στις σελίδες κοινωνικής δικτύωσης.

[163] http://www.protothema.gr/economy/article/606619/stathera-proti-stin-anergia-i-ellada-me-235/, 27/11/2016

- Παρόλο που η πλειοψηφία των χρηστών απαντά πως δεν θα συνέχιζε την σύνδεση της σε ιστοσελίδες που απαιτούσαν συνδρομή, οι χρήστες που συνδέονται περισσότερο από τέσσερεις (4) φορές την ημέρα φαίνεται να επιθυμούν να καταβάλουν το χρηματικό ποσό που απαιτείται ώστε να συνεχίσουν την σύνδεση τους. Συνήθως πρόκειται για άτομα που έχουν δημοσίως ανοιχτά τα προσωπικά τους στοιχεία.
- Η ανασφάλεια για την χρήση των προσωπικών δεδομένων στις ιστοσελίδες κοινωνικής δικτύωσης κυριαρχεί σε όλες τις ηλικιακές κλάσεις. Ο έλεγχος της προσβασιμότητας στις προσωπικές πληροφορίες των χρηστών είναι ικανός να μειώσει τα επίπεδα ανασφάλειας των χρηστών. Επιπλέον όσοι δεν έχουν ενημερωθεί διαβάζοντας τους όρους και τις πολιτικές απορρήτου τείνουν να παρουσιάζουν υψηλότερα ποσοστά ανασφάλειας σε σχέση με τους ενημερωμένους χρήστες (86,8% και 67,4% αντίστοιχα).
- Παρά το γεγονός της ανασφάλειας των χρηστών και της επιθυμίας τους για μη καταγραφή των κινήσεων τους εντός του διαδικτύου δεν παρατηρούνται ιδιαιτέρως υψηλά ποσοστά ως προς την τροποποίηση των παραμέτρων για περιορισμό των καταγραφών.

ΓΕΝΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

Το ζήτημα της προστασίας των προσωπικών δεδομένων έχει απασχολήσει τα τελευταία χρόνια τους χρήστες. Η καθημερινή χρήση του διαδικτύου και οι διευκολύνσεις που παρέχει, το έχουν καταστήσει αναπόσπαστο μέρος της καθημερινότητας τους. Ιδιαίτερες διευκολύνσεις παρέχει στην κοινωνική δικτύωση και επικοινωνία των χρηστών, καθιστώντας την άμεση και ανέξοδη μέσα από την χρήση των ιστοσελίδων κοινωνικής δικτύωσης, με μοναδική προϋπόθεση την καταγραφή ορισμένων προσωπικών στοιχείων. Με την εγγραφή στην ιστοσελίδα ο χρήστης αυτομάτως αποδέχεται την συλλογή και επεξεργασία των προσωπικών του δεδομένων από την ιστοσελίδα, τις θυγατρικές και τις συνεργαζόμενες με αυτήν εταιρίες, με σκοπό την μεταπώληση ή την ιδία χρήση, έχοντας σαν τελικό στόχο την χρηματοδότηση. Ο κίνδυνος όμως παράνομης χρήσης και υποκλοπής των προσωπικών δεδομένων των χρηστών ελλοχεύει, ιδιαιτέρως αν αναλογιστούμε τα τεράστια οικονομικά οφέλη που υποβόσκουν. Αυτό όμως δεν αποτελεί ανασταλτικό παράγοντά στην χρήση τους. Παρόλο, που όλες οι ιστοσελίδες κοινωνικής δικτύωσης ακολουθούν ορισμένες βασικές εφαρμογές προστασίας προσωπικών δεδομένων, οι κίνδυνοι της παράνομης χρήσης των προσωπικών στοιχείων είναι ικανοί να βλάψουν το άτομο που τα φέρει.

Για την καταστολή του φαινομένου θεσπιστήκαν νόμοι για την διασφάλιση της ασφάλειας των χρηστών. Η ελληνική νομοθεσία ακολουθεί Ευρωπαϊκές Οδηγίες και Κανονισμούς. Η Οδηγία 95/46 με τον Ν. 2472/1997 εισήγαγε στην Ελλάδα ένα πλήρες ρυθμιστικό πλαίσιο χωρίς αποσπασματικό χαρακτήρα, με κύριο στόχο την ουσιαστική και καθολική προστασία τον πολιτών από μια νέα μέχρι τότε μορφή κινδύνου. Η βάση του Ν.2472/1997 στηρίχθηκε στην αποφυγή της εναξέλεκτης επεξεργασίας προσωπικών δεδομένων προσδιορίζοντας τα δικαιώματα και τις υποχρεώσεις των υπευθύνων επεξεργασίας, των υποκείμενων και των «τρίτων». Στόχος, είναι η δημιουργία μιας κοινωνίας πληροφοριών χωρίς την καταπάτηση ελευθεριών και θεμελιωδών ανθρωπίνων δικαιωμάτων. Επιτυγχάνοντας το, ο διαδικτυακός φόβος θα εξαλειφθεί. Ωστόσο ο χαρακτήρας των νόμων κρίνεται κατασταλτικός και δεν αποκλείει την εμφάνιση παραβάσεων και προβλημάτων. Ο εκσυγχρονισμός των νόμων κρίθηκε απαραίτητος και είναι υπό εξέλιξη, με τον Ευρωπαϊκό Κανονισμό 2016/679 περί «προστασίας φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών». Ο εν λόγω κανονισμός τέθηκε σε ισχύει στις 24 Μάιου 2016, η εφαρμογή του όμως θα λάβει χώρα τον Μάϊο του 2018 μέσα από

την εναρμόνιση των εγχώριων νόμων, καταργώντας την μέχρι πρότινος Οδηγία 95/46/ΕΚ και καλώντας όλες τις χώρες-μέλη της Ευρωπαϊκής Ένωσης να τροποποιήσουν την υπάρχουσα νομοθεσία ως προς τον άνωθεν κανονισμό.

Η ανασφάλεια για την χρήση των προσωπικών δεδομένων στις ιστοσελίδες κοινωνικής δικτύωσης κυριαρχεί σε όλες τις ηλικίες. Η έλλειψη ενημέρωσης είναι ένας από τους κυρίους παράγοντες που επιδεινώνει την έντονη ανησυχία την χρηστών καθώς παρατηρείται πως όσοι δεν έχουν ενημερωθεί διαβάζοντας τους όρους και τις πολιτικές απορρήτου τείνουν να παρουσιάζουν υψηλότερα ποσοστά ανασφάλειας σε σχέση με τους ενημερωμένους χρήστες. Επιπλέον ο έλεγχος της προσβασιμότητας στις προσωπικές πληροφορίες των χρηστών και η τροποποίηση των παραμέτρων για περιορισμό των καταγραφών μπορεί να μειώσει τα επίπεδα ανασφάλειας τους. Η δυνατότητα επιλογής των χρηστών σε θέματα ασφάλειας, όπως η ορατότητα των προσωπικών τους δεδομένων σε άλλους χρήστες και η τροποποίηση των ρυθμίσεων, βοηθούν στον περιορισμό διοχέτευσης και μεταβίβασης των δεδομένων αποτελώντας ένα «όπλο» στα χεριά τους.

Τέλος, δεν μπορούμε να παραβλέψουμε την ανάγκη για περαιτέρω ερευνά και διερεύνηση ενός μελανού σημείου. Από την έρευνα που πραγματοποιήθηκε προέκυψε πως παρά το γεγονός της ανασφάλειας των χρηστών και της επιθυμίας τους για μη καταγραφή των κινήσεων τους, δεν παρατηρούνται ιδιαιτέρως υψηλά ποσοστά ως προς την τροποποίηση των παραμέτρων για περιορισμό της ορατότητας και των καταγραφών. Η εν λόγω αντίφαση μπορεί να χρησιμοποιηθεί ως θέμα προς περεταίρω ανάλυση και διερεύνηση σε μελλοντική έρευνα, καθώς και ως έναυσμα για την απλοποίηση των όρων χρήσης και των πολιτικών απορρήτου των ιστοσελίδων.

ΠΑΡΑΡΤΗΜΑΤΑ

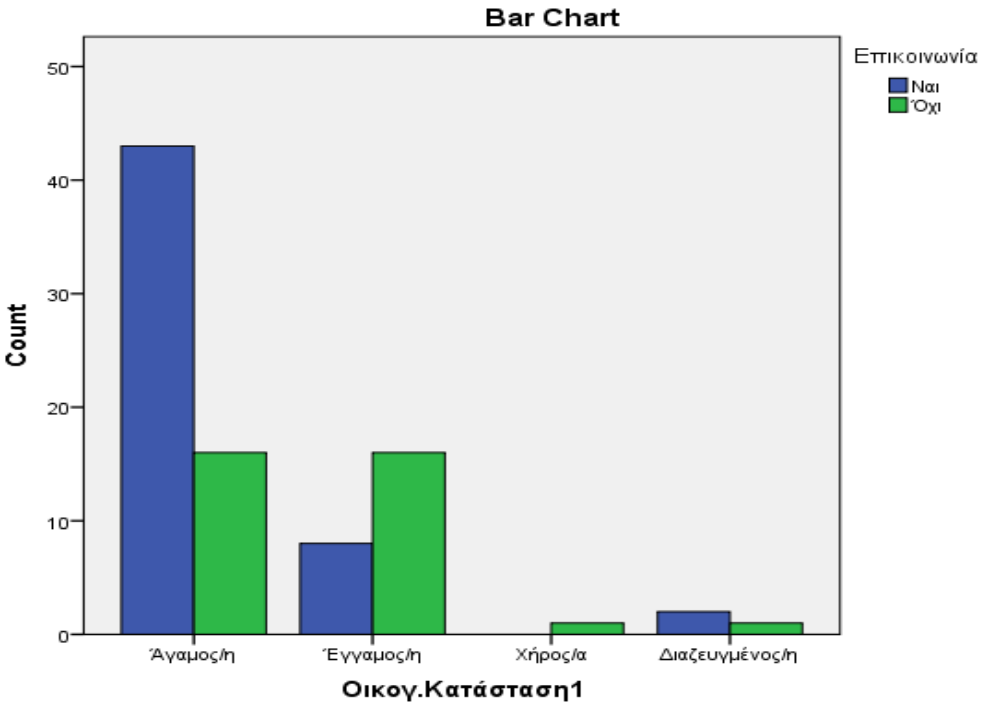
1. Παράρτημα Αρχικών Πινάκων SPSS

- Οικογενειακή Κατάσταση* Επικοινωνία

Crosstab

Count

		Επικοινωνία		
		Ναι	Όχι	Total
Οικογ.Κατάσταση1	Άγαμος/η	43	16	59
	Έγγαμος/η	8	16	24
	Χήρος/α	0	1	1
	Διαζευγμένος/η	2	1	3
Total		53	34	87

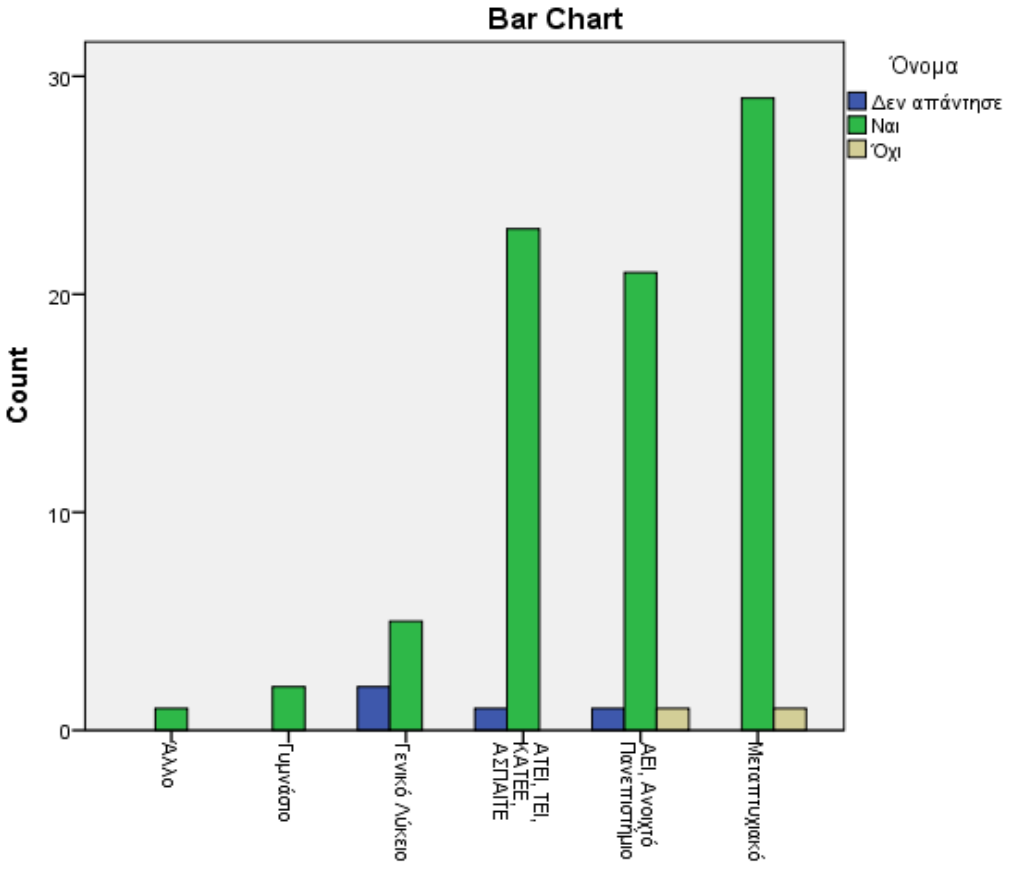


- Όνομα* Εκπαίδευση

Crosstab

Count

		Όνομα			Total
		Δεν απάντησε	Ναι	Όχι	
Εκπαίδευση1	Άλλο	0	1	0	1
	Γυμνάσιο	0	2	0	2
	Γενικό Λύκειο	2	5	0	7
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	1	23	0	24
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	1	21	1	23
	Μεταπτυχιακό	0	29	1	30
Total		4	81	2	87

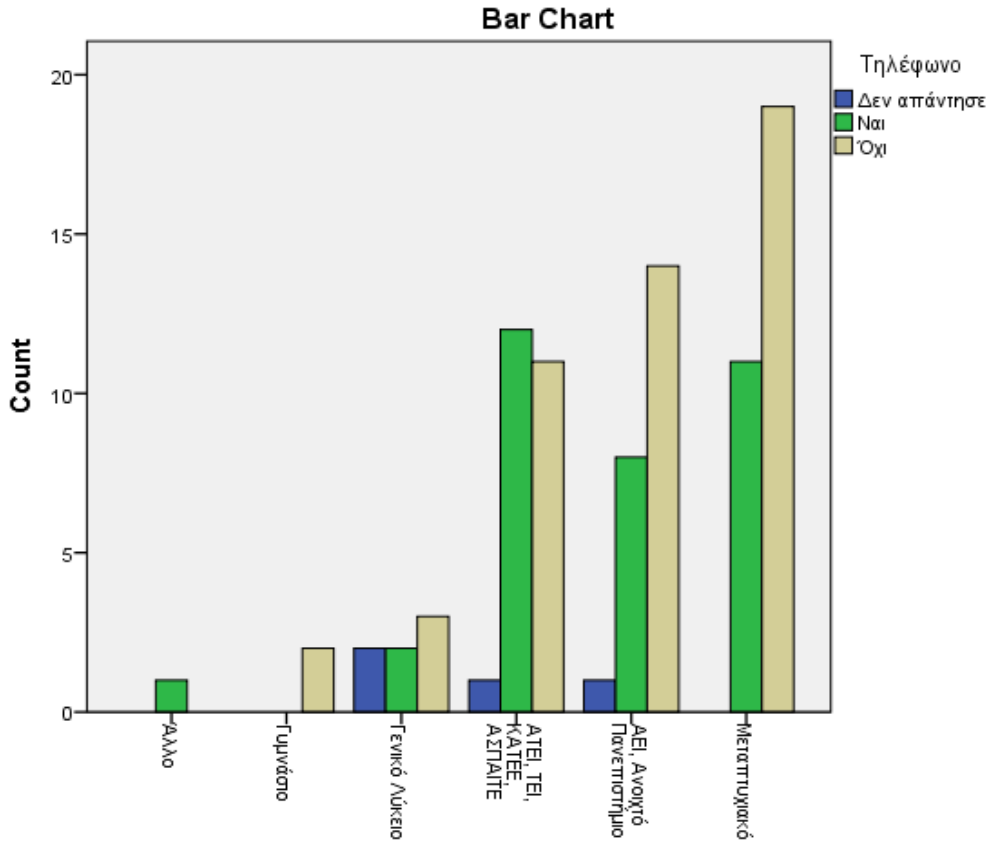


- Εκπαίδευση* Τηλέφωνο

Crosstab

Count

		Τηλέφωνο			
		Δεν απάντησε	Ναι	Όχι	Total
Εκπαίδευση1	Άλλο	0	1	0	1
	Γυμνάσιο	0	0	2	2
	Γενικό Λύκειο	2	2	3	7
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	1	12	11	24
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	1	8	14	23
	Μεταπτυχιακό	0	11	19	30
Total		4	34	49	87

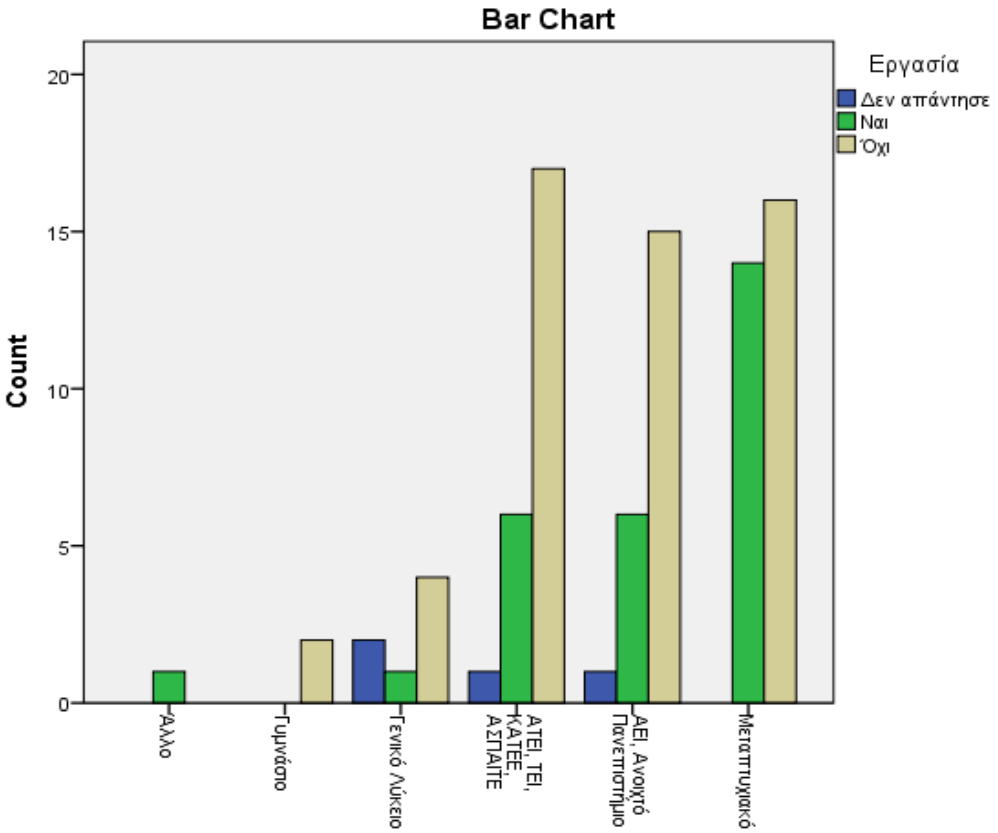


- Εκπαίδευση* Εργασία

Crosstab

Count

		Εργασία			
		Δεν απάντησε	Ναι	Όχι	Total
Εκπαίδευση1	Άλλο	0	1	0	1
	Γυμνάσιο	0	0	2	2
	Γενικό Λύκειο	2	1	4	7
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	1	6	17	24
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	1	6	15	22
	Μεταπτυχιακό	0	14	16	30
	Total	4	28	54	86

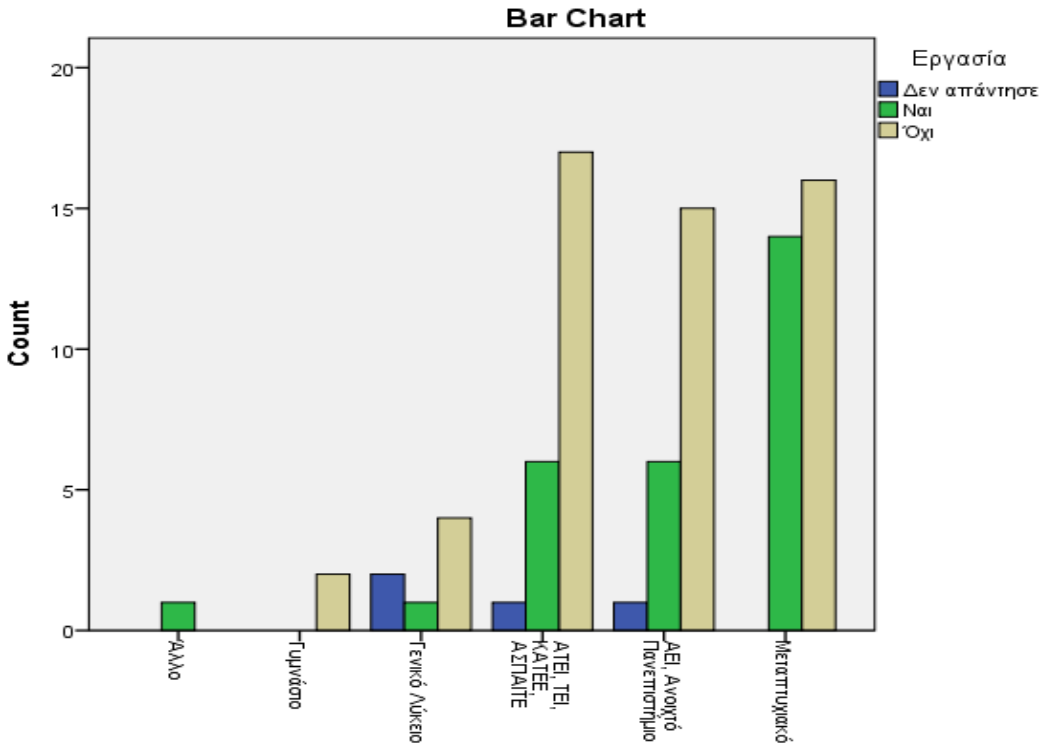


- Εκπαίδευση* Χρόνος_Σύνδεσης

Crosstab

Count

		Χρόνος_Σύνδεσης1				
		Δεν απάντησε	1-20 λεπτά	20-40 λεπτά	>40 λεπτά	Total
Εκπαίδευση1	Άλλο	0	1	0	0	1
	Γυμνάσιο	0	0	1	1	2
	Γενικό Λύκειο	2	2	3	0	7
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	1	9	8	6	24
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	1	9	6	7	23
	Μεταπτυχιακό	0	20	3	7	30
	Total	4	41	21	21	87

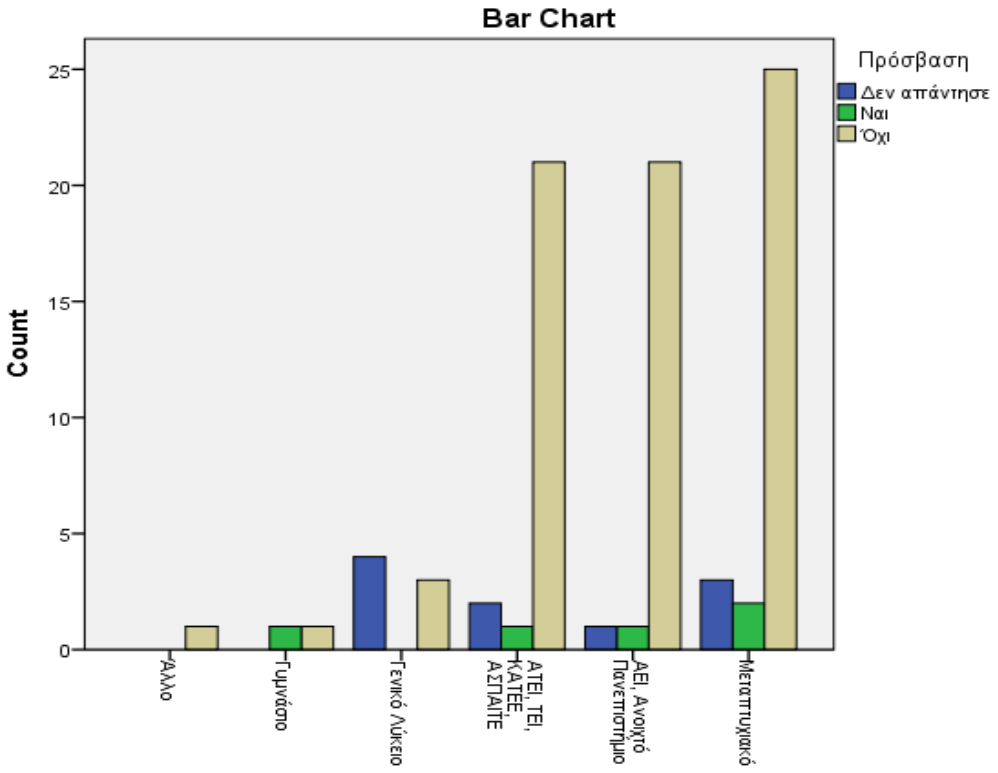


- Εκπαίδευση * Πρόσβαση

Crosstabulation

Count

		Πρόσβαση			
		Δεν απάντησε	Ναι	Όχι	Total
Εκπαίδευση1	Άλλο	0	0	1	1
	Γυμνάσιο	0	1	1	2
	Γενικό Λύκειο	4	0	3	7
	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	2	1	21	24
	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	1	1	21	23
	Μεταπτυχιακό	3	2	25	30
	Total	10	5	72	87

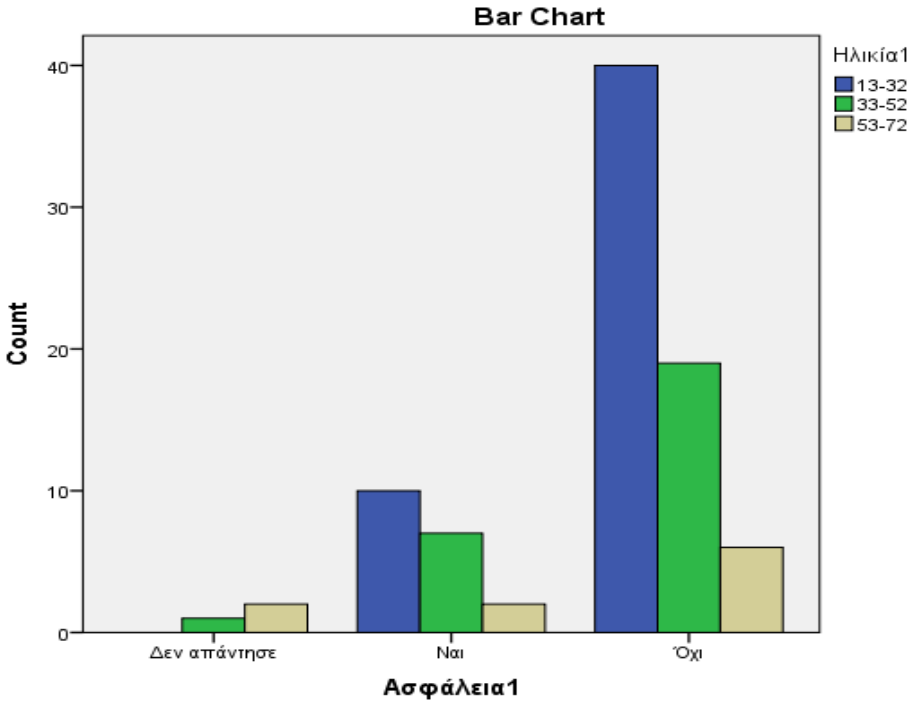


- Ασφάλεια* Ηλικία

Crosstab

Count

		Ηλικία1			
		13-32	33-52	53-72	Total
Ασφάλεια1	Δεν απάντησε	0	1	2	3
	Ναι	10	7	2	19
	Όχι	40	19	6	65
Total		50	27	10	87

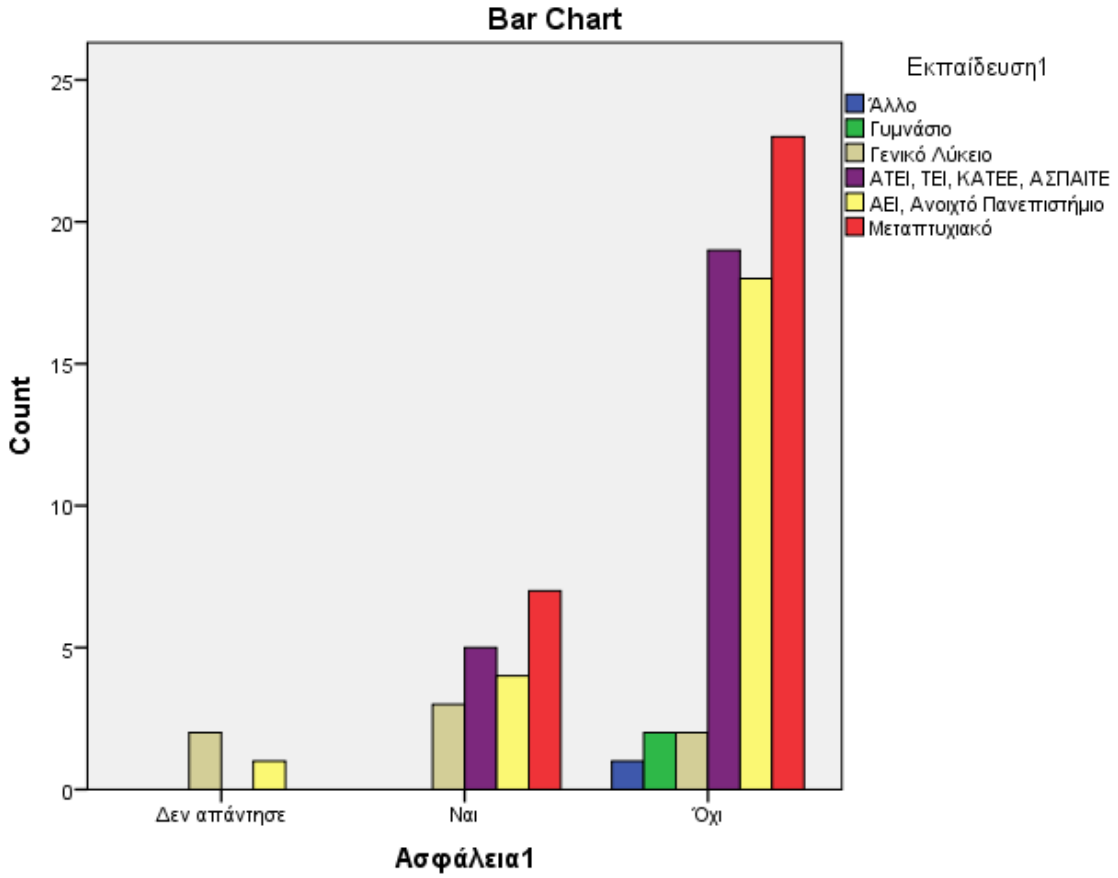


- Ασφάλεια* Ασφάλεια

Crosstab

Count

		Ασφάλεια						
		Άλλο	Γυμνάσιο	Γενικό Λύκειο	ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ	ΑΕΙ, Ανοιχτό Πανεπιστήμιο	Μεταπτυχιακό	Total
Ασφάλεια1	Δεν απάντησε	0	0	2	0	1	0	3
	Ναι	0	0	3	5	4	7	19
	Όχι	1	2	2	19	18	23	65
Total		1	2	7	24	23	30	87

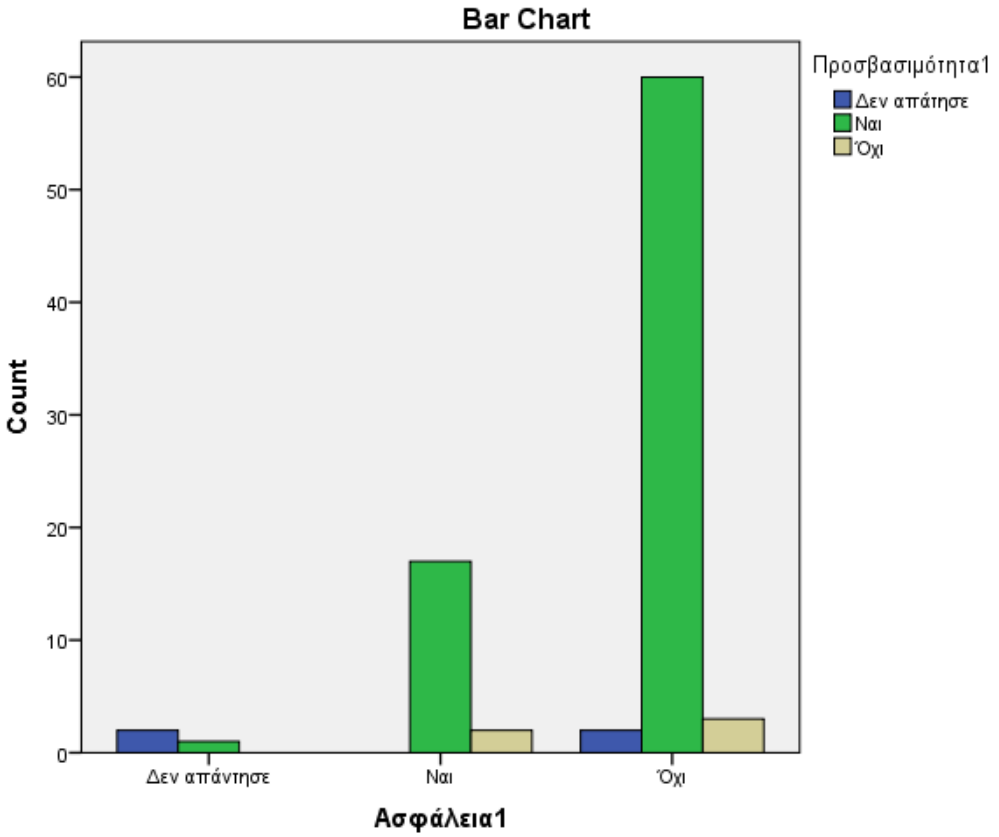


- Ασφάλεια* Εκπαίδευση

Crosstab

Count

		Εκπαίδευση							Total
			ΑΕΙ...	ΑΤΕΙ, ΤΕΙ...	Γενικό Λύκειο	ΙΕΚ	Μεταπτυχιακό	Τ.Ε.Ε	ΙΕΚ	
Ασφάλεια		3	1	0	2	0	0	0	0	6
	Ναι	0	4	5	3	0	7	0	0	19
	Όχι	0	18	19	2	1	23	1	1	65
Total		3	23	24	7	1	30	1	1	90

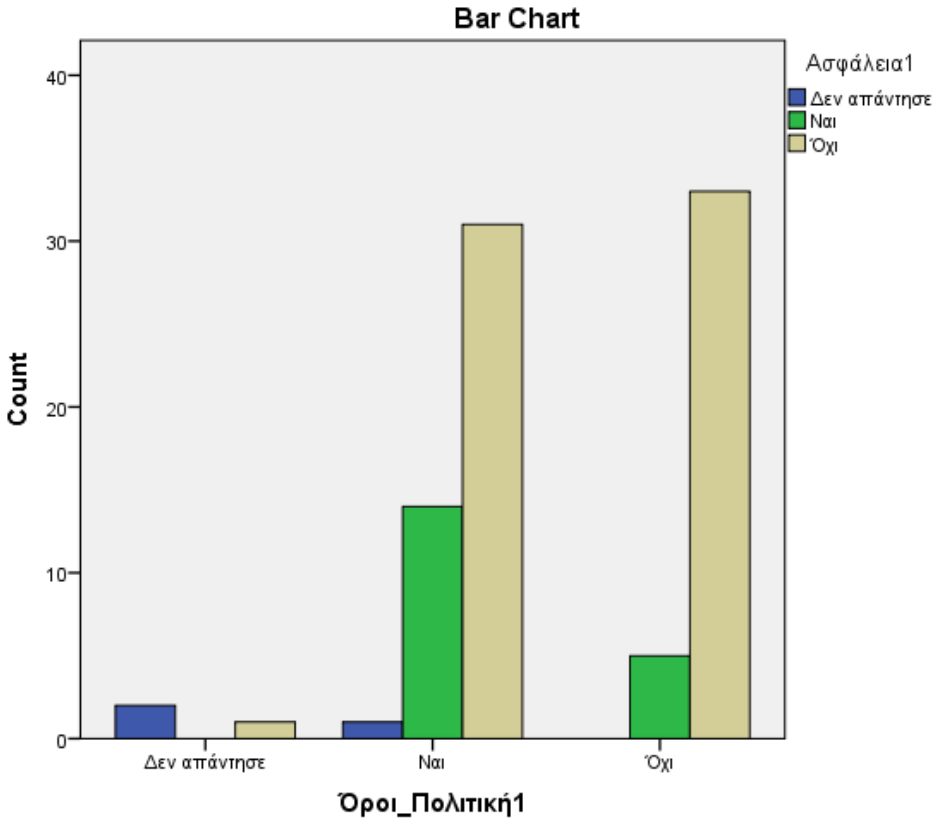


- Όροι_Πολιτική1 *Ασφάλεια1

Crosstabulation

Count

		Ασφάλεια1			
		Δεν απάντησε	Ναι	Όχι	Total
Όροι_Πολιτική1	Δεν απάντησε	2	0	1	3
	Ναι	1	14	31	46
	Όχι	0	5	33	38
Total		3	19	65	87



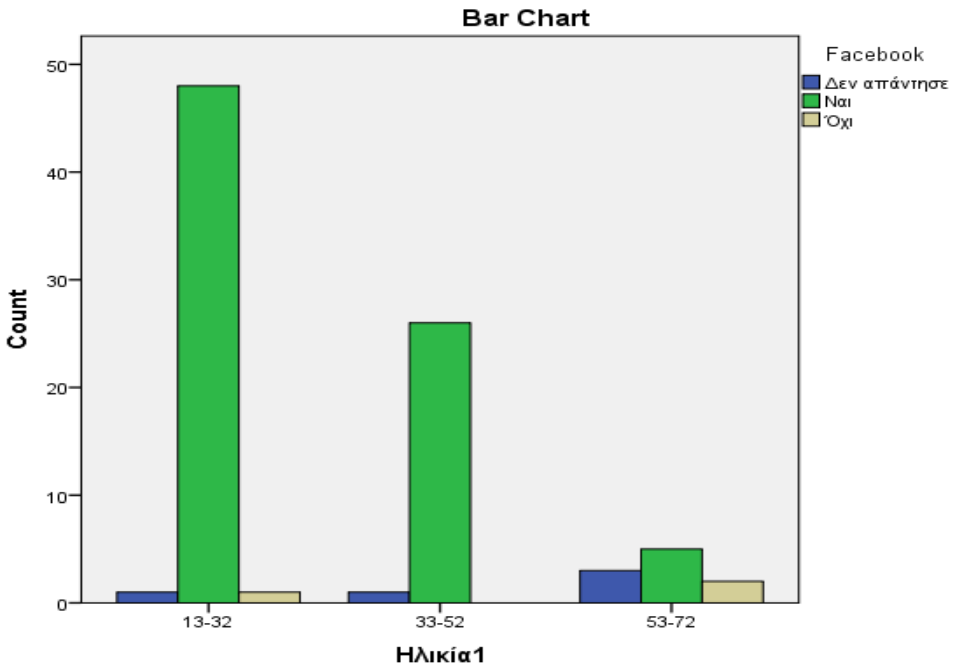
- Ηλικία1 * Facebook, Twitter, LinkedIn, Pinterest, Άλλο

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Ηλικία1 * Facebook	87	96,7%	3	3,3%	90	100,0%
Ηλικία1 * Twitter	87	96,7%	3	3,3%	90	100,0%
Ηλικία1 * LinkedIn	87	96,7%	3	3,3%	90	100,0%
Ηλικία1 * Pinterest	87	96,7%	3	3,3%	90	100,0%
Ηλικία1 * Άλλο	87	96,7%	3	3,3%	90	100,0%

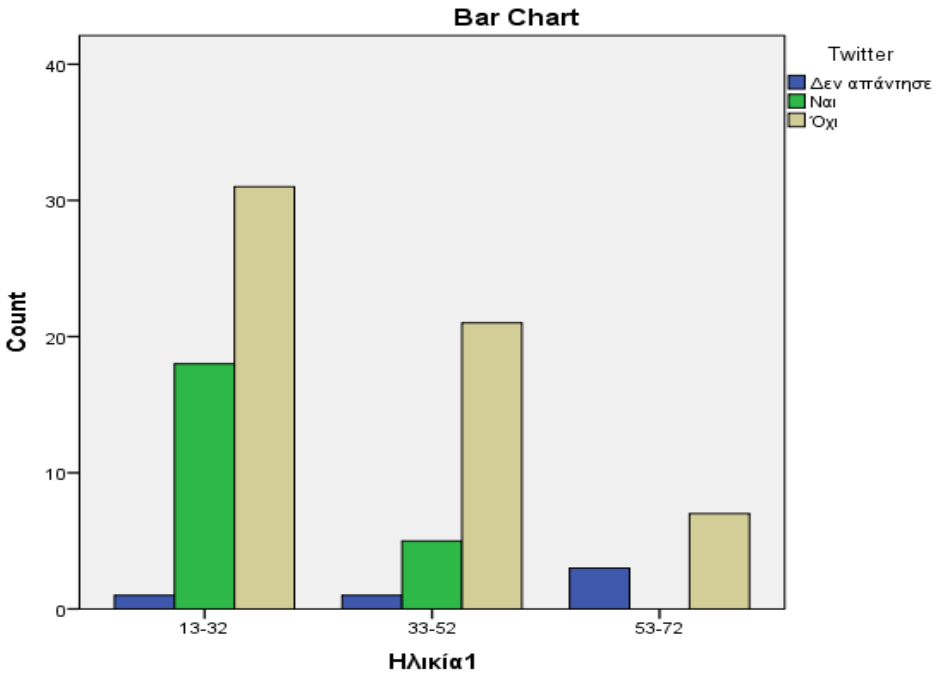
Ηλικία1 * Facebook Crosstabulation

			Facebook			
			Δεν απάντησε	Ναι	Όχι	Total
Ηλικία1	13-32	Count	1	48	1	50
		% within Ηλικία1	2,0%	96,0%	2,0%	100,0%
		% within Facebook	20,0%	60,8%	33,3%	57,5%
		% of Total	1,1%	55,2%	1,1%	57,5%
	33-52	Count	1	26	0	27
		% within Ηλικία1	3,7%	96,3%	0,0%	100,0%
		% within Facebook	20,0%	32,9%	0,0%	31,0%
		% of Total	1,1%	29,9%	0,0%	31,0%
	53-72	Count	3	5	2	10
		% within Ηλικία1	30,0%	50,0%	20,0%	100,0%
		% within Facebook	60,0%	6,3%	66,7%	11,5%
		% of Total	3,4%	5,7%	2,3%	11,5%
Total		Count	5	79	3	87
		% within Ηλικία1	5,7%	90,8%	3,4%	100,0%
		% within Facebook	100,0%	100,0%	100,0%	100,0%
		% of Total	5,7%	90,8%	3,4%	100,0%



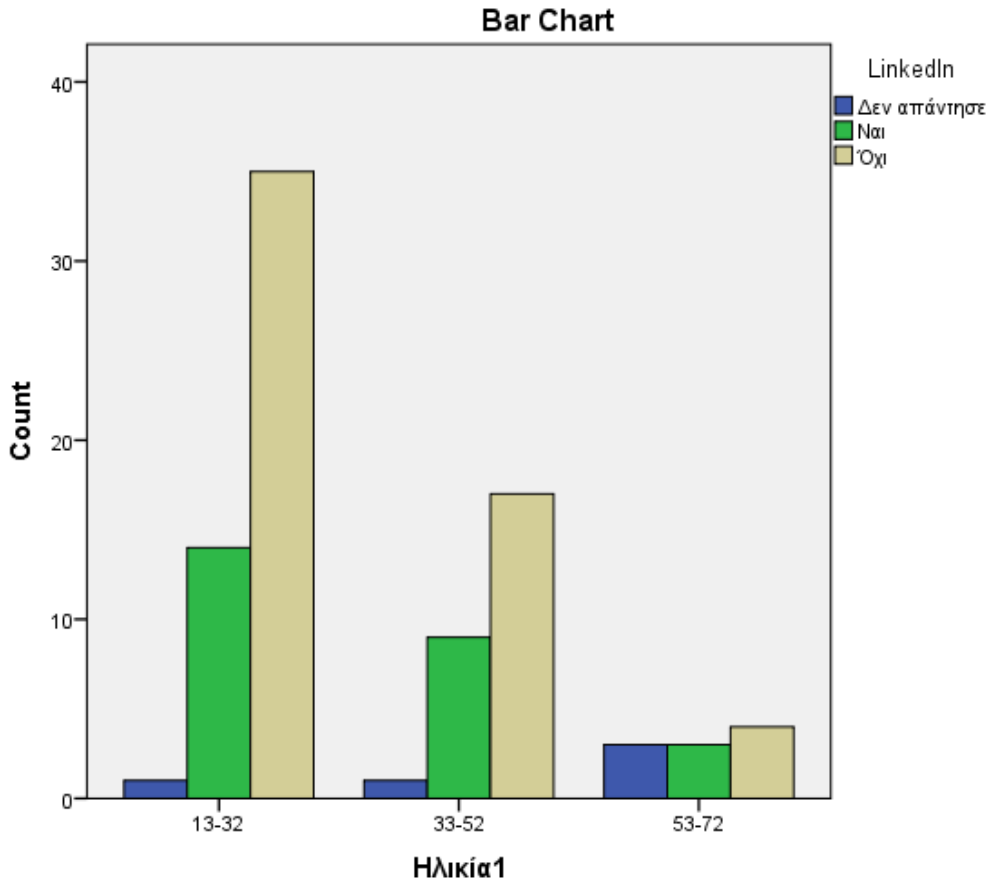
Ηλικία1 * Twitter Crosstabulation

			Twitter			Total
			Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	Count	1	18	31	50
		% within Ηλικία1	2,0%	36,0%	62,0%	100,0%
		% within Twitter	20,0%	78,3%	52,5%	57,5%
		% of Total	1,1%	20,7%	35,6%	57,5%
	33-52	Count	1	5	21	27
		% within Ηλικία1	3,7%	18,5%	77,8%	100,0%
		% within Twitter	20,0%	21,7%	35,6%	31,0%
		% of Total	1,1%	5,7%	24,1%	31,0%
	53-72	Count	3	0	7	10
		% within Ηλικία1	30,0%	0,0%	70,0%	100,0%
		% within Twitter	60,0%	0,0%	11,9%	11,5%
		% of Total	3,4%	0,0%	8,0%	11,5%
Total		Count	5	23	59	87
		% within Ηλικία1	5,7%	26,4%	67,8%	100,0%
		% within Twitter	100,0%	100,0%	100,0%	100,0%
		% of Total	5,7%	26,4%	67,8%	100,0%



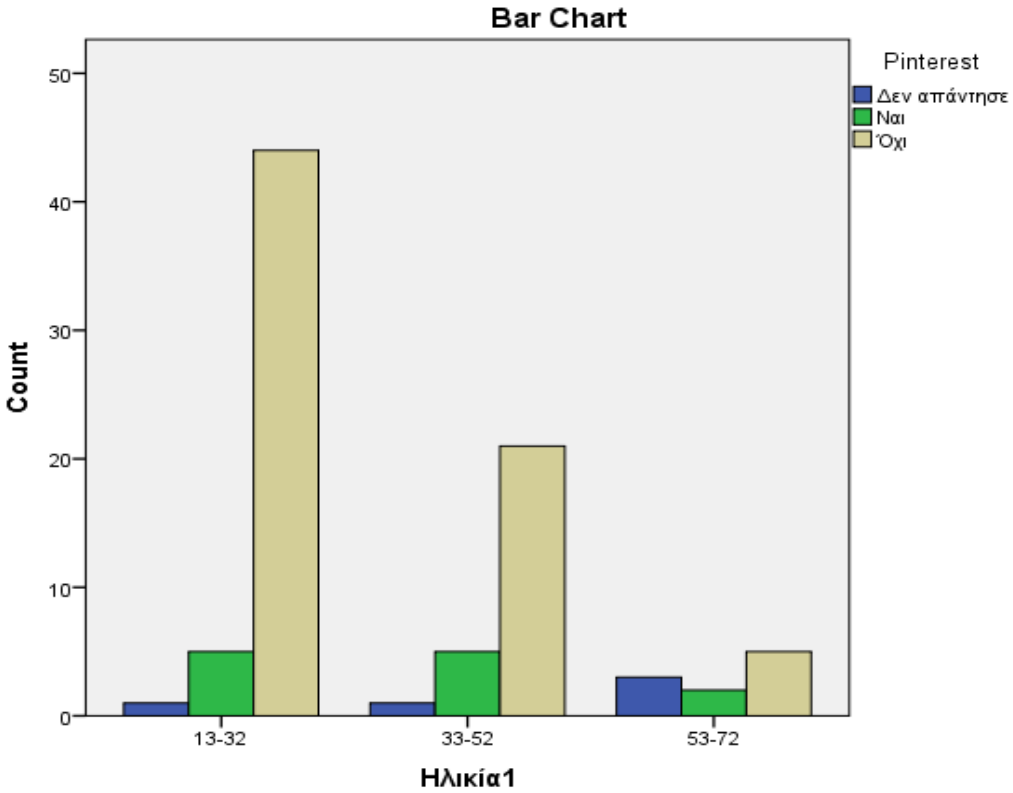
Ηλικία1 * LinkedIn Crosstabulation

			LinkedIn			Total
			Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	Count	1	14	35	50
		% within Ηλικία1	2,0%	28,0%	70,0%	100,0%
		% within LinkedIn	20,0%	53,8%	62,5%	57,5%
		% of Total	1,1%	16,1%	40,2%	57,5%
	33-52	Count	1	9	17	27
		% within Ηλικία1	3,7%	33,3%	63,0%	100,0%
		% within LinkedIn	20,0%	34,6%	30,4%	31,0%
		% of Total	1,1%	10,3%	19,5%	31,0%
	53-72	Count	3	3	4	10
		% within Ηλικία1	30,0%	30,0%	40,0%	100,0%
		% within LinkedIn	60,0%	11,5%	7,1%	11,5%
		% of Total	3,4%	3,4%	4,6%	11,5%
Total		Count	5	26	56	87
		% within Ηλικία1	5,7%	29,9%	64,4%	100,0%
		% within LinkedIn	100,0%	100,0%	100,0%	100,0%
		% of Total	5,7%	29,9%	64,4%	100,0%



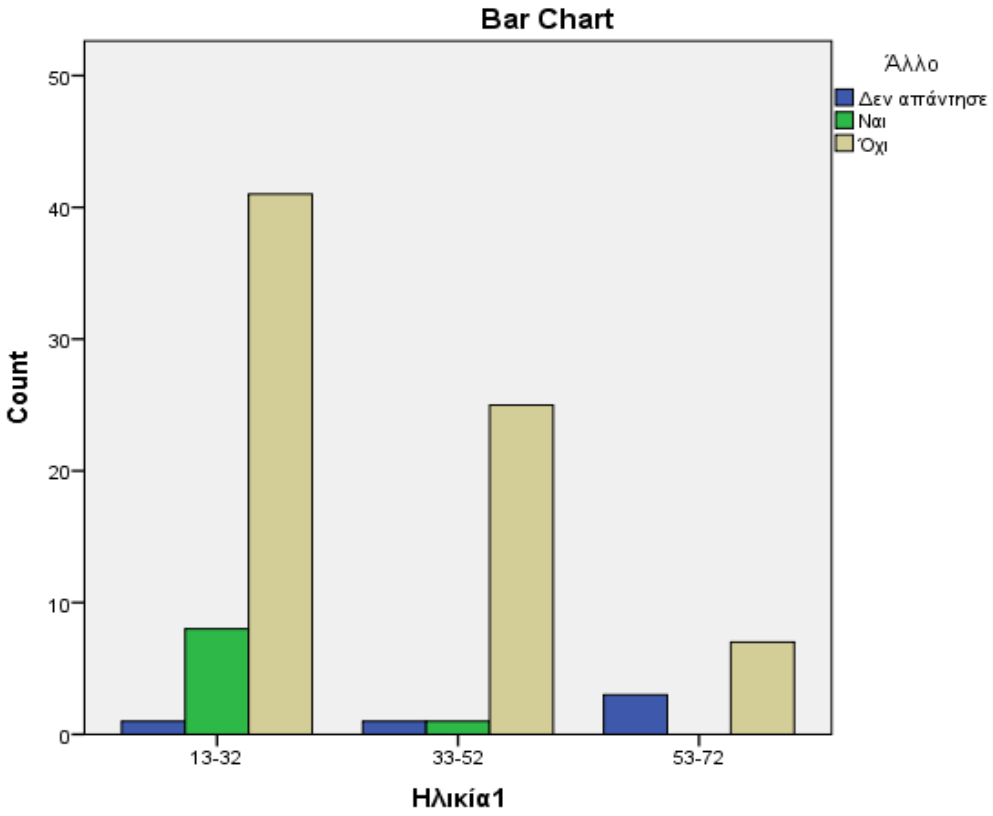
Ηλικία1 * Pinterest Crosstabulation

			Pinterest			
			Δεν απάντησε	Ναι	Όχι	Total
Ηλικία1	13-32	Count	1	5	44	50
		% within Ηλικία1	2,0%	10,0%	88,0%	100,0%
		% within Pinterest	20,0%	41,7%	62,9%	57,5%
		% of Total	1,1%	5,7%	50,6%	57,5%
	33-52	Count	1	5	21	27
		% within Ηλικία1	3,7%	18,5%	77,8%	100,0%
		% within Pinterest	20,0%	41,7%	30,0%	31,0%
		% of Total	1,1%	5,7%	24,1%	31,0%
	53-72	Count	3	2	5	10
		% within Ηλικία1	30,0%	20,0%	50,0%	100,0%
		% within Pinterest	60,0%	16,7%	7,1%	11,5%
		% of Total	3,4%	2,3%	5,7%	11,5%
Total		Count	5	12	70	87
		% within Ηλικία1	5,7%	13,8%	80,5%	100,0%
		% within Pinterest	100,0%	100,0%	100,0%	100,0%
		% of Total	5,7%	13,8%	80,5%	100,0%



Ηλικία1 * Άλλο Crosstabulation

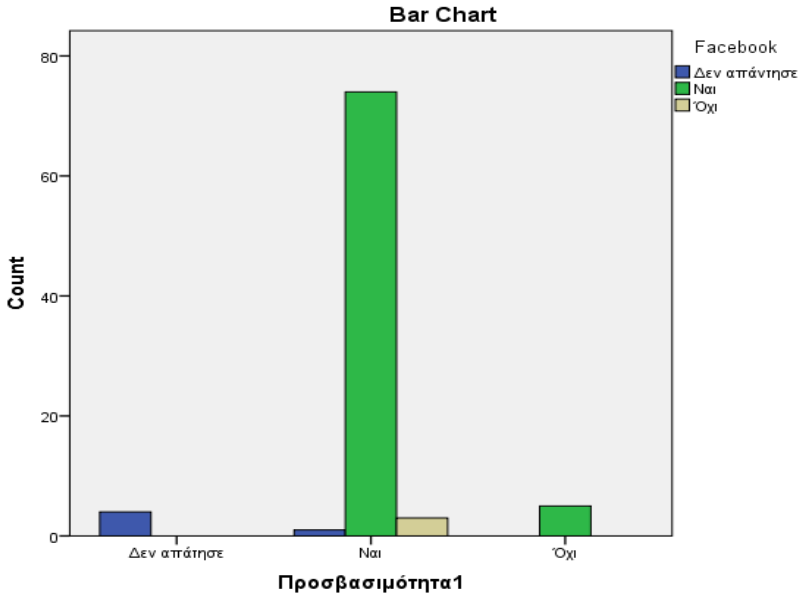
			Άλλο			
			Δεν απάντησε	Ναι	Όχι	Total
Ηλικία1	13-32	Count	1	8	41	50
		% within Ηλικία1	2,0%	16,0%	82,0%	100,0%
		% within Άλλο	20,0%	88,9%	56,2%	57,5%
		% of Total	1,1%	9,2%	47,1%	57,5%
	33-52	Count	1	1	25	27
		% within Ηλικία1	3,7%	3,7%	92,6%	100,0%
		% within Άλλο	20,0%	11,1%	34,2%	31,0%
		% of Total	1,1%	1,1%	28,7%	31,0%
	53-72	Count	3	0	7	10
		% within Ηλικία1	30,0%	0,0%	70,0%	100,0%
		% within Άλλο	60,0%	0,0%	9,6%	11,5%
		% of Total	3,4%	0,0%	8,0%	11,5%
Total		Count	5	9	73	87
		% within Ηλικία1	5,7%	10,3%	83,9%	100,0%
		% within Άλλο	100,0%	100,0%	100,0%	100,0%
		% of Total	5,7%	10,3%	83,9%	100,0%



- Προσβασιμότητα* Facebook, Twitter, LinkedIn, Pinterest, Άλλο

Count

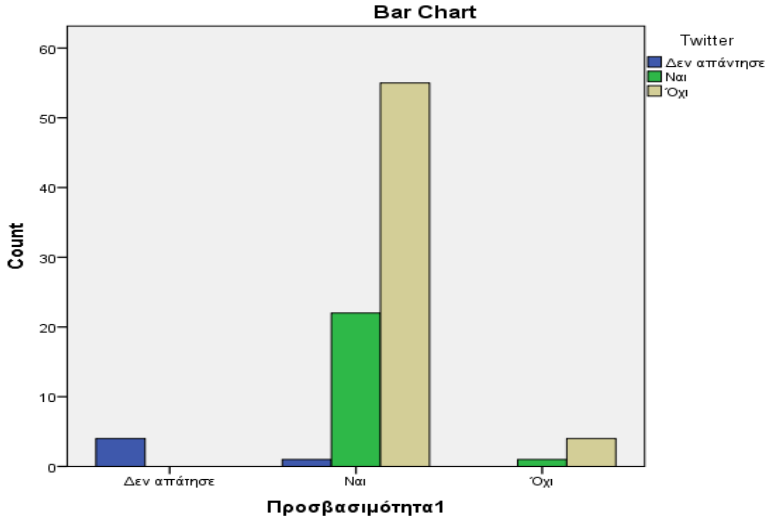
		Facebook			
		Δεν απάντησε	Ναι	Όχι	Total
Προσβασιμότητα1	Δεν απάτησε	4	0	0	4
	Ναι	1	74	3	78
	Όχι	0	5	0	5
Total		5	79	3	87



Crosstab

Count

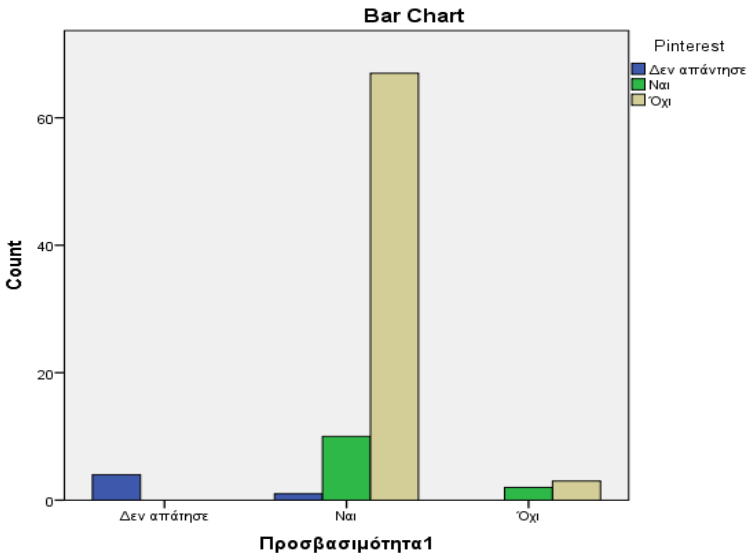
		Twitter			
		Δεν απάντησε	Ναι	Όχι	Total
Προσβασιμότητα1	Δεν απάτησε	4	0	0	4
	Ναι	1	22	55	78
	Όχι	0	1	4	5
Total		5	23	59	87



Crosstab

Count

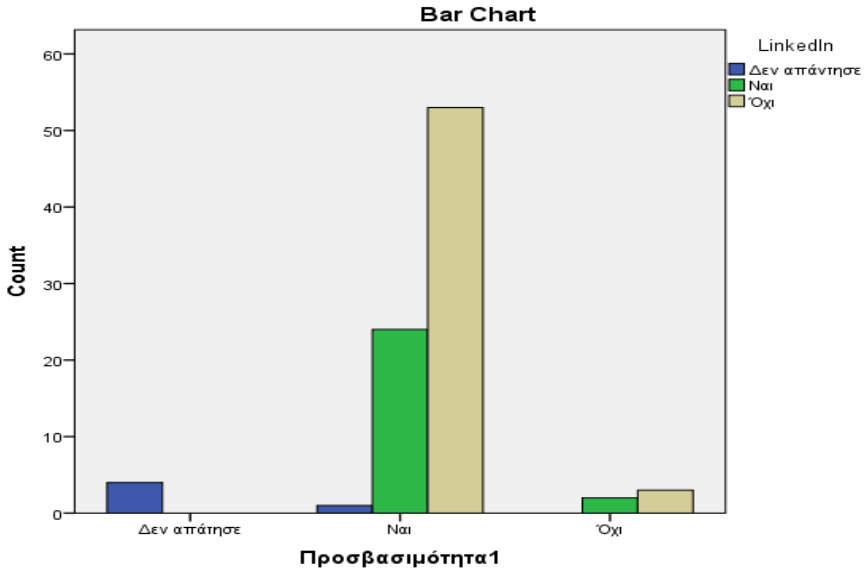
		Pinterest			Total
		Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα1	Δεν απάτησε	4	0	0	4
	Ναι	1	10	67	78
	Όχι	0	2	3	5
Total		5	12	70	87



Crosstab

Count

		LinkedIn			Total
		Δεν απάντησε	Ναι	Όχι	
Προσβασιμότητα1	Δεν απάτησε	4	0	0	4
	Ναι	1	24	53	78
	Όχι	0	2	3	5
Total		5	26	56	87

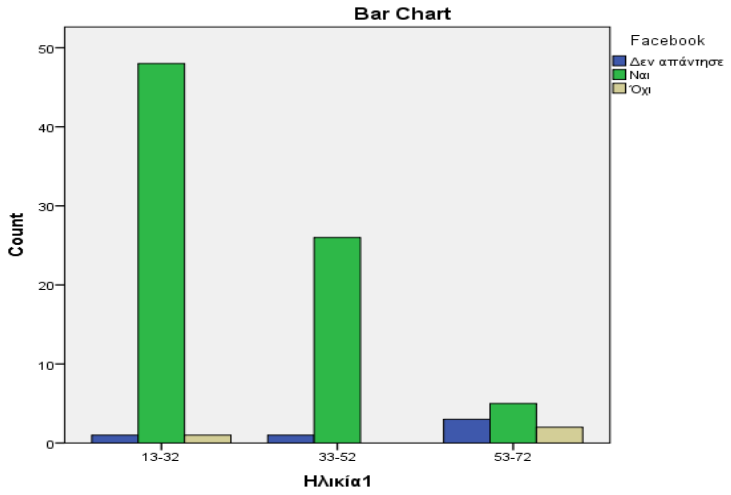


- Ηλικία* Facebook

Crosstab

Count

		Facebook			Total
		Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	1	48	1	50
	33-52	1	26	0	27
	53-72	3	5	2	10
Total		5	79	3	87

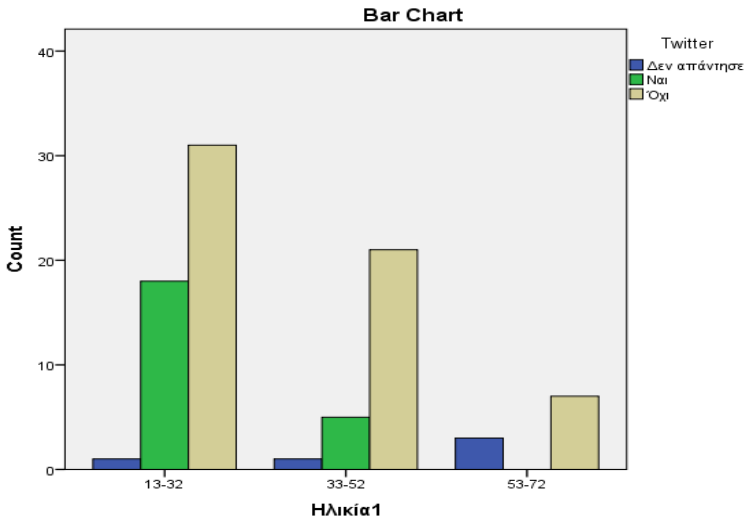


- Ηλικία* Twitter

Crosstab

Count

		Twitter			Total
		Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	1	18	31	50
	33-52	1	5	21	27
	53-72	3	0	7	10
Total		5	23	59	87

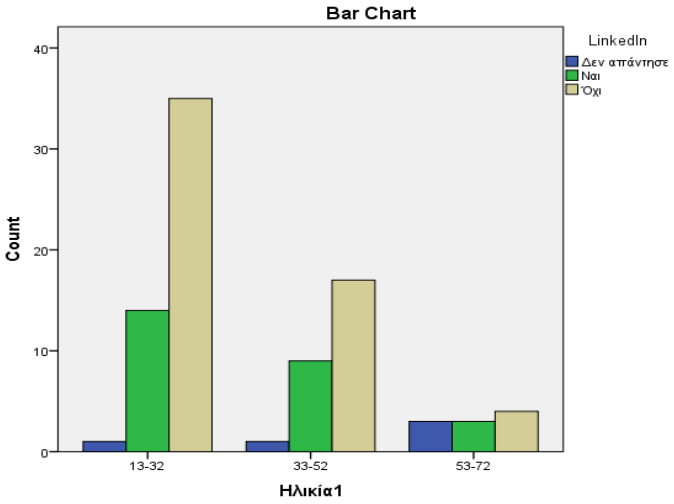


- Ηλικία* LinkedIn

Crosstab

Count

		LinkedIn			Total
		Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	1	14	35	50
	33-52	1	9	17	27
	53-72	3	3	4	10
Total		5	26	56	87

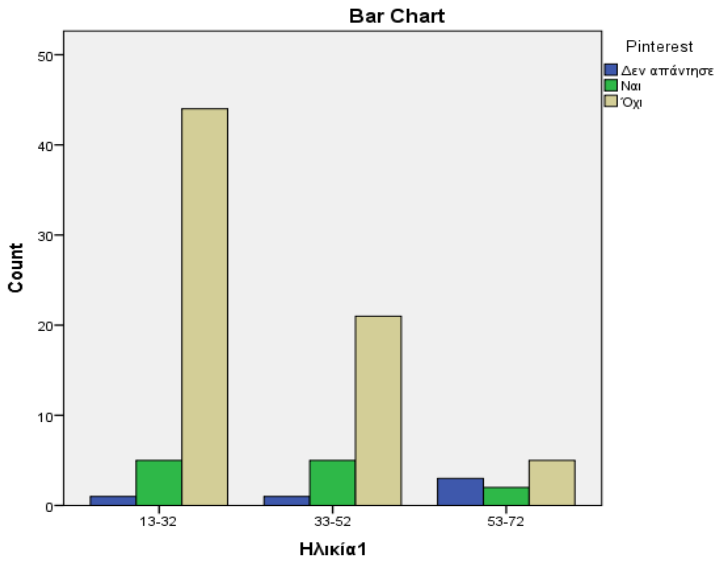


- Ηλικία* Pinterest

Crosstab

Count

		Pinterest			Total
		Δεν απάντησε	Ναι	Όχι	
Ηλικία1	13-32	1	5	44	50
	33-52	1	5	21	27
	53-72	3	2	5	10
Total		5	12	70	87



- Ηλικία* Συχνότητα_Σύνδεσης

Correlations

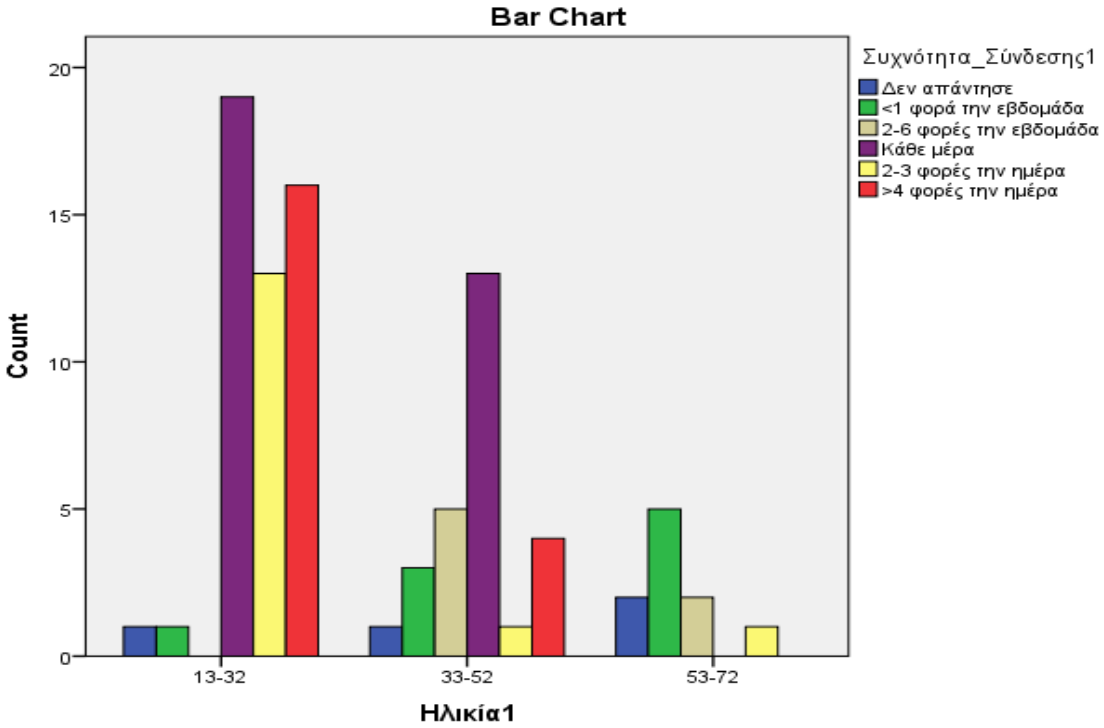
		Ηλικία1	Συχνότητα_Σύνδεσης1
Ηλικία1	Pearson Correlation	1	-,579**
	Sig. (2-tailed)		,000
	N	87	87
Συχνότητα_Σύνδεσης1	Pearson Correlation	-,579**	1
	Sig. (2-tailed)	,000	
	N	87	87

**. Correlation is significant at the 0.01 level (2-tailed).

Crosstab

Count

	Συχνότητα_Σύνδεσης1						
	Δεν απάντησε	<1 φορά την εβδομάδα	2-6 φορές την εβδομάδα	Κάθε μέρα	2-3 φορές την ημέρα	>4 φορές την ημέρα	Total
13-32	1	1	0	19	13	16	50
33-52	1	3	5	13	1	4	27
53-72	2	5	2	0	1	0	10
Total	4	9	7	32	15	20	87

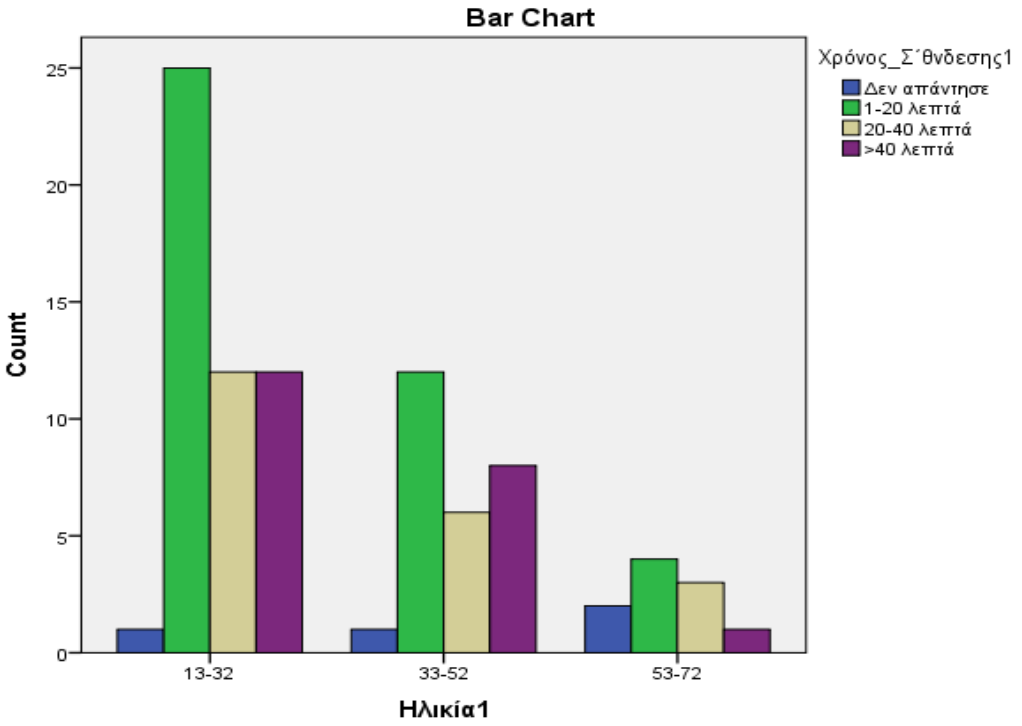


- Ηλικία* Χρόνος_Σύνδεσης

Crosstab

Count

		Χρόνος_Σύνδεσης				
		Δεν απάντησε	1-20 λεπτά	20-40 λεπτά	>40 λεπτά	Total
Ηλικία	13-32	1	25	12	12	50
	33-52	1	12	6	8	27
	53-72	2	4	3	1	10
Total		4	41	21	21	87

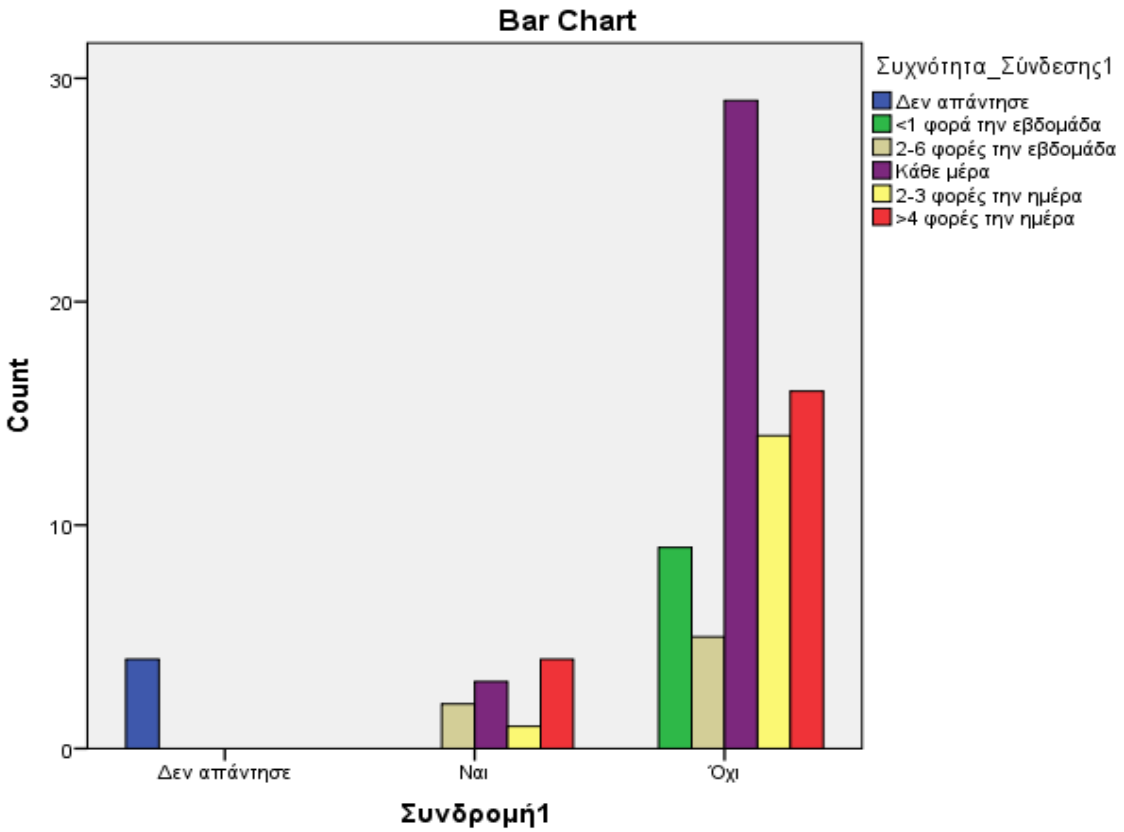


- Συνδρομή1 * Συχνότητα_Σύνδεσης1

Crosstabulation

Count

	Συχνότητα_Σύνδεσης						
	Δεν απάντησε	<1 φορά την εβδομάδα	2-6 φορές την εβδομάδα	Κάθε μέρα	2-3 φορές την ημέρα	>4 φορές την ημέρα	Total
Δεν απάντησε	4	0	0	0	0	0	4
Ναι	0	0	2	3	1	4	10
Όχι	0	9	5	29	14	16	73
Total	4	9	7	32	15	20	87



- Συνδρομή1 * Δημόσια_Στοιχεία1

Correlations

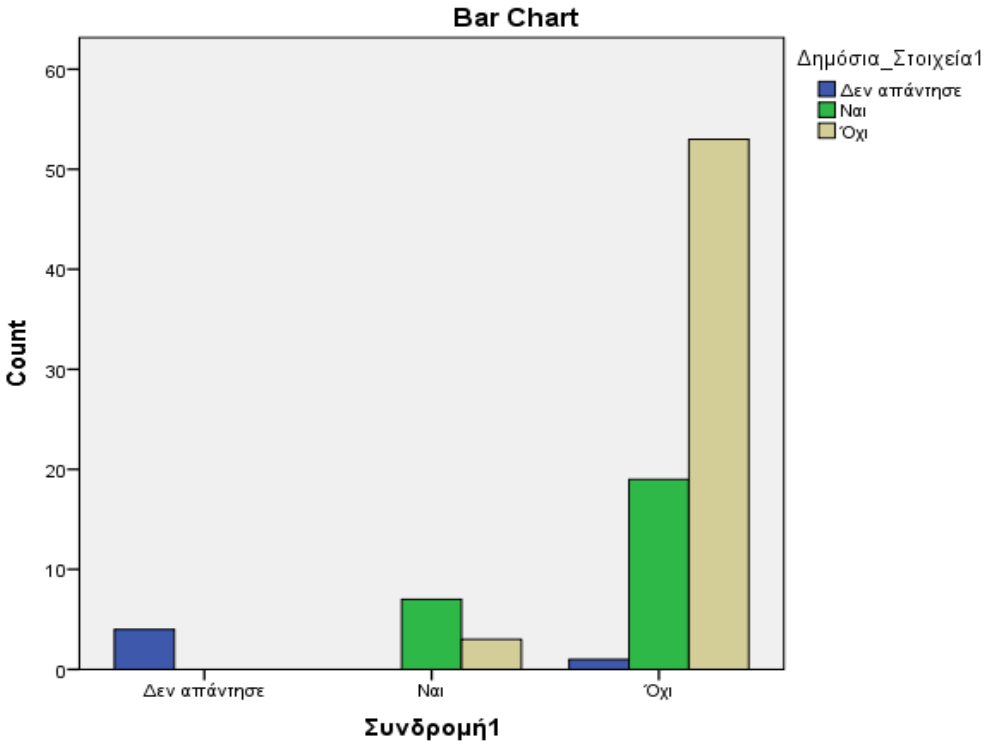
		Συνδρομή	Δημόσια_Στοιχεία
Συνδρομή	Pearson Correlation	1	,591**
	Sig. (2-tailed)		,000
	N	87	87
Δημόσια_Στοιχεία	Pearson Correlation	,591**	1
	Sig. (2-tailed)	,000	
	N	87	87

**. Correlation is significant at the 0.01 level (2-tailed).

Συνδρομή * Δημόσια_ΣτοιχείαCrosstabulation

Count

		Δημόσια_Στοιχεία			
		Δεν απάντησε	Ναι	Όχι	Total
Συνδρομή	Δεν απάντησε	4	0	0	4
	Ναι	0	7	3	10
	Όχι	1	19	53	73
Total		5	26	56	87

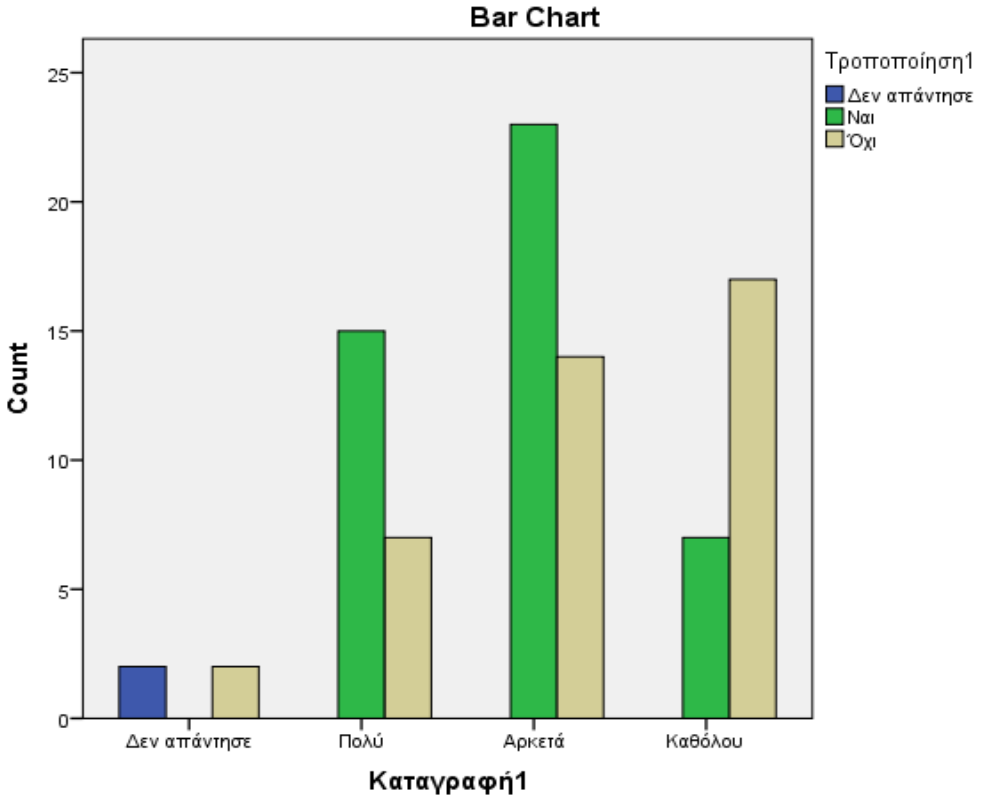


- Καταγραφή * Τροποποίηση

Καταγραφή * Τροποποίηση Crosstabulation

Count

		Τροποποίηση			Total
		Δεν απάντησε	Ναι	Όχι	
Καταγραφή	Δεν απάντησε	2	0	2	4
	Πολύ	0	15	7	22
	Αρκετά	0	23	14	37
	Καθόλου	0	7	17	24
Total		2	45	40	87



2. Ερωτηματολόγιο

Προστασία προσωπικών δεδομένων στα κοινωνικά δίκτυα

Η παρούσα έρευνα πραγματοποιείται στα πλαίσια διπλωματικής εργασίας με τίτλο: " Η προστασία των προσωπικων δεδομένων στα κοινωνικά δίκτυα στην Ελλάδα", του Πανεπιστημίου Πελοποννήσου. Με τον όρο "προσωπικά δεδομένα" αναφερόμαστε στις ιδιωτικές πληροφορίες που δεν κοινοποιούνται δημοσίως. Στην παρούσα έρευνα θα εξεταστούν τα προσωπικά δεδομένα που χρησιμοποιούνται στο διαδίκτυο. Σκοπός της είναι η διερεύνηση του ενδιαφέροντος ως προς το θέμα της προστασίας των προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης. Η έρευνα δεν είναι ονομαστική.

1. **Φύλο**
   Mark only one oval.
   - ◯ Άρρεν
   - ◯ Θήλυ

2. **Ηλικία**

3. **Οικογενειακή κατάσταση**
   Mark only one oval.
   - ◯ Άγαμος/η
   - ◯ Έγγαμος/η
   - ◯ Χήρος/α
   - ◯ Διαζευγμένος/η

4. **Επίπεδο εκπαίδευσης**
   Mark only one oval.
   - ◯ Γυμνάσιο
   - ◯ Γενικό Λύκειο
   - ◯ ΑΤΕΙ, ΤΕΙ, ΚΑΤΕΕ, ΑΣΠΑΙΤΕ
   - ◯ ΑΕΙ, Ανοιχτό Πανεπιστήμιο
   - ◯ Μεταπτυχιακό
   - ◯ Διδακτορικό
   - ◯ Other: _____

5. **Κύρια ασχολία**
   Mark only one oval.
   - ◯ Μισθωτός
   - ◯ Αυτοαπασχολούμενος
   - ◯ Άνεργος
   - ◯ Μαθητής, Φοιτητής

6. **Έχετε ηλεκτρονικό υπολογιστή στην κατοικία σας;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

7. **Έχετε πρόσβαση στο διαδίκτυο στην κατοικία σας;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

8. **Πόσο συχνά χρησιμοποιείτε κατά μέσο όρο το διαδίκτυο;**
Mark only one oval.

- ◯ Κάθε μέρα ή σχεδόν κάθε μέρα
- ◯ Τουλάχιστον μια φορά την εβδομάδα
- ◯ Λιγότερο από μια φορά την εβδομάδα

9. **Ποια/ποιες από τις παρακάτω συσκευές χρησιμοποιείτε κυρίως για την σύνδεσή σας στο διαδίκτυο;**
Mark only one oval.

- ◯ Υπολογιστή (σταθερό, φορητό, tablet)
- ◯ Κινητό τηλέφωνο

10. **Για ποιους λόγους χρησιμοποιείτε κυρίως το διαδίκτυο;**
Check all that apply.

- ☐ Για επικοινωνία
- ☐ Για πρόσβαση σε πληροφορίες
- ☐ Για ψυχαγωγία
- ☐ Για υγεία
- ☐ Για online υπηρεσίες

11. **Χρησιμοποιείτε το διαδίκτυο για να πραγματοποιείτε αγορές;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

12. **Αν ναι, τα προϊόντα ή οι υπηρεσίες που αγοράσατε μέσω διαδικτύου προέρχονταν από:**
Check all that apply.

- ☐ Εγχώριους πωλητές
- ☐ Πωλητές εντός της Ε.Ε.
- ☐ Πωλητές εκτός της Ε.Ε.
- ☐ Δεν γνωρίζω

13. **Ποιο από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στο διαδίκτυο;**
Check all that apply.

- [ ] Προσωπικά στοιχεία
- [ ] Στοιχεία επικοινωνίας
- [ ] Στοιχεία πληρωμών
- [ ] Άλλα προσωπικά στοιχεία (φωτογραφίες, τοποθεσίες, εισόδημα κ.α.)
- [ ] Κανένα στοιχείο

14. **Έχετε προβεί σε κάποια από τις παρακάτω ενέργειες για να διαχειριστείτε τις ρυθμίσεις πρόσβασης σε προσωπικά σας δεδομένα;**
Check all that apply.

- [ ] Διαβάσατε την πολιτική απορρήτου προτού δώσετε προσωπικά σας στοιχεία
- [ ] Επιλέξατε να υπάρχει περιορισμένη πρόσβαση σε προσωπικά σας στοιχεία
- [ ] Αρνηθήκατε να χρησημοποιηθούν τα προσωπικά σας στοιχεία για διαφημηστικούς λόγους
- [ ] Ελέγξατε την ασφάλεια της ιστοσελίδας προτου δώσετε τα προσωπικά σας στοιχεία
- [ ] Ζητήσατε από ιστοσελιδες που τηρούν προσωπικά σας στοιχεία πως μπορίτε να έχετε πρόσβαση σε αυτά για να τα επικαιροποιήσετε ή να τα διαγράψετε

15. **Γνωρίζετε ότι τα cookies μπορούν να χρησιμοποιηθούν για ανίχνευση των κινήσεων στο διαδίκτυο και στην συνέχεια για την δημιουργία προφίλ του κάθε χρήστη και την αποστολή διαφημίσεων για θέματα που τον ενδιαφέρουν;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

16. **Πόσο σας απασχολεί το γεγονός ότι οι online δραστηριότητές σας στο διαδίκτυο καταγράφονται προκειμένου να χρησιμοποιηθούν για την αποστολή διαφημίσεων για θέματα που σας ενδιαφέρουν;**
Mark only one oval.

- ◯ Πολύ
- ◯ Αρκετά
- ◯ Καθόλου

17. **Έχετε ποτέ τροποποιήσει τις παραμέτρους των προγραμμάτων πλοήγησης προκειμένου να αποφύγετε ή να περιορίσετε την είσοδο cookies στον υπολογιστή σας;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

18. **Χρησιμοποιείτε αντι-ανιχνευτικά προγράμματα προκειμένου να περιορίσετε τη δυνατότητα ανίχνευσης των δραστηριοτήτων σας στο διαδίκτυο;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

19. **Διατηρείτε λογαριασμό σε κάποια από τις παρακάτω σελίδες κοινωνικής δικτύωσης;**
Check all that apply.

- [ ] Facebook
- [ ] Twitter
- [ ] LinkedIn
- [ ] Pinterest
- [ ] Other: .....

20. **Ποια από τα παρακάτω στοιχεία που έχετε δώσει στα δίκτυα κοινωνικής δικτύωσης είναι πραγματικά;**
Check all that apply.

- [ ] Όνομα
- [ ] Ηλικία
- [ ] Φωτογραφία
- [ ] Τηλέφωνο
- [ ] Διεύθυνση
- [ ] Εργασία

21. **Πόσο συχνά επισκέπτεστε την σελίδα κοινωνικής δικτύωσης;**
Mark only one oval.

- ◯ <1 φορά την εβδομάδα
- ◯ 2-6 φορές την εβδομάδα
- ◯ Κάθε μέρα
- ◯ 2-3 φορές την ημέρα
- ◯ >4 φορές την ημέρα

22. **Πόσο χρόνο αφιερώνεται σε κάθε σας σύνδεση στις σελίδες κοινωνικής δικτύωσης;**
Mark only one oval.

- ◯ 1-20 λεπτά
- ◯ 20-40 λεπτά
- ◯ >40 λεπτά

23. **Η σύνδεση στον λογαριασμό σας πραγματοποιείτε από:**
Check all that apply.

- [ ] Το σπίτι
- [ ] Internet cafe
- [ ] Χώρο εργασίας/σπουδών
- [ ] Χώρο διασκέδασης

24. **Τα προσωπικά σας στοιχεία είναι δημόσια κοινοποιημένα στις σελίδες κοινωνικής δικτύωσης σας;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

25. **Έχετε κάνει τις απαραίτητες ρυθμίσεις ώστε να ελέγχετε σε ποιους είναι ορατά τα στοιχεία που αναρτάται;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

26. **Θέλετε να μπορείτε να επιλέγετε ποιοι θα έχουν πρόσβαση στο περιεχόμενο που κοινοποιείτε στον λογαριασμό σας;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

27. **Θα συνεχίζατε να χρησιμοποιείτε τις ιστοσελίδες κοινωνικής δικτύωσης εάν απαιτούσαν συνδρομή;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

28. **Έχετε διαβάσει τους "όρους χρήσεις" και την " πολιτική απορρήτου" των σελίδων κοινωνικής δικτύωσης στις οποίες διαθέτετε λογαριασμό/ους;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

29. **Θεωρείτε ότι οι σελίδες κοινωνικής δικτύωσης είναι ασφαλείς;**
Mark only one oval.

- ◯ Ναι
- ◯ Όχι

Powered by
Google Forms

3. Κατάλογος Αναφορών

Βιβλιογραφία

- Αλεξανδροπούλου-Αιγυπτιάδου Ευγενία, Ζητήματα από το Δίκαιο της Πληροφορικής, εκδόσεις Σάκκουλα, Αθήνα – Κομοτηνή, 2002

- Αρμαμέντος Δ. Παναγιώτης, Σωτηρόπουλος Α. Βασίλης, Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2005

- Βλαχόπουλος Κωνσταντίνος, Ηλεκτρονικό Έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, 2007

- Γέροντας Απόστολος, Η Προστασία Του Πολίτη Από Την Ηλεκτρονική Επεξεργασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα, 2002

- Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Πληροφοριακών Συστημάτων, εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004

- Ελληνική Εταιρία Ηλεκτρονικών Υπολογιστών και Πληροφορικής, Ασφάλεια Πληροφοριών: Τεχνικά, Νομικά και Κοινωνικά Θέματα, Αθήνα 1995

- Ιγγλεζάκης Ιωάννης, Ευαίσθητα Προσωπικά Δεδομένα, εκδόσεις Σάκκουλα, 2004

- Καράκωστας Κ. Ιωάννης, Δίκαιο & Internet, Νομικά ζητήματα του Διαδικτύου, εκδόσεις Σάκκουλα, 2Κ01

- Λαζακίδου Α. Αθηνά, Σύγχρονες Τεχνολογίες και Υπηρεσίες Πληροφορικής και Τηλεπικοινωνιών

- Λαζακίδου Α. Αθηνά, Χατζημιτσης Γ. Διοφαντος, Ευαγγέλου Ε. Ιορδάνης, Εικονικός Κόσμος Και Νέες Τεχνολογίες, εκδόσεις Κλειδάριθμος

- Μήτρου Λίλιαν, Προστασία Προσωπικών Δεδομένων, εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004

- Νούσκαλης Γεώργιος, Ποινική Προστασία Προσωπικών Δεδομένων, εκδόσεις Σάκκουλα 2005

- Σιδηρόπουλος Θεόδωρος, Το Δίκαιο Του Διαδικτύου, εκδόσεις Σάκκουλα, 2003,

- Χοχλιούρος Π. Ιωάννης, Θέματα Ασφάλειας Ηλεκτρονικών Υποδομών Και Εφαρμογών, Διασφάλιση Του Απορρήτου Και Νόμιμη Παρακολούθηση Των Επικοινωνιών, Εκδόσεις Σάκκουλα 2006

- Diamond Ian and Jefferies Julie, Αρχίζοντας Την Στατιστική: Μια Εισαγωγή Για Τους Κοινωνικούς Επιστήμονες, εκδόσεις Παπαζήση, 2006

- Eloff, M.M., and von Solms, S.H., Information Security Management: An Approach to Combine Process Certification and Product Evaluation, Computers & Security, 2000

- Garfinkel Simson with Spafford Gene, Web Security, Privacy & Commerce, O'REILLY, 2002, 2nd Edition

- Harrington L. Jan, Network Security: A Practical Approach, Morgan Kaufmann Publishers, 2005

- Lindskog Helena and Lindskog Stefan, Web Site Privacy with P3P, Wiley Publishing, 2003

- Pfleeger P. Charles and Pfleeger Shari Lawrence, Security in Computing, Prentice Hall, 4th Edition, 2007

- Robson Colin , Η Έρευνα Του Πραγματικού Κόσμου: Ένα Μέσον Για Κοινωνικούς Επιστήμονες Και Επαγγελματίες Ερευνητές, GUTENBERG, 2007

- Woodcock Jo Anne, Εισαγωγή στα δίκτυα Υπολογιστών, Κλειδάριθμος 2003

Ιστότοποι

- Ασφάλεια ανηλίκων YouTube, Διαθέσιμο σε: https://support.google.com/youtube/answer/2802244, (last view 03/09/2016)

- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,123482&_dad=portal, (last view 25/10/2016)

- Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα, Διαθέσιμο σε: http://www.dpa.gr/portal/page?_pageid=33,123482&_dad=portal&_schema=PORTAL, (last view 26/10/2016)

- Αρχή Προστασία Δεδομένων Προσωπικού Χαρακτήρα, Διαθέσιμο σε: http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/LAW/NOMOTHESIA%20PR

OSOPIKA%20DEDOMENA/FILES/CELEX_32016L0681_EL_TXT.PDF, (last view 29/10/2016)

- Η Βρετανία επενδύει 2,32 δισ. δολάρια στη διαδικτυακή ασφάλεια, Διαθέσιμο σε: http://www.skai.gr/news/technology/article/329415/vretania-ependuseis-232-dis-dolarion-gia-ti-diadiktuaki-asfaleia/, (last view 06/11/2016)

- Μεταπτυχιακό Πρόγραμμα στη Λογιστική & Χρηματοοικονομική Master of Science (MSc) in Accounting and Finance ΤΕΙ ΠΕΙΡΑΙΑ, Διαθέσιμο σε: http://mscinaccounting.teipir.gr/uploads/0b7ced8314f51ffea03704122c399f32.pdf , (last view 07/11/2016)

- Πολιτική Απορρήτου της Google, Διαθέσιμο σε: https://www.google.com/intl/el/policies/privacy/#infocollect, (last view 03/09/2016)

- Πολιτική Απορρήτου της Google, Διαθέσιμο σε: https://www.google.com/intl/el/policies/privacy/#infouse, (last view 03/09/2016)

- Πολιτική Απορρήτου της Google, Διαθέσιμο σε: https://privacy.google.com/intl/el/how-ads-work.html, (last view 03/09/2016)

- Πολιτική Απορρήτου της Google, Διαθέσιμο σε:
- https://www.google.com/intl/el/policies/privacy/, (last view 03/09/2016)

- ΠρώτοΘέμα.gr, Διαθέσιμο σε: http://www.prototothema.gr/economy/article/606619/stathera-proti-stin-anergia-i-ellada-me-235/, (last view 27/11/2016)

- Συμβούλιο της Ευρώπης 2014, Εγχειρίδιο Ευρωπαϊκής Νομοθεσίας Για Την Προστασία Προσωπικών Δεδομένων, Διαθέσιμο σε: http://www.adae.gr/fileadmin/docs/Handbook_data_protection_ELL.pdf, (last view 25/10/2016)

- Φακιόλας Νικόλαος, Επίδραση κοινωνικών δικτύων στην υγεία, e-publishing, 2012, Διαθέσιμο σε: file:///C:/Users/Maria/Downloads/6716-11898-1-SM%20(1).pdf, (last view 04/09/2016)

- CNN, 15 companies that will change the world, Available at: http://money.cnn.com/galleries/2007/biz2/0708/gallery.next_disruptors.biz2/7.html, (last view 11/10/2016)

- Common Criteria, Available at: http://www.commoncriteria.org/, (last view 13/09/2016)

- Cyberkid, Available at: http://www.cyberkid.gov.gr/, (last view 10/11/2016)

- EUR-Lex, Access to European Union law, Available at: http://eur-lex.europa.eu/legal-content/EL/TXT/?toc=OJ%3AL%3A2016%3A119%3ATOC&uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ELL, (last view 26/10/2016)

- Facebook, Οι εταιρείες του Facebook, Available at: https://www.facebook.com/help/111814505650678, (last view 03/10/2016)

- Facebook, Ποια είναι η διαφορά μεταξύ απενεργοποίησης και διαγραφής του λογαριασμού μου; Available at: https://www.facebook.com/help/125338004213029 , (last view 03/10/2016)

- Facebook, Πολιτική Δεδομένων, Available at: https://www.facebook.com/privacy/explanation, (last view 03/10/2016)

- Facebook, Τα προσωπικά δεδομένα σας, Available at: https://www.facebook.com/help/330229433729799/ , (last view 03/10/2016)

- Facebook, Τι είναι ο έλεγχος ασφάλειας και πώς μπορώ να τον ξεκινήσω;, Available at: https://www.facebook.com/help/android-app/799880743466869?ref=related, (last view 03/10/2016)

- Finding the Missing Link for Big Biomedical Data, Available at: http://jamanetwork.com/journals/jama/article-abstract/1883026, (last view 11/10/2016)

- LinkedIn, Available at: https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv, (last view 03/09//2016)

- LinkedIn, Available at: http://www.cnn.gr/money/tech/story/32746/logariasmoi-toy-linkedin-poloyntai-sto-darknet , (last view 30/9/2016)

- LinkedIn, Available at: https://ourstory.linkedin.com/#year-2014, (last view 07/10/2016)

- LinkedIn, Available at: https://www.linkedin.com/uas/login, (last view 07/10/2016)

- LinkedIn, Available at: https://www.linkedin.com/help/linkedin?lang=en, (last view 07/10/2016)

- Information Security Adviser, Available at: http://informationsecurityadviser.co.uk/cia-triad/, (last view 04/11/2016)

- Patientslikeme, About us, Available at: https://www.patientslikeme.com/about, (last view 11/10/2016)

- Patientslikeme, Available at: http://patientslikeme_posters.s3.amazonaws.com/2013_PatientsLikeMe%20epilepsy%20community-%20factors%20affecting%20quality%20of%20life.pdf, (last view 11/10/2016)

- Patientslikeme, Partners, Available at: https://www.patientslikeme.com/about/partners, (last view 11/10/2016)

- Patientslikeme, Privacy Policy, Available at: https://www.patientslikeme.com/about/privacy, (last view 13/10/2016)

- Patientslikeme, Publications & talks, Available at: https://www.patientslikeme.com/research/publications, (last view 11/10/2016)

- Patientslikeme, Our philosophy, Available at: https://www.patientslikeme.com/about/openness, (last view 13/10/2016)

- Patientslikeme, Terms and Conditions of Use, Available at: https://www.patientslikeme.com/about/user_agreement, (last view 11/10/2016)

- Pinterest, Available at: http://www.engauge.com/assets/pdf/Engauge-Pinterest.pdf, (last view 30/09/2016)

- Pinterest, Privacy Policy, Available at: https://about.pinterest.com/el/privacy-policy, (last view 30/09/2016)

- Pinterest, Privacy Policy, Available at: https://about.pinterest.com/en/privacy-policy, (last view 30/09/2016)

- SimilarWeb, «Top 50 sites in the world for Arts And Entertainment > TV And Video», Available at: https://www.similarweb.com/top-websites/category/arts-and-entertainment/tv-and-video

- Smolan Rick , Erwitt Jennifer, The Human Face Of Data, Available at: http://www.humanfaceofbigdata.com/ , (last view 07/10/2016)

- STATISTA, Facebook's Remarkable User Growth, https://www.statista.com/chart/870/facebooks-user-growth-since-, (last view 17/12/2016)

- Twitter, Available at: https://about.twitter.com/company, (last view 03/10/2016)

- Twitter, Available at: https://twitter.com/tos?lang=en#privacy, (last view 30/09/2016)

- Twitter, Available at: https://twitter.com/privacy?lang=en, (last view 30/9/2016)

- Twitter, Available at: https://twitter.com/tos?lang=en#privacy, (last view 30/09/2016)

- WhatIs.com, EU Data Protection Directive (Directive 95/46/EC), Available at: http://whatis.techtarget.com/definition/EU-Data-Protection-Directive-Directive-95-46-EC, (last view 25/10/2016)

Άρθρα- Ευρωπαϊκές Οδηγίες

- Ιγγλεζάκη Ιωάννης , Ελευθερία Έκφρασης Και Ανωνυμία Στο Διαδίκτυο: Το Παράδειγμα Των Ιστολογιών, ΔΙΜΕΕ τεύχος 3/2011

- Οδηγία 97/66/ΕΕ Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου , Της 15ης Δεκέμβριου 1997 περί Επεξεργασίας Των Δεδομένων Προσωπικού Χαρακτήρα Και Της Προστασίας Της Ιδιωτικής Ζωής Στον Τηλεπικοινωνιακό Τομές, Επίσημη Εφημερίδα, 30/01/1998

- Οδηγία 2006/24/ΕΚ Του Ευρωπαϊκού Κοινοβουλίου Και Του Συμβουλίου Της 15ης Μάρτιου 2006 , Για Τη Διατήρηση Δεδομένων Που Παράγονται Ή Υποβάλλονται Σε Επεξεργασία Σε Συνάρτηση Με Την Παροχή Διαθεσίμων Στο Κοινό Υπηρεσιών Ηλεκτρονικών Επικοινωνιών Ή Δημοσίων Δικτυών Επικοινωνιών Και Για Την Τροποποίηση Της Οδηγίας 2002/58/ΕΚ, Επίσημη Εφημερίδα, 13/04/2006

- Σπηλιοπούλου, Α.Σ., και Χοχλιούρος, Ι.Π.(2004).Σύγχρονες Προκλήσεις Από Την Παράλληλη Ανάπτυξη Κανονιστικών Παρεμβάσεων Και Μέτρων Αυτορρύθμισης

Στους Τομείς Των Καινοτόμων Προηγμένων Εφαρμογών Και Υπηρεσιών Ηλεκτρονικής Επικοινωνίας Στο Διαδίκτυο, Νομικό Βήμα ΔΣΑ, Νοέμβριος 2004

- Σταθόπουλος Μ. Θεόδωρος, Η Χρήση Προσωπικών Δε Δομών Και Η Διαπάλη Μεταξύ Ελευθέριων Των Κατόχων Τους Και Ελευθέριων Των Υποκειμένων Τους, NoB 2000

- Συμβούλιο Της Ευρωπαϊκής Ένωσης: Απόφαση -Πλαίσιο 2005/222/ΔΕΥ Της 24ης Φεβρουάριου 2005, Για Τις Επιθέσεις Κατά Των Συστημάτων Πληροφοριών», Επίσημη Εφημερίδα (ΕΕ)

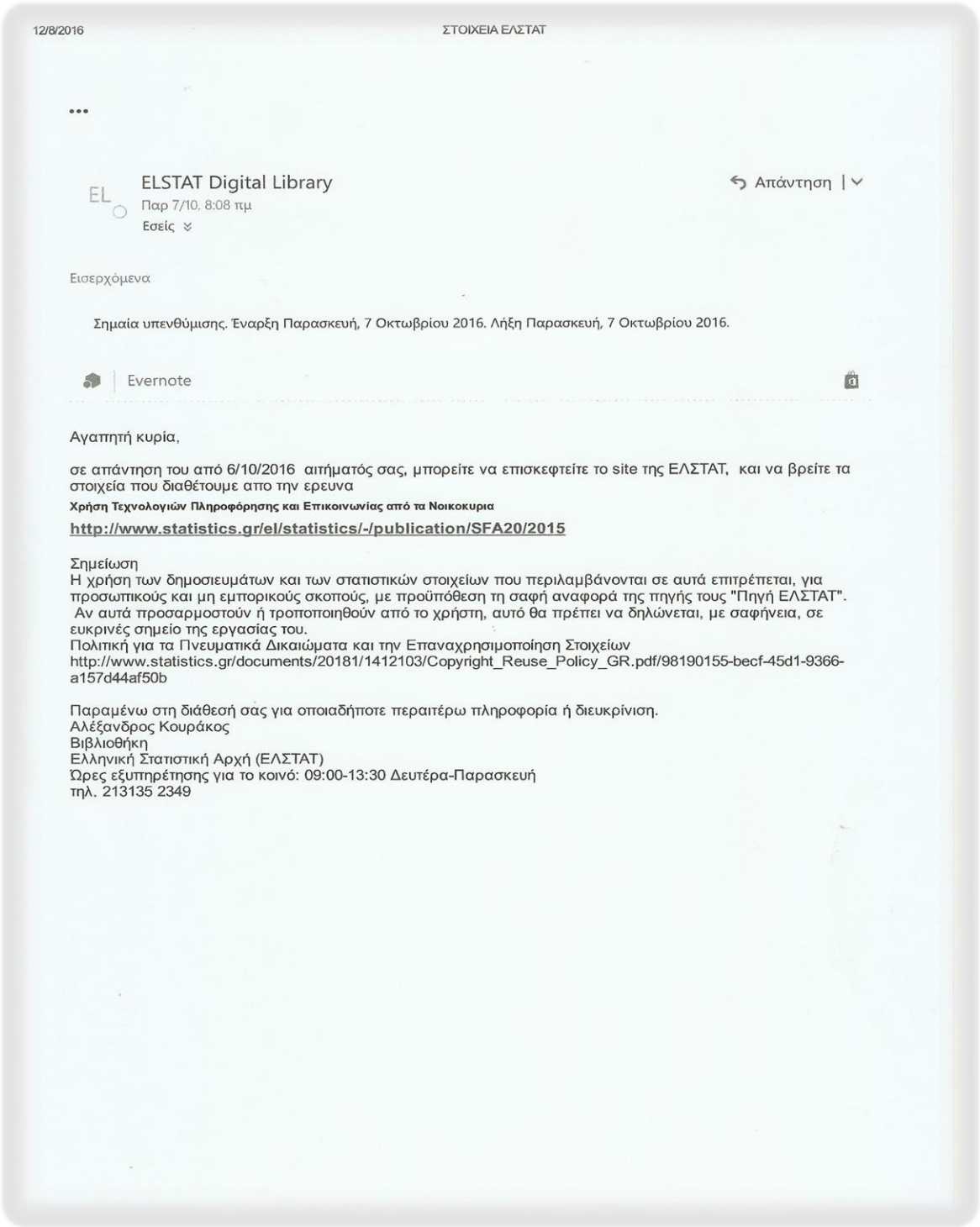
- Χοχλιούρος Π. Ιωάννης, Ι.Π., Και Σπηλιοπούλου, Α.Σ., Δυναμικό Και Βασικές Προοπτικές Της Ευρωπαϊκής Οδηγίας Για Το Ηλεκτρονικό Εμπόριο Για Την Αποτελεσματική Προώθηση Συγχρόνων Επιχειρηματικών Εφαρμογών Στο Διαδίκτυο. Τηλεπικοινωνιακή Επιθεώρηση Και Δίκαιο Νέας Τεχνολογίας, Τεύχος Δ, Δεκέμβριος 2004

- "eEurope 2005: κοινωνία της πληροφορίας για όλους -Σχέδιο δράσης που υποβάλλεται ενόψει του ευρωπαϊκού συμβουλίου της Σεβίλλης, 21/22 Ιουνίου 2002»

- Grossman Theodore and Grossman M. Aaron, Understanding Internet Privacy: the US perspective, IBL, 2001

4. Απαντήσεις Αιτημάτων Παροχής Στοιχείων

Απάντηση αιτήματος παροχής στοιχείων ΕΛΣΤΑΤ



12/8/2016 ΣΤΟΙΧΕΙΑ ΕΛΣΤΑΤ

...

EL ELSTAT Digital Library
Παρ 7/10, 8:08 πμ
Εσείς

Απάντηση

Εισερχόμενα

Σημαία υπενθύμισης. Έναρξη Παρασκευή, 7 Οκτωβρίου 2016. Λήξη Παρασκευή, 7 Οκτωβρίου 2016.

Evernote

Αγαπητή κυρία,

σε απάντηση του από 6/10/2016 αιτήματός σας, μπορείτε να επισκεφτείτε το site της ΕΛΣΤΑΤ, και να βρείτε τα στοιχεία που διαθέτουμε απο την ερευνα

Χρήση Τεχνολογιών Πληροφόρησης και Επικοινωνίας από τα Νοικοκυρια

http://www.statistics.gr/el/statistics/-/publication/SFA20/2015

Σημείωση
Η χρήση των δημοσιευμάτων και των στατιστικών στοιχείων που περιλαμβάνονται σε αυτά επιτρέπεται, για προσωπικούς και μη εμπορικούς σκοπούς, με προϋπόθεση τη σαφή αναφορά της πηγής τους "Πηγή ΕΛΣΤΑΤ". Αν αυτά προσαρμοστούν ή τροποποιηθούν από το χρήστη, αυτό θα πρέπει να δηλώνεται, με σαφήνεια, σε ευκρινές σημείο της εργασίας του.
Πολιτική για τα Πνευματικά Δικαιώματα και την Επαναχρησιμοποίηση Στοιχείων
http://www.statistics.gr/documents/20181/1412103/Copyright_Reuse_Policy_GR.pdf/98190155-becf-45d1-9366-a157d44af50b

Παραμένω στη διάθεσή σας για οποιαδήποτε περαιτέρω πληροφορία ή διευκρίνιση.
Αλέξανδρος Κουράκος
Βιβλιοθήκη
Ελληνική Στατιστική Αρχή (ΕΛΣΤΑΤ)
Ώρες εξυπηρέτησης για το κοινό: 09:00-13:30 Δευτέρα-Παρασκευή
τηλ. 213135 2349

Απάντηση αιτήματος παροχής στοιχείων Διευθύνσεως Διώξης Ηλεκτρονικού Εγκλήματος

Απάντηση σε αίτημα παροχής στατιστικών στοιχείων

Olga Galani

Σαβ 15/10/2016 8:24 μμ

Εισερχόμενα

Προς:mariakons@windowslive.com <mariakons@windowslive.com>;

Γεια σας κ. Κωνσταντινίδου,

στον παρακάτω υπερσύνδεσμο (Link) θα βρείτε στατιστικά στοιχεία για τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και τα οποία συμπεριλαμβάνονται στον Ετήσιο Απολογισμό Συνολικής Δραστηριότητας της Ελληνικής Αστυνομίας:

http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=62129&Itemid=1694&lang=

Στη διάθεσή σας,

--

ΓΑΛΑΝΗ Όλγα
Αστυνόμος Β' Ειδικών Καθηκόντων
Δίωξης Ηλεκτρονικού Εγκλήματος
Λ. Αλεξάνδρας 173, Τ.Κ. 115 22, Αθήνα
Τηλ. : +30 210 6476486
Fax : +30 210 6476462