ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

"ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ"

Κόλλια Φωτεινή-Ευαγγελία
Κονδυλίδου Ιουλία
Γραμμένου Αγαθή-Ελένη

Εποπτεύων καθηγητής: Γιωτόπουλος Κωνσταντίνος

Πάτρα - 2021

Πρόλογος

Η ανάγκη της επικοινωνίας και της ενημέρωσης έχει ως αποτέλεσμα την γρήγορη ανάπτυξη των Μέσων Κοινωνικής Δικτύωσης τα οποία έχουν δημιουργήσει έναν καινούργιο κόσμο συνεργασίας και σχέσεων μεταξύ των ανθρώπων με την ανταλλαγή απόψεων και πληροφοριών μέσω μηνυμάτων, φωτογραφιών, βίντεο κτλ. Τα δίκτυα έχουν εδραιωθεί ως απαραίτητα στοιχεία των ανθρωπίνων δραστηριοτήτων, καθώς είναι εμφανές πως πλέον η καθημερινότητα των ατόμων είναι πλέον πλήρη συνδεδεμένη με τη χρήση δικτύου. Όμως όσο και αν διευκολύνει αυτό τις διαπροσωπικές σχέσεις των ανθρώπων οι κίνδυνοι είναι πολύ μεγάλοι και η διαχείριση αρκετά δύσκολη. Η καταγραφή προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης αυτομάτως παραπέμπει στην παρακολούθηση των πληροφοριών αυτών με αποτέλεσμα να τα θέτει σε κίνδυνο παραβίασης τους. Επίσης πέραν του ότι εκθέτει τους χρήστες σε κίνδυνο, προσβάλλει το δικαίωμα της ελευθερίας τους και σαφώς δυσχεραίνει την απόλαυση άλλων δικαιωμάτων. Είναι δυσδιάκριτη η αναγνώριση των ορίων για την προστασία των προσωπικών δεδομένων εντός των μέσων κοινωνικής δικτύωσης, γι ‘αυτό μερικές φορές οι πράξεις των χρηστών και οι πληροφορίες οι οποίες καταγράφουν μπορούν να παραβιαστούν και να αναγκαστούν να υποστούν τις συνέπειες οι οποίες μπορούν να επεκταθούν στην πραγματική τους ζωή, όμως πολλές φορές δεν φαίνεται να πτοούνται ουσιαστικά .Εν κατακλείδι, η τεχνολογία και η κοινωνία συνήθως εξελίσσονται παράλληλα. Ως αντάλλαγμα μπορεί να θεωρηθεί η ιδιωτικότητα και τα ανθρώπινα δικαιώματα για διάφορες ανταμοιβές όπως είναι η κοινωνικοποίηση, η κοινωνική αποδοχή, δωρεάν υπηρεσίες, κ.ο.κ..

Περίληψη

Η παρούσα πτυχιακή εργασία πραγματεύεται σχετικά με την επικαιρότητα και την σημασία της ιδιωτικότητας του ατόμου στα μέσα κοινωνικής δικτύωσης τα οποία αποτελούν μια έντονη καθημερινότητα στην ζωή των ανθρώπων τα τελευταία χρόνια. Επίσης σχετίζεται με την αυξημένη ζήτηση προσωπικών πληροφοριών, κάτι το οποίο αποτελεί πρόβλημα στην προσωπική ζωή των χρηστών. Μέσα από σχετική βιβλιογραφική ανασκόπηση προσδιορίστηκε η σημαντικότητα της ιδιωτικότητας στα Μέσα Κοινωνικής Δικτύωσης, η αλληλεπίδρασή τους στην καθημερινότητα των χρηστών, οι απειλές ,καθώς και οι τρόποι αντιμετώπισής τους. Υπάρχει μεγάλη ανησυχία σχετικά με την απειλή της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης, καθώς πλέον είναι πολύ εύκολο να παραβιαστούν προσωπικές πληροφορίες για όλους όσους αποτελούν χρήστες του διαδικτύου και των μέσων. Όσον αφορά στην παραβίαση της ιδιωτικότητας, έχουν θεσπιστεί σχετικές νομοθεσίες όσο σε Διεθνές τόσο και σε Ευρωπαϊκό αλλά και σε Εθνικό επίπεδο. Αναφέρεται η ιστορική αναδρομή του Διαδικτύου ξεκινώντας από την δεκαετία το 50’ έως και του 90’ και έπειτα στο σύγχρονο περιβάλλον, περιγράφοντας τα εργαλεία του Διαδικτύου καθώς και τις εφαρμογές του. Παράλληλα, παρουσιάζονται δύο σημαντικοί όροι του Παγκόσμιου Ιστού (World Wide Web), το Web 1.0 και το Web 2.0, και αναλύονται οι έννοιες, καθώς και τα κύρια χαρακτηριστικά τους όπως και οι διαφορές τους μέσα από την εξέλιξή τους. Εν συνεχεία, κρίνεται σημαντική η ανάλυση του όρου της Κοινωνικής Δικτύωσης και των Μέσων Κοινωνικής Δικτύωσης. Αναγράφεται συνοπτικά η κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης κατά Zhang και ακολουθούν στατιστικά χρήσης τους από το 1996 έως και σήμερα. Γνωρίζοντας ότι τα μέσα κοινωνικής δικτύωσης έχουν καθοριστικό ρόλο τα τελευταία χρόνια στο διαδίκτυο για κάθε χρήστη, φαίνεται η ιστορική εξέλιξη και πως εξαπλώνονται και κερδίζουν όλο και περισσότερο έδαφος στην αγορά. Είναι γνωστό το γεγονός ότι η χρήση των μέσων μπορεί να επιφέρει πολύ εύκολα αρνητικές συνέπειες, για αυτόν τον λόγο ορίζονται κάποιες συμβουλές για την ασφαλή χρήση τους. Επιβάλλεται να είναι σε όλους γνωστό και κατανοητό το πώς να αντιλαμβάνονται τους κακόβουλους χρήστες και να προστατεύουν τα προσωπικά τους δεδομένα. Πρέπει να είναι εις γνώση όλων ποιες ορίζονται ως περιπτώσεις παραβίασης στα προσωπικά δεδομένα, και να λαμβάνονται υπόψιν οι τέσσερις τυπικές απειλές των κοινωνικών μέσων. Το να προστατεύεις τα προσωπικά σου δεδομένα είναι αρκετά σημαντικό, γ ’αυτόν τον λόγο πρέπει να λαμβάνονται πολύ καλά υπόψη οι πολιτικές προστασίας των μέσων που χρησιμοποιούνται, δηλαδή να διέπονται από το τρίπτυχο Ακεραιότητα – Διαθεσιμότητα – Εμπιστευτικότητα. Ταυτόχρονα, όλοι οι χρήστες των μέσων κοινωνικής Δικτύωσης πρέπει να αντιληφθούν την κατάσταση στην οποία βρισκόμαστε και να λάβουν όλοι τα ανάλογα μέτρα ασφάλειας. Τέλος, πρέπει να ικανοποιούνται και οι κύριες απαιτήσεις Ιδιωτικότητας ώστε να διαφυλάσσονται τα προσωπικά δεδομένα και η προσωπική ζωή.

Abstract

This dissertation deals with the timeliness and importance of personal privacy on social media which are an intense daily occurrence in people's lives in recent years. It is also related to the increased demand for personal information which is a problem in the personal life of users. It is also related to the increased demand for personal information, which is a problem for users' privacy. This relevant literature review identified the importance of privacy on social media, their interaction in daily life of users, threats, and ways to overcome them. There is a great deal of concern about the threat of privacy on social media, as it is now very easy to breach personal information about anyone who is an internet and media user. Regarding the invasion of privacy, relevant legislation has been adopted at both International and European as well as National level. The historical background of the Internet is mentioned, starting from the 50's to the 90's and then in the modern environment, describing the tools of the Internet as well as its applications. At the same time, two important terms of the World Wide Web, Web 1.0 and Web 2.0, are presented, analyzing the concepts, their main characteristics and their differences through their evolution. Moving forward, the analysis of the terms, Social Networking and Social Media, is considered important. Zhang's social media categorization is summarized and their usage statistics from 1996 until today are given. Knowing that social media has played a key role in recent years on the Internet for every user, this research shows the historical development and how they are spreading and gaining more and more ground in the market. It is a well-known fact that the use of Social Media can very easily lead to negative consequences, for this reason some tips for their safe use are defined. It is necessary for everyone to know and understand how to perceive malicious users and protect their personal data. Everyone should be aware of the cases of violation of their personal data and consider the four typical threats of social media. The protection of personal data is important, which is why the protection policies of the media used must be taken very seriously. That is, social media should be governed by the triptych Integrity - Availability - Confidentiality. At the same time, all social media users must be aware of the situation we are in and take all appropriate security measures. Finally, the main requirements of Privacy must be met in order to preserve personal data and personal life.

Περιεχόμενα

Κατάλογος Γραφημάτων

Κατάλογος Εικόνων

ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ

1.1 Σκοπός και αντικείμενο της εργασίας

Τα κοινωνικά δίκτυα όπως και οποιοδήποτε άλλο κοινωνικό φαινόμενο, βλέπουμε πως έχουν μια ισχυρή επίδραση πάνω στην ζωή των ανθρώπων, στην πολιτική όπως ακόμα και στην οικονομία. Αυτές οι επιδράσεις αποτελούν αντικείμενο ανάλυσης αλλά και παρατήρησης. Η παρούσα πτυχιακή εργασία, με βάση την βιβλιογραφική ανασκόπηση σχετικά με το θέμα της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης, έχει ως σκοπό να παρουσιάσει μία ολοκληρωμένη "εικόνα" της ραγδαίας εξέλιξης των μέσων κοινωνικής δικτύωσης και των κινδύνων που "παραμονεύουν" σε αυτά. Το αντικείμενο της εργασίας βασίζεται στην ανάπτυξη και παρουσίαση των βασικών εννοιών της θεωρίας του Διαδικτύου, των κοινωνικών δικτύων και της ιδιωτικότητας.

Η παρούσα εργασία διαρθρώνεται σε έξι κεφάλαια ενώ ταυτόχρονα χωρίζεται σε δύο μέρη, Το πρώτο κομμάτι είναι το θεωρητικό και το δεύτερο το ερευνητικό. Ξεκινώντας από το θεωρητικό μέρος, στο πρώτο κεφάλαιο αναφέρεται ο σκοπός και το αντικείμενο της εργασίας. Έπειτα στο δεύτερο κεφάλαιο επεκτείνεται η έννοια της ιδιωτικότητας και τα νομικά πλαίσια, και ακολουθεί το κεφάλαιο τρία όπου εδώ αναπτύσσεται η εξέλιξη του Διαδικτύου, ο ορισμός της Κοινωνικής Δικτύωσης και η εξάπλωση των μέσων Κοινωνικής Δικτύωσης. Περνώντας στο τέταρτο κεφάλαιο σημειώνεται η κατανόηση και οι περιπτώσεις παραβίασης των προσωπικών δεδομένων καθώς και βασικές πολιτικές προστασίας. Τέλος, το θεωρητικό μέρος κλείνει με το έκτο κεφάλαιο το οποίο αναφέρει συμπεράσματα και προτάσεις καθώς μας δίνει έναν δεκάλογο συμβουλών για την σωστή χρήση των κοινωνικών μέσων. Όσον αφορά το πέμπτο κεφάλαιο, εκεί αναγράφεται το ερευνητικό κομμάτι, καθώς και η καταγραφή του σκοπού και των συμπερασμάτων της έρευνας αυτής με την διεξαγωγή ενός ερωτηματολογίου που συμπληρώθηκε από ένα σύνολο ατόμων.

1.2 Αναγκαιότητα και σπουδαιότητα έρευνας

Λόγω της γρήγορης εξάπλωσης του Internet και ιδίως των Μέσων Κοινωνικής Δικτύωσης, είναι αναγκαίο να γίνει μια θεωρητική αναφορά καθώς και μια έρευνα πάνω στο πιο επικρατέστερο θέμα των τελευταίων δεκαετιών. Τα Μέσα Κοινωνικής Δικτύωσης έχουν εισέλθει δυναμικά στη καθημερινότητα της πλειοψηφίας των ανθρώπων επηρεάζοντας τους θετικά αλλά και αρνητικά. Όσον αφορά τη θετική επίδραση των μέσων στους ανθρώπους, βλέπουμε τα οφέλη ως προς την εύκολη επικοινωνία των χρηστών μεταξύ τους αλλά και τη συνεχή ενημέρωση για διάφορα ζητήματα τα οποία τους απασχολούν. Όμως η σπουδαιότητα της έρευνας αυτής κορυφώνεται καθώς βλέπουμε μέσα από το ερωτηματολόγιο το πώς αντιλαμβάνονται οι άνθρωποι τα μέσα κοινωνικής δικτύωσης και το πόσο ενημερωμένοι είναι για αυτά. Μέσα από αυτή την έρευνα θα εστιάσουμε στους κινδύνους που παραμονεύουν στα μέσα καθώς και τους τρόπος προφύλαξης αλλά και αντιμετώπισής σε πιθανή εξόρυξη δεδομένων των χρηστών παρά την θέληση τους παραβιάζοντας την δικαίωμα της ιδιωτικότητας τους.

ΚΕΦΑΛΑΙΟ 2 : Η ΈΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

2.1 Ορισμός Ιδιωτικότητας

Αποτελεί δύσκολο να ξεκινήσει κάποιος τη συζήτηση σχετικά με την προστασία της ιδιωτικής ζωής, αν πρώτα δεν απαντήσει στην προφανή ερώτηση: «τί ορίζεται ως ιδιωτικότητα;». Συζητήσεις πολλών ετών ανάμεσα σε εμπειρογνώμονες αλλά και ακαδημαϊκούς, στη προσπάθεια σύνταξης του ορισμού της ιδιωτικότητας στον οικουμενικό κατάλογο των ανθρώπινων δικαιωμάτων καταλήγουμε ότι είναι ιδιαίτερα ακανθώδες το ζήτημα καθώς δεν έχουμε καταλήξει ακόμα σε κάτι το οποίο να είναι αποδεκτό από όλους.

Η ιδιωτικότητα είναι εκ θεμελίων ζήτημα αξίας, συμφέροντος και εξουσίας. Ένας από τους πρώτους ο οποίος πήρε τα ηνία για να ασχοληθεί με το πεδίο αυτό ήταν ο Alan Westin ,ο οποίος είχε καταλήξει στο συμπέρασμα πως κανένας ορισμός της ιδιωτικότητας δεν είναι μπορεί να είναι εφικτός. Γίνεται λοιπόν κατανοητό για άλλη μια φορά ότι για να οριστεί η έννοια της ιδιωτικότητας υπάρχουν διάφορες και ποικίλες γνώμες ανάλογα με το κοινωνικοπολιτικό πλαίσιο και το περιβάλλον στο οποίο θα οριστούν.

Την έννοια της ιδιωτικότητας, την έχουν ορίσει κατά καιρούς πολλοί επιστήμονες και από διάφορα πεδία.

- Ως βασική προϋπόθεση για την αξιοπρέπεια των ανθρώπων κρίνει ο Edward Bloustein το δικαίωμα στην ιδιωτικότητα.
- Ο James Rachels, θεωρεί πως η έννοια της ιδιωτικότητας έχει να κάνει με την διαφορετικότητα του ατόμου και την αλληλεπίδραση των ανθρώπων στις διαπροσωπικές τους σχέσεις. Επίσης, υποστηρίζει πως ιδιωτικότητα μπορεί να είναι και η ικανότητα που μπορούμε να έχουμε ούτως ώστε να ελέγχουμε το ποιος έχει πρόσβαση σε εμάς.
- Ο Robert Ellis Smith δίνει μια πιο σύγχρονη ερμηνεία στον ορισμό της ιδιωτικότητας ως την επιθυμία του καθένα για ένα χώρο στον οποίο θα μπορεί να είναι ελεύθερος για κάθε εισβολή, υπευθυνότητα ή αμηχανία, καθώς καταβάλλεται μια προσπάθεια για τον έλεγχο του χρόνου αλλά και του τρόπου που γίνονται οι κοινοποιήσεις των προσωπικών μας πληροφοριών.
- Τέλος, ο Warren και ο Brandeis ορίζουν την ιδιωτικότητα ως την μοναξιά του κάθε ανθρώπου και το δικαίωμά του ως προς αυτήν.

Η επιτροπής του Ηνωμένου Βασιλείου, έκαμε μια αναφορά πάνω στο ζήτημα του ορισμού της ιδιωτικότητας και αναφέρει πως μπορεί να μη έχει βρέθηκε ακόμα ένας ικανοποιητικός ορισμός ο οποίος θα είναι πλήρης, όμως, κατέληξαν πως Ιδιωτικότητα σημαίνει το άτομο έχει το δικαίωμα να προστατεύεται ενάντια στην εισβολή κάποιου τρίτου στην προσωπική του ζωή ή της οικογένειάς δημοσίευση πληροφοριών ή με άλλα φυσικά μέσα».

Τέλος, ένας γενικότερος ορισμός που έχει συσταθεί στο Διαδίκτυο είναι ότι η ιδιωτικότητα είναι το δικαίωμα να αποφασίζει ο κάθε ένας ατομικά έως ποιο σημείο επιθυμεί οι προσωπικές του πληροφορίες να διαβιβάζονται σε τρίτους. Η ιδιωτικότητα είναι ανθρώπινο δικαίωμα οπότε μέσα σε μια δημοκρατική κοινωνία είναι απαραίτητο να προστατεύεται.

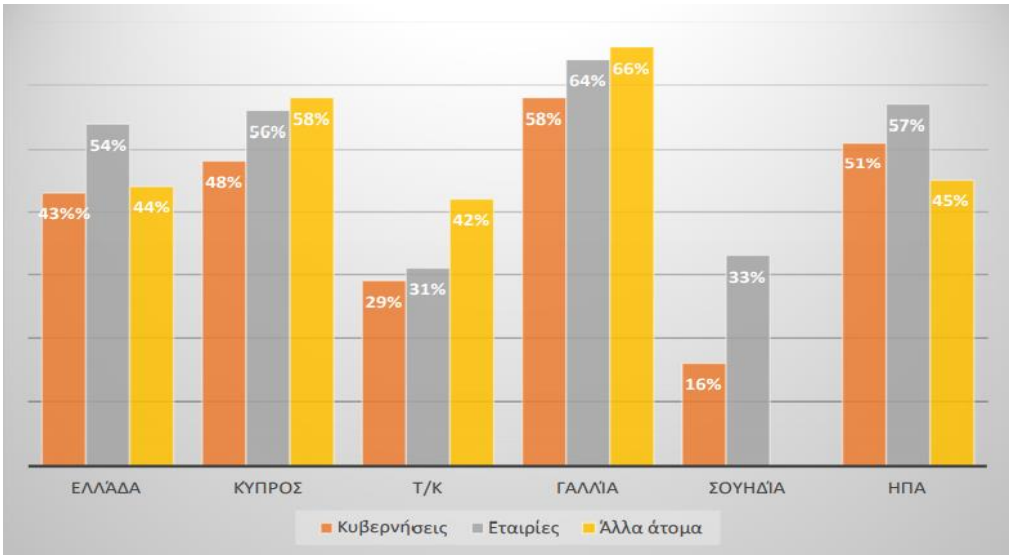
2.2 Ανησυχία σχετικά με την «απειλή» της ιδιωτικότητας

Από το 1960 με την αύξηση της χρήσης των υπολογιστών υπάρχουν ανησυχίες για την ιδιωτικότητα, οι οποίες αυξήθηκαν κατά την εξέλιξη του παγκόσμιου ιστού και την εξέλιξη του web 1.0 σε web 2.0 και τέλος σε web 3.0. Ο όγκος των πληροφοριών από διαφορετικές πηγές και η εξαγωγή συμπερασμάτων αποτελεί μια από τις μεγαλύτερες προκλήσεις για την ιδιωτικότητα. Ειδικότερα με την χρήση των μέσων κοινωνικής δικτύωσης, όπου τα τελευταία χρόνια αποτελεί μια έντονη πραγματικότητα και μια ισχυρή τάση μόδας της εποχής. Οι χρήστες του διαδικτύου και των μέσων εκφράζουν έντονα την ανησυχία σχετικά με την απειλή της ιδιωτικότητα τους, όπου αυτό είναι ένα μεγάλο εμπόδιο στην ανάπτυξη των εφαρμογών αυτών. Με την ραγδαία ανάπτυξη της τεχνολογίας αναπτύσσεται η εύκολη δυνατότητα συλλογής,διάδοσης αλλά και επεξεργασίας των προσωπικών δεδομένων των χρηστών των μέσων, η οποία καταλήγει σε παραβίαση της ιδιωτικότητας και των πληροφοριών του ατόμου. Εκφράζονται πολλοί φόβοι παγκοσμίως πάνω στην παραβίαση της ιδιωτικής ζωής. Οι λόγοι για τους οποίους γίνεται ευκολότερη η εισβολή στις πληροφορίες των χρηστών που αφορούν την προσωπική τους ζωή είναι οι εξής:

- Η ροή των δεδομένων σε όλο τον κόσμο.
- Η ανταλλαγή μεγάλου όγκου πληροφοριών και επεξεργασίας δεδομένων από τα σύγχρονα πληροφοριακά συστήματά.
- Η μετάδοση εικόνων αλλά και των δεδομένων ώστε οι πληροφορίες που συγκεντρώνονται μπορούν εύκολα να μεταφραστούν σε άλλες μορφές. (Μαθιουδάκη, 2014)

Υπάρχουν τρεις πιθανές πηγές παραβίασης διαδικτυακής ιδιωτικότητας οι κυβερνήσεις, οι εταιρίες και τα άτομα.

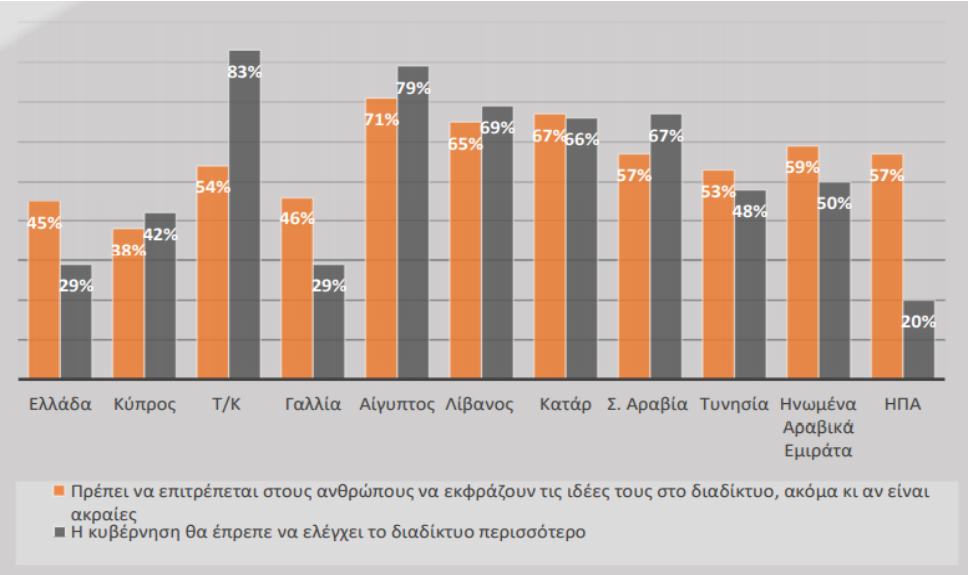
Από την έρευνα του WIP(World Internet Project), ανάμεσα στις τρείς πιθανές πηγές, στις κυβερνήσεις υπάρχει η χαμηλότερη ανησυχία σε σχέση με τις εταιρείες και τα άτομα (βλ. Γράφημα 1).



Γράφημα 1: Ανησυχίες παραβίασης ιδιωτικότητας στο διαδίκτυο. (Δεμερτζής και συν., 2020)

Όπως φαίνεται στην παραπάνω στατιστική έρευνα, κατά πλειοψηφία οι συμμετέχοντες θεωρούν ότι το διαδίκτυο έχει ως ρίσκο την έκθεση τόσο απέναντι σε κέντρα εξουσίας που μπορεί να τους παρακολουθούν όσο και τα άλλα άτομα που μπορεί να επιτεθούν. Όσον αφορά την Ελλάδα η εταιρίες θεωρούνται μεγαλύτερη απειλή για την ιδιωτικότητα των Ελλήνων όμως δεν διαφέρουν πολύ τα ποσοστά που θεωρούν απειλή οι χρήστες τα άλλα άτομα καθώς και τις κυβερνήσεις.

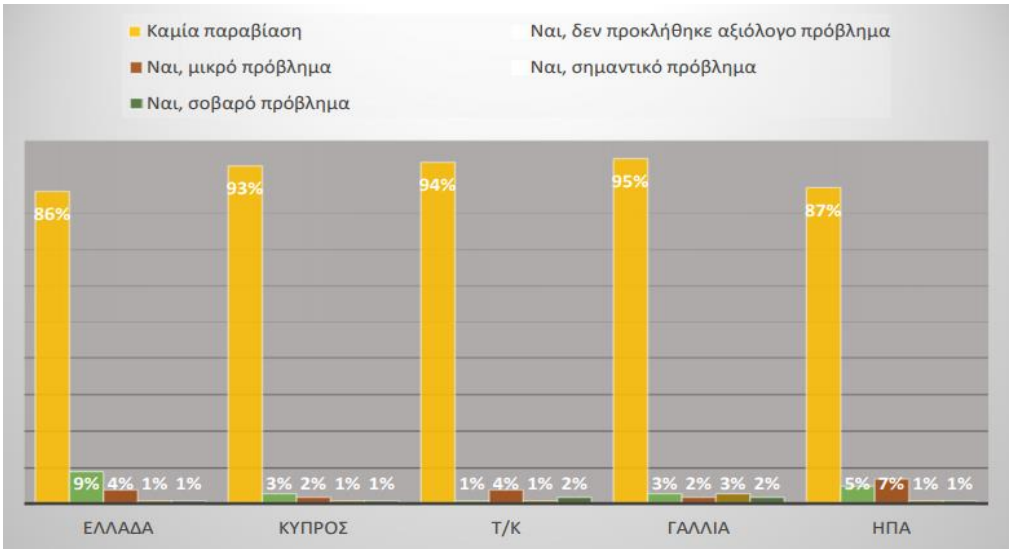
Ωστόσο, η ερώτηση για το αν «θα έπρεπε η κυβέρνηση να ελέγχει περισσότερο το διαδίκτυο», συμφωνεί το μεγαλύτερο ποσοστό των συμμετεχόντων. Δεν είναι λίγες οι περιπτώσεις του διαδικτυακού εκφοβισμού (cyberbullying) με αφορμή πολιτικές διαφωνίες και όχι μόνο. Μετρώντας τις στάσεις των συμμετεχόντων για το αν πιστεύουν ότι το διαδίκτυο μπορεί να είναι ένα πεδίο ελεύθερης διακίνησης ιδεών «ακόμα κι αν είναι ακραίες». Η ανησυχία παραβίασης που αφορά τις εταιρίες πιθανότατα συνάδει με το ότι οι περισσότεροι χρήστες του διαδικτύου είχαν ήδη εμπειρίες στοχοποιημένων διαφημίσεων και προτάσεων για υπηρεσίες και προϊόντα με δεδομένο το προφίλ των αναζητήσεών τους (Γράφημα 2).



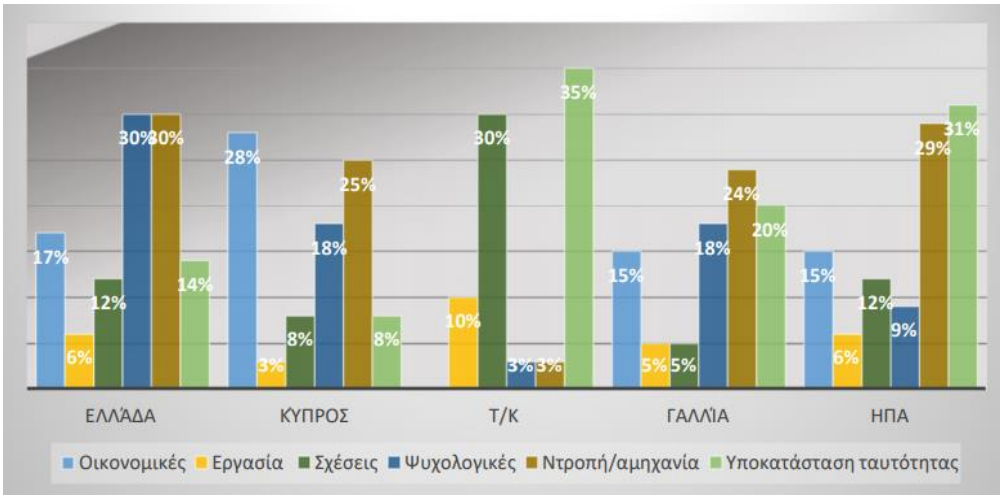
Γράφημα 2: Ελευθερία του λόγου και διαδίκτυο. (Δεμερτζής και συν., 2020)

Σύμφωνα με τα στοιχεία της έρευνας του WIP από τις τρεις πιθανές πηγές παραβίασης της διαδικτυακής ιδιωτικότητας (κυβερνήσεις, εταιρίες, άτομα), τα άλλα άτομα βρίσκονται στην πρώτη θέση σε αρκετές χώρες. Εκτός από τις εταιρείες και τις κυβερνήσεις, τα δεδομένα των χρηστών είναι εύκολο να παραβιαστούν και από μεμονωμένα άτομα με στόχους παραβατικής φύσης, όπως κλοπή ταυτότητας, υποκλοπή τραπεζικών δεδομένων, παρενόχληση ή εκβιασμό. Τα μέλη τις έρευνας αυτής, παρατήρησαν ότι οι ανησυχίες των ατόμων πάνω στην παραβίαση των δεδομένων τους από άλλα άτομα συσχετίζονται με την έλλειψη επίγνωσης και ενημέρωση. Συγκεκριμένες ανησυχίες αφορούν την «κοινωνική ιδιωτικότητα» και το πώς οι ψηφιακές τεχνολογίες την απειλούν σε επίπεδο διαπροσωπικών σχέσεων, έκθεσης και αμηχανίας ενώπιον του κοινωνικού ή επαγγελματικού περίγυρου. Όμως αυτό μπορεί να διαφέρει καθώς οι παραβιάσεις μπορούν να γίνουν από εταιρίες ή κυβερνήσεις. Αυτό που ανησυχεί περισσότερο τους χρήστες όμως δεν είναι η συλλογή και επεξεργασία δεδομένων από το κοινωνικοοικονομικό υπόβαθρο των χρηστών για κερδοσκοπικούς σκοπούς, όσο το

να δουν, π.χ., ντροπιαστικές φωτογραφίες που μπορεί κάποιος κακόβουλος να αναρτήσει στα κοινωνικά δίκτυα παρά την θέληση του χρήστη. Ωστόσο, παρά τις εκπεφρασμένες ανησυχίες τους, οι ερωτηθέντες δηλώνουν σε μεγάλο ποσοστό ότι δεν υπέστησαν καμία παραβίαση (Γράφημα 3). Βέβαια γίνονται και αναφορές σοβαρών προβλημάτων από την παραβίαση της ιδιωτικότητας (Γράφημα 4).



Γράφημα 3: Παραβίαση ιδιωτικότητας στο διαδίκτυο. (Δεμερτζής και συν., 2020)



Γράφημα 4: Αποτελέσματα παραβιάσεων ιδιωτικότητας στο διαδίκτυο. (Δεμερτζής και συν., 2020)

Το 2005 ο Richard Posner ένας από τους γνωστότερους Αμερικανούς νομικούς, έγραψε πως «το να συλλέγεις και να επεξεργάζεσαι τα δεδομένα από μηχανές δεν θεωρείται ότι παραβιάζεται η ιδιωτικότητα». Εξάλλου ο υπολογιστής δεν είναι ένα νοήμον ον. Εξαιτίας του τεράστιου όγκου τους, τα δεδομένα “κοσκινίζονται” από υπολογιστές που αναζητούν μόνο ονόματα, τηλέφωνα ή διευθύνσεις που μπορεί να έχουν κάποια αξία για την ασφάλεια και δεν επιτρέπουν σε κανέναν άνθρωπο να έχει πρόσβαση σε αυτά. Όμως βλέπουμε ότι αυτή η θεωρία καταρρίπτει τα τελευταία χρόνια γιατί ενώ βλέπουμε πως το ποσοστό των χρηστών οι οποίοι δηλώνουν ότι δεν έχουν υποστεί καμία παραβίαση, υπάρχει μεγάλη ανησυχία και

γνωρίζουμε πλέον ότι αυτό το πρόβλημα ολοένα και μεγαλώνει.Ένα συμπέρασμα ακόμα στο οποίο καταλήγουμε είναι ότι οι περισσότεροι έχουν το αίσθημα την ντροπής να αναφέρουν ότι έπεσα θύματα ή δεν αποδέχονται τον κίνδυνο. Η υιοθέτηση της στάσης «δεν έχω τίποτα να κρύψω» η οποία είναι μια φράση που χρησιμοποιείται από πολλούς χρήστες φανερώνει μια σιωπηλή παραδοχή ότι ο ψηφιακός εαυτός των χρηστών είναι πιθανότατα αντικείμενο παρακολούθησης, αλλά αφού δεν έχουν τίποτα να κρύψουν τότε και η διατήρησή τους δεν θα είναι βλαπτική. Οι άνθρωποι υποθέτουν ότι οι πληροφορίες τους ή θα γίνουν αντικείμενο στοχοποίησης από εταιρείες για να τους αποστέλλονται διαφημίσεις, τις οποίες απλώς θα αγνοήσουν χωρίς καμία επίπτωση στην ιδιωτικότητά τους. Η στάση «δεν έχω τίποτα να κρύψω» πιθανόν να φανερώνει δύο προβλήματα. Πρώτον, προϋποθέτει ότι η ιδιωτικότητα αφορά το να μπορεί κανείς να κρύψει κάτι κακό, και δεύτερον είναι η λανθασμένη υπόθεση των ανθρώπων που πιστεύουν ότι, επειδή δεν «έχουν τίποτα να κρύψουν», θα είναι μόνιμα «αθώοι», παραμελώντας την εκδοχή ότι η ψηφιακή τους ύπαρξη μπορεί να γίνει αντικείμενο ενοχοποίησης στα χέρια κάποιου (Δεμερτζής και συν., 2020). Τα βασικά ερωτήματα είναι:

- Ποιος είναι υπεύθυνος στο να ελέγχει τους συλλέκτες δεδομένων και ποιοι είναι οι ιδιοκτήτες των δεδομένων που αναλύονται;
- Μήπως είναι αναγκαίο να υπάρξει δημόσιος διάλογος σχετικά με την εφαρμογή τρόπων παρακολούθησης και ελέγχου των δεδομένων των ατόμων;
- Αυτοί που συλλέγουν δεδομένα από τους χρήστες των μέσων έχουν τη συναίνεση τους;
- Τί σχέση υπάρχει ανάμεσα στις εταιρείες εξόρυξης δεδομένων, τις πλατφόρμες κοινωνικής δικτύωσης και τις υπηρεσίες παρακολούθησης;

Αποκαλύπτεται μια κοινωνία όπου η προστασία σταδιακά περιορίζεται. Έχει παρατηρηθεί ότι όταν «ένα άτομο χάνει τον έλεγχο των πληροφοριών του, χάνει επίσης και τον έλεγχο των δυνητικών μεταμορφώσεων αυτών των πληροφοριών» (Δεμερτζής και συν., 2020).

2.3 Νομικό πλαίσιο

Οι εξελίξεις των τελευταίων δεκαετιών πάνω στον τομέα της τεχνολογίας, έχουν δημιουργήσει άθελα τους ένα νέο κοινωνικοπολιτικό στρώμα στο οποίο τα ανθρώπινα δικαιώματα, εκτίθενται μπροστά από πολλές προκλήσεις. Ο ΟΗΕ έχει οριστεί ως εισηγητής για τα δικαιώματα τον ατόμων στην ιδιωτικότητα. Ο ΟΗΕ έχει θέσει σαν στόχο πως στα προσεχώς έτη θα προσπαθήσει να κάνει την σωστή προώθηση των κοινών αξιών των ανθρώπων, οι οποίες σχετίζονται με τις ελευθερίες και τα δικαιώματα τους μέσα στον ψηφιακό κόσμο. Στις 4 Νοεμβρίου το 1950 δημιουργείται η σύμβαση της Ρώμης η οποία έχει ως στόχο την μεγάλη ανάγκη για την προστασία της ιδιωτικότητας. Στη Σύμβαση αυτή, ορίζεται ως ιδιωτικότητα το δικαίωμα του κάθε ατόμου να έχει ως ιδιωτική την ζωή του, την οικογένεια του την κατοικία του και την αλληλογραφία του.

Εάν λάβουμε υπόψιν μας και τα δικαιώματα των τρίτων, για παράδειγμα το δικαίωμα των ανθρώπων στην ενημέρωση, στην έρευνα αλλά και στις γενικότερες ανάγκες που έχει δημιουργήσει η κοινωνία, ερχόμαστε σε μεγάλη αντιπαράθεση διότι με την διαμόρφωση των κανόνων για την ιδιωτικότητα των χρηστών των μέσων και γενικότερα των ανθρώπων,

ανακαλύπτουμε ότι περιορίζεται η ροή και η δυνατότητα την επεξεργασίας των δεδομένων και των πληροφοριών.

2.3.1 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Ο Γενικός Κανονισμός 679/2016 General Data Protection Regulation (GDPR) της 27.04.2016 της Ευρωπαϊκής Ένωσης απευθύνετε στα δικαιώματα των φυσικών προσώπων όσο αφορά τα προσωπικά τους δεδομένα, την επεξεργασία αυτών των δεδομένων, την κυκλοφορία τους αλλά και μεταβίβαση των δεδομένων αυτών εντός των της Ευρωπαϊκής Ένωσης που είναι και το πιο φλεγόμενο ζήτημα καθώς και πιθανής μεταφοράς των προσωπικών δεδομένων και εκτός της Ευρωπαϊκής Ένωσης (Γρίβας, 2018). Ο Γενικός κανονισμός (GDPR) απευθύνετε στη διαμόρφωση ενός νομοθετικού πλαισίου που έχει ως στόχο να οριοθετήσει την επεξεργασία προσωπικών δεδομένων δημιουργώντας αίσθημα ασφαλείας όχι μόνο στα κράτη μέλη της ΕΕ αλλά και σε ολόκληρο τον κόσμο.

Το GDPR έχει ορίσει τα προσωπικά δεδομένα και τι έννοια της επεξεργασίας των δεδομένων αυτών ούτως ώστε να είναι ξεκάθαρο το περιβάλλον στο οποίο θα μπουν τα όρια της νομοθεσίας του. Αρχικά να διευκρινίσουμε ότι το GDPR απευθύνεται σε όλες τις επιχειρήσεις, εντός και εκτός ΕΕ, με προϋπόθεση τα δεδομένα να αφορούν Ευρωπαίους πολίτες. Το GDPR αναφέρετε σε όλες τις δημόσιες και τις ιδιωτικές επιχειρήσεις, καθώς και τις κρατικές αρχές οι οποίες διαχειρίζονται δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων όπως πελατών, συνεργατών και εργαζομένων.

Σύμφωνα με το άρθρο 4 του Γενικού Κανονισμού δίνονται οι κάτωθι κύριοι ορισμοί για καλύτερη κατανόηση του θέματος:

Τι είναι τα «Δεδομένα προσωπικού χαρακτήρα»: Κάθε (προσωπική) πληροφορία που αφορά ένα φυσικό πρόσωπο το οποίο είναι ταυτοποιήσιμο. Ένα ταυτοποιήσιμο πρόσωπο είναι εκείνο του οποίου τα προσωπικά του στοιχεία έχουν την δυνατότητα να εξακριβωθούν άμεσα ή έμμεσα, ιδίως με μια αναφορά σε στοιχεία του ατόμου όπως για παράδειγμα το όνομα του, ο αριθμός ταυτότητας όπως ακόμα και σε άλλα προσωπικά δεδομένα τα οποία μπορεί να είναι η οικονομική κατάσταση, κοινωνική, ακόμα και η ψυχολογική κατάσταση του φυσικού προσώπου.

Τι είναι η «Επεξεργασία»: Επεξεργασία είναι μια πράξη η μια σειρά από πράξεις οι οποίες γίνονται με τη βοήθεια και μη, μηχανών δηλαδή αυτοματοποιημένων μέσων τα οποία έχουν αποκτούν πρόσβαση στα προσωπικά δεδομένα των φυσικών προσώπων με αποτέλεσμα να γίνεται συλλογή των δεδομένων και η οποία επιφέρει την αποθήκευση τους, επεξεργασία τους, την μεταβολή τους την διαγραφή τους η ακόμα και την καταστροφή τους.

Η παράγραφος 1 & 2 του άρθρου 5 του Γενικού Κανονισμού μας ορίζει τις βασικές αρχές οι οποίες επηρεάζουν την επεξεργασία των προσωπικών δεδομένων και είναι οι εξής:

- Η Νομιμότητα, η αντικειμενικότητα και η διαφάνεια: Δηλαδή τα δεδομένα των φυσικών προσώπων, υποβάλλονται σε θεμιτή επεξεργασία και με τρόπο τέτοιο ο οποίος να μην είναι ορατός στον εν λόγο χρήστη.
- Ο Περιορισμός του σκοπού: Γίνεται συλλογή των προσωπικών δεδομένων για καθορισμένους και νόμιμους σκοπούς οι οποίοι δεν υποβάλλουν τα δεδομένα σε επεξεργασία η γενικότερα να σε περαιτέρω επεξεργασίες προς όφελος τρίτων.

- Η Ελαχιστοποίηση των δεδομένων: Είναι αναγκαίο να περιορίζονται τα δεδομένα και να ευνοούν μόνο τους νόμιμους σκοπούς για τους οποίους γίνεται η διαδικασία της επεξεργασίας.
- Η Ακρίβεια: Η ακρίβεια είναι απαραίτητη καθώς όταν υπάρχουν δεδομένα τα οποία είναι ανακριβή πρέπει να επικαιροποιούνται και να λαμβάνονται τα απαραίτητα μέτρα.
- Ο Περιορισμός της περιόδου αποθήκευσης: Η αποθήκευση των δεδομένων υπάρχουν υπό μορφή η οποία τα διατηρεί για ένα χρονικό διάστημα ούτως ώστε να γίνει η επικαιροποίησή τους. Υπάρχει η δυνατότητα τα της αύξησής του χρονικού ορίου αυτού όταν κριθεί αναγκαίο με την απαραίτητη τήρηση του νόμου.
- Η Ακεραιότητα και εμπιστευτικότητα: Απαραίτητη είναι η εγγύηση ότι η επεξεργασία των δεδομένων γίνεται με τέτοιο τρόπο ο οποίος να είναι εντός των νομικών ορίων, χωρίς να γίνεται οποιαδήποτε παράνομη επεξεργασία, τυχόν φθορά καταστροφή η διαγραφή των δεδομένων.
- Η Λογοδοσία: Όσον αφορά την λογοδοσία, το άτομο το οποίο έχει οριστεί ως υπεύθυνος επεξεργασίας, έχει την ευθύνη για οποιοδήποτε πρόβλημα προκύψει και πρέπει να είναι σε θέση να αποδείξει με υπευθυνότητα την συμμόρφωση, την οποία θα αναλύσουμε παρακάτω.

Για να γίνει ο έλεγχος συμμόρφωσης υπάρχει κανονισμός ο οποίος επιβάλει την νόμιμη επεξεργασία επεξεργασίας. Ο κανονισμός αυτός ορίζει συγκεκριμένες ενέργειες και συνθήκες οι οποίες είναι νόμιμες για την επεξεργασία των προσωπικών δεδομένων. Μέσα σε έναν οργανισμό ή σε μια επιχείρηση, πρέπει να ληφθούν μέτρα τόσο οργανωτικά όσο και τεχνικά με αποτέλεσμα να γίνεται τήρηση των βασικών αρχών του κανονισμού χωρίς να ξεφεύγουν από τα δικαιώματα. Τα δικαιώματα είναι τα εξής:

- Η Συγκατάθεση για κάθε επεξεργασία.
- Η διαχείριση των αιτημάτων.
- Την Ικανοποίηση ως προς τα δικαιώματα για παράδειγμα στην πρόσβαση των δεδομένων, την διάδοση των δεδομένων σε ηλεκτρονικό μορφότυπο και την διαγραφή των δεδομένων (δικαίωμα στη λήθη).

Είναι αναγκαίο να οριστεί ένας Υπεύθυνος Επεξεργασίας (Data Controller) ο οποίος ορίζει τους λόγους και τους σκοπούς, ελέγχει τις προϋποθέσεις και τον τρόπο που γίνεται η επεξεργασία των προσωπικών δεδομένων. Ο Data Controller μπορεί να είναι η ίδια η εταιρεία, ένα σωματείο η ένας σύλλογος. Αυτοί έχουν στην κατοχή τους και είναι υπόχρεοι να ελέγχουν τα προσωπικά δεδομένα των φυσικών προσώπων από τα οποία αποτελούνται, για παράδειγμα οι υπάλληλοι οι οποίοι εργάζονται η τα μέλη τα οποία συνεισφέρουν.

Άλλος ένας ακόμα βασικός πυλώνας, είναι ο Υπεύθυνος Προστασίας Δεδομένων / DPO (Data Protection Officer) ο οποίος δρα για να την συμμόρφωση του Υπεύθυνου επεξεργασία και για τον έλεγχο αν οι επεξεργασίες γίνονται με βάση τον Γενικού Κανονισμού (GDPR). Έχει ως ρόλο το να συμβουλεύει και όχι να επιβάλει και δεν φέρει καμία απολύτως ευθύνη σε περίπτωση που δεν γίνει η συμμόρφωση. Ένας τέτοιος Υπεύθυνος DPO ορίζεται ανάλογα με τη δραστηριότητα της επιχείρησης ή οργανισμού.

Εκτός από τον βασικό ρόλο που έχει το περιεχόμενο του GDPR, δηλαδή την ανάγκη συμμόρφωσης, ορίζονται και οι επιπτώσεις σε περίπτωση μη συμμόρφωσης. Παρακάτω

αναλύονται μερικές επιπτώσεις της μη συμμόρφωσης οι οποίες ορίζονται στον Γενικό Κανονισμό.

Τα πρόστιμα τα οποία έχει ορίσει ο Γενικός Κανονισμός είναι υψηλά. Αρχικά, μεγάλα πρόστιμα επιφέρει σε όσους δεν λαμβάνουν τα απαραίτητα μέτρα τα οποία ορίζονται εντός της νομοθεσίας, όπως επίσης την παραβίαση χωρίς την συγκατάθεση του ατόμου, την μεταφορά δεδομένων εκτός της ΕΕ των Ευρωπαίων πολίτων και άλλες πράξεις οι οποίες μας δείχνουν την μη συμμόρφωσή υπό την απόδειξη βέβαια των Εποπτικών Αρχών που έχουν οριστεί. Αυτό θεωρείται και το πιο μεγάλο πρόστιμο το οποίο έχει επιβληθεί. Το αντίκτυπο σε τέτοιου είδους ενέργεια είναι το πρόστιμο των 20.000.000 ευρώ. Ένα αυτό συμβεί εντός μιας επιχείρησης, η επίπτωση θα είναι το πρόστιμο που αντιστοιχεί στο ποσό 4% του ετήσιου κύκλου εργασιών προηγούμενου έτους και θα επιλέγει το υψηλότερο.

Εικόνα 1: Logo GDPR – Complete guide to GDPR compliance.

2.3.2 Διεθνή Νομοθεσίες

Η συνεχής τεχνολογική εξέλιξη, έκανε απαραίτητη την λήψη μέτρων για να αντιμετωπίσει τους κινδύνους οι οποίοι επέρχονται από την μη τήρηση των μέτρων όσο αφορά την προστασία των ατόμων αλλά και των προσωπικών τους δεδομένων. Όμως η πρόωρη αντιμετώπιση των πιθανών «απειλών» άλλα και των μετέπειτα επιπτώσεων δεν είναι ίδια σε όλο τον κόσμο, καθώς λίγες χώρες εκτός την ΕΕ έχουν εισάγει κανόνες για την προστασία των προσωπικών δεδομένων.

Υπήρχε μία απόφαση η οποία έγινε ο 2450/19.12.1968, ο οποίος αφορούσε τους κινδύνους που επιφέρει η τεχνολογική εξέλιξη, καθώς τα αποτελέσματά της είχαν σαν αποτέλεσμα να μην υπάρχει ο απαραίτητος σεβασμός ως προς τα ανθρώπινα δικαιώματα. Αυτή η απόφαση, ήταν από τα πρώτα κείμενα τα οποία γράφτηκαν από την Γενική Συνέλευση των Ηνωμένων Εθνών. Έπειτα, ορίστηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) οι λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων», οι οποίες έχουν αναλυθεί παραπάνω. Στο πλαίσιο των γενικών αρχών όμως, υπάρχει μια στέρηση του δεσμευτικού χαρακτήρα.Για αυτόν ακριβώς τον λόγο, έγινε μια προσπάθεια συγκέντρωσης χωρών οι οποίες υστερούν στην νομοθεσία τους για την προστασία των προσωπικών δεδομένων και ζητήθηκε η συναίνεση τους. Μια από τις χώρες ήταν και η ΗΠΑ . Η ασταμάτητη εξέλιξη και η ροή προσωπικών δεδομένων σε όλο τον κόσμο, οδήγησαν στην δημιουργία κανόνων για την νόμιμη ροή των δεδομένων αυτών. Η Ευρώπη απαιτεί την προστασία των προσωπικών δεδομένων σε περίπτωση διαβίβασης των δεδομένων σε μια Τρίτη χώρα, έτσι για να δημιουργήσει ένα ικανοποιητικό αίσθημα ασφάλειας στους χρήστες δημιούργησε την Οδηγία 95/46/ΕΚ , άρθρο 25.

Είναι αξιοσημείωτο να αναφερθούμε σε μερικές διεθνή νομοθεσίες εφαρμοσμένες το 2019 σε χώρες εκτός ΕΕ όπως:

- Η Αργεντινή είναι η πρώτη χώρα της Λατινικής Αμερικής που εφαρμόζει κανονισμό παρόμοιο με αυτόν της ΕΕ.Η Αργεντινή, βασίζεται στον Γενικό Κανονισμό της προστασία των προσωπικών δεδομένων της Ευρωπαϊκής Ένωσης.
- Η Κολομβία η οποία είναι σε θέση να κατανοήσει το πόσο σημαντική είναι η διατήρηση της ασφάλειας των προσωπικών δεδομένων. Συνεπώς προσπαθεί να συμμορφωθεί και να αποκτήσει μια νομοθεσία στα πλαίσια του GDPR της ΕΕ.
- Η Κίνα η οποία είναι μια χώρα που δέχεται κυβερνο-επιθέσεις σε καθημερινή βάση, παρόλα αυτά μέσα στο 2019 υπήρξε πρόοδος σχετικά με την νομοθεσία για την κυβερνο-ασφάλεια και έγινε ενημέρωση σχετικά για το μπορεί να επηρεαστεί η επεξεργασία των δεδομένων.
- Και τέλος το Ηνωμένο Βασίλειο το οποίο είχε προειδοποιηθεί ότι αν τελικά ψηφίσει την έξοδο από την Ευρωπαϊκή Ένωση, τότε η μεταφορά από την Ευρωπαϊκή Ένωση στο Ηνωμένο Βασίλειο των προσωπικών δεδομένων θα απαγορεύεται εκτός και εάν το Ηνωμένο Βασίλειο αποφασίσει να εφαρμόσει νομοθεσία βασισμένη στον Γενικό Κανονισμό (GDPR).

2.3.3 Ευρωπαϊκή Νομοθεσία

Την δεκαετία του ’70 άρχισαν σιγά σιγά να γράφονται τα πρώτα νομοθετικά κείμενα τα οποία βέβαια λόγο της διαφορετικής σημασίας που έδινε το κάθε κράτος για τους κινδύνους που μπορεί να επιφέρει η επεξεργασία της πληροφορίας, οι νομοθεσίες μεταξύ κρατών είχαν αρκετές διαφοροποιήσεις. Όσον αφορά την Ευρώπη, οι πρώτες κανονιστικές ρυθμίσεις για την προστασία προσωπικών δεδομένων έγιναν τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο. Το Συμβούλιο της Ευρώπης έκανε την πρώτη κίνηση ούτως ώστε να υπάρξει ένα ουσιαστικό αποτέλεσμα για τους κινδύνους που επέρχονται από την επεξεργασία των προσωπικών δεδομένων. Μια μεγάλη νομοθετική επιρροή ήταν εκείνη της Σύμβασης 108/28.1.1981 η οποία αφορούσε την προστασία των ατόμων από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εκτός από τους κανονισμούς οι οποίοι αφορούσαν την επεξεργασία, η σύμβαση περιείχε κανόνες για τα ευαίσθητα περιεχόμενα καθώς και τα δικαιώματα των ατόμων αλλά και τα δεδομένα τους τα οποία έρχονται σε επεξεργασία. Επιπλέον, έθεσε κανονισμούς σε στην περίπτωση ροής πληροφοριών εκτός της ΕΕ.

Η Οδηγία 95/46/ΕΚ η οποία θεωρείται σταθμός για την προστασία προσωπικού χαρακτήρα δεδομένων και αναφέρεται στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, θέσπισε βασικές αρχές επεξεργασίας δεδομένων όπως για παράδειγμα θεώρει έγκυρη την επεξεργασία μόνο εφόσον δημιουργείτε σε μία από τις πλαισιωμένες βάσεις επεξεργασίας. Επιπλέον, κατοχυρώθηκαν τα δικαιώματα των ατόμων, όπως για παράδειγμα η ενημέρωση και η πρόσβαση. Επίσης όρισε τον ορθό ρόλο των ελεγκτικών αρχών για αποτελεσματικότερη προστασία των δεδομένων.

Κάθε κράτος που ανήκει στην Ευρωπαϊκή Ένωση έχει μία Αρχή Προστασίας Δεδομένων η οποία είναι μια ανεξάρτητη δημόσια- εποπτική αρχή. Ο ρόλος της είναι να επιβλέπει εάν γίνεται

η σωστή εφαρμογή του δικαίου σχετικά με την προστασία των προσωπικών δεδομένων. Η εποπτική αρχή προσπαθεί να διερευνά και να ανιχνεύει τυχών παραβιάσεις. Την σχέση που έχουν Αρχές Προστασίας Προσωπικών Δεδομένων των κρατών της Ευρωπαϊκής Ένωσης, την ελέγχει το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) το οποίο δημιουργήθηκε μαζί με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ / GDPR) ο οποίος εδρεύει στις Βρυξέλλες. Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ / GDPR) είναι ανεξάρτητος μηχανισμός με νομική προσωπικότητα, ο οποίος αποτελείται από διάφορους εκπροσώπους. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων-ΕΣΠΔ έχει ως στόχο την σωστή εφαρμογή του GDPR και της αντίστοιχης Οδηγίας εντός της ΕΕ.

Στις 25 Μαΐου 2018 τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 2016/679, ο οποίος αποτελεί την μεγαλύτερη νομοθετική ρύθμιση όσο αφορά την προστασία των προσωπικών δεδομένων των κατοίκων της ΕΕ. Η παλαιότερη οδηγία 95/46/ΕΚ αντικαταστάθηκε από τον GDPR και παρέχει νέα δικαιώματα στους κατοίκους της ΕΕ σχετικά με την επεξεργασία και την διάδοση των προσωπικών τους δεδομένων. Δηλαδή, όσοι είναι μέλη της ΕΕ έχουν ως δικαίωμα πρώτον, οι πληροφορίες σχετικά με το ποιος μπορεί να επεξεργαστεί τα δεδομένα τους να είναι σαφείς, δεύτερον να μπορούν να έχουν πρόσβαση στα προσωπικά τους δεδομένα τα οποία συλλέγονται από κάποιον τρίτο, επίσης, να μπορούν να έχουν πρόσβαση η ίδιοι στην διαγραφή των δεδομένων ένα δεν υπάρχει πλέον λόγος ύπαρξής τους, άλλο ένα δικαίωμα είναι να μπορούν να ζητήσουν διόρθωσης των δεδομένων σε περίπτωση που αυτά είναι λανθασμένα, αλλά και να πραγματοποιήσουν μεταφορά προσωπικών δεδομένων από ένα κοινωνικό δίκτυο σε ένα άλλο. Ο GDPR , αποτελεί περίοδο-τομή για την προστασία της ιδιωτικότητας. Είναι θετικό ότι το άτομο βρίσκεται στο επίκεντρο της προστασίας. Είναι αναγκαία η εύρεση ορθής σχέσης ανάμεσα στο άτομο και στις εταιρείες. Μια καλή αρχή για την βελτίωση αυτής της σχέσης είναι πως στις εταιρείες προσπαθεί να επιβληθεί η προστασία των χρηστών τους. Ο GDPR προσπαθεί να κάνει αλλαγές και εκτός Ευρωπαϊκής Ένωσης, με παραδείγματα την προστασία που λαμβάνουν οι χρήστες εντός της ΕΕ, ούτως ώστε να τους δημιουργήσει την ανάγκη εφαρμογής την νομοθεσίας για την προστασία των προσωπικών τους δεδομένων.

2.3.4 Ελληνική Νομοθεσία

Μία από τις πρώτες χώρες της Ευρωπαϊκής Ένωσης η οποία ένταξη την Οδηγία του GDPR στο εσωτερικό της ήταν η Ελλάδα. Η Ελλάδα αναγνώρισε εξ αρχής το δικαίωμα των πολίτων της σχετικά με προστασία των προσωπικών τους δεδομένων έναντι στις απειλές που μπορούν να επέλθουν. Η Ελλάδα για την προστασία των προσωπικών δεδομένων των πολιτών της, έχει ως γνώμονα για το νομοθετικό της πλαίσιο το άρθρο 9Α το οποίο απευθύνεται στο δικαίωμα επεξεργασίας, συλλογής και χρήσης των προσωπικών δεδομένων, την Εποπτεύουσα Αρχή η οποία είναι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και ορίστηκε με τον νόμο 2472/1997. Στον νόμο αυτό εισάχθηκε και η Οδηγία 95/46/ΦΕΚ η οποία αναφέρεται στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας και έθεσε κανόνες για όλες τις χώρες της ΕΕ. Πολλές τροποποιήσεις πραγματοποιήθηκαν κατά καιρούς όπως για παράδειγμα στον 2472/1997 ο οποίος επέφερε τον Ν. 3471/06 και απευθύνετε στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών.

Η ελληνική νομοθεσία άλλαξε και επέφερε αλλαγή του νόμου, με τον νέο νόμο 4624/2019.Με τον εν λόγο νόμο, εκτός από τον ορισμό των μέτρων της εφαρμογής του Νόμου 679/2016 (GDPR), παράλληλα, ενσωματώνεται στην ελληνική νομοθεσία η Οδηγία 2016/680/ΕΕ Οδηγία η οποία απευθύνεται στην προστασία των δεδομένων μέσα στο πλαίσιο επιβολής του νόμου.

Αξίζει να αναφερθούν κάποιες ποινικές κυρώσεις που μπορεί να επιφέρει η μη τήρηση του νόμου στην Ελλάδα:

1. Όποιος δεν έχει το δικαίωμα να: 1) εισέρχεται σε δεδομένα προσωπικού χαρακτήρα με οποιονδήποτε τρόπο και 2) συλλέγει, τα αντιγράφει, αλλοιώνει, διαγράφει, καταστρέφει κτλ. προσωπικά δεδομένα χωρίς την άδεια του κάτοχου, έχει ως τίμημα φυλάκιση έως ενός (1) έτους.
2. Όποιος πήρε δεδομένα σύμφωνα με την παραπάνω αναφορά και μεταδώσει, διαδώσει κ.τ.λ., τιμωρείται πάλι με φυλάκιση.
3. Εάν γίνει η μετάδοση-διαβίβαση δεδομένων προσωπικού χαρακτήρα όπως δεδομένα τα οποία αφορούν ποινικές καταδίκες, αδικήματα ή σχετικά με αυτά μέτρα ο υπεύθυνος έχει ως τιμωρία φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή έως εκατό χιλιάδες (100.000) ευρώ.
4. Σε περίπτωση παραβιάσεων των παραπάνω λόγων με εσκεμμένο σκοπό εκμετάλλευσης δηλαδή να προσπορίσει τον εαυτό του η κάποιον τρίτο και να επωφεληθεί από παράνομο περιουσιακό όφελος η ακόμα και ζημία περιουσιακή, τιμωρείτε με κάθειρξη μέχρι δέκα (10) χρόνια η ως πρόστιμο το ποσό των εκατό είκοσι χιλιάδων (120.000) ευρώ.
5. Σε περίπτωση που προκλήθηκε κίνδυνος για την εθνική ασφάλεια η την λειτουργία του δημοκρατικού πολιτεύματος κατά τους λόγους 1 έως 3 που προαναφέρθηκαν τότε οι ποινές είναι η κάθειρξη και το ποσό κυμαίνεται στις τριακόσιες χιλιάδες (300.000) ευρώ.

Το Τριμελές Εφετείο Κακουργημάτων είναι αρμόδιο για την απόφαση που θα προκύψει με βάση τους 5 παραπάνω λόγους σε περίπτωση οποιασδήποτε παραβίασης του Γενικού Κανονισμού Προστασίας Δεδομένων GDPR – Ν. 2016/679 που έχουν εφαρμοστεί στο Ελληνικό κράτος, με βάση το Ευρωπαϊκό Κοινοβούλιο.

ΚΕΦΑΛΑΙΟ 3: ΔΙΑΔΙΚΤΥΟ - ΚΟΙΝΩΝΙΚΑ ΜΕΣΑ

3.1 Η εξέλιξη του Διαδικτύου

Μέσα από τα διαφορετικά στάδια της εξέλιξής του, το Διαδίκτυο σταδιακά άλλαξε από ένα τεχνολογικό δίκτυο εγγράφων σε ένα δίκτυο όπου έγγραφα, δεδομένα, άτομα και οργανισμοί αλληλοσυνδέονται με διάφορους και συχνά απροσδόκητους τρόπους. Έχει αναπτυχθεί από ένα τεχνολογικό αντικείμενο ξεχωριστό από τους ανθρώπους σε ένα αναπόσπαστο μέρος της ανθρώπινης δραστηριότητας που έχει όλο και πιο μεγάλο αντίκτυπο στον κόσμο.

Από τις απαρχές της δεκαετίας του 1950 ξετυλίγεται η ιστορία του Διαδικτύου ξεκινώντας από τη δημιουργία του δικτύου ARPANET, την τροποποίησή του στη συνέχεια σε Internet, καταλήγοντας στην τελική μορφή ως World Wide Web. Αυτή η ιστορία βασίζεται σε τέσσερις διαφορετικές πτυχές. Ως πρώτη πτυχή μπορεί να τεθεί το ζήτημα της τεχνολογικής εξέλιξης, η οποία στηρίχθηκε σε έγκαιρη έρευνα σχετικά με την εναλλαγή πακέτων και το ARPANET και εξακολουθεί να επεκτείνεται σε διάφορες διαστάσεις όπως η κλίμακα, η απόδοση και η λειτουργικότητα υψηλότερου επιπέδου. Οι επόμενες πτυχές που αξίζει να σημειωθούν αφορούν αφενός τη λειτουργία και τη διαχείριση μιας παγκόσμιας και σύνθετης επιχειρησιακής υποδομής και αφετέρου την κοινωνία του Διαδικτύου που εκτυλίχθηκε σε μία συνεργασία των Internauts (συχνών χρηστών του Διαδικτύου) προκειμένου να δημιουργηθεί και να εξελιχθεί η τεχνολογία. Εν κατακλείδι, συναντάμε την πτυχή της εμπορευματοποίησης, με επακόλουθο μία ιδιαιτέρως δραστική μετάβαση των συμπερασμάτων της έρευνας σε μία πλήρως διαδεδομένη και διαθέσιμη υποδομή πληροφοριών.

Μία σειρά γεγονότων κατά τον Ψυχρό Πόλεμο, κατά τις δεκαετίες του ’50 και ’60, δημιούργησαν επείγουσα ανάγκη για τις Η.Π.Α. να σχεδιαστεί ένα σύστημα επικοινωνιών ικανό να επιβιώσει από μια καταστροφική θερμοπυρηνική επίθεση. Η ιδέα ενός δικτύου «κατανομής πόρων» εμφανίστηκε για πρώτη φορά το 1966 από το Υπουργείο Άμυνας που ίδρυσε τον οργανισμό ARPA (Advanced Research Projects Agency) απ’ όπου δόθηκε και η ονομασία ARPANET. Σε σύντομο χρόνο, η ARPA χρηματοδότησε τουλάχιστον δώδεκα ακριβούς υπολογιστές Mainframe για τα διάφορα πανεπιστημιακά τμήματα και ινστιτούτα που πραγματοποίησαν ερευνητικές συμβάσεις από τον οργανισμό. Το δίκτυο ARPANET κατασκευάστηκε με εκπληκτική ταχύτητα, όπου τον Οκτώβριο του 1969 έφερε το πρώτο του μήνυμα και μέχρι το 1972 ήταν ουσιαστικά πλήρες και είχε φτάσει τους 23 συνδεδεμένους hosts. Τον Οκτώβριο του 1972, κατά το πρώτο Διεθνές Συνέδριο για Υπολογιστές και Επικοινωνίες, που πραγματοποιήθηκε στην Ουάσιγκτον, οργανώθηκε μία μεγάλη και επιτυχής παρουσίαση του δικτύου, δημιουργώντας μία σύνδεση υπολογιστών από σαράντα διαφορετικές τοποθεσίες.

Από την αρχή της δεκαετίας τους 1970 έως τα μέσα, επομένως, η ARPA είχε τρία διαφορετικά “πειραματικά” δίκτυα - ARPANET, PRNET και SATNET - τα οποία χρησιμοποιούσαν όλα τα πακέτα εναλλαγής τεχνολογίας, αλλά με διαφορετικούς τρόπους. Στα τέλη του 1973, ξεκινάει η ανάπτυξη μιας νέας μεθόδου, η οποία ονομάζεται «διαδικτυακή εργασία», με βασική πρόκληση την εύρεση ενός τρόπου μετάβασης από ένα ενιαίο δίκτυο όπως το ARPANET σε κάτι που θα μπορούσε να ενσωματώσει μία ποικιλία διαφορετικών δικτύων που ανήκαν και λειτουργούσαν από ανεξάρτητους οργανισμούς και οντότητες. Για την υλοποίηση του έργου, απαιτήθηκε από όλα τα υποψήφια δίκτυα να υιοθετήσουν ένα νέο σύνολο πρωτοκόλλων, τα

οποία θα γίνονταν η κοινή γλώσσα του νέου γενικού δικτύου. Το σκεπτικό αυτό φέρει την εξέλιξη μιας σειράς από πρωτόκολλα αλληλοσύνδεσης που επικεντρώθηκαν σε δύο νέα – TCP και IP. Το 1974 οι Vinte Cerf και Bob Kahn παρουσιάζουν σε ένα άρθρο τους τη λεπτομερή περιγραφή του πρωτοκόλλου TCP (Transmission Control Protocol), οι οποίοι αργότερα, θεωρήθηκαν «πατέρες του Internet» λόγω της δημοσίευσης αυτής και της μετέπειτα συνεισφοράς τους στην εξέλιξη του Διαδικτύου. Επομένως, δύο κύριες καινοτόμες τεχνολογίες οδήγησαν την παγκόσμια εμφάνιση του Διαδικτύου μέσω της ενσωμάτωσης των υφιστάμενων συστημάτων τηλεφώνου, οπτικών ινών και δορυφόρων. Μιλάμε για την τεχνολογική καινοτομία της μεταγωγής πακέτων, το TCP / IP (Πρωτόκολλο Ελέγχου Μετάδοσης / Πρωτόκολλο Διαδικτύου) και την τεχνολογία Ψηφιακού Δικτύου Ενοποιημένων Υπηρεσιών (Integrated Services Digital Network – ISDN), στις οποίες μπορούν να αποσυντεθούν μεμονωμένα μηνύματα, τα συστατικά στοιχεία να μεταδίδονται από διάφορα κανάλια, και στη συνέχεια να επανασυναρμολογούνται στον προορισμό. Το μεγάλο πλεονέκτημα αυτής της προσέγγισης ήταν το γεγονός ότι, όσο ένα δεδομένο δίκτυο «μιλούσε» TCP / IP ήταν ελεύθερο να συνδεθεί στο Διαδίκτυο. Το World Wide Web έκανε την εμφάνισή του στη Γενεύη τη δεκαετία του ’90, θεσπίζοντας την εικονική διεύθυνση (URL) σε όλες τις σελίδες του διαδικτύου.

3.1.1 Ορισμός Διαδικτύου

Το Διαδίκτυο αποτελεί τη σημερινή εποχή ένα παγκόσμιο, επικοινωνιακό δίκτυο, που προβαίνει στην ένωση πολλών ετερογενών δικτύων και επιτρέπει την αλληλεπίδραση και την διακίνηση πληροφοριών σε διεθνές επίπεδο. Η πιο διαδεδομένη μορφή του Διαδικτύου ορίζεται ως «*το παγκόσμιο πλέγμα διασυνδεδεμένων υπολογιστών και των υπηρεσιών και πληροφοριών που παρέχει στους χρήστες του»* (Βικιπαίδεια). Η μεγάλη απήχησή του οφείλεται κυρίως:

- Στις τεράστιες δυνατότητες για πληροφόρηση και επικοινωνία.
- Στον εύκολο τρόπο χρήσης των υπηρεσιών του.
- Στο ότι οποιοσδήποτε μπορεί να συνδεθεί εύκολα και γρήγορα στο Διαδίκτυο με ελάχιστο επιπρόσθετο εξοπλισμό, είτε μέσω υπολογιστή ή κινητού τηλεφώνου ή μέσω tablet.

Η τεχνολογική επιτυχία του Διαδικτύου βασίζεται στη σουίτα πρωτοκόλλων Transmission Control Protocol (TCP) / Internet Protocol (IP). Ένα πρωτόκολλο είναι ένα συμφωνημένο σύνολο συμβάσεων που καθορίζει τους κανόνες επικοινωνίας. Το TCP διασπά και επανασυναρμολογεί πακέτα, ενώ η IP είναι υπεύθυνη για τη διασφάλιση της αποστολής των πακέτων στον σωστό προορισμό. Τα δεδομένα ταξιδεύουν μέσω Διαδικτύου μέσω διαφόρων επιπέδων δικτύων μέχρι να φτάσουν στον προορισμό τους. Τα μηνύματα ηλεκτρονικού ταχυδρομείου φτάνουν στον διακομιστή αλληλογραφίας (παρόμοιο με το τοπικό ταχυδρομείο) από έναν απομακρυσμένο προσωπικό υπολογιστή που συνδέεται με μόντεμ ή από έναν κόμβο σε ένα τοπικό δίκτυο. Από το διακομιστή, τα μηνύματα περνούν μέσω ενός δρομολογητή, ενός υπολογιστή ειδικού σκοπού που διασφαλίζει ότι κάθε μήνυμα αποστέλλεται στον σωστό προορισμό του. Ένα μήνυμα μπορεί να περάσει από διάφορα δίκτυα για να φτάσει στον παραλήπτη.

Η ευρεία ανάπτυξη και η απήχησή του, ανέδειξε νέες μορφές συμμετοχικού Διαδικτύου στην τεχνολογία, όπου οι χρήστες μπορούν να κάνουν εκτεταμένη χρήση των διαδικτυακών υπηρεσιών. Η επιβλητική εκδίπλωση νέων μορφών ηλεκτρονικής επικοινωνίας, δηλαδή τα Ιστολόγια (blogs) και τα μέσα κοινωνικής δικτύωσης, βασίζεται στην δυνατότητα που δίνεται στους χρήστες για άμεση επικοινωνία, καθώς και η δημοσίευση προσωπικών δεδομένων και απόψεων. Κυριότερες υπηρεσίες που το απαρτίζουν αποτελούν το ηλεκτρονικό ταχυδρομείο (email), ο Παγκόσμιος Ιστός (World Wide Web), οι κοινότητες (communities ή newsgroups), η μεταφορά αρχείων. Οι υπηρεσίες αυτές και η ανάπτυξη πολλών ακόμη, έχουν διαμορφώσει μία νέα εποχή, την ψηφιακή, η οποία κερδίζει σήμερα σημαίνοντα ρόλο στον τομέα της επικοινωνίας. Ο τρόπος με τον οποίο οι άνθρωποι αλληλεπιδρούν και ενημερώνονται σε μαζικό επίπεδο έχει εξελιχθεί ραγδαία και σε αυτό συνεργεί σχεδόν συνολικά η ανάπτυξη νέων μέσων που συνδυάζουν την πληροφόρηση, την επικοινωνία και την ψυχαγωγία των χρηστών, τα γνωστά σε όλους μας σχεδόν μέσα κοινωνικής δικτύωσης (Social Media).

3.1.2 Η εξέλιξη από το Web 1.0 στο Web 2.0

Σημαντικό για την κατανόηση της ανάλυσης των δύο μορφών του Ιστού που θα αναφερθεί παρακάτω, είναι ο διαχωρισμός των όρων ‘Διαδίκτυο’ και ‘Παγκόσμιος Ιστός’. Οι δύο αυτοί όροι, γνωστοί από δισεκατομμύρια ανθρώπους στον κόσμο, τείνουν συχνά να χρησιμοποιούνται εναλλακτικά χωρίς να είναι ακριβώς το ίδιο πράγμα. Όπως προαναφέρθηκε προηγουμένως, το Διαδίκτυο αποτελεί το παγκόσμιο σύστημα επικοινωνίας, συμπεριλαμβανομένου του υλικού και της υποδομής, ενώ ο Παγκόσμιος Ιστός (World Wide Web), είναι μία από τις υπηρεσίες του Διαδικτύου.

Μέσω του κύκλου ζωής του, το World Wide Web πέρασε διάφορες φάσεις ανάπτυξης. Όπως πολλοί γνωρίζουν, οι τρεις καινοτομίες που συνήθως συνδέονται με τρεις φάσεις είναι, ο Ιστός των εγγράφων (το Web 1.0), ο Ιστός των ανθρώπων (το Web 2.0) και ο Ιστός των δεδομένων (το Web 3.0 που δεν έχει πραγματοποιηθεί ακόμη).

Το Web 1.0 ήταν η πρώτη υλοποίηση του Διαδικτύου, διήρκησε από το 1991 έως το 2005 και αναφέρεται ως η πρώτη γενιά του World Wide Web που αρχικά ορίστηκε ως «*ένας χώρος πληροφοριών στον οποίο τα αντικείμενα ενδιαφέροντος που αναφέρονται ως πόροι προσδιορίζονται από το παγκόσμιο αναγνωριστικό που ονομάζεται Uniform Resources Identifiers (URIs)*» (Choudhury, 2014). Δημιουργός αυτής της πρωτοπόρας τεχνολογίας είναι ο Tim Berners-Lee, Βρετανός επιστήμονας και μηχανικός λογισμικού στο CERN. Το 1989 είχε την ιδέα να χρησιμοποιήσει ένα νέο είδος πρωτοκόλλου για την κοινή χρήση εγγράφων και πληροφοριών σε όλο το τοπικό δίκτυο του CERN. Η ιδέα αυτή τον οδήγησε στη δημιουργία μιας νέας γλώσσας που ονομάζεται γλώσσα σήμανσης υπερκειμένου (HTML) και την εμφάνιση του όρου «hypertext» (υπερκείμενο). Ο Berners-Lee και ο Βέλγος επιστήμονας υπολογιστών Robert Cailliau πρότειναν το 1990 τη χρήση υπερκειμένου «για τη σύνδεση και την πρόσβαση πληροφοριών διαφόρων ειδών ως ιστός κόμβων στους οποίους ο χρήστης μπορεί να περιηγηθεί κατά βούληση». Με αυτούς τους τρόπους η πρώτη διαδικτυακή υπηρεσία σχεδιάστηκε και δοκιμάστηκε και αργότερα περιορίστηκε ως World Wide Web.

Αρχικά, ο Ιστός πρώτης γενιάς είχε μοναδικό σκοπό την παράδοση περιεχομένου. Επομένως, ξεκίνησαν να δημιουργούνται οι σημαντικότερες εφαρμογές μέσω του Διαδικτύου, με

μεγαλύτερες το ηλεκτρονικό ταχυδρομείο (email) και η παροχή βιβλίων, ειδήσεων και μουσικής σε ψηφιακή μορφή. Αυτή η ανταλλαγή δεδομένων μέσω Διαδικτύου έκανε το μεγάλο μέρος της τεχνολογικής έρευνας να επικεντρωθεί στη βελτίωση των συνθηκών ανταλλαγής δεδομένων. Η τεχνολογία του Web 1.0 περιλαμβάνει βασικά πρωτόκολλα ιστού: HTML, HTTP και URI. Τα κύρια χαρακτηριστικά του είναι τα εξής:

- Έχει περιεχόμενο μόνο για ανάγνωση.
- Δημιουργία διαδικτυακής παρουσίας και διάθεση πληροφοριών σε οποιονδήποτε ανά πάσα στιγμή.
- Περιλαμβάνει στατικές ιστοσελίδες και χρησιμοποιεί βασική Hypertext Mark-up Language.

Αυτό που έκανε όμως το περιβάλλον του μη διαδραστικό, ήταν το γεγονός ότι ο χρήστης δεν μπορούσε να επεξεργαστεί περιεχόμενο του Ιστού παρά μόνο να κάνει «παθητική» ανάγνωση. Βασικά στοιχεία του Web 1.0, όπως η μη υποστήριξη αμφίδρομης επικοινωνίας και ο μικρός αριθμός δημιουργών ιστοσελίδων που υπήρχε, λόγω έλλειψης γνώσης της γλώσσας HTML, αρχίζουν να προκαλούν το δίκτυο αργό και κάνουν τον χρήστη να λιμοκτονεί για πόρους. Αργότερα, πραγματοποιούνται πειράματα με τα εργαλεία συνεργασίας του WWW χωρίς όμως τελικά να κερδίσουν αρκετή έλξη και να παρουσιάζεται σιγά σιγά έλλειψη συμμετοχής των χρηστών και σημαντικά τεχνικά εμπόδια.

Από πολλές απόψεις, η έκρηξη της φούσκας dot-com του 2000 είχε μακροχρόνιες επιπτώσεις στο Διαδίκτυο, που κυμαίνονται από οικονομικά έως θέματα εμπιστοσύνης, με σημαντικότερες:

1. Η εμπιστοσύνη στις διαδικτυακές επιχειρήσεις χάθηκε.
2. Οι επενδύσεις αποσύρθηκαν από εταιρείες τεχνολογίας, επομένως η καινοτομία επιβραδύνθηκε.
3. Οι εταιρείες που επέζησαν της φούσκας θεωρήθηκαν ότι κάνουν κάτι καλύτερο από τις υπόλοιπες.

Όπως σημειώνει ο O'Reilly - «*η ανάγκη για το Web 2.0 δημιουργήθηκε από μια προφανή συνειδητοποίηση ότι η κατάρρευση του dot-com σηματοδότησε κάποιο είδος καμπής για τον Ιστό*». Η εξέλιξη του Διαδικτύου έρχεται με την εμφάνιση του όρου Web 2.0 ο οποίος περιγράφει την τάση αλλαγής στη χρήση της τεχνολογίας του World Wide Web καθώς και στη σχεδίαση ιστοσελίδων, που έχει ως σκοπό να ενισχύσει τη δημιουργικότητα, τις επικοινωνίες, τον ασφαλή διαμοιρασμό πληροφοριών, τη συνεργασία και την λειτουργικότητα στον Παγκόσμιο Ιστό. Η αλλαγή αυτή όμως δεν προϋποθέτει τεχνικές αλλαγές στο Διαδίκτυο ή δομικές αλλαγές λειτουργίας, αλλά μία εντελώς διαφορετική προσέγγιση της χρήσης του.

Το Web 2.0 αφορά τη δεύτερη γενιά ιστού και εισήχθη από τον Tim O'Reilly στην επιρροή του στο blog του το 2005 (οπ. αναφ. Choudhury, 2014), μετά από μία αυθόρμητη συζήτηση διάσκεψης με άλλους επιχειρηματίες και ακαδημαϊκούς εμπειρογνώμονες όπου συζητούσαν τις αλλαγές στην ανάπτυξη και τη χρήση του Παγκόσμιου Ιστού. Πιο συγκεκριμένα ορίζει στο blog του το Web 2.0 ως εξής: «*Το Web 2.0 είναι η επιχειρηματική επανάσταση στον κλάδο των υπολογιστών που προκαλείται από τη μετάβαση στο Διαδίκτυο ως πλατφόρμα, και η απόπειρα κατανόησης των κανόνων για την επιτυχία σε αυτή την πλατφόρμα*». Με άλλα λόγια, το Διαδίκτυο πρέπει να χρησιμοποιείται από όλους τους χρήστες δυναμικά σαν μία πλατφόρμα

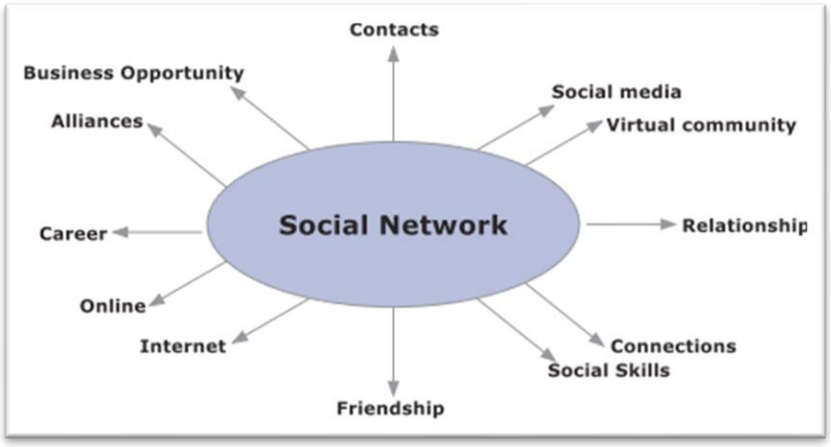
που να μπορεί να αλλάζει συνεχώς, και όχι να υπάρχει μόνο για να παρέχει συγκεκριμένες υπηρεσίες.

Η εξέλιξή του έφερε την αλλαγή στον τρόπο αλληλεπίδρασης μεταξύ των ανθρώπων μέσω της εμφάνισης νέων διαδικτυακών τεχνολογιών, όπως wikis, Ιστολόγια (blogs), ιστοσελίδες κοινωνικής δικτύωσης, κ.ά., που επέτρεψαν την ανοιχτή πρόσβαση, την άμεση επικοινωνία μεταξύ των χρηστών και την επαναχρησιμοποίηση δωρεάν δεδομένων. Αντί για απλή ανάγνωση μιας ιστοσελίδας, ο χρήστης καλείται να συνεισφέρει στο περιεχόμενό της, σχολιάζοντας δημοσιεύματα ή με τη δημιουργία ενός λογαριασμού χρήστη ή προφίλ στην ιστοσελίδα, η οποία μπορεί να επιτρέψει αυξημένη συμμετοχή. Ελαφρές τεχνολογικές εξελίξεις, αλλά κυρίως βελτιώσεις στην εμπιστοσύνη και έμφαση στα οικονομικά βιώσιμα επιχειρηματικά μοντέλα ήταν πίσω από μια παγκόσμια ανάκαμψη στο Διαδίκτυο. Τα παραπάνω επιφέρουν εξαιρετικά περισσότερες δυνατότητες στη χρηστική του αξία με αυτόματη αύξηση των χρηστών και της δράσης τους, καθώς και της εμπορικής του χρησιμότητας. Σημαντική αύξηση παρουσιάζει επίσης, η εμπιστοσύνη στον Ιστό η οποία εμφανίστηκε λόγω της τυποποίησης της υποκείμενης τεχνολογίας σήμανσης Ιστού (HTML, CSS, κ.λπ.), μετατρέποντας την εμπειρία πιο συνεπής μεταξύ των προγραμμάτων περιήγησης. Και όλα αυτά, σε συνδυασμό με καλύτερους νομικούς κανονισμούς και πολλές βελτιώσεις ασφάλειας των συναλλαγών σε μετρητά στο Διαδίκτυο. Προσπαθώντας να προσδιορίσουμε τις αλλαγές που έγιναν στην εξέλιξη του World Wide Web εστιάζουμε στα εξής χαρακτηριστικά:

1. **Προσβασιμότητα** σε όλους τους χρήστες ανεξαρτήτως ηλικίας, φύλου, φυλής που ανήκουν, τόπου κατοικίας, κοινωνικο-οικονομικού και μορφωτικού επιπέδου. Το Web 2.0 είναι ανοικτό για επικοινωνία και αλληλεπίδραση.
2. **Συνεργασία και συλλογική δράση** μέσω της κοινωνικής δικτύωσης. Μέσα από αλληλεπιδραστικές δυναμικές ιστοσελίδες οι χρήστες ανταλλάσσουν απόψεις, σκέψεις, πρακτικές, διαμοιράζουν μηνύματα, αρχεία, δημιουργούν Ιστολόγια και ιστοσελίδες και προβάλλοντας τις ιδέες τους επιχειρούν να επηρεάσουν και να διαμορφώσουν κοινωνικές, πολιτικές κ.ά. τάσεις.
3. **Έκφραση προσωπικών απόψεων** σε Ιστολόγια (Blogs) και Φόρμες (Forums), καθώς και διατύπωση κρίσεων και σχολιασμού σε ιδέες που δημοσιεύονται στο www.
4. **Δημιουργία ιστοσελίδων**, Ιστολογιών κτλ. και διαμοιρασμός πληροφοριών σε ψηφιακή μορφή.
5. **Εξάπλωση καινοτόμων ιστοχώρων** στο διαδίκτυο, καθώς υπάρχει η τάση να αναπτύσσονται όλο και πιο πρωτότυπες σελίδες που επιδιώκουν να γίνουν δημοφιλείς.

3.2 Ορισμός Κοινωνικής Δικτύωσης

«*Όταν ένα δίκτυο υπολογιστών συνδέει άτομα ή οργανισμούς, είναι ένα κοινωνικό δίκτυο, δηλαδή ένα δίκτυο κοινωνικών αλληλεπιδράσεων και προσωπικών σχέσεων. Ακριβώς όπως ένα δίκτυο υπολογιστών είναι ένα σύνολο μηχανών που συνδέονται με ένα σύνολο καλωδίων, έτσι ένα κοινωνικό δίκτυο είναι ένα σύνολο ατόμων (ή οργανισμών ή άλλων κοινωνικών οντοτήτων) που συνδέονται με ένα σύνολο κοινωνικών σχέσεων, όπως η φιλία, η συνεργασία ή η ανταλλαγή πληροφορίας*» (Garton et al, 1997).



Εικόνα 2: Η θεμελιώδης έννοια των Ιστοσελίδων Κοινωνικής Δικτύωσης (SNS).

Λόγω της ταχύτατης εξάπλωσης του διαδικτύου και της επιτακτικής ανάγκης για χρήση του, τα διαδικτυακά κοινωνικά δίκτυα αποκτούν συνεχώς με τη σειρά τους μεγαλύτερη δημοτικότητα. Τα κοινωνικά δίκτυα φέρουν σε σύνδεση σύνολα ατόμων όχι αποκλειστικά κοινωνικά, αλλά και γεωγραφικά. Για τον λόγο αυτό, στις μέρες μας έχουν γίνει μία σημαντική βάση για την αμοιβαία επικοινωνία και δεν μπορούν να αγνοηθούν με κανένα τρόπο, γιατί αποτελούν αναπόσπαστο κομμάτι της καθημερινότητας. Για τον λόγο αυτό, στις μέρες μας έχουν γίνει μία σημαντική βάση για την αμοιβαία επικοινωνία και δεν είναι εφικτό να αγνοηθούν, καθώς αποτελούν αναπόσπαστο μέρος της ρουτίνας. Ο τρόπος που επιτυγχάνεται η επικοινωνία είναι κατά τη χρήση ιστοσελίδων μέσω των οποίων γίνεται η διεπαφή μεταξύ των χρηστών, όπως για παράδειγμα με σχόλια, ανταλλαγή μηνυμάτων, με φωτογραφίες ή άλλες πληροφορίες. Οι κοινώς γνωστές και δημοφιλέστερες τέτοιες ιστοσελίδες είναι το Facebook, το Twitter, το Instagram και το LinkedIn. Παρά το άκαμπτο ανταγωνισμό, το Facebook παραμένει το μεγαλύτερο και πιο δημοφιλές κοινωνικό δίκτυο, με πάνω από δύο δισεκατομμύρια ανθρώπους που χρησιμοποιούν την πλατφόρμα. Ακολουθήθηκε, κατά σειρά δημοτικότητας, από το Instagram, το Facebook Messenger, το Twitter και το Pinterest, σύμφωνα με το Statistica.com (Kenton, 2020).

3.3 Μέσα Κοινωνικής Δικτύωσης

Αρχικά, πριν αναφερθούμε στον επιστημονικό ορισμό των μέσων κοινωνικής δικτύωσης, ας αναρωτηθούμε ποια είναι τα παραδοσιακά μέσα ενημέρωσης που προυπήρχαν του Διαδικτύου. Πρόκειται για την τηλεόραση, τις εφημερίδες, τα περιοδικά κ.λπ.. Σήμερα, τα διαδικτυακά κοινωνικά μέσα μπορούν να λάβουν τη μορφή μιας ποικιλίας τεχνολογικά ενεργοποιημένων δραστηριοτήτων. Αυτές οι δραστηριότητες περιλαμβάνουν: κοινή χρήση φωτογραφιών, blogging, κοινωνικά παιχνίδια, κοινωνικά δίκτυα, κοινή χρήση βίντεο, επιχειρηματικά δίκτυα, εικονικούς κόσμους, κριτικές και πολλά άλλα.

Οι Kaplan & Haenlein (2010) σημειώνουν ότι, «*Ο όρος Κοινωνικά Μέσα (Social Media) αναφέρεται στα μέσα διαμοιρασμού πληροφορίας, ενημέρωσης και κοινωνικής δικτύωσης και αξιοποιούν τεχνολογίες Web 2.0 των οποίων η φιλοσοφία βασίζεται στη δημιουργία και*

ανταλλαγή περιεχομένου από τους χρήστες.». Αυτό που δίνει ισχύ στα Κοινωνικά Μέσα είναι η ευκαιρία σύνδεσης και ανταλλαγής πληροφοριών ανεξαρτήτως τοποθεσίας, καθώς και με απεριόριστο αριθμό ανθρώπων ταυτοχρόνως. Η άνοδος των ψηφιακών και κινητών τεχνολογιών επηρέασε και διευκόλυνε την αλληλεπίδραση των ατόμων όσο ποτέ. Αυτό έφερε στο προσκήνιο τη νέα εποχή των κοινωνικών μέσων με τη δραστικότητα να απαρτίζει τις νέες λειτουργίες των μέσων.

Το 2019, η Merriam-Webster, Inc. καθόρισε τα μέσα κοινωνικής δικτύωσης ως «*οι μορφές ηλεκτρονικής επικοινωνίας (όπως ιστότοποι για κοινωνική δικτύωση και microblogging) μέσω των οποίων οι χρήστες δημιουργούν διαδικτυακές κοινότητες για να μοιράζονται πληροφορίες, ιδέες, προσωπικά μηνύματα και άλλο περιεχόμενο (όπως βίντεο)*». Στις μέρες μας, υπάρχουν εκατοντάδες κοινωνικά μέσα με διάφορα τεχνολογικά οφέλη, που υποστηρίζουν ένα ευρύ φάσμα συμφερόντων και πρακτικών. Ενώ τα βασικά τεχνολογικά χαρακτηριστικά τους είναι αρκετά συνεπή, οι πολιτισμοί που εμφανίζονται γύρω από τους ιστότοπους ποικίλλουν. Για παράδειγμα, οι ιστότοποι όπως το MySpace, το Facebook, το Twitter και άλλοι , έχουν προσελκύσει εκατομμύρια χρήστες με μεγάλο αριθμό αυτών να έχουν ενσωματώσει τους ιστότοπους αυτούς στις ημερήσιες πρακτικές τους. Τα περισσότερα μέσα κοινωνικής δικτύωσης βασίζονται στην ίδια λογική, αλλά δεν παύουν να υπάρχουν και αυτά που έχουν διαφορετικό σκοπό και εξυπηρετούν διαφορετικό κοινό. Άλλα πάλι προσελκύουν άτομα που βασίζονται σε κοινή γλώσσα ή σε κοινές φυλετικές, σεξουαλικές, θρησκευτικές ή εθνικές ταυτότητες. Τα μέσα διαφέρουν επίσης ως προς το επίπεδο κατά το οποίο τοποθετούν νέα εργαλεία πληροφόρησης και επικοινωνίας, όπως συνδεσιμότητα κινητής τηλεφωνίας, blogging και κοινή χρήση φωτογραφιών/βίντεο.

Οι Hu & Lin (2013) παραθέτουν τέσσερα χαρακτηριστικά των κοινωνικών μέσων που αποκομίστηκαν εφαρμόζοντας τη θεωρία νοημοσύνης. Τα χαρακτηριστικά αυτά είναι τα κάτωθι:

- Ενσωμάτωση (Integration). Η ενσωμάτωση εκφράζεται κυρίως στην σύνδεση εκατομμυρίων χρηστών ανά τον κόσμο με διαφορετικά χαρακτηριστικά. Η ενσωμάτωση είναι η παρούσα μικρή παγκόσμια θεωρία και αρχή διανομής της σκέψης, καθώς τα κοινωνικά μέσα αποσκοπούν στο να μπορούν οι χρήστες να συναλλάσσουν και να μοιράζονται πληροφορίες. Αυτό προέρχεται από τεχνολογίες ολοκλήρωσης (ενσωμάτωσης) πληροφοριών όπως είναι το πρωτόκολλο TCP / IP και το World Wide Web, που παρέχουν αποτελεσματικότητα για ετερογενείς πληροφορίες, πλατφόρμες και τερματικά για την επίτευξη διασύνδεσης. Οι ενέργειες αυτές, καθιστούν τη διαδρομή των πληροφοριών συντομότερη και προσφέρει βελτιωμένη υποστήριξη στον χρήστη (Hu & Lin, 2013).
- Αποτελεσματικότητα χρόνου (Time Effectiveness). Στα μέσα κοινωνικής δικτύωσης επικρατεί συγχρονισμός στην ανταλλαγή πληροφοριών και γρήγορη προσβασιμότητα αυτών από τους χρήστες, καθώς η αποστολή και η λήψη πληροφοριών μπορεί να επιτευχθεί ανά πάσα στιγμή. Η αποτελεσματικότητα του χρόνου αποτελεί μέτρο σημαντικού δείκτη της ευφυΐας, με αποτέλεσμα οι πληροφορίες κοινωνικών μέσων να είναι υψηλής αξίας και να προσελκύουν ευρέως τους χρήστες. Προκειμένου η αποτελεσματικότητα του χρόνου να έχει αυξητικές τάσεις διαρκώς, οι τεχνολογίες υπολογιστών, τερματικών κινητής τηλεφωνίας και δικτύου θα εξακολουθούν να είναι υψηλής ταχύτητας, ευρυζωνικές και με εύκολη κατεύθυνση (Hu & Lin, 2013).

- Λιγότερη προσπάθεια (Least Effort). Τα κοινωνικά μέσα αποτελούν ανοικτές και δωρεάν υπηρεσίες, χωρίς την απαραίτητη ειδική δεξιότητα ή εκπαίδευση για τη χρήση τους. Χάρις αυτών, ο χρήστης θα καταβάλει λιγότερη προσπάθεια για την λήψη και την χρήση των πληροφοριών. Αυτή είναι η απόδοση της αρχής λιγότερης προσπάθειας στην Επιστήμη της Πληροφόρησης. Με βάση την αρχή αυτή, τα μέσα κοινωνικής δικτύωσης θα λάβουν δύο αντίθετες δυνάμεις. Ο ρόλος της μίας, είναι να διατηρεί τις πληροφορίες σύντομες και απλές για σωστή διαχείριση και χρήση, ενώ ο ρόλος της άλλης είναι να τις διατηρεί λεπτομερείς και πλούσιες ώστε να φέρουν μεγαλύτερη αξία (Hu & Lin, 2013).
- Τάξη (Orderliness). Η δυναμική και το κοινό των κοινωνικών μέσων δικτύωσης κάνουν μία ταξινόμηση των κοινωνικών μέσων. Επειδή οι χρήστες κοινωνικών μέσων μπορούν να επεξεργαστούν και να αναθεωρήσουν τις πληροφορίες, οι λανθασμένες και άχρηστες πληροφορίες στα μέσα κοινωνικής δικτύωσης θα φιλτραριστούν. Αυτή η χρήση της δημιουργικότητας του ανθρώπου και η τακτική της νοημοσύνης καθιστούν το σύνολο των πληροφοριών κοινωνικών μέσων πιο πολύτιμες (Hu & Lin, 2013).

3.3.1 Κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης

Καθώς τα μέσα κοινωνικής δικτύωσης υφίσταται περίπλοκο θέμα που εμπεριέχει μεγάλο αριθμό προσεγγίσεων, εργαλεία και τεχνικές, θα ήταν ωφέλιμο να δοθεί βάση στην κατηγοριοποίησή τους καθώς παρατηρείται συχνά λανθασμένη ταύτισή τους με άλλους όρους. Τα κοινωνικά μέσα αναφέρονται σε νέες μορφές μέσων που περιλαμβάνουν διαδραστική συμμετοχή. Εφόσον έχουν μία κοινή λογική, οι κατηγορίες τους θα ταξινομηθούν με βάση τους διαφορετικούς τρόπους εκδήλωσης των δυνατοτήτων τους.

Οι Kaplan & Haenlein (2010) παρουσιάζουν μία διάκριση των κοινωνικών μέσων που βασίζεται στο συνδυασμό δύο διαστάσεων, του βαθμού αυτό-αποκάλυψης που απαιτείται και του τύπου αυτό-παρουσίασης που επιτρέπεται. Οι τύποι των κοινωνικών μέσων που διέκριναν λεπτομερώς είναι έξι και συμπεριλαμβάνουν: τα Συνεργατικά Έργα (Collaborative Projects), τα Ιστολόγια (Blogs), τις Κοινότητες Περιεχομένου (Content Communities), τις Σελίδες Κοινωνικής Δικτύωσης (Social Networking Sites - SNS), τους Εικονικούς Κόσμους παιχνιδιών (Virtual Game Worlds) και τους Εικονικούς Κοινωνικούς Κόσμους (Virtual Social Worlds).

Τα συνεργατικά έργα ορίζονται ως εφαρμογές κοινωνικών μέσων που επιτρέπουν την από κοινού και ταυτόχρονη δημιουργία περιεχομένου που σχετίζεται με τη γνώση από πολλούς τελικούς χρήστες. Τέτοιες εφαρμογές αποτελούν τα Wikis, Social bookmarking sites, Forums και Review sites (Kaplan & Haenlein, 2014). Στις εφαρμογές αυτές, γίνεται διάκριση μεταξύ των Wikis και τις ιστοσελίδες κοινωνικής σελιδοσήμανσης (Social bookmarking sites). Τα Wikis επιτρέπουν σε όλους τους χρήστες να δημιουργούν , να αφαιρούν και να τροποποιούν περιεχόμενο ακόμη και χωρίς συνδρομή, με κορυφαία εφαρμογή την ηλεκτρονική εγκυκλοπαίδεια Wikipedia. «*Οι ιστοσελίδες κοινωνικής σελιδοσήμανσης αφορούν τη συλλογή και βαθμολόγηση ομαδικών συνδέσμων διαδικτύου ή περιεχομένου πολυμέσων με την δυνατότητα εκχώρησης ετικετών*». Πιο γνωστό μέσο αποτελεί το Delicious το οποίο επιτρέπει την αποθήκευση και την κοινή χρήση σελιδοδεικτών ιστού (Kaplan & Haenlein, 2010).

Τα Ιστολόγια αποτελούν ιστότοπους συζήτησης ή πληροφόρησης που εμφανίζουν συνήθως καταχωρήσεις σε στυλ ημερολόγιου. Ο τρόπος εμφάνισης των κοινοποιήσεων είναι συνήθως σε αντίστροφη χρονολογική σειρά προκειμένου στο πάνω μέρος της ιστοσελίδας να βρίσκεται η πιο πρόσφατη. Ένα Ιστολόγιο συνήθως διαχειρίζεται από ένα άτομο αλλά επιτρέπει την αλληλεπίδραση με άλλους μέσω της προσθήκης δημόσιων σχολίων, μία δυνατότητα που έχει συμβάλλει σημαντικά στη δημοτικότητα πολλών Ιστολογίων.

Οι κοινότητες περιεχομένου επιτρέπουν στους χρήστες να μοιράζονται διαδικτυακό υλικό πολυμέσων διαφορετικού τύπου όπως, κείμενο (π.χ. BookCrossing), φωτογραφίες (π.χ. Flickr, Pinterest), βίντεο (π.χ. YouTube) και παρουσιάσεις PowerPoint (π.χ. SlideShare). Ένα σχετικά πρόσφατο φαινόμενο σε αυτήν την κατηγορία κοινωνικών μέσων είναι το Pinterest, στο οποίο ο χρήστης κοινοποιεί ό,τι περιεχόμενο του αρέσει (εικόνα, βίντεο, κείμενο) με όποιον τον ακολουθεί.

Οι σελίδες κοινωνικής δικτύωσης (social networking sites) είναι ιστοσελίδες που επιτρέπουν τους χρήστες να συνδέονται και να αλληλεπιδρούν με άλλους χρήστες, μέσω της δημιουργίας δημόσιου ή ήμι-δημόσιου προσωπικού προφίλ. Είναι εφικτή η πρόσκληση φίλων, ώστε να υπάρχει πρόσβαση σε αυτά τα προφίλ, καθώς και η αποστολή άμεσων μηνυμάτων μεταξύ τους ή ηλεκτρονικού ταχυδρομείου. Οι σελίδες αυτές στις μέρες μας, είναι πανταχού παρούσες καθώς έχουν διεισδύσει δυναμικά στην σύγχρονη κουλτούρα. Στην κορυφή της λίστας εδώ και χρόνια, βρίσκεται το Facebook με έδρα τις Η.Π.Α..

Όσον αφορά τους εικονικούς κόσμους (virtual worlds), είναι ένα διαδικτυακό τρισδιάστατο περιβάλλον στο οποίο οι χρήστες εμφανίζονται με τη μορφή εξατομικευμένων ειδώλων. Μπορούν να αναγνωριστούν δύο μορφές εικονικών κόσμων. Μία μορφή είναι οι εικονικοί κόσμοι παιχνιδιών (virtual game worlds) οι οποίοι απαιτούν από τους χρήστες να ακολουθούν πιο συγκεκριμένους κανόνες στο πλαίσιο ενός μαζικά διαδικτυακού παιχνιδιού ρόλων πολλαπλών παικτών (MMORPG). Η δεύτερη μορφή αφορά τους εικονικούς κοινωνικούς κόσμους (virtual social worlds). Αποτελούν ένα πιο αδέσμευτο εικονικό περιβάλλον στο οποίο οι χρήστες ουσιαστικά μπορούν να συμπεριφέρονται όπως στην πραγματική ζωή καθώς δεν υπάρχουν κανόνες που μετριάζουν το εύρος των ενδεχόμενων αλληλεπιδράσεων (Kaplan & Haenlein, 2010). Η πιο δημοφιλής έκφραση αυτής της μορφής είναι το Second Life στο οποίο με την δημιουργία ενός avatar, οι χρήστες της πλατφόρμας αποφασίζουν αν θα αναπαράγουν την πραγματική τους ζωή ή μία νέα βελτιωμένη έκδοσή της.

Μία άλλη κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης η οποία δόθηκε από τον Zhang (2010), είναι η ακόλουθη:

- Κοινωνική δικτύωση (Social networking): Γνωρίζοντας τα Facebook, LinkedIn, MySpace, τα κοινωνικά δίκτυα δίνουν τη δυνατότητα αλληλεπίδρασης με άλλους χρήστες, άμεσης επικοινωνίας μεταξύ τους και ανταλλαγή πληροφοριών.

- Ιστολόγια (blogging / microblogging): Τα πιο δημοφιλή σήμερα είναι τα Twitter, Blogger, WordPress. Αυτοί οι τύποι κοινωνικών μέσων επιλέγονται για δημοσίευση, ανακάλυψη και σχολιασμό άρθρων κάθε είδους θέματος και κυρίως λόγω της ελευθερίας έκφρασης της άποψης και της προσωπικής καταχώρησης περιεχομένου.

- Μέσα κοινωνικής σελιδοσήμανσης (Social bookmarking), όπως τα Blinklist, Delicious, Diggo κ.ά. . Η προσφορά των μέσων αυτών είναι η δυνατότητα επισήμανσης ιστοσελίδων και διαμοιρασμού αυτών με άλλους ενδιαφερόμενους χρήστες.

- Ιστοσελίδες συνεργατικής συγγραφής (Collaborative authoring), με πιο γνωστά τα Wikipedia, Google docs, Zoho office suite, όπου επιτρέπεται η προσθήκη περιεχομένου από όλους τους χρήστες και η επεξεργασία των ήδη υπαρχόντων.

- Μέσα διαμοιρασμού πολυμέσων (Multimedia sharing), όπως είναι τα: YouTube, Spotify, Flickr, Twitch και πολλά άλλα. Οι χρήστες των μέσων αυτών μπορούν να δημιουργούν και να διαμοιράζονται αρχεία ήχου, εικόνας και βίντεο.

- Διαδικτυακές τηλεδιασκέψεις (Web conferencing), όπως τα: GoToMeeting, WebEx, DimDim.

(Μανούσου και Χαρτοφύλακα, 2011)

3.3.2 Στατιστικά χρήσης

Ένα φαινόμενο που λειτούργησε αποφασιστικά στην ανακατασκευή του κόσμου όπως παρουσιάζεται σήμερα, είναι η παγκόσμια προσβασιμότητα στο Διαδίκτυο. Προτιμώμενο κομμάτι του World Wide Web για τους χρήστες, αποτελούν τα μέσα κοινωνικής δικτύωσης, τα οποία μπορεί να τα βρει κανείς σε διάφορους τύπους όπως φόρουμ, Ιστολόγια, εφαρμογές συνομιλίας, επιχειρηματικά δίκτυα, πλατφόρμες κοινής χρήσης φωτογραφιών, microblogs κ.ά.. Η χρήση των κοινωνικών μέσων σε όλο τον κόσμο αυξάνεται συνεχώς. Είναι αναμφίβολα μία από τις πιο δημοφιλείς διαδικτυακές δραστηριότητες στις οποίες συμμετέχουν οι χρήστες.

Από την πρώτη εμφάνισή τους το 1996, τα μέσα κοινωνικής δικτύωσης κατάφεραν να διεισδύσουν στα μισά από τα 7,7 δισεκατομμύρια άτομα στον κόσμο. Οι πλατφόρμες κοινωνικών δικτύων σχεδόν τριπλασίασαν τη συνολική τους βάση χρηστών την τελευταία δεκαετία, από 970 εκατομμύρια το 2010 σε αριθμό που περνά τους 3,81 δισεκατομμύρια χρήστες το 2020. Φέτος το παγκόσμιο ποσοστό διείσδυσης έφτασε το 49%, με την Ανατολική Ασία και τη Βόρεια Αμερική να έχουν το υψηλότερο ποσοστό στο 71 και 69 τοις εκατό αντίστοιχα, ακολουθούμενο από τη Βόρεια Ευρώπη στο 67%.

Σε αυτό το σημείο, αξίζει να παρουσιαστούν κάποια σημαντικά στατιστικά χρήσης των μέσων κοινωνικής δικτύωσης στις μέρες μας.

Το 2020 ο αριθμός των χρηστών των Social Media ανέρχεται στα 3.81 δισεκατομμύρια, σχεδόν διπλάσιο από τα 2.07 δισεκατομμύρια που ήταν το 2015. Από 3,81 δισεκατομμύρια χρήστες κοινωνικών μέσων, το 98,68% έχει πρόσβαση σε ιστότοπους ή εφαρμογές μέσω κινητής συσκευής, με μόνο 1,32% σε πλατφόρμες πρόσβασης αποκλειστικά μέσω επιτραπέζιου υπολογιστή. Επιπλέον, οι χρήστες του Διαδικτύου ξοδεύουν κατά μέσο όρο 144 λεπτά την ημέρα σε κοινωνικά μέσα και εφαρμογές ανταλλαγής μηνυμάτων. Ο ρυθμός αύξησης της χρήσης των κοινωνικών μέσων από το 2015 είναι κατά μέσο όρο 12,5% ανά έτος. Ωστόσο, το 2019-2020 παρουσιάζεται μία πτώση με τον ρυθμό αύξησης να πέφτει στο 9,2%.

Όσον αφορά τα κορυφαία κοινωνικά δίκτυα παγκοσμίως, αυτά συνήθως διαθέτουν μεγάλο αριθμό λογαριασμών χρηστών ή ισχυρές μετρήσεις αφοσίωσης χρηστών. Σύμφωνα με την Statista, τα πιο δημοφιλή κοινωνικά δίκτυα παγκοσμίως, που κατατάσσονται κατά αριθμό μηνιαίων ενεργών χρηστών, από τον Οκτώβριο του 2020, είναι:

1. Facebook (2,7 δισεκατομμύρια)
2. YouTube (2 δισεκατομμύρια)
3. WhatsApp (2 δισεκατομμύρια)
4. Facebook Messenger (1,3 δισεκατομμύρια)
5. WeChat (1,2 δισεκατομμύρια)
6. Instagram (1,16 δισεκατομμύρια)

Κατανοώντας και γνωρίζοντας την ισχύ που έχει η κοινωνική δικτύωση έως τώρα, ο αριθμός των χρηστών παγκοσμίως υπολογίζεται ότι θα φτάσει τους 3,43 δισεκατομμύρια μηνιαίους ενεργούς χρήστες κοινωνικών μέσων έως το 2023. Ένας τέτοιος αριθμός αποτελεί σχεδόν το ένα τρίτο του συνολικού πληθυσμού της Γης.

3.4 Ιστορική εξέλιξη και εξάπλωση των Μέσων Κοινωνικής Δικτύωσης

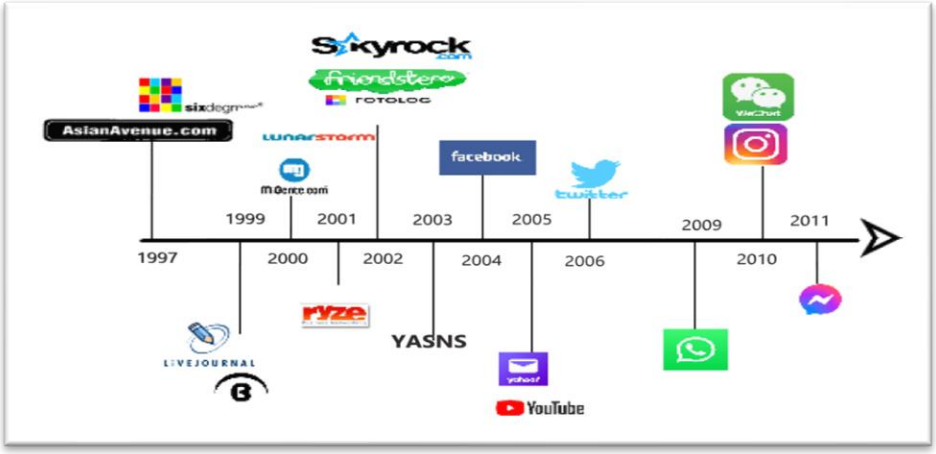
- Το 1997, πρώτο δίκτυο που δημιουργήθηκε και ανταποκρίθηκε στον ορισμό των μέσων κοινωνικής δικτύωσης ήταν το SixDegrees.com. Το δίκτυο αφορούσε χρήστες ο οποίοι έφτιαχναν προφίλ και λίστες από φίλους και τους άφηνε να περιηγηθούν σε στις λίστες αυτές. Οι χρήστες μπορούσαν να στέλνουν μηνύματα μεταξύ τους όμως δεν τους έφτανε μόνο αυτό. Έτσι μετά από πολλές διαμαρτυρίες των χρηστών ότι δεν μπορούσαν να κάνουν πολλά πράγματα το 2000 έκλεισε το κοινωνικό δίκτυο. Ο δημιουργός του SixDegrees θεωρεί ότι το μέσο αυτό ήταν αρκετά μπροστά για την εποχή του. Επίσης, το 1997 δημιουργήθηκε τα δίκτυο AsianAvenue.com το οποίο ήταν μια πλατφόρμα στην οποία μπορούσες να δημοσιεύσεις προσωπικές ιστοσελίδες, αγγελίες για θέσεις εργασίας, ειδήσεις και δημοσκοπήσεις για τροφή συζητήσεων (Τικπασανούδη, 2019).
- Το 1999, εμφανίστηκε το LiveJournal το όποιο είχε να κάνει με επιστημονικά περιοδικά όπου οι χρήστες επισήμαναν άλλους χρήστες για ανάγνωση των δημοσιευμένων άρθρων, δηλαδή οι χρήστες μπορούσαν να διαχειριστούν το απόρρητο. Το ίδιο έτος, δημιουργήθηκε το blackplanet.com το οποίο επέτρεπε ότι και το AsianAvenue.com. έγινε ιδιαίτερα γνωστό στους Αφρό-Αμερικανούς.
- Το 2000, δημιουργήθηκε το LunarStorm το οποίο είχε καταλόγους βιβλίων, βιβλία και ημερολόγια. Την ίδια χρονολογία ξεκίνησε και το MiGente, όπου επέτρεπε ακριβώς ότι και τα blackplanet και AsianAvenue (Τικπασανούδη, 2019).
- Το 2001, δημιουργήθηκε το Ryze.com, το οποίο ήταν ο πρωταρχικός πυλώνας της νέας γενιάς των κοινωνικών δικτύων. Το όνομά "rize up" αποσκοπούσε στην βοήθεια των ανθρώπων μεταξύ τους για καλύτερη ποιότητα δικτύωσης. Μπορούμε να πούμε πώς ουσιαστικά πήγε ένα βήμα παρακάτω την ιδέα του SixDegrees απλά είχε ως εφαρμογή την δημιουργία επαγγελματικών και επιχειρηματικών επαφών (Τικπασανούδη, 2019).
- Το 2002, ήρθαν στην επιφάνεια τρία μέσα κοινωνικής δικτύωσης: το Fotolog, το Friendster και το Skyrock. Το Fotolog.com ήταν ένα δίκτυο που επέτρεπε την κοινή

χρήση φωτογραφιών. Το Friendster, ήταν μία προ επέκταση του Ryze. Βέβαια ο κύριος σκοπός του ήταν να ανταγωνιστεί το MiGente. Το Friendester, αποτελούνταν κυρίως από χρήστε κοντά στην ηλικία των 20 ετών οι οποίοι ήταν μορφωμένοι και είχαν ιδιαιτέρα ερεθίσματα δηλαδή διαφορετικές κοινωνικές αλλά και σεξουαλικές προτιμήσεις. Το πρόβλημα του κοινωνικού δικτιού ήταν πως είχε θέσει περιορισμούς οι οποίο έπρεπε να μαζέψεις κάποιους βαθμούς προσθέτοντας φίλους έτσι ώστε να δεις το προφίλ κάποιου ο οποίος είχε περισσότερους βαθμούς από εσένα. Αυτό έφερε σαν αποτέλεσμα την δημιουργία πολλών ψεύτικων προφίλ κάτι το οποίο εξόργισε τους δημιουργούς του κοινωνικού δικτύου. Αυτοί οι χρήστες που είχαν στην κατοχή τους ψεύτικα προφίλ ονομάστηκαν Fakesters. Έπειτα από αίτημα των δημιουργών αναγκάστηκαν να διαγράψουν τα ψεύτικα προφίλ. Τέλος, το Skyrock. προσέφερε έναν ελεύθερο χώρο στον ιστό για να επιτρέποντάς στους χρήστες του να δημιουργούν Ιστολόγια, να προσθέτουν προφίλ και να ανταλλάσσουν μηνύματα.

- Το 2003, δημιουργήθηκε ο όρος YASNS (Yet Another Social Networking Service) το οποίο είχες ως κύριο σκοπό τη δημιουργία κοινοτήτων με κοινά ενδιαφέροντα. Ο όρος YASNS αποτελούνταν για επιχειρηματικούς σκοπούς από μέσα όπως τα δίκτυα LinkedIn, OpenBC / XING, Visible Path και Xing. Το LinkedIn είχε ως σκοπό να φέρνει σε επικοινωνία επιχειρηματίες με άλλους επιχειρηματίες, αυτός ο ρόλος τηρείτε και σήμερα με πάνω από 175 εκατομμύρια χρήστες παγκοσμίως. Άλλα μέσα κοινωνικής δικτύωσης τα οποία είναι στον όρο YASNS είναι αυτά που κάλυπταν άλλες υπηρεσίες, όπως για παράδειγμα το Tribe.net το οποίο απευθυνόταν σε ένα εξειδικευμένο πλήθος χρηστών, το Dogster για άτομα τα οποία ασχολούνται με σκύλους, το αντίστοιχο Catster για γάτες, το Care2 για τους ακτιβιστές, το Couchsurfing για ταξιδιώτες και το MyChurch για χριστιανικές εκκλησίες. Σιγά-σιγά βλέπουμε μεγάλη αύξηση των χρηστών στα μέσα και περισσότερη εξοικείωση, έτσι άρχισε η ανάγκη να γίνεται όλο και μεγαλύτερη έτσι δημιουργήθηκαν τα πρώτα δίκτυα το οποία έχουν πολλά κοινά χαρακτηριστικά με τα σημερινά μέσα κοινωνικής δικτύωσης, αυτά ήταν το MySpace και το HiFive. Το HiFive επεκτάθηκε κυρίως σε μικρότερες χώρες όπως η Λατινική Αμερική και η Νότια Αμερική. Το MySpace ήταν ο πρώτος ισότοπος ο οποίος έδινε την δυνατότητα να επικοινωνούν οι χρήστες μεταξύ τους μέσω μηνυμάτων αλλά και να δημιουργούν ένα δικό τους προφίλ όπως εκείνοι θέλουν. Οι χρήστες ήταν κυρίως καλλιτέχνες, έφηβοι αλλά και απόφοιτοι κολλεγίων. Στον όρο YASNS συμπεριλαμβάνονται το LastFM για μουσική, Flickr.com για φωτογραφίες κ.ά. (Τικπασανούδη, 2019).
- Το 2004, δημιουργήθηκε η εταιρεία Facebook Inc. η οποία ιδρύθηκε από τον Mark Zuckerberg. Αρχικά, αποτελούσε δίκτυο με δυνατότητα συμμετοχής μόνο από άτομα που φοιτούσαν στο Harvard, στο οποίο φοιτούσε ο ίδιος ο Zuckerberg. Για τον λόγο αυτό, απαραίτητη προϋπόθεση για να συνδεθεί κάποιος ήταν να διαθέτει email της μορφής 'harvard.edu'. Το 2005 το Facebook έδωσε πρόσβαση σε μαθητές του λυκείου και σε μέλη άλλων μαθητικών ομάδων. Το 2006-2007 το κοινωνικό δίκτυο πήρε παγκόσμιες διαστάσεις για άτομα ηλικίας 13+. Κατά τη διάρκεια λειτουργίας δέκα χρόνων, έως το 2014 έρευνα έδειξε ότι οι χρήστες ξεπερνούσαν τους 900.000.000. Το Facebook, υπάρχει σε πάνω από 70 γλώσσες για όλο τον κόσμο. Λόγω της εφαρμογής η οποία είναι διαθέσιμη σε όλα τα smartphone κινητά, οι επισκέψεις στην εφαρμογή ανά την ημέρα παρατηρήθηκε να ξεπερνάει τα 757 εκατομμύρια.
- Το έτος 2005 δημιουργήθηκαν το Yahoo! και το YouTube. Το Yahoo! Mail είναι μία από τις πρώτες πλατφόρμες οι οποίες περιέχονται στον παγκόσμιο Ιστό (web-based) κύριος ρόλος της είναι η παροχή δωρεάν υπηρεσιών ηλεκτρονικού ταχυδρομείου. Το

YouTube είναι ένας ιστότοπος που έχει σαν κύριο ρόλο την αναπαραγωγή βίντεο ,την κοινοποίηση τους, την αποθήκευσή τους, και την αναζήτηση τους.

- Το 2006 έρχεται στην επιφάνεια άλλο ένα πολύ ισχυρό δίκτυο το Twitter. Το δίκτυο αυτό είναι ένας ιστοχώρος ο οποίος δίνει την δυνατότητα στους χρήστες να κάνουν tweets δηλαδή την δημοσίευση μικρών μηνυμάτων, επίσης τα μηνύματα μπορούν να διαβαστούν και από χρήστες η οποίοι δεν διαθέτουν κάποιο λογαριασμό.
- Το 2009 ιδρύθηκε το WhatsApp Inc από τούς δημιουργούς του Yahoo!. Το WhatsApp είναι μία εφαρμογή στην οποία γίνονται ανταλλαγές μηνυμάτων, φωτογραφιών και βίντεο μέσω του Smartphone.
- Το 2010 ιδρύθηκε το Instagram, το οποίο έχει το ίδιο σκοπό με τα τελευταία μέσα κοινωνικής δικτύωσης την ίδρυση τους την έκαναν δύο απόφοιτοι του Πανεπιστημίου Stanford. Το Instagram “συνεργάζεται” και με τα υπόλοιπα μέσα κοινωνικής δικτύωσης. Το 2012 αγοράστηκε από το Facebook. Επίσης την ίδια χρονιά δημιουργείται το WeChat. Η δραστηριότητα των χρηστών στο WeChat αναλύεται, παρακολουθείται και μοιράζεται με τις κινεζικές αρχές. Το WeChat λογοκρίνει πολιτικά ευαίσθητα θέματα στην Κίνα. Τα δεδομένα που διαβιβάζονται από λογαριασμούς που έχουν καταχωρηθεί εκτός Κίνας παρακολουθούνται, αναλύονται και χρησιμοποιούνται για τη δημιουργία αλγορίθμων λογοκρισίας στην χώρα.
- Το 2011 εμφανίστηκε το Messenger το οποίο είναι μία προέκταση του Facebook και βρίσκεται ουσιαστικά μέσα σε αυτό, καθότι ο λογαριασμός των χρηστών και στα δύο μέσα είναι κοινός και άμεσα συνδεδεμένος. Το Messenger αποτελεί υπηρεσία άμεσων μηνυμάτων, ανταλλαγή φωτογραφιών, βίντεο και άλλων υπηρεσιών και είναι διαθέσιμο και σε εφαρμογή αλλά και στην κεντρική ιστοσελίδα του Facebook.



Εικόνα 3: Ιστορική εξέλιξη βασικότερων Μέσων Κοινωνικής Δικτύωσης.

3.5 Ασφαλής χρήση των μέσων

Ιδιαίτερα τον τελευταίο καιρό, οι ανησυχίες για την προστασία της ιδιωτικής ζωής έχουν αυξηθεί κατά έναν μεγάλο βαθμό. Βλέπουμε ότι οι πλατφόρμες κοινωνικών μέσων όπως το Twitter, , το Facebook, το Instagram, το LinkedIn και το Snapchat κ.τ.λ. έχουν γίνει τρόπος

ζωής των χρηστών του Διαδικτύου ,οι άνθρωποι μοιράζονται ειδήσεις, φωτογραφίες, προσωπικές απόψεις και σχεδόν οτιδήποτε συμβαίνει στη ζωή τους.
Ο μεγάλος όγκος πληροφοριών που μοιράζονται οι άνθρωποι στα κοινωνικά μέσα - μερικές από τις οποίες είναι πολύ προσωπικές - προσελκύουν άλλους θεατές εκτός του αξιόπιστου κύκλου συγγενών και φίλων τους. Γνωρίζοντας αυτά τα ζητήματα απορρήτου, πρέπει να εντοπιστούν τρόποι προστασίας του απορρήτου στα κοινωνικά μέσα.

Τα κοινωνικά μέσα και το απόρρητο δεν μπορούν να συμβαδίσουν, όμως αυτό δεν σημαίνει ότι όποιος χρησιμοποιεί τα μέσα κοινωνικής δικτύωσης δεν μπορεί να έχει μια διαδικτυακή ζωή η οποία διατηρεί ένα βαθμό απορρήτου. Είναι όμως εφικτό να γίνει έλεγχος του απορρήτου στα Social Media;

Κάθε άτομο είναι, σε ένα μέρος, υπεύθυνο για την ιδιωτικότητα του στα κοινωνικά μέσα. Για το λόγο αυτό, με την επιλογή μερικών πλαισίων είναι εφικτό να μετατρέψει κάποιος το απόρρητο των κοινωνικών μέσων που χρησιμοποιεί από «αδύναμο» σε «δυνατό» και επακολούθως να προστατεύσει τις διαδικτυακές του πληροφορίες.

Στην πραγματικότητα, είναι σχεδόν αδύνατο να υπάρχει απόλυτος έλεγχος του απόρρητο των κοινωνικών μέσων. Αυτό συμβαίνει επειδή ακόμα κι αν γίνονται όσο το δυνατόν συνεχόμενες ενέργειες για την προστασία του απορρήτου, συμπεριλαμβανομένης της διαγραφής του λογαριασμού, οι φίλοι και οι συγγενείς θα εξακολουθούν να μοιράζονται προσωπικά στοιχεία του χρήστη. Συμπερασματικά, η απαλλαγή από τα μέσα κοινωνικής δικτύωσης δε συνεπάγεται και αποφυγή διαμοιρασμού προσωπικών δεδομένων και ενδεχομένως να μην είναι χρήσιμη σε αυτήν την περίπτωση.

Η χρήση των μέσων κοινωνικής δικτύωσης επιφέρει πολλές θετικές συνέπειες, όπως η ενημέρωση, η ψυχαγωγία, η διευκόλυνση σε γραφειοκρατικό επίπεδο, αλλά δεν παύει να έχει και αρνητικές. Στις μέρες μας, η ασφάλεια των πληροφοριών είναι πρωταρχικός παράγοντας για όλους τους χρήστες και τους οργανισμούς που λειτουργούν καθημερινά κάνοντας χρήση υπολογιστών και δικτύων. Μία σημαντική περίπτωση που κάνει την προστασία προσωπικών στοιχείων αναγκαία, είναι ο κίνδυνος που γεννιέται κατά την χρήση της τεχνολογίας για επεξεργασία πληροφοριών, καθώς αυτό μπορεί να οδηγήσει σε λανθασμένη αποκάλυψή τους. Η υπηρεσία κοινωνικής δικτύωσης όπως το Facebook δεν αποτελεί ένα ασφαλές μέρος, παρά τις τεχνολογίες που εφαρμόζουν στις εγκαταστάσεις τους ή τις πολιτικές ασφάλειας που ακολουθούν. Αυτό οφείλεται κυρίως, στο μεγάλο όγκο πληροφοριών που προσθέτουν οι χρήστες στα κοινωνικά δίκτυα αυτού του τύπου. Πιο συγκεκριμένα, η Barnes (2006) αναφέρει ότι η εντυπωσιακή δημοτικότητα των μέσων αυτών, στα οποία παρατηρείται τακτική χρήση από έφηβους και άτομα που δεν συλλογίζονται το απόρρητο ή την ασφάλεια, οδηγεί στη δημιουργία μεγάλης ποσότητας ιδιωτικών πληροφοριών στο Διαδίκτυο όπου επιτρέπεται η πρόσβαση σε αυτό από τρίτους. Επομένως, με τη συνεχόμενη υπερίσχυση της κοινωνικής δικτύωσης, την παραμονή των χάκερ ή των κλεφτών στο Διαδίκτυο αλλά και την αναληθή εμπιστοσύνη των ανθρώπων απέναντι σε αυτό, υπάρχει συνεχής κίνδυνος για την ασφάλεια των πληροφοριών.

Οι Vladlena et. al. (2015) επισημαίνουν ότι «*Ο τομέας της ασφάλειας πληροφοριών στο Διαδίκτυο είναι καλά αναπτυγμένος και εξελίσσεται συνεχώς ως απάντηση σε νέες απειλές και έτσι πρέπει να εξελιχθεί και με τα κοινωνικά μέσα.*». Προκειμένου να προστατευτούν οι εκατομμύρια χρήστες και τα κοινωνικά δίκτυα από τις απειλές του κυβερνοχώρου και να αντιμετωπιστεί η πιθανή απώλεια ιδιωτικών και προσωπικών πληροφοριών, πρέπει να

δράσουν πιο ενεργά αφομοιώνοντας τους κινδύνους και τις προκλήσεις που παραμονεύουν. Παρακάτω καταγράφονται ορισμένες χρήσιμες οδηγίες και συμβουλές για τους χρήστες των μέσων κοινωνικής δικτύωσης όσον αφορά την προστασία των προσωπικών τους δεδομένων και περιλαμβάνουν τα ακόλουθα:

- Ο αριθμός των προσωπικών πληροφοριών που δημοσιεύονται θα πρέπει να είναι περιορισμένος. Η κοινή χρήση μη απαραίτητων προσωπικών στοιχείων, όπως η διεύθυνση, προσωπικά στοιχεία επικοινωνίας ή πληροφορίες σχετικά με την ρουτίνα, σας καθιστά ευάλωτους. Μπορεί, επίσης, να προσφέρει σε εγκληματίες του κυβερνοχώρου αφορμές να συλλέγουν προσωπικές πληροφορίες, θέτοντας έτσι σε κίνδυνο την ασφάλειά σας. Βοηθητικό ρόλο στην αποφυγή της υπερβολικής κοινής χρήσης έχει η αποφυγή αναζητήσεων μέσω των διαδικτυακών κοινωνικών μέσων. Οι αναζητήσεις μέσω Facebook ή Twitter για παράδειγμα, καταγράφονται και χρησιμοποιούνται για τη διαμόρφωση ενός προφίλ χρήστη, οπότε η χρήση μηχανών αναζήτησης μεσολάβησης όπως το Startpage.com καθίσταται πιο ασφαλή.[1]

- Η είσοδος οποιασδήποτε πληροφορίας στο Διαδίκτυο την καθιστά άμεσα διαθέσιμη στο κοινό και δύσκολη στη διαγραφή της από αυτό. Υπάρχουν περιπτώσεις όπου, ακόμη και αν διαγράψετε πληροφορίες του λογαριασμού σας, τα δεδομένα αυτά να βρίσκονται αποθηκευμένα ως αντίγραφα σε άλλους υπολογιστές ή κρυφές μνήμες του δικτύου. Βεβαιωθείτε λοιπόν, ότι τα δεδομένα σας διαγράφονται οριστικά και προτιμήστε να μην κοινοποιείτε εμπιστευτικές πληροφορίες.

- Το Διαδίκτυο αποτελεί μέρος το οποίο διευκολύνει τους ανθρώπους να παρουσιάζουν αναληθείς ή απατηλές πληροφορίες τόσο για διάφορα θέματα όσο και για στοιχεία της ταυτότητάς τους. Οι απατεώνες χρησιμοποιούν συνήθως ψεύτικους λογαριασμούς για καμπάνιες ηλεκτρονικού ψαρέματος, οπότε η προσθήκη ενός ατόμου σε μία πλατφόρμα όπως το Facebook, βοηθάει στη συλλογή πληροφοριών που θα τελέσουν τα email απάτης πιο πειστικά. Για τον λόγο αυτό, συνιστάται να μην γίνεται αποδοχή αιτημάτων φιλίας ή επικοινωνίας από άγνωστα άτομα καθώς και άμεση εμπιστοσύνη των πληροφοριών που παρουσιάζονται από τρίτους. Είναι σημαντικό να γίνεται επαλήθευση της αυθεντικότητας των πληροφοριών που παρουσιάζονται και τακτική εκκαθάριση της λίστας φίλων ώστε να αφαιρούνται τα ανεπιθύμητα άτομα.

- Πριν την εγγραφή σε οποιαδήποτε πλατφόρμα κοινωνικής δικτύωσης, είναι ζωτικής σημασίας η ανάγνωση και η πλήρης κατανόηση των Όρων Χρήσης και της Πολιτικής Απορρήτου του διαδικτυακού κοινωνικού μέσου. Η αμέριμνη αποδοχή των όρων μπορεί να οδηγήσει σε ευπάθεια δεδομένων.

- Διαμορφώστε και παραμείνετε ενημερωμένοι για τις ρυθμίσεις απορρήτου του κοινωνικού δικτύου που χρησιμοποιείτε. Τα περισσότερα δίκτυα έχουν ως προεπιλεγμένη ρύθμιση την ορατότητα του λογαριασμού σας σε όλους. Επομένως, προβείτε στην αλλαγή αυτής της ρύθμισης έτσι ώστε να περιορίσετε την προσβασιμότητα στις πληροφορίες σας από συγκεκριμένους χρήστες.

- Χρησιμοποιείστε ισχυρούς κωδικούς πρόσβασης οι οποίοι δεν μπορούν να παραβιαστούν εύκολα. Οι κωδικοί που περιέχουν συνδυασμό πεζών και κεφαλαίων γραμμάτων, αριθμών

[1] https://www.makeuseof.com/tag/social-media-privacy-issues/

και διάφορων συμβόλων αποτελούν πιο «δυνατοί» και δύσκολοι στο να ανιχνευτούν. Επιπροσθέτως, η συχνή τροποποίησή τους καθώς και χρήση άλλων κωδικών για διαφορετικούς λογαριασμούς καταφέρνει να μπερδέψει τους εγκληματίες του κυβερνοχώρου.

- Όσον αφορά τους γονείς, προτείνεται η συχνή παρακολούθηση των παιδιών κατά την διάρκεια χρήσης των ιστοσελίδων κοινωνικής δικτύωσης. Τα παιδιά έχουν έλλειψη επίγνωσης των κινδύνων, κάτι που τα κάνει πιο ευαίσθητα στις απειλές των μέσων. Με την κατάλληλη διδασκαλία πάνω σε θέματα ασφάλειας στο Διαδίκτυο και εφόσον σας είναι γνώριμες οι διαδικτυακές τους συνήθειες, διασφαλίζετε την ασφαλή χρήση του Διαδικτύου από την μεριά των παιδιών.

- Πρέπει να αναφέρονται τυχόν ανησυχίες που υπάρχουν σχετικά με το απόρρητο και την ασφάλειά σας, όπως εκφοβισμός (cyberbullying), ανεπιθύμητο περιεχόμενο κ.ά.. Αν αντιληφθείτε ότι ο λογαριασμός σας έχει κλαπεί, κινηθείτε άμεσα στην προτεινόμενη διαδικασία αναφοράς (report).

Πρόσφατες μελέτες αποκάλυψαν ότι το 80% των ανθρώπων ανησυχεί για το ποιος μπορεί να έχει πρόσβαση στα δεδομένα του σε ιστότοπους κοινωνικών μέσων και για καλό λόγο. Σχεδόν το ένα τέταρτο των χρηστών των μέσων κοινωνικής δικτύωσης έχουν πέσει θύματα μιας επίθεσης στον κυβερνοχώρο, με το hack του Ιουλίου 2020 να τροφοδοτεί αυξημένο σκεπτικισμό σχετικά με την αποτελεσματικότητα των μέτρων που έχουν λάβει οι πάροχοι υπηρεσιών.

Οι τακτικοί χρήστες των κοινωνικών μέσων είναι σημαντικό να κατανοούν τους μηχανισμούς αποθήκευσης, χρήσης και πρόσβασης στα δεδομένα που χρησιμοποιούν τόσο οι πλατφόρμες όσο και οι εφαρμογές τρίτων. Η ανάλυση των κύριων ζητημάτων απορρήτου στα κοινωνικά μέσα καθώς και των τρόπων αποφυγής τους, περιλαμβάνει:

Διανομή προσωπικών πληροφοριών (Oversharing Personal Information)

Πληροφορίες που είναι σημαντικό να μη διαμοιράζονται ή προβάλλονται στο προφίλ κοινωνικών μέσων όπως:

- Διεύθυνση σπιτιού
- Αριθμός τηλεφώνου ή προσωπική διεύθυνση email
- Οποιαδήποτε οικονομική πληροφορία
- Ακριβείς ετικέτες τοποθεσίας
- Εικόνες που κάνουν το σπίτι διαμονής αναγνωρίσιμο από το δρόμο
- Εικόνες παιδιών που κάνουν τα σχολεία τους αναγνωρίσιμα
- Ακριβείς ημερομηνίες ταξιδιού και πληροφορίες σχετικά με το πότε μετακινείται κάποιος

Για την αποφυγή της υπερβολικής έκθεσης των προσωπικών πληροφοριών στο διαδίκτυο είναι χρήσιμες οι παρακάτω ενέργειες:

Όταν πρόκειται για πλατφόρμες όπως το Facebook, θα πρέπει να βεβαιωθείτε ότι το προφίλ, οι πληροφορίες και οι αναρτήσεις σας είναι ορατά μόνο από φίλους. Εάν δεν χρησιμοποιείτε το λογαριασμό σας για να προσελκύσετε κοινό, μπορείτε να ορίσετε το προφίλ σε ιδιωτικό.

Αυτό σημαίνει ότι έχετε τον έλεγχο του ποιος μπορεί να σας ακολουθήσει και, επομένως, ποιος μπορεί να δει το περιεχόμενό σας.

Εξουσιοδότηση μη αξιόπιστων εφαρμογών

Επιπλέον, πολλοί άνθρωποι χρησιμοποιούν εφαρμογές με τους λογαριασμούς τους στα μέσα κοινωνικής δικτύωσης όπως διάφορα παιχνίδια για κινητά που συγχρονίζονται με τον λογαριασμό σας κοινωνικών μέσων. Κατά την έγκριση μιας εφαρμογής, πρέπει να γίνουν οι παρακάτω ενέργειες για την προστασία του απορρήτου.

- Ποτέ μην χρησιμοποιείτε εφαρμογές που ισχυρίζονται ότι ξεκλειδώνουν κρυφές ή μυστικές λειτουργίες
- Αποφύγετε κουίζ που απαιτούν να συνδεθείτε με κοινωνικά μέσα
- Ελέγχετε πάντα τα δικαιώματα που ζητά η εφαρμογή
- Εξουσιοδοτείτε μόνο εφαρμογές από αξιόπιστους προγραμματιστές
- Όταν δοκιμάζετε μια νέα εφαρμογή, επικοινωνήστε πρώτα με άτομα που γνωρίζετε για να δείτε αν το έχουν χρησιμοποιήσει στο παρελθόν

Απόρρητο στα μέσα κοινωνικής δικτύωσης: Το κενό των φίλων

Ένας άλλος μεγάλος κίνδυνος είναι «Το κενό των φίλων». Παρόλο που μπορεί να φαίνεται αβλαβές να προσθέσετε άτομα που δεν γνωρίζετε στα κοινωνικά μέσα, αυτό μπορεί να σας εκθέσει σε μεγάλο κίνδυνο. Για παράδειγμα, οι απατεώνες ενδέχεται να χρησιμοποιούν ψεύτικους λογαριασμούς για καμπάνιες ηλεκτρονικού ψαρέματος. Προσθέτοντας ένα άτομο σε μια πλατφόρμα όπως το Facebook, μπορούν να συλλέξουν πληροφορίες που θα κάνουν τα email απάτης πιο πειστικά. Ένας άλλος τρόπος που μπορεί να θέσει σε κίνδυνο την ασφάλειά σας είναι όταν οι εφαρμογές έχουν πρόσβαση στις πληροφορίες σας μέσω του λογαριασμού ενός φίλου σας. Ενώ για παράδειγμα το Facebook έχει ενισχύσει το απόρρητο στο δίκτυο από αυτή την άποψη, οι διάφοροι τρόποι με τους οποίους οι φίλοι μπορούν να θέσουν σε κίνδυνο το απόρρητό μας εξακολουθούν να προκαλούν ανησυχία.

Για να προσπαθήσετε να μετριάσετε τον κίνδυνο που θέτουν οι “φίλοι” σας στους λογαριασμούς αυτούς, θα πρέπει να αποφύγετε την αποδοχή αιτήσεων σύνδεσης από αγνώστους. Θα πρέπει επίσης να κάνετε τακτική εκκαθάριση της λίστας των φίλων για να αφαιρέσετε άτομα με τα οποία δεν ενδιαφέρεστε πραγματικά να παραμείνετε συνδεδεμένοι.

Χάκερ που χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης ως εργαλείο

Υπάρχουν διάφοροι τρόποι με τους οποίους οι χάκερ μπορούν να χρησιμοποιήσουν τον λογαριασμό σας στα μέσα κοινωνικής δικτύωσης για να θέσουν σε κίνδυνο την ασφάλειά σας. Μερικοί τρόποι με τους οποίους οι χάκερ χρησιμοποιούν τα κοινωνικά μέσα για να στοχεύουν τα θύματα περιλαμβάνουν:

- Παραβίαση λογαριασμών για τη συλλογή κωδικών πρόσβασης που ενδέχεται να επαναχρησιμοποιηθούν σε άλλους λογαριασμούς
- Catfishing απάτες, όπου κάποιος προσποιείται ότι είναι κάποιος που δεν είναι
- Αποστολή συνδέσμων κακόβουλου λογισμικού μέσω ιδιωτικών μηνυμάτων

Για να αποτρέψετε τους χάκερ από τη χρήση του λογαριασμού κοινωνικών μέσων εναντίον σας είναι να μην επαναχρησιμοποιήσετε ποτέ τον κωδικό πρόσβασής σας σε λογαριασμούς.

Μόλις ο κωδικός πρόσβασης και το email σας παραβιαστούν σε έναν ιστότοπο, θα παραβιαστούν σε όλους τους ιστότοπους. Επιπλέον, δεν πρέπει ποτέ να κάνετε κλικ σε τυχαίους συνδέσμους που αποστέλλονται στα εισερχόμενα κοινωνικών μέσων. Μπορεί να σας σώσει από την επίσκεψη σε έναν ιστότοπο απάτης ή την ένεση κακόβουλου λογισμικού στο πρόγραμμα περιήγησής σας.

Αλλαγή των Όρων Παροχής Υπηρεσιών

Καθώς τα μοντέλα εσόδων και οι επιχειρηματικές δομές αλλάζουν, τα δίκτυα κοινωνικών μέσων ενδέχεται να προσαρμόσουν τους όρους παροχής υπηρεσιών τους. Αυτό ισχύει ιδιαίτερα όταν μια εταιρεία αποκτά άλλη. Για παράδειγμα, όταν το Facebook αποκτά μια εταιρεία, τα δεδομένα χρήστη της κοινοποιούνται συχνά στο δίκτυο του Facebook. Οι όροι της εταιρείας ενδέχεται επίσης να αλλάξουν για να ενταχθούν στο νέο όραμα της μητρικής της εταιρείας όπως για παράδειγμα αυτό που συμβαίνει με το WhatsApp υπό την κυριότητα του Facebook.

Για να αποφύγετε την συλλογή των δεδομένων σας, θα πρέπει να κάνετε περιοδικά μια ανασκόπηση των ρυθμίσεων απορρήτου του κοινωνικού σας λογαριασμού και των όρων της πλατφόρμας για να μετριάσετε την κοινοποίηση των δεδομένων σας. Δεν υπάρχουν πάντα πολλά που μπορείτε να κάνετε, ωστόσο, μπορείτε να ενημερώνεστε σχετικά με τον τρόπο με τον οποίο χρησιμοποιούνται τα δεδομένα σας και να προσπαθήσετε να μειώσετε τις πληροφορίες σας.

Συνεργασία φορέων για την ασφαλή χρήση του διαδικτύου για παιδιά:

1. Το σχολείο με την εφαρμογή χρονικών ορίων χρήσης αλλά και την προώθησή των παιδιών για συμμετοχή σε άλλες δραστηριότητες.
2. Το σχολείο το οποίο πρέπει να κάνει εκμάθηση της ασφαλούς χρήσης του διαδικτύου, να ενημερώσει για τα φαινόμενα εθισμού, κατάχρησης και παρενόχλησης.
3. Τα Μέσα Μαζικής Ενημέρωσης με τρόπο αντικειμενικό χωρίς άρωμα reality.
4. Η Πολιτεία η οποία θα απαιτεί να τηρείται το νομικό πλαίσιο στα internet caffe και να γίνεται εκπαίδευση γονέων και ενημέρωση τους από ειδικούς.

(Τσίτσικα, 2014)

ΚΕΦΑΛΑΙΟ 4 : ΚΑΤΑΝΟΗΣΗ ΤΩΝ ΘΕΜΑΤΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

4.1 Προσωπικά δεδομένα των Μέσων Κοινωνικής Δικτύωσης

Με την κοινωνία μας να έχει εισέλθει καταλυτικά σε μία ψηφιακή εποχή, μεγάλο μέρος της καθημερινότητας των περισσότερων χρηστών του Διαδικτύου αποτελούν οι σελίδες κοινωνικής δικτύωσης. Τα μέσα αυτά έχουν πλάσει ένα νέο περιβάλλον στο Διαδίκτυο, όπου καθημερινά ανταλλάσσονται, αναδημοσιεύονται κι αποθηκεύονται τεράστιες ποσότητες πληροφοριών σε ατέλειωτες βάσεις δεδομένων. Δεύτερον, έχει γεννηθεί η ανάγκη για αλληλεπίδραση και προβολή σε έναν ολοένα εναλλασσόμενο κόσμο, όπου δισεκατομμύρια χρήστες δημοσιεύουν προσωπικά δεδομένα με σκοπό να δημιουργήσουν μία επιφανειακή σχέση ή να γίνουν αποδεκτοί από έναν όμοιο κύκλο χρηστών.

Σύμφωνα με την Ευρωπαϊκή Επιτροπή, «*ως δεδομένα προσωπικού χαρακτήρα ορίζονται οι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο*». Με άλλα λόγια ως προσωπικό δεδομένο θεωρείται κάθε πληροφορία από την οποία μπορεί να φανερωθεί η ταυτότητα του υποκειμένου. Μερικά υποδείγματα τέτοιων δεδομένων είναι τα παρακάτω:

- Ονοματεπώνυμο
- Διεύθυνση κατοικίας
- Ηλεκτρονική διεύθυνση (email)
- Αναγνωριστικός αριθμός κάρτας
- Πληροφορίες τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- Διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- Αναγνωριστικό cookie
- Δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

(Ευρωπαϊκή Επιτροπή – Προσωπικά Δεδομένα)

Ιδιαίτερης σημασίας, προσωπικά δεδομένα είναι κάθε πληροφορία στα μέσα κοινωνικής δικτύωσης όπως είναι για παράδειγμα, το προσωπικό ψηφιακό προφίλ στο Facebook, στο Twitter κ.ά., οι φωτογραφίες και τα βίντεο που ανεβάζουμε (π.χ. στο Instagram), τα μέρη όπου βρισκόμαστε, ακόμα και οι απόψεις μας που μοιραζόμαστε. Πολλά από αυτά τα δεδομένα θεωρούνται ευαίσθητα προσωπικά δεδομένα, με το νόμο να παρέχει διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και την τήρηση αρχείων που να τα περιέχουν. Τέτοια δεδομένα αφορούν τη φυλετική ή εθνική προέλευση, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, την υγεία, την κοινωνική πρόνοια, την ερωτική ζωή, δεδομένα σχετικά με ποινικές διώξεις ή καταδίκες.

Ο Schneier (2010) έχει αναπτύξει μία ταξινόμηση των προσωπικών δεδομένων χρησιμοποιώντας τα κοινωνικά δίκτυα και ξεχώρισε έξι τύπους:

- Δεδομένα εξυπηρέτησης (service data), τα οποία καταχωρούνται για τη δημιουργία ενός λογαριασμού.

- Δεδομένα γνωστοποίησης (disclosed data), τα οποία καταχωρούνται εθελοντικά από τον χρήστη.
- Εμπιστευτικά δεδομένα, όπως δημοσιεύσεις που γίνονται στις σελίδες άλλων ατόμων (π.χ. σχόλια).
- Συμπτωματικά ή τυχαία δεδομένα (incidental data), που αφορούν δεδομένα που δημοσιεύουν άλλα άτομα για κάποιον συγκεκριμένο χρήστη.
- Δεδομένα Συμπεριφοράς (behavioral data), τα οποία συλλέγει ο ιστότοπος όσον αφορά τη δραστηριότητα και τις συνήθειες των χρηστών του.
- Συναγόμενα δεδομένα (inferred data), είναι δεδομένα ενός χρήστη που προέρχονται από δεδομένα χρηστών που αλληλοεπιδρά.

4.1.1 Η περίπτωση του Facebook

Το Facebook αποτελεί ένα από τα πιο δημοφιλή μέσα κοινωνικής δικτύωσης με πάνω από δύο δισεκατομμύρια μηνιαίους ενεργούς χρήστες παγκοσμίως. Όπως δηλώνει στην επίσημη σελίδα των όρων χρήσης του, «το Facebook αναπτύσσει τεχνολογίες και υπηρεσίες που επιτρέπουν στους ανθρώπους να συνδέονται μεταξύ τους, να δημιουργούν κοινότητες και να αναπτύσσουν τις επιχειρήσεις τους.».

Εικόνα 4: Λογότυπο του κοινωνικού δικτύου Facebook.

Κατά την εγγραφή στο Facebook, ο χρήστης δημιουργεί ένα προφίλ καταχωρώντας το ονοματεπώνυμό του, διεύθυνση ηλεκτρονικού ταχυδρομείου ή αριθμό τηλεφώνου, ηλικία, φύλο και κωδικό πρόσβασης. Τελώντας τη διαδικασία αυτή ο χρήστης δύναται να συμφωνήσει με τους Όρους χρήσης, ότι έχει διαβάσει την Πολιτική Δεδομένων και την Πολιτική των cookies.

Οι όροι χρήσης αποτελούν τις υποχρεώσεις και τα δικαιώματα τόσο των χρηστών όσο και της εταιρείας κατά την αλληλεπίδρασή τους. Οι αρχές που διέπουν τους όρους αυτούς επιτρέπουν τον ελεύθερο διαμοιρασμό πληροφοριών, καθώς κάθε χρήστης θεωρείται ιδιοκτήτης των δεδομένων του και υπεύθυνος αυτών. Επιπλέον, ο καθένας έχει τον έλεγχο των πληροφοριών και τη δυνατότητα ρύθμισης του απορρήτου χωρίς αυτό να εγγυάται τον περιορισμό χρήσης των δεδομένων που έχουν λάβει άλλοι χρήστες.

Αναφέρεται κυρίως, η δωρεάν χρήση του Facebook και των υπόλοιπων υπηρεσιών της εταιρείας καθώς και ότι δε γίνεται πώληση και κοινοποίηση δεδομένων προσωπικού χαρακτήρα στους διαφημιζόμενους. Εφόσον όμως ο χρήστης συμφωνήσει με τους όρους, αυτομάτως παραχωρεί το δικαίωμα στην εταιρεία να μπορεί να συλλέγει και να χρησιμοποιεί προσωπικά του δεδομένα για να παρέχει τις υπηρεσίες της καθώς και να προβάλλει

διαφημίσεις πάνω στα ενδιαφέροντά του. Πιο συγκεκριμένα, τα δικαιώματα που παραχωρεί είναι τα εξής:

1. Άδεια χρήσης του περιεχομένου που δημιουργεί και κοινοποιεί ο χρήστης.
2. Άδεια χρήσης του ονόματος, της εικόνας προφίλ και πληροφοριών για τις δραστηριότητες αναφορικά με διαφημίσεις και χορηγούμενο περιεχόμενο.
3. Άδεια ενημέρωσης του λογισμικού που χρησιμοποιεί ή κατεβάζει ο χρήστης.

Βασική αρχή της πολιτικής απορρήτου που ακολουθεί η εταιρεία είναι ότι κάθε χρήστης έχει τον έλεγχο των προσωπικών του δεδομένων. Δηλαδή, είναι ο ίδιος υπεύθυνος για τις πληροφορίες που κοινοποιεί στο προφίλ του και του κοινού στο οποίο θα είναι ορατές.

Το Facebook, όπως αναφέραμε, λειτουργεί βασιζόμενο στη συλλογή και χρήση των δεδομένων προσωπικού χαρακτήρα των χρηστών, έτσι ώστε να εξατομικεύει τις διαφημίσεις που θα προβάλει και να παρέχει γενικά τις υπηρεσίες του. Κατά την εγγραφή, η εταιρεία Facebook Inc. συλλέγει και αποθηκεύει σε μία βάση δεδομένων τα στοιχεία που καταχωρούνται, τον φυλλομετρητή (browser) και την διεύθυνση πρωτοκόλλου διαδικτύου (IP address) των χρηστών. Αναφέρει, επίσης, ότι συλλέγει το περιεχόμενο που παρέχεται κατά τη δημιουργία λογαριασμού, που δημιουργείται ή κοινοποιείται κατά τη χρήση του μέσου, προκειμένου να παρέχει εξατομικευμένες λειτουργίες και περιεχόμενο. Σύμφωνα με το κοινωνικό δίκτυο, οι πληροφορίες που συλλέγονται δεν μοιράζονται στους διαφημιστές χωρίς την άδεια των χρηστών-μελών. Παρακάτω αναφέρονται οι κατηγορίες και οι πηγές από τις οποίες γίνεται η συλλογή και η χρήση των δεδομένων για την εμφάνιση διαφημίσεων σύμφωνα με το Facebook.[2]

- Δραστηριότητα του χρήστη στις εταιρείες και τα προϊόντα του Facebook
    - Σελίδες που αρέσουν στον χρήστη και τους φίλους του
    - Πληροφορίες από προφίλ στο Facebook και στο Instagram
    - Τοποθεσίες κοινοποίησης της παρουσίας μέσω Facebook

- Δραστηριότητα χρήστη σε άλλες επιχειρήσεις
  Κοινοποίηση πληροφοριών, όπως αριθμό τηλεφώνου ή διεύθυνση email, σε επιχειρήσεις και αντιστοίχιση αυτών με το προφίλ στο Facebook μέσω:
    - Εγγραφή για λήψη ενημερωτικού δελτίου μέσω email
    - Αγορές σε καταστήματα λιανικής
    - Εγγραφή για κουπόνι ή έκπτωση

- Δραστηριότητα χρήστη σε άλλους ιστότοπους και εφαρμογές
  Αποστολή δεδομένων στο Facebook από ιστότοπους που χρησιμοποιούν τα εργαλεία για επιχειρήσεις του Facebook. Παραδείγματα:
    - Προβολή κάποιας ιστοσελίδας
    - Λήψη εφαρμογής για κινητά
    - Προσθήκη προϊόντων στο καλάθι αγορών ή πραγματοποίηση αγοράς

- Τοποθεσία χρήστη
    - Από πού συνδέεται στο Internet
    - Πού χρησιμοποιεί το κινητό του

[2] https://www.facebook.com/about/ads

- Την τοποθεσία από τα προφίλ του στο Facebook και στο Instagram

Όσον αφορά τη διατήρηση δεδομένων κατά την διαγραφή δημοσιεύσεων ή του λογαριασμού, η πολιτική δεδομένων του Facebook αναφέρει ότι τα δεδομένα αποθηκεύονται όσο θεωρούνται απαραίτητα για την παροχή των υπηρεσιών του ή έως ότου γίνει διαγραφή του λογαριασμού του μέλους. Το ερώτημα που γεννάται σε αρκετούς αφορά το τι γίνεται με τις δημοσιεύσεις, τις εικόνες, κ.ά. που διαγράφουν από το Facebook. Η απάντηση που δίνει το κοινωνικό δίκτυο είναι ότι ορισμένα διαγράφονται από τους διακομιστές, αλλά κάποια εφόσον μόνο καταργηθεί οριστικά ο λογαριασμός. Για την διαγραφή του λογαριασμού χρειάζονται να περάσουν 30 μέρες έτσι ώστε να διαγραφεί οριστικά και να μην μπορούν να ανακτηθούν οι πληροφορίες. Με την ενέργεια αυτή γίνεται διαγραφή όλων των δημοσιεύσεων του χρήστη χωρίς τη δυνατότητα ανάκτησής τους αργότερα. Παρ΄ όλα αυτά, κοινοποιήσεις από τρίτα άτομα που αφορούν τον χρήστη, καθώς και μηνύματα που έχουν σταλθεί σε φίλους μπορεί να παραμένουν ορατά και μετά την διαγραφή του λογαριασμού.

Προκειμένου η εταιρεία να βελτιώσει, να διευκολύνει και να υποστηρίξει τις υπηρεσίες της προβαίνει στην κοινοποίηση πληροφοριών και στις άλλες εταιρείες του ομίλου της (Facebook Payments Inc., Onavo, Facebook Technologies, WhatsApp Inc., CrowdTangle κ.ά.).[3] Περαιτέρω, έπειτα από επιβολή αυστηρών περιορισμών στη χρήση των προσωπικών δεδομένων, η εταιρεία κοινοποιεί πληροφορίες σε τρίτους συνεργάτες. Αυτοί μπορεί να είναι συνεργάτες που χρησιμοποιούν τις υπηρεσίες αναλύσεων, διαφημιζόμενοι, συνεργάτες που προσφέρουν αγαθά και υπηρεσίες στα προϊόντα της Facebook, προμηθευτές και πάροχοι υπηρεσιών κ.ά.. Οι πληροφορίες που λαμβάνουν οι τρίτοι αφορούν συγκεντρωτικά στατιστικά στοιχεία, δημογραφικά στοιχεία και κατηγορίες ανθρώπων που βλέπουν τις διαφημίσεις (όχι πληροφορίες που ταυτοποιούν τον χρήστη), δημόσιες πληροφορίες καθώς και πληροφορίες συναλλαγών κατά την αγορά από πωλητές μέσω των προϊόντων του Facebook (π.χ. στοιχεία επικοινωνίας και λεπτομέρειες αποστολής).[4]

Το Facebook παρέχει διάφορους τρόπους ρυθμίσεων αναφορικά με την προστασία του λογαριασμού και των προσωπικών δεδομένων του χρήστη. Οι ρυθμίσεις αυτές αφορούν, είτε ενέργειες που μπορεί να κάνει ο χρήστης από μεριάς του ώστε να έχει τον έλεγχο των προσωπικών του δεδομένων, είτε βήματα που προτείνει το κοινωνικό δίκτυο να ακολουθήσει ο χρήστης ούτως ώστε να διατηρήσει τον λογαριασμό του ασφαλή. Κατά την πρόσβαση στις ρυθμίσεις και τα εργαλεία απορρήτου, ο χρήστης έχει τη δυνατότητα να ενημερωθεί και να προσαρμόσει τις ρυθμίσεις με όποιον τρόπο πιστεύει ότι είναι ασφαλής. Στις συντομεύσεις απορρήτου μπορεί κανείς να κάνει έλεγχο του απορρήτου και τις κατάλληλες επιλογές πάνω σε θέματα:

- <u>Ποιοι μπορούν να δουν τις κοινοποιήσεις</u>
  Τα μέλη του Facebook έχουν τη δυνατότητα να επιλέξουν σε ποιους επιθυμούν να είναι ορατό το προφίλ τους καθώς και οι προσωπικές τους κοινοποιήσεις. Αρχικά, πρόσβαση μπορεί να έχει οποιοσδήποτε εντός ή εκτός Facebook, δηλαδή οι δημοσιεύσεις να είναι ορατές τόσο σε γνωστά άτομα όσο και σε εντελώς άγνωστα. Επιπλέον, ο χρήστης έχει ως δεύτερη επιλογή η πρόσβαση να γίνεται μόνο από φίλους του και ως τρίτη επιλογή να έχει μόνο ο ίδιος. Τέλος, παρέχεται η επιλογή της προσαρμογής του κοινού πρόσβασης με τη δυνατότητα εξαίρεσης φίλων και λιστών.

- <u>Διατήρηση του λογαριασμού ασφαλή</u>

[3] https://www.facebook.com/help/111814505650678?ref=dp
[4] https://www.facebook.com/about/privacy/update

Το κοινωνικό δίκτυο προτείνει συμβουλές για την ασφαλή χρήση κωδικού πρόσβασης και για θέματα ασφάλειας του λογαριασμού. Πιο συγκεκριμένα, συνιστά ο κωδικός να είναι ισχυρός ώστε να είναι δυσεύρετος από τρίτους, να μην κοινοποιείται, καθώς και να μην χρησιμοποιείται από τον χρήστη πουθενά στο υπόλοιπο διαδίκτυο. Επιπλέον, στις ρυθμίσεις μπορεί κάποιος να επιλέξει "Ενεργοποιήστε τις ειδοποιήσεις για μη αναγνωρισμένες συνδέσεις" έτσι ώστε να ειδοποιείται όταν παρατηρείται σύνδεση στο λογαριασμό του από μη αναγνωρισμένη συσκευή. Σε αυτό το σημείο, το Facebook παρέχει την πρόσθεση ενός επιπλέον επιπέδου ασφάλειας όπως αναφέρει. Ο χρήστης μπορεί να ενεργοποιήσει τον έλεγχο ταυτότητας δύο παραγόντων, είτε μέσω SMS είτε μέσω εφαρμογής. Κατά την επιλογή αυτής της ρύθμισης, ο χρήστης θα πρέπει να πληκτρολογεί έναν ειδικό κωδικό ασφαλείας κάθε φορά που θα συνδέεται στο Facebook από νέο υπολογιστή, κινητό ή tablet.

- <u>Πώς μπορούν οι άλλοι να σας βρίσκουν στο Facebook</u>
  Οι ρυθμίσεις αυτές προσφέρουν τον έλεγχο τον ατόμων που μπορούν να στέλνουν αιτήματα φιλίας στον χρήστη, οι οποίοι μπορούν να είναι είτε όλοι οι χρήστες του κοινωνικού δικτύου, είτε μόνο φίλοι των φίλων του. Επιπρόσθετα, η δυνατότητα αναζήτησης ενός μέλους του Facebook μέσω του κινητού αριθμού ή της διεύθυνσης email του, μπορεί να επιτραπεί σε όλους, σε φίλους, σε φίλους των φίλων ή μόνο στον ίδιο. Τέλος, ο χρήστης έχει το δικαίωμα να επιτρέψει ή όχι τις μηχανές αναζήτησης εκτός του Facebook να οδηγούν στο προσωπικό του προφίλ.

- <u>Ρυθμίσεις των δεδομένων στο Facebook</u>
  Στο σημείο αυτό μπορεί κανείς να διαχειριστεί και να αφαιρέσει τις εφαρμογές και τους ιστότοπους στα οποία έχει συνδεθεί μέσω του λογαριασμού του στο Facebook. Η επόμενη ρύθμιση αφορά την αναγνώριση προσώπου κατά την οποία δημιουργείται ένα πρότυπο του χρήστη έτσι ώστε να αναγνωρίζεται σε εικόνες ή βίντεο που έχει προστεθεί ή όχι με ετικέτα.

- <u>Διαφημιστικές προτιμήσεις</u>
  Λόγω του ότι το συγκεκριμένο κοινωνικό μέσο χρησιμοποιεί προσωπικά δεδομένα προκειμένου να εξατομικεύσει τις διαφημίσεις, προτείνει ορισμένες επιλογές για να επιτρέψει ο χρήστης ή όχι την ενέργεια αυτή. Αναλυτικότερα μπορεί να αποφασίσει κανείς ποιες πληροφορίες του προφίλ του μπορούν να χρησιμοποιούν οι διαφημιζόμενοι. Τέλος, δίνεται η επιλογή να καθοριστεί ποιοι μπορούν να δουν τις κοινωνικές αλληλεπιδράσεις του χρήστη όπως τα σχόλια, οι κοινοποιήσεις, οι εκδηλώσεις που παίρνει μέρος κ.ά., σε συνδυασμό με διαφημίσεις.

4.1.2 Η περίπτωση του Twitter

Εικόνα 5: Λογότυπο του κοινωνικού δικτύου Twitter.

Το Twitter αποτελεί υπηρεσία κοινωνικής δικτύωσης και μικρό-ιστολογιών (microblogging) που προσφέρει στους χρήστες του να αλληλεπιδρούν μέσω μηνυμάτων που είναι γνωστά ως "Tweets". Αρχικά, τα Tweets ήταν περιορισμένα στους 140 χαρακτήρες αλλά μετά το Νοέμβριο του 2017 αυξήθηκαν στους 280 εκτός των CJK[5] γλωσσών. Μετά το 2013, λόγω της ιδιαίτερης διάδοσης του τρόπου λειτουργίας του, το κοινωνικό δίκτυο πήρε από πολλούς τον τίτλο "Το SMS του Διαδικτύου". Σήμερα, βρίσκεται ανάμεσα στις τρεις κορυφαίες εφαρμογές κοινωνικής δικτύωσης με περισσότερους από 350 εκατομμύρια μηνιαίους ενεργούς χρήστες.

Οι κύριες προτεραιότητες, σύμφωνα με την εταιρεία Twitter Inc., είναι η παροχή ενός ασφαλούς μέρους για ελεύθερη έκφραση και εύρεση αξιόπιστων πληροφοριών, η δέσμευση με την προστασία των πληροφοριών αυτών και η ακεραιότητα των χρηστών ενάντια σε δραστηριότητες που παραβιάζουν τα προσωπικά δικαιώματα και του Όρους Χρήσης των υπηρεσιών.

Όπως όλα τα μέσα κοινωνικής δικτύωσης, έτσι και το Twitter κάνει συλλογή των προσωπικών στοιχείων τόσο των εγγεγραμμένων χρηστών όσο και των μη εγγεγραμμένων. Με τη χρήση οποιασδήποτε υπηρεσίας, ο χρήστης δίνει τη συγκατάθεσή του με περιορισμένα δικαιώματα και σε παγκόσμιο επίπεδο, για χρήση, αντιγραφή, αναπαραγωγή, προσαρμογή, επεξεργασία, δημοσίευση, μετάδοση, εμφάνιση και διανομή του περιεχομένου που παρέχει.[6] Με την άδεια αυτή εξουσιοδοτείται το Twitter για μεταφορά, αποθήκευση και διάθεση των πληροφοριών στις Ηνωμένες Πολιτείες, την Ιρλανδία και σε οποιαδήποτε χώρα εκτείνεται η εταιρεία.[7] Κατά την εγγραφή, απαιτείται ένα εμφανιζόμενο όνομα και ένα όνομα χρήστη τα οποία είναι πάντα δημόσια, ένας κωδικός πρόσβασης και μία διεύθυνση email ή αριθμός τηλεφώνου. Εάν ο χρήστης θέλει να δραστηριοποιηθεί δημόσια, τότε σύμφωνα με την Πολιτική Απορρήτου παρέχει δημόσια:

- το προφίλ, τη ζώνη ώρας και γλώσσας,
- τα Tweets, μαζί με ημερομηνία, ώρα και έκδοση εφαρμογής όπου έγινε η δημοσίευση,
- τις λίστες, τα άτομα που ακολουθεί και τον ακολουθούν,
- τα Tweets που του αρέσουν ή τα Retweet

[5] Οι χαρακτήρες CJK είναι ένας συλλογικός όρος για τις κινεζικές, ιαπωνικές και κορεατικές γλώσσες.

[6] https://twitter.com/en/tos#intlTerms

[7] https://twitter.com/en/privacy#chapt

Καθώς το Twitter δημιουργήθηκε για να προβάλλει το περιεχόμενό του όλο και πιο γρήγορα και ευρύτερα, χρησιμοποιεί τεχνολογία όπως διεπαφή προγραμματισμού εφαρμογών (API), η οποία παρέχει σε εταιρείες, προγραμματιστές και χρήστες πρόσβαση μέσω προγραμματισμού σε δημόσια μόνο δεδομένα του όπως τα παραπάνω.[8] Επιπλέον, κάνει χρήση των cookies[9] προκειμένου να γίνει έλεγχος ταυτότητας και ασφάλειας, παρακολούθηση του τρόπου χρήσης και αλληλεπίδρασης με τις υπηρεσίες της εταιρείας, ανάλυση και έρευνα, παροχή εξατομικευμένων υπηρεσιών αναφορικά με το περιεχόμενο και τις διαφημίσεις.

Η εταιρεία, συνεργάζεται επίσης με διαφημιστές και άλλες εταιρείες για την προβολή διαφημίσεων εντός και εκτός του Twitter. Πιο συγκεκριμένα, για να επιτύχει αυτό, χρησιμοποιεί δεδομένα όπως πληροφορίες τοποθεσίας, cookies, links (υπερσυνδέσμους) και 'δεδομένα καταγραφής[10], καθώς και πληροφορίες που παρέχουν οι συνεργάτες διαφημίσεων όπως αναγνωριστικά κινητής συσκευής, κατακερματισμένα email, δημογραφικά ή δεδομένα ενδιαφέροντος.[11] Στις πρόσθετες πληροφορίες σχετικά με την επεξεργασία δεδομένων σημειώνεται ότι κοινοποιούνται μη δημόσια προσωπικά στοιχεία σε διαφημιζόμενους που δε διενεργούν ως επεξεργαστές δεδομένων προκειμένου να τους επιτρέψουν να μετρήσουν την αποτελεσματικότητα των διαφημίσεών τους. Για χώρες της Ευρωπαϊκής Ένωσης, της ΕΖΕΣ (Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών) ή το Ηνωμένο Βασίλειο, επιβάλλεται ενεργοποίηση της ρύθμισης «Να επιτρέπεται η πρόσθετη κοινή χρήση πληροφοριών με συνεργάτες» έτσι ώστε να γίνει η παραπάνω ενέργεια.

Κατά τη διαγραφή των Tweets, πρέπει κάποιος να έχει υπόψη ότι το Twitter δεν μπορεί να καταργήσει τα Retweet που έχουν γίνει από άλλους χρήστες καθώς και τα Tweet που περιέχουν μέρος ή όλο το κείμενο της δημοσίευσης. Αξίζει να σημειωθεί, ότι τα Tweets ενδέχεται να αποθηκευτούν σε εφαρμογές τρίτων ή μηχανές αναζήτησης. Εφόσον το Google και άλλες μηχανές αναζήτησης δεν ενημερώσουν τα συστήματά τους, τότε υπάρχει το ενδεχόμενο παλιές πληροφορίες να εξακολουθούν να αναζητούνται. Εάν κάποιος επιθυμεί να διαγράψει τον λογαριασμό του, σύμφωνα με την πολιτική απορρήτου του κοινωνικού δικτύου, αυτό θα γίνει 30 μέρες μετά από την αίτηση απενεργοποίησης και εφόσον δεν έχει συνδεθεί εντός αυτού του διαστήματος. Δεδομένα όπως εμφανιζόμενο όνομα, όνομα χρήστη και προσωπικό προφίλ παύουν να εμφανίζονται στις υπηρεσίες και εφαρμογές της εταιρείας. Από την άλλη όμως, υπάρχει η περίπτωση διατήρησης κάποιων πληροφοριών για χρήση σε θέματα ασφάλειας της πλατφόρμας και των χρηστών. Τέλος, δεν αποκλείεται η διατήρηση αντίγραφων των δημόσιων πληροφοριών του χρήστη από τρίτα μέρη και τις μηχανές αναζήτησης.

Ο χρήστης είναι σε μεγάλο βαθμό υπεύθυνος για τον έλεγχο των πληροφοριών που μοιράζεται. Για τον λόγο αυτό, το Twitter διαθέτει μία πληθώρα ρυθμίσεων έτσι ώστε ο χρήστης

[8] https://help.twitter.com/en/rules-and-policies/twitter-api

[9] Τα cookie είναι μικρά αρχεία που τοποθετούν οι ιστότοποι στον υπολογιστή καθώς περιηγείται κάποιος στον Ιστό.

[10] Ως Δεδομένα καταγραφής, σύμφωνα με το Twitter, αναφέρονται οι πληροφορίες που συλλέγονται όταν κάποιος βλέπει περιεχόμενο ή αλληλεπιδρά με άλλο τρόπο με τις υπηρεσίες της εταιρείας ακόμα και αν δεν έχει δημιουργήσει λογαριασμό. Τέτοια δεδομένα περιλαμβάνουν πληροφορίες όπως διεύθυνση IP, τύπος προγράμματος περιήγησης, λειτουργικό σύστημα, σελίδες που επισκέφτηκαν, τοποθεσία, πληροφορίες συσκευής και cookies.

[11] https://twitter.com/en/privacy#chapter2

να προφυλάξει τον λογαριασμό και τα προσωπικά του δεδομένα. Στις ρυθμίσεις απορρήτου και ασφάλειας μπορεί κάποιος να ορίσει:

- Εάν τα Tweet θα είναι δημόσια ή όχι
- Αν επιτρέπεται στους άλλους να τον επισημαίνουν σε φωτογραφίες
- Να λαμβάνει άμεσα μηνύματα από οποιονδήποτε ή μόνο από τους ακόλουθούς του
- Να μπορεί να αναζητηθεί μέσω του προσωπικού του email ή αριθμό τηλεφώνου του
- Πότε και πού ενδέχεται να δει ευαίσθητο περιεχόμενο στο Twitter
- Εάν θέλει να αποκλείσει ή απενεργοποιήσει άλλους λογαριασμούς Twitter

Το κοινωνικό δίκτυο διαθέτει στο κοινό του επιπλέον ρυθμίσεις αναφορικά με τις πρόσθετες πληροφορίες που λαμβάνονται, δίνοντας πρόσβαση και έλεγχο των δεδομένων που συλλέγονται. Όσον αφορά τις διαφημίσεις, τα μέλη έχουν το δικαίωμα να αποκλείσουν ή να κάνουν σίγαση διαφημιζόμενους και να αναφέρουν κακές ή προσβλητικές διαφημίσεις. Δίνεται, επίσης, η δυνατότητα πρόσβασης στα δεδομένα που συλλέχθηκαν για την προβολή της διαφήμισης και τροποποίησης των δεδομένων αυτών για να επηρεαστούν οι μελλοντικές διαφημίσεις. Σε αυτό το σημείο, μπορεί να οριστεί εάν θα εμφανίζονται διαφημίσεις βάσει ενδιαφέροντος εντός και εκτός του Twitter. Πρόσθετα, τα άτομα μπορούν να επιλέξουν την ενεργοποίηση της ακριβούς τοποθεσίας (προσθήκη τοποθεσίας στα Tweets), η οποία από προεπιλογή είναι απενεργοποιημένη. Επιτρέπεται η ενεργοποίηση και απενεργοποίηση της ρύθμισης ανά πάσα στιγμή, η διαγραφή προηγούμενων δεδομένων τοποθεσίας καθώς και η επιλογή εξατομίκευσης της εμπειρίας με βάση την τοποθεσία. Η υπηρεσία διαθέτει επίσης έκδοση των παραπάνω εργαλείων για όσους δεν έχουν λογαριασμό Twitter ή έχουν αποσυνδεθεί από τον λογαριασμό τους. Εκτός από τις ρυθμίσεις, τα μέλη του κοινωνικού αυτού μέσου έχουν το δικαίωμα για πρόσβαση, διόρθωση, διαγραφή ή τροποποίηση των προσωπικών τους δεδομένων που παραχώρησαν και συσχετίστηκαν με τον λογαριασμό τους. Επιτρέπεται η πρόσβαση σε πρόσθετες πληροφορίες που καταχωρήθηκαν καθώς και η υποβολή αιτήματος για τροποποίηση ή διαγραφή των πληροφοριών αυτών.

4.2 Περιπτώσεις παραβίασης των προσωπικών δεδομένων

Αρχικά ως παραβίαση προσωπικών δεδομένων ορίζεται «*η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, χωρίς άδεια γνωστοποίηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που αποτέλεσαν αντικείμενο επεξεργασίας*» (Γαμπά, 2018).

Η υποκλοπή στοιχείων ταυτότητας είναι η κατάχρηση προσωπικών δεδομένων και η κατακρεούργηση της προσωπικής διαδικτυακής ελευθερίας του ατόμου με σκοπό την υποβάθμιση και εκμετάλλευση κάποιου προσώπου χωρίς τη συγκατάθεσή του. Εκτός από τις βασικές πληροφορίες όπως το όνομα και τη διεύθυνση, ο υποκλοπέας τρίτων στοιχείων αναζητά αριθμούς πιστωτικών καρτών ή και αριθμούς τραπεζικών λογαριασμών, πιστοποιητικά γέννησης ή διαβατήρια. Συνεπώς, είναι απαραίτητο να δίνετε προσοχή ότι η προστασία των δεδομένων δεν σχετίζεται μόνο με την αποτροπή διαρροής, αλλά και την αποτροπή της αλλοίωσής τους και την αποτροπή απώλειας τους (Θεοδώρου, 2017).

Υπάρχουν διάφοροι κίνδυνοι σχετικά με την ανάρτηση στοιχείων προσωπικών πληροφοριών στα κοινωνικά δίκτυα. Αυτές οι απειλές μπορεί να προκληθούν από hackers ή spammers που λαμβάνουν τα προσωπικά στοιχεία των χρηστών και η πρόσβαση σε ευαίσθητες πληροφορίες από αυτά τα άτομα μπορεί επίσης να οδηγήσει σε κινδύνους τρομοκρατίας, οικονομικούς κινδύνους και σωματική ή σεξουαλική εκβίαση (Aldhafferi et. al., 2013).

Σήμερα με την εξέλιξη της τεχνολογίας, ο υποκλοπέας είναι έμπειρος στο να εξαπατήσει τους χρήστες των κοινωνικών μέσων, να παίρνει ευαίσθητες πληροφορίες, να κλέβει προσωπικά δεδομένα και να αποκτά πρόσβαση. Γενικά, οι πλατφόρμες κοινωνικών μέσων, οι οποίες συλλέγουν και αποθηκεύουν τεράστιες ποσότητες προσωπικών πληροφοριών με περιορισμένη κυβερνητική επίβλεψη, χρησιμεύουν ως ελκυστικοί στόχοι για τους κακούς φορείς που επιδιώκουν να χρησιμοποιήσουν τα δεδομένα αυτά για να διαπράξουν απάτη και κλοπή.

Ας μην πάμε μακριά καθώς οι κοινές επιθέσεις παραβίασης της ιδιωτικής ζωής στα διαδικτυακά κοινωνικά δίκτυα βρίσκονται σε πιο απλά μέρη. Αρχικά, οι χρήστες συνήθως ανεβάζουν τα προσωπικά τους στοιχεία όταν εμπιστεύονται τον πάροχο υπηρεσιών, αλλά αγνοούν το γεγονός ότι ο πάροχος μπορεί να χρησιμοποιήσει αυτές τις λεπτομέρειες για επιχειρηματικούς σκοπούς, όπως η διαφήμιση. Μία δεύτερη παραβίαση που αξίζει να σημειωθεί αφορά παραβιάσεις που μπορούν να προκληθούν από τους φίλους του χρήστη. Οι φίλοι αυτοί, έχουν την δυνατότητα να μοιραστούν προσωπικά στοιχεία του χρήστη, να αντιγράψουν και να δημοσιεύσουν πληροφορίες με άλλους χρήστες.

Επομένως, ευαίσθητες πληροφορίες όπως η διεύθυνση κατοικίας και η ημερομηνία γέννησης δεν πρέπει να δημοσιεύονται στο Διαδίκτυο, προκειμένου να αποφεύγονται κίνδυνοι για το διαδικτυακό απόρρητο. Η αύξηση της ευαισθητοποίησης των χρηστών σχετικά με αυτούς τους κινδύνους, η παροχή ενός συστήματος διαχείρισης απορρήτου για τους χρήστες να ελέγχουν τα προσωπικά τους στοιχεία και η συνεχής ενημέρωση των πολιτικών απορρήτου μπορεί να οδηγήσει σε μείωση αυτών των κινδύνων (Aldhafferi et. al., 2013).

4.2.1 Κλασικές απειλές

Από τη στιγμή που το Διαδίκτυο αποκτά ευρεία χρήση και οι ιστότοποι κοινωνικής δικτύωσης εμφανίζουν ταχεία ανάπτυξη, προκύπτουν επίσης διάφορα είδη απειλών με τις πιο κλασικές να καθιστούν τους χρήστες ενός δεδομένου δικτύου ευάλωτους σε επιθέσεις. Οι κλασικές ή αλλιώς παραδοσιακές απειλές είναι μοναδικές για το περιβάλλον SNS (Social Network Sites) και περιλαμβάνουν διάφορες παραδοσιακές τεχνικές επίθεσης, όπως ηλεκτρονικό ψάρεμα, κακόβουλο λογισμικό, για να αποκτήσουν τα προσωπικά στοιχεία ενός χρήστη (Rathore, 2017). Αν και αυτές οι απειλές έχουν αντιμετωπιστεί στο παρελθόν, έχουν γίνει όλο και πιο ιογενείς λόγω της δομής και της φύσης των ιστοσελίδων κοινωνικής δικτύωσης και μπορούν να εξαπλωθούν γρήγορα μεταξύ των χρηστών του δικτύου. Μπορούν να επωφεληθούν από τα προσωπικά στοιχεία ενός χρήστη που δημοσιεύονται για να επιτεθούν όχι μόνο σε αυτόν αλλά και στους φίλους του και στοχεύουν καθημερινούς πόρους χρηστών όπως κωδικό πρόσβασης λογαριασμού, αριθμό πιστωτικών καρτών ή στοιχεία τραπεζικού λογαριασμού καθώς και αριθμό κοινωνικής ασφάλισης. Αυτές οι πληροφορίες είναι πολύ ευεργετικές για έναν εισβολέα καθώς μόλις τις λάβει θα μπορεί να διαπράξει άλλα εγκλήματα και σοβαρές επιθέσεις, όπως το ηλεκτρονικό ψάρεμα και η κλοπή ταυτότητας (Rathore, 2017).

Malware – Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό έχει σχεδιαστεί για να αποκτά πρόσβαση στους υπολογιστές και στα δεδομένα που περιέχουν. Μόλις το κακόβουλο λογισμικό έχει διεισδύσει στον υπολογιστή ενός χρήστη, μπορεί να χρησιμοποιηθεί για να κλέψει ευαίσθητες πληροφορίες, να εξαπολύσει χρήματα ή να επωφεληθεί από την αναγκαστική διαφήμιση. Μόλις ο λογαριασμός έχει διακυβευτεί (συχνά αποκτώντας κωδικούς πρόσβασης μέσω μιας επίθεσης ηλεκτρονικού "ψαρέματος"), οι κυβερνο-εγκληματίες μπορούν να αναλάβουν αυτόν τον λογαριασμό για τη διανομή κακόβουλου λογισμικού σε όλους τους φίλους ή τις επαφές του χρήστη. Το malware περιέχει οποιοδήποτε είδος κακόβουλου λογισμικού, με μερικές από τις πιο οικείες μορφές όπως:

- Trojan Horses ή αλλιώς backdoor (δούρειος ίππος): Κακόβουλο λογισμικό το οποίο έχει ως βασικό στοιχείο την εξαπάτηση, αφού σχεδόν πάντα μετατρέπεται σε μια αξιοποιήσιμη εφαρμογή, παρ' όλο που την ίδια στιγμή ενδόμυχα εγκαθιστά στον υπολογιστή άλλα κακόβουλα προγράμματα. Κατά κανόνα, ένας δούρειος ίππος φτιάχνει πίσω πόρτα (backdoor) στο σύστημα, όπου εκεί ο εισβολέας θα μπορέσει να διαχειριστεί από απόσταση το σύστημα, όποτε εκείνος θελήσει να συνδεθεί.
- Ransomware (εξαπόλυση χρημάτων): Κακόβουλο λογισμικό που διαφθείρει το σύστημα, κρυπτογραφεί τα δεδομένα καταλήγοντας να ζητάει χρήματα από το θύμα ώστε να ξεκλειδώσει τα προσωπικά του αρχεία. Αυτό το χρηματικό ποσό θα πρέπει να έχει καταχωρηθεί εντός του χρονικού διαστήματος που έχει ζητήσει ο επιτιθέμενος, διαφορετικά τα αρχεία του υπολογιστή παραμένουν άχρηστα. Παρόμοιο κακόβουλο λογισμικό σαν και αυτό είναι και το Scareware με το οποίο ο επιτιθέμενος επίσης απειλή και παραπλανά τα θύματα του έχοντας ως στόχο να αρπάξει χρήματα.
- Virus (ιούς): Κακόβουλο λογισμικό το οποίο όταν εγκατασταθεί σε έναν υπολογιστή έχει την δυνατότητα να πολλαπλασιάζεται και να μολύνει πολλά προγράμματα σε αυτόν τον υπολογιστή. Η καταστροφή που μπορεί να επιφέρει ένας ιός μπορεί να είναι από μια απλή εμφάνιση στην οθόνη, μέχρι και να κυριεύσει τη μνήμη που αξιοποιείται από τα σωστά προγράμματα και χωρίς να το έχει καταλάβει ο χρήστης, φτάνει σε απώλεια δεδομένων και σε κατεύρεση το υπολογιστικό σύστημα. Πιο γνώριμο, είναι ότι ο σκοπός του ιού είναι να παρενοχλήσει τον χρήστη ή να του καταστρέψει τα δεδομένα, αλλά μεγάλο ποσοστό ιών έχουν ως σκοπό να κλέβουν τα δεδομένα ή ακόμα και να εισάγουν τον υπολογιστή που έχουν βάλει στόχο σε κάποιο παράνομο δίκτυο. Στην ιστορία του Διαδικτύου καταγράφηκε για πρώτη φορά εμφάνιση ιού στο ARPANET στις αρχές της δεκαετίας το 70'.
- Worms (σκουλήκι): Κακόβουλο λογισμικό το οποίο πολλαπλασιάζεται φτιάχνοντας αντίτυπα του εαυτού από τον έναν υπολογιστή στον άλλον. Αυτό το λογισμικό έχει την ικανότητα να προσβάλει το δίκτυο έχοντας ως αποτέλεσμα να ελαττώσει πάρα πολύ την ταχύτητα της σύνδεσης στο Διαδίκτυο δαπανώντας όλους τους πόρους του υπολογιστή και να προκαλέσει ακόμα και τερματισμό του υπολογιστή.
- Rootkit Malware: Κακόβουλο λογισμικό το οποίο είναι "αόρατο" και έτσι παρακάμπτει τους μηχανισμούς πρόληψης και ανίχνευσης. Λόγω αυτού, είναι δύσκολο έως και αδύνατο να ανιχνευτεί αυτό το λογισμικό. Στόχος αυτού του λογισμικού είναι να παρέχει τα δικαιώματα του προνομιούχου λογαριασμού (Root) στον κακόβουλο χρήστη, έχοντας τον πλήρη έλεγχο στον υπολογιστή.

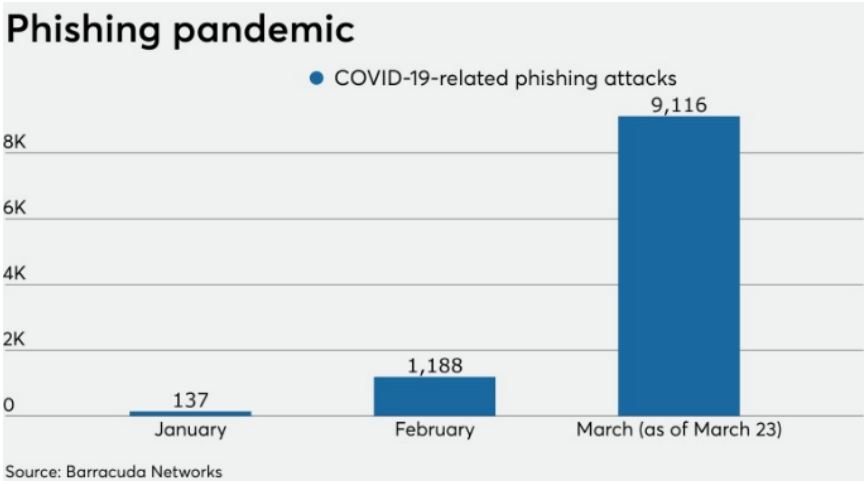
Το κοινό χαρακτηριστικό που κατέχουν τα παραπάνω λογισμικά είναι ο κακεντρεχής σκοπός των κατασκευαστών τους. Οι πλατφόρμες κοινωνικών μέσων είναι ένα ιδανικό σύστημα παράδοσης για διανομείς κακόβουλων προγραμμάτων. Παράδειγμα τέτοιου κακόβουλου λογισμικού αποτελεί το Koobface, το οποίο ήταν το πρώτο που διαδόθηκε με επιτυχία μέσω κοινωνικών δικτύων όπως το Facebook και το Twitter. Σκοπός του, είναι η συλλογή δεδομένων σύνδεσης και η συμμετοχή του στον υπολογιστή-στόχο για να υπάρξει μέρος ενός botnet, δηλαδή μέρος ενός "στρατού ζόμπι" υπολογιστών που πράττουν εγκληματικές δραστηριότητες στο Διαδίκτυο. Ένα άλλο παράδειγμα είναι το Twitter Worm που κάνει επίθεση στον κοινωνικό ιστότοπο Twitter. Τέτοιο σκουλήκι αποτελεί το Profile Spy Worm, με το οποίο ο εισβολέας κάνει tweet στο οποίο παραθέτει έναν σύνδεσμο για τη λήψη της εφαρμογής τρίτου μέρους Profile Spy. Κατά τη λήψη, η εφαρμογή ζητάει μία φόρμα για συλλογή προσωπικών δεδομένων από τον χρήστη, με αποτέλεσμα η συνεχής αποστολή κακόβουλων μηνυμάτων στους ακόλουθους του χρήστη στο Twitter (Obiniyi et al., 2014).

Phishing Attacks – Επιθέσεις ηλεκτρονικού "ψαρέματος"

Το ηλεκτρονικό "ψάρεμα" είναι ο πιο γνωστός τύπος απειλής των κοινωνικών μέσων, με τον οποίο οι εγκληματίες προσπαθούν να αποκτήσουν πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες. Μία επίθεση ηλεκτρονικού "ψαρέματος" παρουσιάζεται ως κακόβουλος σύνδεσμος ή αρχείο συνημμένου από έναν νόμιμο οργανισμό με τη μορφή μηνύματος ηλεκτρονικού ταχυδρομείου (email), μηνύματος ή τηλεφωνικής κλήσης. Αυτά τα μηνύματα εξαπατούν τους ανθρώπους να μοιράζονται ευαίσθητα δεδομένα, συμπεριλαμβανομένων των κωδικών πρόσβασης, των τραπεζικών πληροφοριών ή των στοιχείων της πιστωτικής κάρτας. Στο παρελθόν τα λανθασμένα Domain Names (όνομα χώρου Ίντερνετ) χρησιμοποιούνταν τακτικά για αυτόν τον σκοπό. Την σήμερον ημέρα, οι εγκληματίες χρησιμοποιούν πιο σύγχρονες μεθόδους όπως την κοινωνική μηχανική [12](social engineering) και μέσα κοινωνικής δικτύωσης όπως το LinkedIn, το Facebook και το Twitter, προκειμένου να συλλέξουν το ιστορικό, προσωπικές πληροφορίες, ενδιαφέροντα και δραστηριότητες του ατόμου και να τον μιμηθούν. Για παράδειγμα, κατά τη διάρκεια μιας επίθεσης που αποδόθηκε σε κινεζικές υπηρεσίες πληροφοριών, ανώτεροι στρατιωτικοί αξιωματούχοι του Ηνωμένου Βασιλείου και των ΗΠΑ εξαπατήθηκαν να γίνουν «φίλοι» στο Facebook με κάποιον που μιμείται τον Ναύαρχο του Ναυτικού των ΗΠΑ Τζέιμς Σταυρίδης (Almarabeh & Sulieman, 2019).

Με αφορμή την πανδημία που διανύουμε το 2020, δεν αποτελεί έκπληξη το γεγονός ότι οι hacker εκμεταλλεύονται τη κατάσταση του Κορονοϊού για να κάνουν τα χειρότερα, από την στιγμή που μιλάμε για περίπου 75 εκατομμύρια ανθρώπους που εργάζονται ξαφνικά από το σπίτι. Ερευνητές της Barracuda Networks, η οποία παρέχει ασφάλεια δικτύου σε 220.000 εταιρικούς πελάτες, ανέφεραν ότι ο αριθμός των επιθέσεων μέσω ηλεκτρονικού ταχυδρομείου που σχετίζονται με τον COVID-19 (Κορονοϊός) άρχισε να αυξάνεται τον Ιανουάριο του 2020. Στη συνέχεια, τις πρώτες τρεις εβδομάδες του Μαρτίου όπου ήδη είχε ξεκινήσει το παγκόσμιο Lockdown και πολύ μεγάλο ποσοστό εργαζομένων δούλευαν από το σπίτι, εξερράγη. Ο όγκος του ηλεκτρονικού "ψαρέματος" αυξήθηκε κατά 66,7% από τον Φεβρουάριο σε περισσότερα από 9.000 περιστατικά (Crosman, 2020).

[12] Κοινωνική μηχανική (Social engineering) είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών (Βικιπαίδεια). https://el.wikipedia.org/wiki/Κοινωνική_μηχανική



Γράφημα 5: Επιθέσεις ηλεκτρονικού "ψαρέματος" κατά την διάρκεια του COVID-19.

Cross-Site scripting – XSS

Η απειλή Cross-site scripting θεωρείται μία από τις πιο κοινές μορφές επίθεσης σε εφαρμογές του διαδικτύου. Αποτελεί μία ευπάθεια ασφάλειας που επιτρέπει τον εισβολέα να δημιουργήσει κακόβουλο κώδικα, να τον εισαγάγει σε μία εφαρμογή ιστού και αυτό με τη σειρά του να αποσταλθεί στο πρόγραμμα περιήγησης ενός χρήστη. Ο κώδικας αυτός χρησιμοποιείται για τη μεταφορά ευαίσθητων δεδομένων στον εισβολέα. Οι εισβολείς μπορούν επίσης να χρησιμοποιήσουν το XSS σε συνδυασμό με μια υποδομή κοινωνικού δικτύου για να αναπτύξουν ένα worm XSS το οποίο θα εξαπλωθεί ιογενώς στους χρήστες (Fire et al., 2014). Τον Απρίλιο του 2009, ένα τέτοιο worm XSS, που ονομάζεται Mikeyy, μετέδωσε γρήγορα αυτοματοποιημένα tweets στο Twitter και μόλυνε πολλούς χρήστες, μεταξύ των οποίων διασημότητες όπως η Oprah Winfrey και η Ashton Kutcher. Το σκουλήκι Mikeyy χρησιμοποίησε μια αδυναμία XSS και τη δομή του κοινωνικού δικτύου Twitter για να εξαπλωθεί μέσω προφίλ χρήστη (Fire et al., 2014). Οι ενέργειες αυτές, μπορεί να προκύψουν είτε λόγω έλλειψης ευαισθητοποίησης αναφορικά με την ασφάλεια από τους προγραμματιστές, είτε λόγω σφαλμάτων προγραμματισμού που οφείλονται σε οικονομικούς και χρονικούς περιορισμούς (Vogt et al., 2007).

Οι επιθέσεις XSS επηρεάζουν το θύμα κλέβοντας cookie από τον υπολογιστή του, τροποποιώντας ιστοσελίδα, καταγράφοντας περιεχόμενο κ.ά.. Μπορούν να διακριθούν σε τρεις κατηγορίες επιθέσεων, τις μόνιμες, τις μη μόνιμες και στις επιθέσεις βασισμένες στο Μοντέλο Αντικειμένου Εγγράφου (Document Object Model – DOM). Η πρώτη μέθοδος μπορεί να οδηγήσει σε πιο καταστροφικές ευπάθειες. Ο εισβολέας στέλνει τα δεδομένα τα οποία αποθηκεύονται επίμονα στον εξυπηρετητή, με σκοπό να είναι εμφανή στις ιστοσελίδες του εξυπηρετητή όταν τις επισκέπτονται άλλοι χρήστες. Στην δεύτερη μέθοδο, μη μόνιμη ή ανακλαστική, τα κακόβουλα δεδομένα δεν είναι αποθηκευμένα. Η επίθεση εκτελείται όταν το πιθανό θύμα επιτελέσει είσοδο στην ιστοσελίδα και τότε τα δεδομένα αποθηκεύονται με συνδέσμους και διαδίδονται στο διαδίκτυο μέσω email ή μέσα κοινωνικής δικτύωσης. Ο τρίτος τύπος επιθέσεων που βασίζεται στο Μοντέλο Αντικειμένου Εγγράφου, εμφανίστηκε από την ανάπτυξη των εφαρμογών του Web 2.0. Η χρήση της μεθόδου αυτής, επιτρέπει τους κακόβουλους χρήστες να έχουν πρόσβαση σε ευαίσθητα προσωπικά δεδομένα από τον υπολογιστή του θύματος. Διαφέρει από τους προηγούμενους τύπους καθώς οι ευπάθειες δεν

οφείλονται στον εξυπηρετητή που ετοιμάζει έναν κώδικα για μια ιστοσελίδα, αλλά λαμβάνουν χώρα στα στάδια επεξεργασίας περιεχομένου που εκτελούνται στην πλευρά του χρήστη.

Data Mining – Εξόρυξη Δεδομένων

Η εξόρυξη δεδομένων είναι μία τεχνική στην οποία επεξεργάζεται και αναλύεται τεράστια ποσότητα δεδομένων έχοντας ως πρόθεση την απόσπαση πολύτιμων πληροφοριών από μεγάλες βάσεις δεδομένων. Η συγκεκριμένη απειλή αποτελεί ένα διεπιστημονικό πεδίο το οποίο έχει τις βάσεις του στη στατιστική, την τεχνητή νοημοσύνη (ΤΝ), τη μηχανική μάθηση και τις βάσεις δεδομένων (βλ. Εικόνα 6).

Εικόνα 6: Η εξόρυξη δεδομένων ως τομή της Στατιστικής, της Μηχανικής Μάθησης και των Βάσεων Δεδομένων. (Παπαποστόλου, 2017)

Ο σκοπός της Data mining είναι η ανάλυση τεράστιων ποσοτήτων δεδομένων έχοντας ως αποτέλεσμα την συλλογή ενδιαφέρων στοιχείων που μπορούν να φανούν χρήσιμα για κάποιους οργανισμούς ή κάποιες επιχειρήσεις, που ήταν άγνωστο μέχρι εκείνη τη στιγμή.

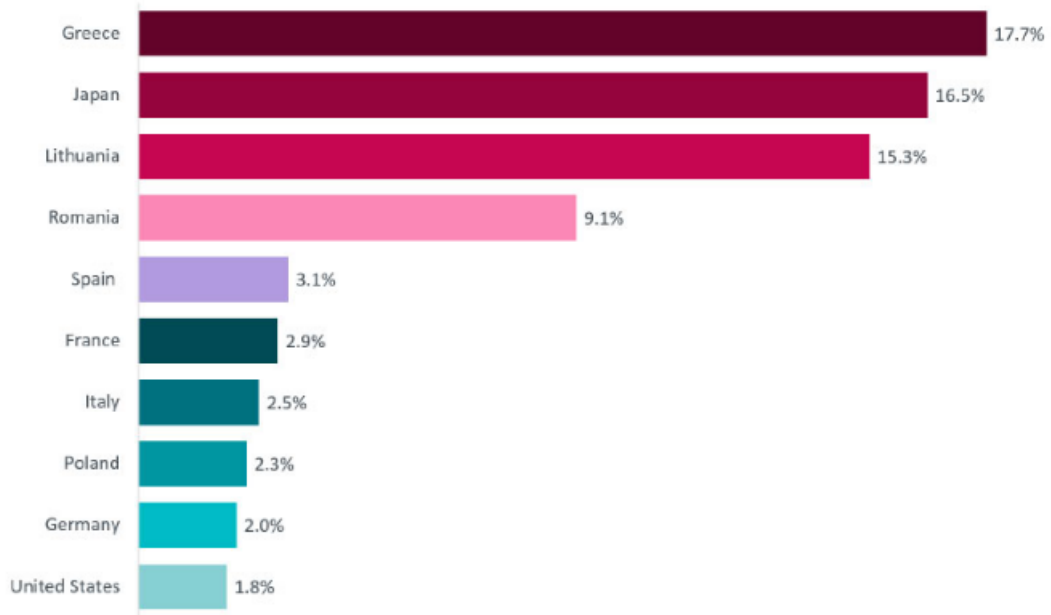
Όλοι αφήνουν πίσω τους μια διαδρομή δεδομένων στο Διαδίκτυο. Κάθε φορά που κάποιος δημιουργεί ένα νέο λογαριασμό κοινωνικών μέσων, δίνει προσωπικές πληροφορίες που μπορούν να περιλαμβάνουν το όνομα, τη γέννηση, τη γεωγραφική θέση και τα προσωπικά τους ενδιαφέροντα. Διάφορες εταιρείες συλλέγουν στοιχεία σχετικά με τις συμπεριφορές των χρηστών: πότε, πού και πώς αλληλοεπιδρούν οι χρήστες με την πλατφόρμα τους. Όλα αυτά τα δεδομένα αποθηκεύονται και αξιοποιούνται από εταιρείες για καλύτερη στόχευση της διαφήμισης στους χρήστες τους. Μερικές φορές, οι εταιρείες μοιράζονται τα δεδομένα των χρηστών με οντότητες τρίτων, συχνά χωρίς γνώση ή συγκατάθεση των χρηστών.

Botnet Attacks – Επιθέσεις Botnet

Μεταξύ των απειλών που μπορούν να εμφανιστούν στο Διαδίκτυο, οι απειλές από τα δίκτυα botnet συμπεριλαμβάνονται στις πιο σοβαρές. Για να γίνει πιο σαφής ο όρος botnet είναι ένας συνδυασμός των λέξεων «ρομπότ» και «δίκτυο». Με μια ευρεία έννοια, το botnet είναι ένα δίκτυο ρομπότ που χρησιμοποιούνται για την διάπραξη εγκλήματος στον κυβερνοχώρο. Είναι ένα σύνολο συσκευών, τα οποία είναι συνδεδεμένα στο Διαδίκτυο και έχουν μολυνθεί από

κακόβουλο λογισμικό που επιτρέπει στους επιτιθέμενους να τις ελέγχουν. Αυτός ο χρήστης που ελέγχει ένα σύστημα botnet ονομάζεται botmaster. Τα bot (ρομπότ) των κοινωνικών μέσων είναι αυτοματοποιημένοι λογαριασμοί που δημιουργούν αναρτήσεις ή παρακολουθούν αυτόματα νέους ανθρώπους κάθε φορά που αναφέρεται ένας συγκεκριμένος όρος που πιθανόν να τους ενδιαφέρει. Τα bot και τα botnets επικρατούν στα κοινωνικά μέσα και χρησιμοποιούνται για να κλέψουν δεδομένα, να στείλουν ανεπιθύμητα μηνύματα και να ξεκινήσουν κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (Distributed Denial of Service Attacks - DDoS) που βοηθούν τους εγκληματίες του κυβερνοχώρου να αποκτήσουν πρόσβαση στις συσκευές και τα δίκτυα των ανθρώπων. Ο κύκλος ζωής του Botnet αρχίζει από την ώρα που δημιουργείται, έπειτα ακολουθεί με την μόλυνση των υποψηφίων θυμάτων, έχοντας ως κλείσιμο την καταστροφή του, αν τυχόν εντοπιστεί από το θύμα του ή όταν αποφασιστεί ότι αυτό είναι αναγκαίο από τον botmaster, γιατί πλέον δεν παρέχει τις πληροφορίες που αναζητά.

Σύμφωνα με το Forrester (μια αμερικάνικη εταιρεία έρευνας αγοράς που παρέχει συμβουλές για τις υπάρχουσες και πιθανές επιπτώσεις της τεχνολογίας στους πελάτες και στο κοινό), τα botnets είναι μια από τις μεγαλύτερες απειλές στον κυβερνοχώρο που πρέπει να προσέξει κανείς το 2020, και με ένα εργατικό δυναμικό που εργάζεται απομακρυσμένα σε διαφορετικές περιοχές, πολλοί οργανισμοί μπορεί να γίνουν πιο ευάλωτοι από ποτέ. Όπως φαίνεται και στο παρακάτω διάγραμμα οι περισσότερες επιθέσεις έχουν καταγραφεί σε χρήστες στην Ελλάδα (17.7%), ενώ εξίσου σημαντικός αριθμός επιθέσεων σημειώνεται σε Ιαπωνία (16.5%) και Λιθουανία (15.3%) (Holt, 2020).



Γράφημα 6: Χώρες με την μεγαλύτερη στόχευση από Botnet από τον Ιούλιο έως 19 Οκτωβρίου 2020. (Rene Holt,2020)

Distributed denial of services (DDoS) attack – Επίθεση κατανεμημένης άρνησης υπηρεσίας

Η επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) θεωρείται ένα από τα πιο ισχυρά όπλα στο Διαδίκτυο. Όταν γίνεται αναφορά σε ιστότοπο που «κατεδαφίστηκε από χάκερ», σημαίνει ότι έπεσε θύμα επίθεσης DDoS. Αυτό απορρέει στο γεγονός ότι οι εισβολείς προσπάθησαν να κάνουν έναν υπολογιστή ή ιστότοπο μη διαθέσιμο, δηλαδή ανίκανο να δεχτεί άλλες συνδέσεις. Κύριος στόχος είναι να πλημμυρίσει με κίνηση περισσότερη από αυτή που μπορεί να φιλοξενήσει ο διακομιστής ή το δίκτυο ενός ιστότοπου ή μιας διαδικτυακής υπηρεσίας. Αποτέλεσμα είναι ο τερματισμός λειτουργίας του ιστότοπου ή της υπηρεσίας. Η κίνηση μπορεί να αποτελείται από εισερχόμενα μηνύματα, αιτήματα για συνδέσεις ή ψεύτικα πακέτα. Οι πιο ευρέως εμφανιζόμενοι τύποι επιθέσεων DDoS είναι το TCP synchronize flood attack, το teardrop attack, το buffer overflow και το Smurf.

Σε ορισμένες περιπτώσεις, τα στοχευμένα θύματα απειλούνται με επίθεση DDoS ή επιτίθενται σε χαμηλό επίπεδο. Αυτό μπορεί να συνδυαστεί με μια απειλή εκβιασμού μιας πιο καταστροφικής επίθεσης, εκτός εάν η εταιρεία πληρώσει λύτρα κρυπτογράφησης. Σημαντικό παράδειγμα αποτελεί μία από τις πρώτες καταγεγραμμένες επιθέσεις DDoS που εκτελέστηκε το 2000 από τον Michael Calce, ένα αγόρι 15 χρονών χρησιμοποιώντας το διαδικτυακό όνομα «Mafiaboy» (Weisman, 2020). Εισχωρώντας σε δίκτυα υπολογιστών κάποιων πανεπιστημίων και κάνοντας χρήση των διακομιστών τους, κάνει την επίθεση και καταφέρνει να καταρρεύσει σημαντικούς ιστότοπους, όπως το CNN, το eBay και το Yahoo. Τον Οκτώβριο του 2010, πραγματοποιείται επίθεση στις MasterCard, PayPal, Visa και Post Finance. Πιο πρόσφατα, το 2016, η Dyn, ένας μεγάλος πάροχος συστήματος ονόματος domain - ή DNS - χτυπήθηκε με μια μαζική επίθεση DDoS που κατέλυσε σημαντικούς ιστότοπους και υπηρεσίες, όπως Airbnb, CNN, Netflix, PayPal, Spotify, Visa, Amazon, The New York Times κ.ά. (Weisman, 2020).

4.2.2 CAMBRIDGE ANALYTIKA AND FACEBOOK SCANDAL

Η Cambridge Analytica Ltd (CA) ήταν πολιτική συμβουλευτική εταιρεία με έδρα την Μεγάλη Βρετανία και ιδρύθηκε το 2014 ως θυγατρική της εταιρείας πληροφοριών SCL – Strategic Communication Limited που ειδικεύεται στην επιρροή των εκλογών.

Το 2013, οι Alexander Nix (πρώην CEO, CA) και Christopher Wylie συζήτησαν την ιδέα τους με τον Steve Bannon (πρώην αντιπρόεδρος, CA) για το πώς θα μπορούσαν να επηρεάσουν τις απόψεις των ψηφοφόρων κατά τη διάρκεια των εκλογών στις Η.Π.Α. Η ιδέα ήταν να συνδυαστεί η μικρο-στόχευση (micro-targeting) που υπήρχε στην πολιτική και στη συνέχεια να στοχεύσει άτομα όχι μόνο ως ψηφοφόρους αλλά και ως προσωπικότητες και τελικά να δημιουργήσει ένα ψυχολογικό προφίλ κάθε ψηφοφόρου σε μια συγκεκριμένη περιοχή ή σε αυτήν την περίπτωση στο σύνολο των Ηνωμένων Πολιτειών (Rehman, 2019). Για να λειτουργήσει η ιδέα αυτή, η CA χρειάστηκε δεδομένα τα οποία αγόρασε από την εταιρεία Global Science Research με ιδρυτή τον Aleksandr Kogan, καθηγητής ψυχολογίας στο πανεπιστήμιο του Cambridge. Την προηγούμενη χρονιά, ο Kogan είχε δημιουργήσει μία εφαρμογή μέσω Facebook με όνομα “thisisyourdigitallife”, η οποία έθετε ένα κουίζ προσωπικότητας στους χρήστες. Όποιος χρήστης του Facebook εγκαθιστούσε την εφαρμογή, αποδεχόταν επίσης τη συλλογή των προσωπικών του δεδομένων από αυτήν. Οι δύο εταιρείες σε συνεργασία, πλήρωσαν περίπου 300.000 χρήστες για να συμμετάσχουν στην έρευνα και να παρέχουν τα προσωπικά τους στοιχεία με σκοπό τη δημιουργία ψυχολογικού προφίλ. Όσοι πήραν μέρος στην έρευνα είχαν συμφωνήσει στην κοινοποίηση των δεδομένων τους όπως

τους επέτρεψαν και οι προεπιλεγμένοι όροι του Facebook, αλλά κανείς δε συμφώνησε στην πώληση των δεδομένων και στην κατάχρησή τους. Η πρόσβαση σε προσωπικές πληροφορίες εκατομμυρίων πολιτών είχε ως στόχο τη συλλογή τους και στην συνέχεια τη χρήση τους για την καθοδήγηση αυτών των ατόμων προς μια συγκεκριμένη επιλογή. Στοιχεία όπως τα πολιτικά και θρησκευτικά πιστεύω, το μορφωτικό επίπεδο, ο σεξουαλικός προσανατολισμός, ακόμα και τα "likes" ("Μου αρέσει") που έχει πατήσει ένας χρήστης συλλέχθηκαν και αναλύθηκαν από ομάδα ειδικών, με σκοπό την δημιουργία προφίλ για τους υποψήφιους. Καθώς η εφαρμογή μπορούσε να συλλέξει πληροφορίες σχετικά με φίλους αυτών των χρηστών (όσοι το είχαν ως επιλογή στις ρυθμίσεις απορρήτου), ο Kogan συγκέντρωσε δεδομένα από περίπου 87 εκατομμύρια άτομα, τα οποία παρέδωσε στην Cambridge Analytica. Η εταιρεία με τη σειρά της τα χρησιμοποίησε για να βοηθήσει την εκστρατεία του Donald Trump στις προεδρικές εκλογές του 2016. Η χρήση των δεδομένων από το Facebook βοήθησε στη δημιουργία προφίλ μεμονωμένων ψηφοφόρων με τις πολιτικές τους προτιμήσεις για στόχευση με διαφημίσεις, στο να εντοπίσουν πού να γίνουν στάσεις εκστρατείας καθώς και στη στρατηγική επικοινωνίας όπως τι να πει σε ομιλίες (Rehman, 2019).

Το 2015, το Facebook μαθαίνει από το "The Guardian" ότι ο Kogan έχει μοιραστεί τα δεδομένα με την CA, που σημαίνει ότι παραβίασε τους όρους και τις πολιτικές του όσον αφορά τη μεταφορά ή πώληση δεδομένων χωρίς την συγκατάθεση των ανθρώπων. Επακολούθως, καταργεί την εφαρμογή και ζητάει από τον Kogan και την Cambridge Analytica να πιστοποιήσουν τη διαγραφή όλων των ακατάλληλα συλλεγμένων δεδομένων, όπως και έγινε. Ταυτόχρονα, το κοινωνικό δίκτυο δεν δηλώνει δημόσια το περιστατικό, ούτε ενημερώνει τους χρήστες των οποίων υποκλάπηκαν τα δεδομένα. Τον Μάρτιο του 2018 σπάει το σκάνδαλο με τους "The Guardian", "New York Times" και το "Channel 4" να φέρουν στη δημοσιότητα ότι τα δεδομένα δεν είχαν διαγραφεί όπως είχαν πιστοποιήσει. Μέσα σε τρεις ημέρες η μετοχή του Facebook μειώνεται κατά 7% και διαγράφει περίπου 40 δισεκατομμύρια δολάρια από την αξία της εταιρείας. Μέχρι το τέλος του μήνα, χάνει περισσότερα από 60 δισεκατομμύρια δολάρια σε κεφαλαιοποίηση αγοράς.

Ενέργειες του Facebook

Η πρόσβαση σε εκατομμύρια προφίλ χρηστών από τον Kogan, οδήγησε το Facebook, το 2014, να αλλάξει ολοκληρωτικά την πλατφόρμα έτσι ώστε να περιορίσουν δραματικά την πρόσβαση των εφαρμογών σε δεδομένα. Το κοινωνικό μέσο απαγορεύει σε αντίστοιχες εφαρμογές με του Kogan, να αιτούν δεδομένα των φίλων ενός ατόμου χωρίς την απαιτούμενη εξουσιοδότηση από τους φίλους του. Απαιτεί επίσης, έγκριση από το Facebook στους προγραμματιστές προτού ζητήσουν ευαίσθητα δεδομένα από τους χρήστες.

Το 2018, όταν η Facebook Inc. μαθαίνει ότι τα δεδομένα δε διαγράφηκαν τελικά, απαγορεύει στις δυο εταιρείες την χρήση οποιασδήποτε υπηρεσίας τους. Ο Διευθύνων Σύμβουλος του Facebook, Mark Zuckerberg, σε προσωπική του δημοσίευση χαρακτηρίζει την κατάσταση αυτή ως «παραβίαση της εμπιστοσύνης» τόσο μεταξύ Kogan, Cambridge Analytica και Facebook, όσο και μεταξύ του Facebook και των χρηστών του. Για να κάνει την πλατφόρμα πιο ασφαλή, στην ίδια δημοσίευση τονίζει ορισμένα μέτρα που θα λάμβαναν. Ως πρώτο βήμα αναφέρει τη διερεύνηση όλων των εφαρμογών που είχαν πρόσβαση σε μεγάλες ποσότητες δεδομένων πριν την αλλαγή της πλατφόρμας το 2014. Αναφέρεται επίσης ο έλεγχος οποιασδήποτε εφαρμογής με τυχόν ύποπτη δραστηριότητα καθώς και ο αποκλεισμός των προγραμματιστών που δε συμμορφώνονται με τον πλήρη έλεγχο. Στο σημείο αυτό, θα

ενημερώνεται όλοι όσοι επηρεάζονται από εφαρμογές που καταχράστηκαν προσωπικά αναγνωρίσιμα στοιχεία (Zuckerberg, 2018). Σε δεύτερο βήμα, προκειμένου να μειωθεί το πρόβλημα από την πηγή του και να αποτραπούν άλλα είδη κατάχρησης, περιορίζονται οι εφαρμογές στις οποίες επιτρέπεται η πρόσβαση στους προγραμματιστές. Για παράδειγμα, θα καταργείται η πρόσβαση στους προγραμματιστές εφόσον ένα μέλος δεν έχει χρησιμοποιήσει την εφαρμογή σε τρεις μήνες. Επιπλέον, μειώνονται τα προσωπικά στοιχεία που δίνουν οι χρήστες κατά τη σύνδεσή τους σε μία εφαρμογή και απαιτείται υπογραφή συμφωνίας από τους προγραμματιστές πριν ζητήσουν πρόσβαση σε δημοσιεύσεις και ευαίσθητες πληροφορίες των χρηστών. Το τρίτο βήμα, αφορά την κατανόηση από μεριάς των ατόμων των εφαρμογών που έχουν επιτρέψει την πρόσβαση στα δεδομένα τους. Το Facebook θα παρέχει ένα εργαλείο, το οποίο ήταν ήδη διαθέσιμο στις ρυθμίσεις απορρήτου, στην «κορυφή της ροής ειδήσεων» που θα επιτρέπει τον έλεγχο και τη διαχείριση των εφαρμογών που έχουν χρησιμοποιήσει «και έναν εύκολο τρόπο ανάκλησης των δικαιωμάτων αυτών των εφαρμογών» (Zuckerberg, 2018).

Η αντίδραση των χρηστών είναι η δημιουργία εκστρατείας μέσω Twitter, το #Deletefacebook, δηλώνοντας ότι θα εγκαταλείψουν το Facebook και παρακινώντας άλλους να το κάνουν. Τους μήνες μετά την αρχική εμφάνιση του σκανδάλου Cambridge Analytica, σχεδόν το 74% των χρηστών διενέργησε αλλιώς αναφορικά με τη χρήση του κοινωνικού μέσου, είτε αλλάζοντας τις ρυθμίσεις απορρήτου, είτε κάνοντας διάλειμμα είτε διαγράφοντας την εφαρμογή από τα κινητά τους τηλέφωνα (Perrin, 2018).

4.2.3 Twitter Data Breach

Μια ακόμα επίθεση, αποτελώντας τη μεγαλύτερη κυβερνο-επίθεση στα μέσα κοινωνικής δικτύωσης, έλαβε χώρο στο Twitter παραβιάζοντας 130 λογαριασμούς. Βέβαια, αυτή δε θεωρείται η πρώτη φορά που το Twitter δέχτηκε παράνομες ενέργειες. Το 2017, ένας υπάλληλος διέγραψε τον λογαριασμό του προέδρου Donald Trump την τελευταία ημέρα της εργασίας του και το 2019 οι χάκερ κατάφεραν να εισβάλουν στον λογαριασμό του Jack Dorsey που είναι συνιδρυτής και Διευθύνων Σύμβουλος του Twitter.

Τον Ιούλιο του 2020, μετά από ένα tweet που ζητούσε δωρεές στην κρυπτογράφηση, που δημοσιεύτηκε από τους επίσημους λογαριασμούς της Apple Inc. & Uber Inc., του Διευθύνων Σύμβουλου της Tesla, Elon Musk, και του συνιδρυτής της Microsoft, Bill Gates, οι χάκερ ανέλαβαν αργότερα και άλλους λογαριασμούς γνωστών προσώπων όπως του Barak Obama, του Joseph R. Biden, Mike Bloomberg, του Jeff Bezos (Διευθύνων Σύμβουλος της Amazon) και άλλων πολλών. Για αρκετές ώρες, ο κόσμος παρακολουθούσε ενώ οι χάκερ πραγματοποιούσαν δημόσια επίθεση στον κυβερνοχώρο, καταλαμβάνοντας τον έναν λογαριασμό υψηλού προφίλ μετά τον άλλο και στέλνοντας tweet γράφοντας «Διπλασίασε τα bitcoin σου» (Tyagi, 2020).

Εικόνα 7: Αναφορές στο Twitter. (Department of Financial Services, 2020)

Οι χάκερ ανέλαβαν τους λογαριασμούς Twitter πολιτικών, διασημοτήτων και επιχειρηματιών, καθώς και λογαριασμούς Twitter πολλών εταιρειών κρυπτογράφησης που ρυθμίζονται από το Υπουργείο Οικονομικών Υπηρεσιών της Νέας Υόρκης. Οι εισβολείς μπόρεσαν να δουν προσωπικά στοιχεία, συμπεριλαμβανομένων διευθύνσεων email και αριθμών τηλεφώνου. Επίσης το Twitter αποκάλυψε ότι οι χάκερ είχαν κατεβάσει προσωπικά στοιχεία, συμπεριλαμβανομένων των ιδιωτικών μηνυμάτων, των εικόνων και των βίντεο σε ιδιωτικά μηνύματα. Και για αρκετές ώρες το Twitter δεν μπόρεσε να σταματήσει την παραβίαση.

Σε χρηματική αξία, οι χάκερ έκλεψαν bitcoin αξίας άνω των 118 χιλιάδες δολαρίων. Το πιο σημαντικό όμως, είναι ότι αυτό το περιστατικό αποκάλυψε την ευπάθεια μιας παγκόσμιας πλατφόρμας κοινωνικών μέσων με περισσότερους από 330 εκατομμύρια συνολικούς μηνιαίους ενεργούς χρήστες και πάνω από 186 εκατομμύρια καθημερινούς ενεργούς χρήστες, συμπεριλαμβανομένων περισσότερων από 36 εκατομμύρια (20%) στις Ηνωμένες Πολιτείες (Department of Financial Services, 2020)[13]. Δεδομένου ότι το Twitter είναι μια εταιρεία τεχνολογίας 37 δισεκατομμυρίων δολαρίων που αποτελεί αντικείμενο δημόσιας διαπραγμάτευσης, ήταν εκπληκτικό το πόσο εύκολα οι χάκερ μπόρεσαν να εισέλθουν στο δίκτυο του και να αποκτήσουν πρόσβαση σε εσωτερικά εργαλεία επιτρέποντάς τους να αναλάβουν οποιονδήποτε λογαριασμό χρήστη.

[13] https://www.dfs.ny.gov/Twitter_Report?fbclid=IwAR3iKe5H2v6BQ-eIPfIxvNVo2iljoKQzahEqHdRmp50YWX6lQHvJey33JQk

Οι φάσεις της επίθεσης

Σε πρώτη φάση, στις 14 Ιουλίου 2020 οι χάκερ, προσπαθώντας να αποκτήσουν πρόσβαση στο δίκτυο του Twitter, μέσω τηλεφωνικών κλήσεων σε πολλούς υπαλλήλους ισχυρίζονταν ότι καλούν από το γραφείο βοήθειας στο τμήμα πληροφορικής της εταιρείας. Κατευθύνοντας έναν υπάλληλο σε ιστότοπο ηλεκτρονικού "ψαρέματος" (phishing) παρόμοιο με το νόμιμο VPN δίκτυο του Twitter, αντιγράφουν και εισαγάγουν τις πληροφορίες που καταχωρεί ο υπάλληλος (στον ψεύτικο ιστότοπο), στον πραγματικό ιστότοπο του κοινωνικού μέσου. Στο σημείο αυτό, ο υπάλληλος αυτός δεν είχε πρόσβαση στα εσωτερικά εργαλεία, αλλά οι εισβολείς συμβιβάστηκαν με ότι είχαν έτσι ώστε να περιηγηθούν στους εσωτερικούς ιστότοπους και να ενημερωθούν περισσότερο για τα συστήματα πληροφοριών του Twitter. Στις 15 Ιουλίου, στοχεύουν υπαλλήλους που τους επιτρέπεται η είσοδος στα εσωτερικά εργαλεία.

Έχοντας τη δυνατότητα ανάληψης λογαριασμού χρήστη, σε επόμενη φάση έσπευσαν την προσοχή τους στα "original gangster" (OG) ονόματα χρήστη Twitter, τα οποία αποτελούν ονόματα αυθεντικών και γνωστών προσωπικοτήτων και υιοθετούνται από τους πρώτους χρήστες του μέσου. Όποιος καταφέρει να υποκλέψει επιτυχώς ένα τέτοιο όνομα χρήστη, μπορεί να πουλήσει πρόσβαση σε αυτό για χιλιάδες δολάρια. Σύμφωνα με αναφορά έρευνας, μεταξύ περίπου 3 π.μ. και 10 π.μ. στις 15 Ιουλίου οι εισβολείς συζήτησαν επιτυχώς την εξαγορά και πώληση των ονομάτων χρήστη OG ως αντάλλαγμα bitcoin, ενδεχομένως μέσω διαδικτυακών μηνυμάτων. Λίγο πριν τις 2 μ.μ., με την εισβολή τους σε OG λογαριασμούς, έκαναν tweets στιγμιότυπων εσωτερικών εργαλείων στους ακόλουθους (followers) ορισμένων λογαριασμών.

Το Twitter Hack έρχεται στην κλιμάκωσή του στην τρίτη φάση, όπου οι χάκερ αποσκοπούν «επαληθευμένους»[14] λογαριασμούς, δηλαδή αυτούς που το Twitter ορίζει «λογαριασμούς δημόσιου ενδιαφέροντος». Αυτό αποτελεί μία έξυπνη κίνηση από τους χάκερ, καθώς τα tweets από αυτούς τους λογαριασμούς έκαναν τις απαιτήσεις τους να φαίνονται πιο νόμιμες. Χειριζόμενοι αρχικά, λογαριασμούς γνωστών εταιρειών και ατόμων κρυπτογράφησης, παραβίασαν το προσωπικό προφίλ του @AngeloBTC, έμπορος κρυπτογράφησης, έκαναν tweet ζητώντας bitcoin και έστειλαν προσωπικά μηνύματα σε άλλους χρήστες που περιλάμβαναν σύνδεσμο (link) για ένα πορτοφόλι bitcoin για πληρωμή. Ελάχιστα λεπτά μετά, καταλαμβάνουν τον λογαριασμό της Binance, κέντρου κρυπτογράφησης, δημοσιεύοντας tweet το οποίο περιείχε έναν σύνδεσμο με μία διεύθυνση απάτης bitcoin.

Εικόνα 8: Το tweet απάτης από τους χάκερ.

[14] Ο επαληθευμένος λογαριασμός διαθέτει ένα μπλε επαληθευμένο σήμα, το οποίο επιτρέπει στους χρήστες να γνωρίζουν ότι ένας λογαριασμός δημοσίου ενδιαφέροντος είναι αυθεντικός. Τέτοιοι λογαριασμοί διατηρούνται συνήθως από πολιτικούς, την κυβέρνηση, μουσικούς, επιχειρήσεις, οργανισμούς, δημοσιογράφους, αθλητές και από άτομα άλλων βασικών τομέων ενδιαφέροντος.

Μέχρι τις 4:12 μ.μ., παραβιάστηκαν δέκα λογαριασμοί που συνδέονται με την κρυπτογράφηση μέσω των οποίων χρησιμοποίησαν παραλλαγές του παραπάνω μηνύματος. Εν συνεχεία, μεταξύ 4:17 μ.μ. και 6:05 μ.μ., δημοσιεύουν περιεχόμενο από προφίλ που ανήκουν στον Elon Musk (CEO της Tesla), στον Bill Gates, στον Kanye West, στην Kim Kardashian, στον Joseph R. Biden, στην Uber Inc. και στην Apple Inc.

Οι χάκερ χρησιμοποίησαν τεχνικές όπως τηλεφωνικές κλήσεις όπου προσποιούταν ότι ήταν από το τμήμα τεχνολογίας πληροφοριών του Twitter. Σύμφωνα με ανακοίνωση του Twitter δεν είχαν όλοι οι υπάλληλοι, που είχαν στοχοποιηθεί, δικαιώματα να χρησιμοποιούν εργαλεία διαχείρισης λογαριασμού, αλλά οι εισβολείς χρησιμοποίησαν τα διαπιστευτήριά τους για πρόσβαση στα εσωτερικά συστήματα και απόκτηση πληροφοριών σχετικά με τις διαδικασίες. Κατάφεραν, επίσης, να έχουν πρόσβαση σε εργαλεία που είναι διαθέσιμα μόνο στις εσωτερικές ομάδες υποστήριξης για να στοχεύσουν 130 λογαριασμούς Twitter. Στους 45 από αυτούς, μπόρεσαν να επαναφέρουν τους κωδικούς πρόσβασης, να συνδεθούν στον λογαριασμό και να στείλουν tweets. Το κοινωνικό μέσο αποκάλυψε ότι οι κακόβουλοι χρήστες είχαν κατεβάσει προσωπικά στοιχεία, συμπεριλαμβανομένων των ιδιωτικών μηνυμάτων, των λογαριασμών email, των εικόνων και των βίντεο σε ιδιωτικά μηνύματα (Department of Financial Services, 2020).

Ενέργειες του Twitter

Το Twitter κλείδωσε όλους τους επηρεαζόμενους λογαριασμούς και κατάργησε αναρτήσεις από τους εισβολείς. Αναγνώρισε το περιστατικό και ανακοίνωσε, «είναι μια συντονισμένη επίθεση κοινωνικής μηχανικής και εργαζόμαστε για να το διορθώσουμε».

Υπήρχε άμεση επικοινωνία με τους κατόχους λογαριασμών που επηρεάστηκαν και έγιναν προσπάθειες να αποκατασταθούν οι προσβάσεις σε λογαριασμούς που ενδέχεται να κλειδώθηκαν. Η έρευνά που έκανε το Twitter συνεργάστηκε με τις αρμόδιες αρχές για να διασφαλισθεί ότι τα άτομα που είναι υπεύθυνα για αυτήν την επίθεση να εντοπιστούν.

Μετά την επίθεση, περιορίστηκε σημαντικά η πρόσβαση στα εσωτερικά εργαλεία και τα συστήματά, για να διασφαλισθεί η ασφάλεια των λογαριασμών. Ως αποτέλεσμα, επηρεάστηκαν ορισμένες δυνατότητες δηλαδή η πρόσβαση στη δυνατότητα λήψης δεδομένων του Twitter, οι διαδικασίες καθώς υπήρξε και βελτίωση των εργαλείων.

Επίσης, έγιναν προσπάθειες βελτίωσης τις μεθόδους για τον εντοπισμό και την αποτροπή ακατάλληλης πρόσβασης στα εσωτερικά συστήματα και δόθηκε προτεραιότητα στην παροχή ασφαλείας σε πολλές από τις ομάδες του Twitter. Εκτός αυτού, συνεχίστηκαν οι διοργανώσεις ασκήσεων ηλεκτρονικού ψαρέματος σε όλους τους εργαζόμενους της εταιρεία.

Η ομάδα του Twitter επικεντρώθηκε στην προσπάθεια να επαναφέρει την πρόσβαση για όλους τους κατόχους λογαριασμών που ήταν πιθανόν να ήταν ακόμα κλειδωμένοι ως αποτέλεσμα των προσπαθειών αποκατάστασης και περαιτέρω ασφάλεια των συστημάτων για την αποτροπή μελλοντικών επιθέσεων (Twitter Inc., 2020).

4.3 Προστασία προσωπικών δεδομένων στα Μέσα Κοινωνικής Δικτύωσης

Ένα σύνθετο ζήτημα που μας απασχολεί στην εποχή που βρισκόμαστε, είναι η προφύλαξη των προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης. Σχεδόν όλοι έχουν χρησιμοποιήσει έστω και μια φορά, κάποια από τις πολλές πλατφόρμες κοινωνικής δικτύωσης, δημοσιεύοντας κάποια προσωπική πληροφορία, είτε αυτό είναι κάποια φωτογραφία είτε κάποια αναφορά για την προσωπική ζωή. Η ανάγκη της Προστασίας Προσωπικών Δεδομένων (PDP-Personal Data Protection) καθορίζεται από το γεγονός ότι το απόρρητο είναι ένα σημαντικό ανθρώπινο δικαίωμα που συνδυάζει ένα σύμπλεγμα ξεχωριστών ατομικών δικαιωμάτων - σωστή και επαρκής επεξεργασία προσωπικών δεδομένων, διαφορετική μορφή προσωπικής επικοινωνίας (ταχυδρομικά, μέσω Διαδικτύου κ.λπ.), ασφαλή διατήρηση προσωπικών προφίλ στα κοινωνικά φόρουμ και ομάδες κ.λπ. (Romansky, 2014).

Το απόρρητο στα μέσα κοινωνικής δικτύωσης έχει σχέση με την προστασία των πληροφοριών και των δικαιωμάτων του χρήστη. Σε κάθε προφίλ ενός μέσου, περιλαμβάνονται διαφορετικοί τύποι δεδομένων χρηστών, όπως ταυτότητα, δημογραφικά στοιχεία, δραστηριότητες και πρόσθετο περιεχόμενο. Επακόλουθο λοιπόν, είναι διαφορετικοί χρήστες να έχουν διαφορετικά προβλήματα απορρήτου για τα διαφορετικά είδη πληροφοριών τους. Οι ιστοσελίδες κοινωνικής δικτύωσης είναι ιδανικοί χώροι για παράνομες διαδικτυακές δραστηριότητες, καθώς αποτελούνται από μεγάλο αριθμό χρηστών με υψηλό επίπεδο εμπιστοσύνης μεταξύ τους. Ως αποτέλεσμα, υπάρχει ένα υψηλό φάσμα κινδύνων, απειλών και προκλήσεων ασφαλείας (Ajami et. al., 2011).

Τα προσωπικά δεδομένα μπορούν να επεξεργαστούν, αλλά με βάση την νομοθεσία θα πρέπει αρχικά να εγκριθεί από το άτομο στο οποίο αναφέρονται τα συγκεκριμένα δεδομένα. Υφίστανται όμως και κάποιες φορές που επιτρέπεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα χωρίς την συναίνεση του ατόμου. Σε τέτοιες περιστάσεις είναι πολλοί οι κακόβουλοι χρήστες που παραβιάζουν τους κανονισμούς και έχει μη εξουσιοδοτημένη πρόσβαση. Στην συγκεκριμένη περίπτωση αυτός ο χρήστης μπορεί να τιμωρηθεί με φυλάκιση και χρηματική ποινή. Επομένως, τα μέσα πρέπει να αποφεύγουν διαφορετικά συμβάντα με τα δεδομένα των χρηστών όπως επεξεργασία, μη εξουσιοδοτημένη πρόσβαση, ιούς, παράνομη μεταφορά σε τρίτους κ.ά.. Σύμφωνα με τον Romansky (2014), ορισμένες προκλήσεις των κοινωνικών μέσων στην προστασία προσωπικών δεδομένων συνοψίζονται παρακάτω.

Κορυφαίο και πρωταρχικό πρόβλημα απορρήτου είναι η έλλειψη ενημέρωσης των χρηστών από τους ιστότοπους κοινωνικής δικτύωσης. Υπάρχει κίνδυνος κατά την εγγραφή αλλά και τη χρήση των κοινωνικών μέσων, με το επίπεδο απορρήτου να διαφέρει κατά πολύ από ιστότοπο σε ιστότοπο. Ορισμένοι ιστότοποι κοινωνικής δικτύωσης συλλέγουν περιορισμένα προσωπικά δεδομένα (όνομα, ημερομηνία γέννησης, αριθμός τηλεφώνου), ενώ άλλοι απαιτούν επιπλέον πληροφορίες (κοινωνική ζωή, φύλο, σχέσεις κ.λπ.). Οι τύποι των δεδομένων αυτών, εξατομικεύουν τους χρήστες σε μεγάλο επίπεδο οπότε αποτελεί δικαίωμα για τα άτομα αυτά να γνωρίζουν τον σκοπό αυτών των δεδομένων και τον λόγο επεξεργασίας.

Ένα σημαντικό χαρακτηριστικό αυτής της πηγής προσωπικών δεδομένων, δηλαδή των μέσων κοινωνικής δικτύωσης, είναι ότι τα δεδομένα είναι διαθέσιμα για ανίχνευση και επεξεργασία, ακόμα και χωρίς τη συγκατάθεση των χρηστών. Συνεπώς, η υποχρέωση των ελεγκτών είναι να εγγυηθεί την εύκολη πρόσβαση στα προσωπικά δεδομένα των χρηστών, το οποίο με τη

σειρά του θα επιτρέψει τον χρήστη να αναθεωρήσει τα δικαιώματά του, να αποκτήσει πρόσβαση, να αποκλείσει ή να διαγράψει τα προσωπικά του δεδομένα στο προφίλ (το οποίο αποτελεί θεμελιώδες δικαίωμα που διασφαλίζεται από τους νόμους περί προστασίας δεδομένων).

Ως επόμενο ενδεχόμενο πρόβλημα της ιδιωτικής ζωής στα μέσα κοινωνικής δικτύωσης, ο Romansky (2014) αναφέρει τη διεθνής μεταφορά δεδομένων. Σύμφωνα με τις βασικές αρχές της Προστασίας Προσωπικών Δεδομένων (PDP), τα προσωπικά δεδομένα θα μπορούσαν να μεταφερθούν σε άλλη χώρα εάν το επίπεδο PDP τους είναι επαρκές. Μία τυπική διαδικασία στα κοινωνικά δίκτυα αποτελεί η μεταφορά δεδομένων μεταξύ διαφορετικών παροχών υπηρεσιών, καθώς οι κόμβοι μεταξύ των παροχών (διακομιστές, αποθήκες, πελάτες κ.λπ.) θα μπορούσαν να βρίσκονται οπουδήποτε στον κόσμο. Συμπερασματικά, οποιαδήποτε προσωπική πληροφορία στα μέσα κοινωνικής δικτύωσης πρέπει να προστατεύεται σύμφωνα με τους κανόνες του Συστήματος Ασφαλείας Προσωπικών Δεδομένων (Personal Data Security System – PDSS) και να γίνεται ενημέρωση του χρήστη για όλες τις μεταφορές των δεδομένων του από έναν πάροχο υπηρεσιών σε άλλο, είτε αυτό γίνεται εντός χώρας είτε εκτός.

Έχουν σχεδιαστεί διάφορες τεχνικές για την ασφάλεια της ιδιωτικής ζωής των προσωπικών πληροφοριών. Οι Williams et al (2009) ανέφεραν ορισμένα βήματα για να παραμείνουν ασφαλείς οι χρήστες διαδικτυακών κοινωνικών δικτύων. Σε αυτά περιλαμβάνονται: η επίγνωση των κινδύνων των κοινωνικών δικτύων, ο περιορισμός της δημοσίευσης στοιχείων προσωπικής πληροφορίας και η προσοχή κατά την επαφή με ξένους στο διαδίκτυο ή κατά την ανάγνωση πληροφοριών από οποιονδήποτε αποστολέα.

4.3.1 Πολιτικές Προστασίας

Είναι αναγκαίο να οριστούν βασικές αρχές της ιδιωτικής ζωής και της προστασίας των δεδομένων για να μπορέσουμε να φτάσουμε όσο πιο κοντά μπορούμε στο νόημα και στην σοβαρότητα του δικαιώματος της ιδιωτικότητας του κάθε ατόμου.

Οι Jim Isaak & Mina J. Hanna (2018), ανέλυσαν την ιδιωτικότητα των χρηστών ιδίως στο Facebook καλύπτοντας την γενικότερη έννοια την ιδιωτικότητας και στοχεύοντας κυρίως στην προστασία της ιδιωτικής ζωής. Κατέληξαν λοιπόν στο συμπέρασμα, θεωρώντας ότι όλες οι νομοθεσίες οι οποίες σχετίζονται με την προστασία της ιδιωτικής ζωής και των δεδομένων πρέπει να περιλαμβάνουν τις ακόλουθες αρχές:

Τη δημόσια διαφάνεια όπου:

- Οι χρήστες πρέπει να μαθαίνουν τους τύπους δεδομένων που συλλέγονται για εκείνους από οποιονδήποτε ιστότοπο ή και από άλλα ηλεκτρονικά μέσα. Επίσης πρέπει να γνωρίζουν ποια δεδομένα διατηρούνται, με ποιόν τρόπο αυτά χρησιμοποιούνται και τι κοινοποιείται σε τρίτα άτομα.
- Όλοι οι μηχανισμοί οι οποίοι συλλέγουν τα δεδομένα των χρηστών, πρέπει να είναι φανερά στους χρήστες, συμπεριλαμβανομένων των ιστοφάρων (web beacons) ή άλλων μηχανισμών παρακολούθησης της δραστηριότητας. Οι χρήστες πρέπει να αναγνωρίζουν και να ελέγχουν τι προσωπικά στοιχεία αποκαλύπτονται.

- Κάθε ιστότοπος και εφαρμογή πρέπει να εμφανίζει οποιοδήποτε περιεχόμενο τοποθετείται στη συσκευή του χρήστη, καθώς και ποιες χρήσεις γίνονται μέσα σε αυτές.

Τη γνωστοποίηση για χρήστες

- Σε ιστότοπο και εφαρμογή, οι χρήστες πρέπει να έχουν πλήρη γνώση και πρόσβαση για το τι προσωπικές πληροφορίες διατηρούνται εντός αυτών.

Τον έλεγχο

- Οι επιλογές του χρήστη "μην παρακολουθείτε" πρέπει να τηρούνται, αποκλείοντας την εμφάνιση των cookies. Οι χρήστες πρέπει να επιλέγουν σε ποιους και σε τι πληροφορίες θέλουν να επιτρέπεται η πρόσβαση. Αυτό είναι μια απαίτηση η οποία επεκτείνεται σε όλους τους ιστότοπους, υπηρεσίες cloud και άλλες συσκευές συλλογής.
- Οι χρήστες πρέπει εύκολα να διαγράφουν τα προσωπικά δεδομένα από οποιονδήποτε ιστότοπο, υπηρεσία cloud ή συσκευή συλλογής.
- Οι χρήστες πρέπει να μπορούν να τερματίζουν, να απεγκαθιστούν ή να διαγράφουν περιεχόμενα ή εφαρμογές που δημιουργούνται στις συσκευές τους ή σε υπηρεσίες cloud.
- Οι διαφορές που δημιουργούνται με την οποιαδήποτε εκκαθάριση δεδομένων του χρήστη ή την εκκαθάριση εφαρμογών δεν πρέπει να είναι προεπιλεγμένες σε άδειες και διαδικασίες που περιορίζουν τις επιλογές νομικής απόκρισης.
- Οι ανήλικοι πρέπει να προστατεύονται από νόμους σε περιπτώσεις δημοσιοποίησης των προσωπικών τους πληροφοριών.

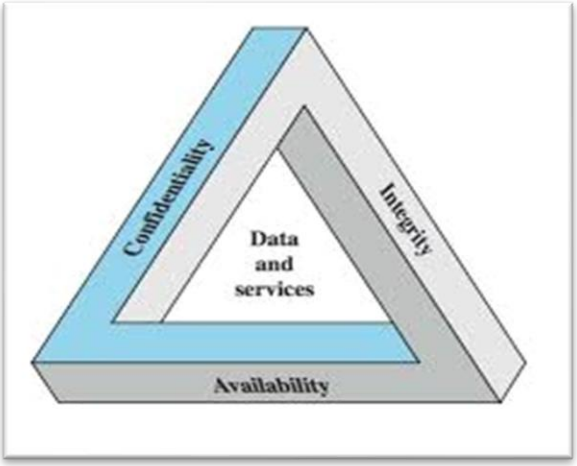
Την ειδοποίηση

- Οι χρήστες πρέπει να ενημερώνονται σε άμεσο χρονικό διάστημα σε περίπτωση απώλειας ή επεξεργασίας προσωπικών τους δεδομένων από οποιονδήποτε οργανισμό συλλέγει και αποθηκεύει προσωπικά δεδομένα.
- Οι χρήστες έχουν το δικαίωμα να γνωρίζουν από που προήλθαν οι παραβιάσεις του απορρήτου τους.
- Για διαδίκτυο πρέπει να ενημερώνει τον χρήστη και να τον κάνει να κατανοήσει αλλά και το βασικότερο να πραγματοποιήσει τις ενέργειες διαφάνειας, αποκάλυψης και ελέγχου οι οποίες αναφέρονται παραπάνω.

Η προφύλαξη των προσωπικών δεδομένων και της ιδιωτικής ζωής είναι απαραίτητη για τα ανθρώπινα δικαιώματα. Σκοπός ενός συστήματος πολιτικής ασφάλειας είναι η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που χρησιμοποιούνται από τα μέλη ενός οργανισμού. Αποτρέπει τη μη εξουσιοδοτημένη αποκάλυψη, διακοπή, πρόσβαση, χρήση και τροποποίηση αυτών των σημαντικών πληροφοριών. Το πιο σημαντικό σημείο για μια ασφαλή πολιτική, είναι ο εντοπισμός των δεδομένων που επρόκειτο να χρησιμοποιηθούν και να προστατευτούν. Για την προστασία αυτών των πληροφοριών θα πρέπει να τηρούνται τρεις θεμελιώδεις αρχές που ονομάζονται τριάδα CIA:

- Εμπιστευτικότητα (Confidentiality) : Αφορά την προστασία της πληροφορίας η οποία δεν θα έπρεπε να αποκαλυφθεί σε μη εξουσιοδοτημένα άτομα.

- Ακεραιότητα Πληροφοριών (Integrity) : Αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη τροποποίηση και διασφάλιση της αυθεντικότητας, της ακρίβειας, της μη αποποίησης και της πληρότητας των πληροφοριών.
- Διαθεσιμότητα Πληροφοριών (Availability) : Αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη καταστροφή και τη διασφάλιση της πρόσβασης των δεδομένων όταν απαιτείται.



Εικόνα 8: Βασικές αρχές πολιτικής ασφάλειας ενός υπολογιστικού συστήματος.

Όπως φαίνεται στο παραπάνω σχήμα οι τρεις αρχές αλληλοσυμπληρώνονται και καθιστούν ένα υπολογιστικό σύστημα ασφαλές, πλήρης και αποδοτικό. Άρα πρέπει να λαμβάνεται σοβαρά υπόψιν οι αρχές της τριάδας της CIA κατά την ανάπτυξη εταιρικών πολιτικών ασφάλειας. Χωρίς την πολιτική ασφάλεια τα στοιχεία ενός οργανισμού είναι επιρρεπείς σε συμβιβασμούς ή επικίνδυνο για κλοπή.

Ο στόχος της πολιτικής ασφάλειας είναι να αποσαφηνίσει και να γνωστοποιήσει τη θέση της διαχείρισης σχετικά με την ασφάλεια, όπως ορίζεται στις αρχές ασφαλείας υψηλού επιπέδου.

4.3.2 Μηχανισμοί Ασφάλειας

Ο λόγος για τον οποίο οι κυβερνο-εγκληματίες μαστίζουν στον χώρο των κοινωνικών δικτύων είναι επειδή η ευκολία προσβασιμότητας των προσωπικών δεδομένων προσελκύει αυτούς που προσπαθούν να εκμεταλλευτούν αυτές τις πληροφορίες. Αυτό που τα κάνει πιο εύκολα προσβάσιμα είναι το ότι οι ίδιοι οι χρήστες μοιράζονται τις προσωπικές τους πληροφορίες, όπως εικόνες, ενδιαφέροντα, κοινωνικές σχέσεις και εμπιστευτικές πληροφορίες σε όλο τον κόσμο μέσω των κοινωνικών δικτύων.

Παρόλη την αυξανόμενη χρήση των μέσων κοινωνικής δικτύωσης, οι κίνδυνοι που συνδέονται με τη μεταφόρτωση ευαίσθητων πληροφοριών δεν είναι αναγνωρίσιμοι από όλους τους χρήστες. Ο τομέας της ασφάλειας των πληροφοριών στο Διαδίκτυο έχει αναπτυχθεί σημαντικά και εξελίσσεται συνεχώς με αφορμή τις νέες απειλές. Αυτό που μένει, αφορά τα μέσα

κοινωνικής δικτύωσης και τους εκατομμύρια χρήστες τους να οργανωθούν και να ενημερωθούν περαιτέρω ώστε να προστατευθούν και να αναγνωρίζουν τον κίνδυνο από προγράμματα κλοπής ταυτότητας, απάτες και επιθέσεις κακόβουλου λογισμικού. Έτσι, κρίνεται αναγκαίο τα μέσα κοινωνικής δικτύωσης να ακολουθούν κάποιες προϋποθέσεις ασφάλειας των προσωπικών δεδομένων ή αλλιώς απαιτήσεις ιδιωτικότητας, ώστε να αποτραπούν διάφορες παραβιάσεις αυτών κατά τη χρήση ενός κοινωνικού δικτύου. Οι κύριες απαιτήσεις που πρέπει να ικανοποιούνται είναι οι εξής:

- Ανωνυμία (Anonymity). Με τη διαδικασία αυτή, ένας χρήστης κατά την πρόσβασή του σε μία σελίδα κοινωνικής δικτύωσης, δεν επιβάλλεται η αποκάλυψη της ταυτότητάς του. Σύμφωνα με τον ορισμό, ανωνυμία ενός οργανισμού σημαίνει ότι ο οργανισμός αυτός δεν είναι αναγνωρίσιμος σε ένα σύνολο ανώνυμων οργανισμών. Ο βαθμός ανωνυμίας μεταξύ ενός συνόλου χρηστών δεν είναι σταθερός, καθώς εξαρτάται από τη συμπεριφορά των υπόλοιπων χρηστών και καθορίζεται από την πολιτική προστασίας κάθε κοινωνικού μέσου. Κάποια κοινωνικά δίκτυα, όπως το Whisper και το Secret, απαιτούν εξ' ορισμού την ανωνυμία για όλους τους χρήστες χωρίς αυτό να μπορεί να αλλάξει.
- Ψευδωνυμία (Pseudonymity). Όσον αφορά τα μέσα κοινωνικής δικτύωσης, η χρήση την ψευδωνυμίας παίζει σημαντικό ρόλο καθώς είναι δύσκολη η υλοποίηση την ανωνυμίας σε αυτά. Το χαρακτηριστικό αυτό προστατεύει την αναγνώριση του χρήστη από μη εξουσιοδοτημένους τρίτους χρήστες, μέσω της χρήσης ενός ψευδώνυμου αντί του πραγματικού ονόματος. Επομένως, η διαδικασία αυτή επιτρέπει την πρόσβαση των χρηστών σε δεδομένα χωρίς την αποκάλυψη της ταυτότητάς τους.
- Μη συνδεσιμότητα (Unlinkability). Η διαδικασία αυτή, αποκλείει έναν επιτιθέμενο να συνδέσει μέρη σχετικών πληροφοριών μεταξύ τους, έχοντας ως αποτέλεσμα την αποκάλυψη της ταυτότητας μιας οντότητας. Ουσιαστικά, ο επιτιθέμενος δεν καταφέρνει να ξεχωρίζει αν τα δεδομένα που τον ενδιαφέρουν (προσωπικές πληροφορίες, μηνύματα κ.ά.) σχετίζονται μεταξύ τους ή όχι.
- Μη παρατηρησιμότητα (Unobservability). Κατά τη χρήση μιας υπηρεσίας, προστατεύεται η ιδιωτικότητα ενός χρήστη ο οποίος είναι μη παρατηρήσιμος σε ένα σύνολο χρηστών. Δηλαδή, ο χρήστης παραμένει ανώνυμος, απαγορεύοντας τους πιθανούς επιτιθέμενους να εντοπίσουν ίχνη τους. Η λειτουργία αυτή, έχει παρατηρηθεί σε αρκετά μέσα κοινωνικής δικτύωσης για ορισμένες λειτουργίες τους. Για παράδειγμα, στα περισσότερα μέσα ο χρήστης μπορεί να γίνει μη ορατός στους άλλους χρήστες καθώς χρησιμοποιεί αυτή τη χρονική στιγμή την υπηρεσία. Όμως αυτό δεν ισχύει και για λειτουργίες όπως η αποστολή μηνυμάτων ή ο σχολιασμός φωτογραφιών.
- Προστασία Δεδομένων (Data Protection). Αποτελεί, ίσως, τη πιο σημαντική απαίτηση ιδιωτικότητας όσο αφορά την ασφάλεια των δεδομένων στα μέσα κοινωνικής δικτύωσης. Σύμφωνα με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, είναι η διαδικασία μέσω της οποίας διασφαλίζονται οι κάτωθι αρχές:
    - Αρχή της νομιμότητας και της δικαιοσύνης.
    - Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
    - Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
    - Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
    - Αρχή της ασφάλειας και της ακεραιότητας.
    - Εποπτεία και Επικύρωση.

ΚΕΦΑΛΑΙΟ 5 : ΕΡΕΥΝΗΤΙΚΟ ΜΕΡΟΣ

5.1 Σκοπός και στόχος

Προκειμένου να διερευνηθεί ο αντίκτυπος των μέσων κοινωνικής δικτύωσης στην ιδιωτικότητα των χρηστών, έγινε η πραγμάτωση σχετικής έρευνας. Σκοπός της έρευνας αυτής είναι η διαπίστωση της διαδικτυακής συμπεριφοράς των χρηστών απέναντι στα μέσα κοινωνικής δικτύωσης. Ως στόχος έχει τεθεί η διερεύνηση του πόσο ευρέως γνωστά και απαραίτητα αποτελούν τα μέσα στην καθημερινότητα των ανθρώπων, ο διαμοιρασμός των προσωπικών δεδομένων από τους ίδιους τους χρήστες και ο βαθμός διαχείρισης των δεδομένων αυτών. Παράλληλα βασικός στόχος της έρευνας, αποτελεί και η ανάλυση του μέτρου εμπιστοσύνης όσων αφορά την ιδιωτικότητά που έχουν οι χρήστες απέναντι στα μέσα και κατά πόσο αυτοί θεωρούν ότι είναι ασφαλείς.

5.2 Μεθοδολογία Έρευνας

Η μεθοδολογία της έρευνας αυτής, είναι η ποσοτική ανάλυση. Το είδος της είναι η δειγματοληπτική μέθοδος (Survey Research) η οποία εφαρμόστηκε σε ένα τυχαίο δείγμα. Η έρευνα αυτή έγινε μέσω ερωτηματολογίου για την συλλογή των απαραίτητων δεδομένων. Για την δημιουργία του δείγματος έγινε σκόπιμη δειγματοληψία ούτως ώστε να γίνει η απαραίτητη επιλογή στοιχείων που εξυπηρετούν τους σκοπούς της έρευνας. Είναι αναγκαία η κατανόηση του προβλήματος της ανακρίβειας των αποτελεσμάτων της έρευνας καθώς πρέπει το δείγμα του πληθυσμού που ελέγχουμε να είναι αρκετά μεγάλο έτσι ώστε να έχει καλύτερη αντιπροσωπευτικότητα. Έτσι, χρησιμοποιήθηκε ένα όσο το δυνατόν μεγαλύτερο δείγμα για περισσότερο ικανοποιητικά αποτελέσματα. Το ερωτηματολόγιο συντάχθηκε με την χρήση του διαδικτυακού προγράμματος Google Forms. Για να επιτευχθεί η ταχεία λήψη αποτελεσμάτων και η ορθή τυχαιοποίηση του δείγματος, το ερωτηματολόγιο προσκομίστηκε μέσω της ιστοσελίδας του Facebook και της εφαρμογής Viber. Πέρα των θετικών στοιχείων που μας δίνει ο συγκεκριμένος τρόπος διεξαγωγής της έρευνας, υπάρχει και ένα σημαντικό μειονέκτημα. Το μειονέκτημα αυτό είναι ότι υπάρχει η πιθανότητα πολλά άτομα από αυτά που έχουν συμπληρώσει το ερωτηματολόγιο να μην είναι έγκυρα, ή ακόμα και να ανήκουν στο ίδιο άτομο, όπου αυτό προκαλεί αλλοίωση στα αποτελέσματα άρα χάνεται και η αντικειμενικότητα της έρευνας.

Οι τύποι των ερωτήσεων που χρησιμοποιήθηκαν στο ερωτηματολόγιο είναι κατά κύριο λόγο κλειστού τύπου στις οποίες οι ερωτηθέντες είναι υπόχρεοι στο να απαντήσουν την ερώτηση. Επίσης υπάρχουν ερωτήσεις πολλαπλών απαντήσεων στις οποίες έχουν το δικαίωμα μίας ή και παραπάνω επιλογής.

5.3 Ερωτηματολόγιο

1. Φύλλο
    - Άνδρας
    - Γυναίκα

2. Ηλικία
    - <18
    - 18-30
    - 31-45
    - 46-60
    - >60

3. Μορφωτικό επίπεδο
    - Απόφοιτος Γυμνασίου
    - Απόφοιτος Λυκείου
    - Απόφοιτος Πανεπιστημίου
    - Φοιτητής/τρια

4. Σας είναι γνώριμος ο όρος Social Media (Μέσα Κοινωνικής Δικτύωσης);
    - Ναι
    - Όχι

5. Έχετε προσωπικό λογαριασμό σε κάποιο από τα Social Media (π.χ. Facebook, Instagram, Twitter, κ.ά.);
    - Ναι
    - Όχι

6. Αν ναι, πόσο συχνά τα χρησιμοποιείτε;
    - Λιγότερο από 1 ώρα την ημέρα
    - Από 1 έως 3 ώρες την ημέρα
    - Πάνω από 3 ώρες την ημέρα

7. Σε ποιο από τα παρακάτω Social Media διαθέτετε προσωπικό λογαριασμό;
    - Facebook
    - Messenger
    - Instagram
    - Twitter
    - YouTube
    - WhatsApp
    - ….. (Άλλο)

8. Τι πιστεύετε ότι μπορούν να προσφέρουν τα Social Media;
    - Ενημέρωση
    - Ψυχαγωγία
    - Επικοινωνία
    - ….. (Άλλο)

9. Σε τι βαθμό μπορείτε να χειριστείτε τις ιστοσελίδες των Social Media;

- Μικρό
- Ικανοποιητικό
- Αρκετά ικανοποιητικό
- Άριστα

10. Ποιοι είναι συνήθως οι λόγοι για τους οποίους επισκέπτεστε τα Social Media;

- Κοινωνική Δικτύωση
- Ενημέρωση – Πληροφόρηση
- Επαγγελματικούς λόγους
- Αξιοποίηση ελεύθερου χρόνου
- Γνώση / Μάθηση
- Ψυχαγωγία / Διασκέδαση
- ….. (Άλλο)

11. Πόσο καιρό πιστεύετε θα μπορούσατε να μην χρησιμοποιείτε τα Μέσα Κοινωνικής Δικτύωσης;

- Καθόλου
- Μία μέρα
- Μία εβδομάδα
- Περισσότερο

12. Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;

- Στοιχεία επικοινωνίας
- Στοιχεία πληρωμών
- Διεύθυνση
- Όνομα
- Φωτογραφία
- Ηλικία

13. Ποιοι είναι οι ενδοιασμοί σας για την χρήση των Social Media;

- Λόγοι ασφάλειας
- Κίνδυνος ασφάλειας
- Χάσιμο χρόνου
- Έλλειψη επαρκών πληροφοριών
- ….. (Άλλο)

14. Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής;

Χαμηλή ανησυχία 1 2 3 4 5 Υψηλή ανησυχία

15. Έχετε διαβάσει ποτέ την πολιτικής ασφάλειας των Social Media που χρησιμοποιείτε;

- Ναι
- Όχι

16. Διαβάζετε τους όρους και τις προϋποθέσεις πριν την χρήση των μέσων που θα χρησιμοποιήσετε;

- Πατάω «Δέχομαι» χωρίς να διαβάσω το κείμενο
- Περνάω γρήγορα το κείμενο χωρίς να το διαβάσω ολόκληρο
- Διαβάζω όλο το κείμενο

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

- Ανάγνωση της πολιτικής απορρήτου
- Επιλογή της περιορισμένης πρόσβασης σε προσωπικά στοιχεία
- Άρνηση χρήση των προσωπικών μου δεδομένων για διαφημιστικούς λόγους
- Έλεγχος της ασφάλειας της ιστοσελίδας προτού δώσω τα προσωπικά μου στοιχεία
- Απαίτηση πρόσβασης σε προσωπικά δεδομένα

18. Τα προσωπικά σας στοιχεία είναι δημόσια κοινοποιημένα στον λογαριασμό σας;

- Ναι
- Όχι

19. Έχετε κάνει τις απαραίτητες ρυθμίσεις ώστε να ελέγχετε σε ποιους είναι ορατά τα στοιχεία που αναρτάτε;

- Ναι
- Όχι

20. Αν μαθαίνατε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζατε να τα χρησιμοποιείτε;

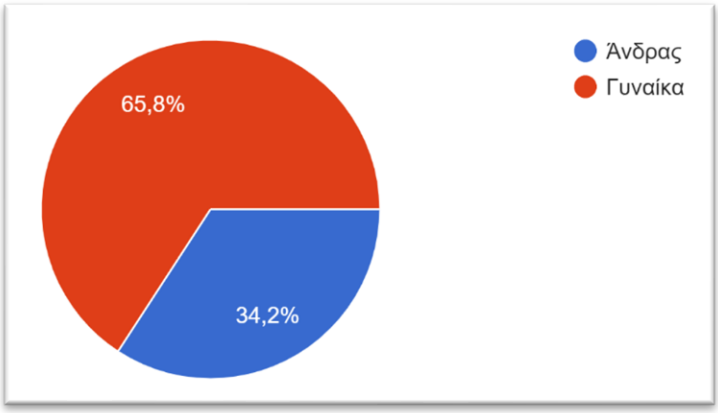
- Θα συνέχιζα τη χρήση τους
- Δεν είμαι σίγουρος/η
- Δε θα συνέχιζα τη χρήση τους

21. Πιστεύετε ότι ο εθισμός στα Μέσα Κοινωνικής Δικτύωσης που παρατηρείται τελευταία, επηρεάζει την κρίση σχετικά με την διαχείριση των προσωπικών δεδομένων;

- Ναι
- Όχι

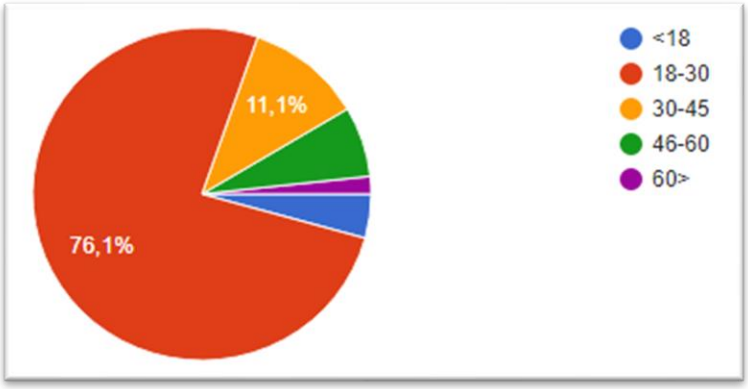
5.4 Ανάλυση ευρημάτων έρευνας

Αφού καταρτίστηκε ο άξονας των ερωτήσεων της έρευνας, στο πρώτο επίπεδο καταγράφηκαν τα δημογραφικά στοιχεία των ερωτηθέντων. Σύμφωνα με αυτά, στο ερωτηματολόγιο συμμετείχαν συνολικά 117 άτομα, από τα οποία 77 ήταν γυναίκες (65,8%) και τα 40 άνδρες (34,2%).



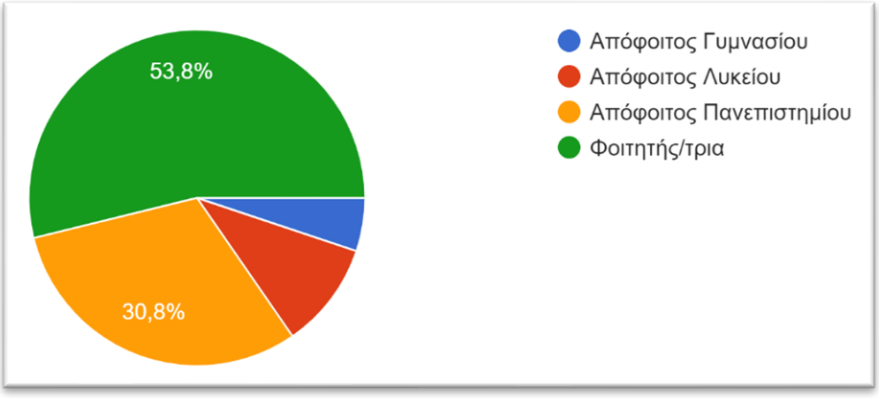
Ερώτηση 1: Φύλο

Έπειτα ρωτήθηκε η ηλικία του δείγματος η οποία χωρίστηκε σε 5 ηλικιακές ομάδες. Το μεγαλύτερο με διαφορά ποσοστό (76,1%) είναι μεταξύ 18 - 30 ετών και ακολουθεί η ηλικιακή ομάδα 30 - 45 ετών (11,1%). Πολύ μικρή ήταν η συμμετοχή ατόμων μεταξύ 46 - 60 ετών (6,8%), κάτω των 18 ετών (4,3%) και άνω των 60 ετών (1,7%).



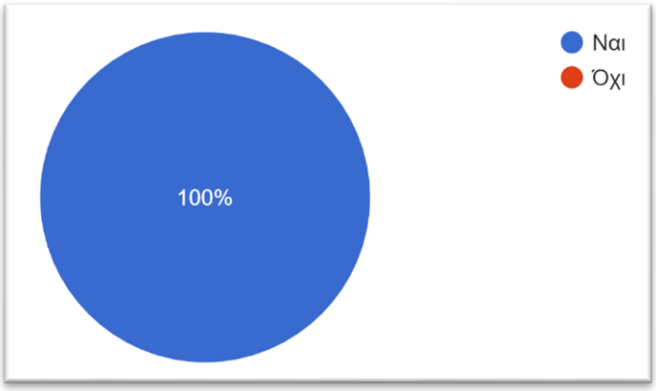
Ερώτηση 2: Ηλικία

Στο παρακάτω διάγραμμα παρατηρούμε το επίπεδο εκπαίδευσης των ερωτηθέντων, το οποίο κατά κύριο λόγο είναι υψηλό, καθώς το 53,8% είναι φοιτητές και το 30,8% απόφοιτοι Πανεπιστημίου. Ακολουθούν με πολύ μικρά ποσοστά οι απόφοιτοι Λυκείου (10,3%) και οι απόφοιτοι Γυμνασίου (5,1%). Ο μεγάλος αριθμός φοιτητών (πάνω από τους μισούς ερωτηθέντες) προέρχεται από το γεγονός ότι το ερωτηματολόγιο αναρτήθηκε σε σελίδα της σχολής μέσω του Facebook και το αίτημα στάλθηκε επίσης κυρίως στη λίστα φίλων των ερευνητών οι περισσότεροι από τους οποίους είναι φοιτητές.



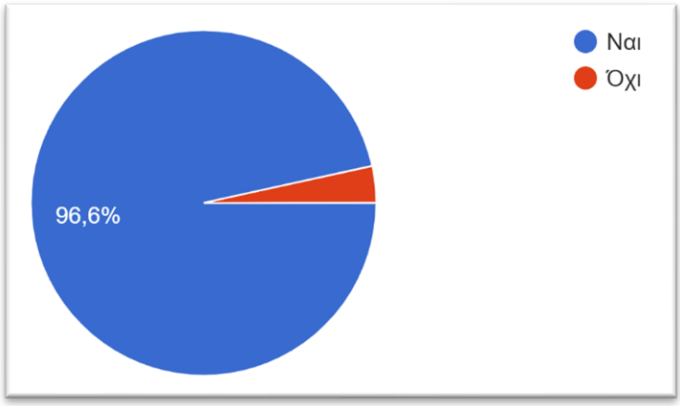
Ερώτηση 3: Μορφωτικό επίπεδο:

Στην συνέχεια ρωτήθηκαν αν γνωρίζουν τον όρο Social Media και απάντησαν Ναι και τα 117 άτομα όπου ήταν ο συνολικός μας αριθμός των ερωτηθέντων. Αυτό μας δείχνει ότι τα Social Media είναι ευρέως διαδεδομένα στο ελληνικό κοινό.



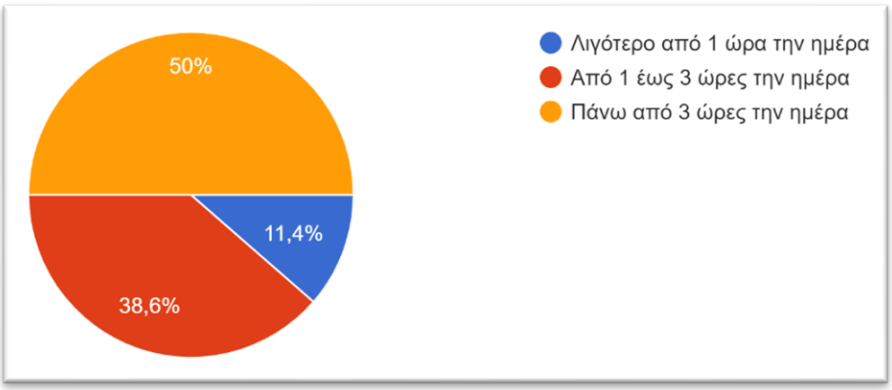
Ερώτηση 4: Σας είναι γνώριμος ο όρος Social Media (Μέσα Κοινωνικής Δικτύωσης);

Όπως είναι πολύ φυσικό, στις μέρες μας οι περισσότεροι χρησιμοποιούν τα Social Media και αυτό φαίνεται επίσης από τα αποτελέσματα της έρευνάς μας. Στην ερώτηση ‘έχετε προσωπικό λογαριασμό σε κάποιο από τα Social Media’ το μεγαλύτερο ποσοστό (96,6%) απάντησε πως έχει και μόνο 4 άτομα (3,4%) απάντησαν πως δεν έχουν κάποιον λογαριασμό. Τα αποτελέσματα ήταν προβλέψιμα αν κρίναμε από την προηγούμενη ερώτηση που σε όλους ήταν γνώριμος ο όρος Μέσα Κοινωνικής Δικτύωσης.



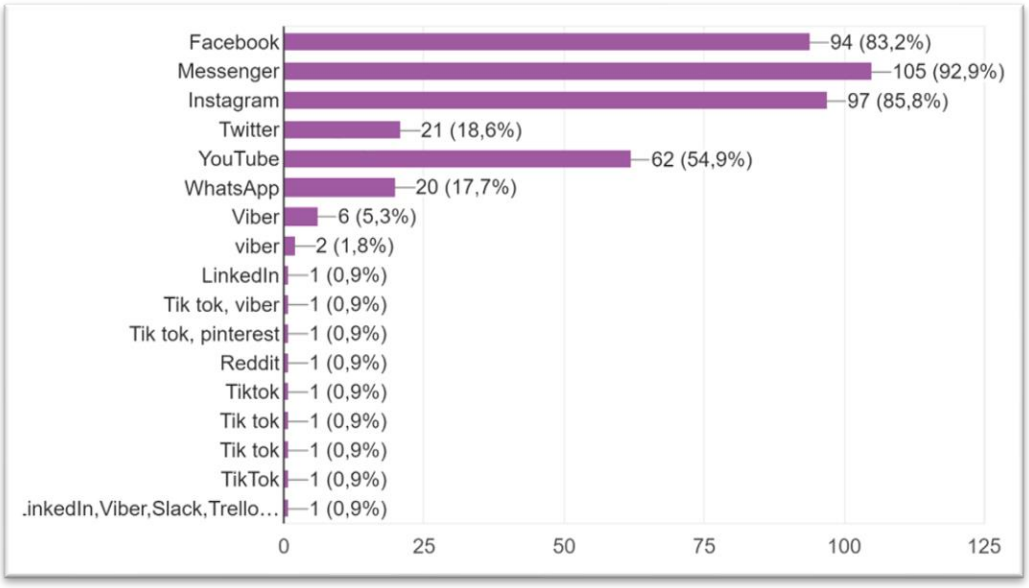
Ερώτηση 5: Έχετε προσωπικό λογαριασμό σε κάποιο από τα Social Media (π.χ. Facebook, Instagram, Twitter, κ.ά.) ;

Η επόμενη ερώτηση απευθυνόταν στα άτομα που στην προηγούμενη απάντησή τους επιβεβαίωσαν ότι διαθέτουν προσωπικό λογαριασμό στα Social Media. Για να κατανοηθεί η συμπεριφορά των χρηστών κοινωνικών δικτύων, οι συμμετέχοντες ρωτήθηκαν για τον χρόνο που αφιερώνουν κατά την περιήγησή τους σε αυτά. Το 50% των ερωτηθέντων απάντησαν ότι κάνουν χρήση πάνω από 3 ώρες την ημέρα, το 38,6% απάντησε ότι τα χρησιμοποιούν από 1 έως 3 ώρες την ημέρα και αξιοσημείωτο είναι ότι μόνο το 11,4% τα χρησιμοποιούν λιγότερο από 1 ώρα την ημέρα. Παρατηρείται λοιπόν εκτεταμένη χρήση καθώς οι περισσότεροι χρήστες αφιερώνουν αρκετό χρόνο της ημέρας τους στα μέσα κοινωνικής δικτύωσης καθώς τα χρησιμοποιούν περισσότερο από τις 3 ώρες.



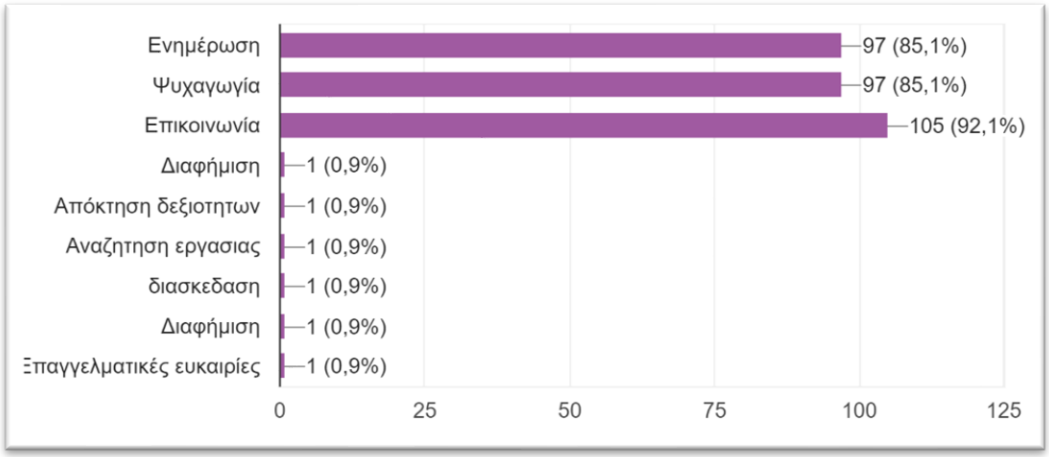
Ερώτηση 6: Αν ναι, πόσο συχνά τα χρησιμοποιείτε;

Όσον αφορά τα Social Media στα οποία διαθέτουν προσωπικό λογαριασμό οι ερωτηθέντες, στην κορυφή βρίσκεται το Messenger με 105 απαντήσεις. Πολύ κοντά συνοδεύει το Instagram με 97 απαντήσεις και με κατά 3 λιγότερες το Facebook. Αρκετά είναι και τα άτομα που διαθέτουν λογαριασμό και στο YouTube, καθώς υπάρχουν 62 απαντήσεις, το οποίο απέχει αρκετά από τα κοινωνικά δίκτυα με τα αρκετά μικρά ποσοστά όπως φαίνονται στο παρακάτω σχήμα. Είναι εύλογο να σημειωθεί ότι τα αποτελέσματα συμπίπτουν με τις αναφορές στο θεωρητικό μέρος της εργασίας. Τα κοινωνικά μέσα με τα υψηλότερα ποσοστά στην έρευνα, είναι αυτά τα οποία σύμφωνα με το Statista αποτελούν τα πιο δημοφιλή κοινωνικά δίκτυα παγκοσμίως.



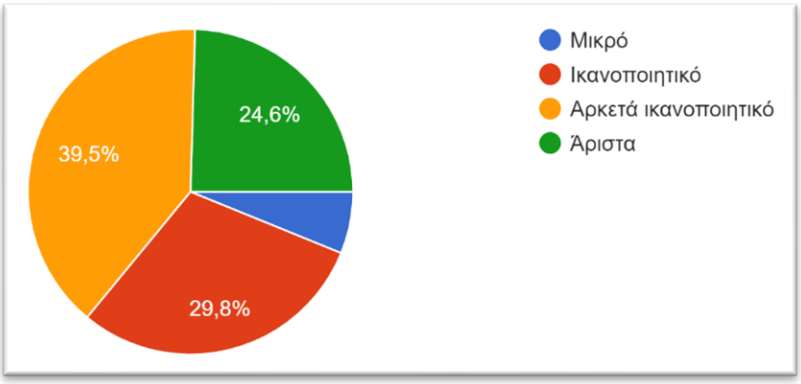
Ερώτηση 7: Σε ποιο από τα παρακάτω Social Media διαθέτετε προσωπικό λογαριασμό;

Εν συνεχεία, το ερώτημα που τέθηκε αφορά την γνώμη τους όσον αφορά την προσφορά των Social Media. Η πλειοψηφία, το 92,1%, επέλεξε επικοινωνία και με ισοδύναμο ποσοστό, 85,1% και τα δύο, ακολουθούν η ενημέρωση και η ψυχαγωγία. Ενώ τα κοινωνικά μέσα είναι πλέον ευρέως γνωστά για την αναζήτηση εργασίας καθώς και τη διαφήμιση οποιασδήποτε επιχείρησης ή επαγγελματικού χώρου, οι ερωτηθέντες σύμφωνα με τις απαντήσεις τους δε φαίνεται να συμφωνούν σε αυτό.



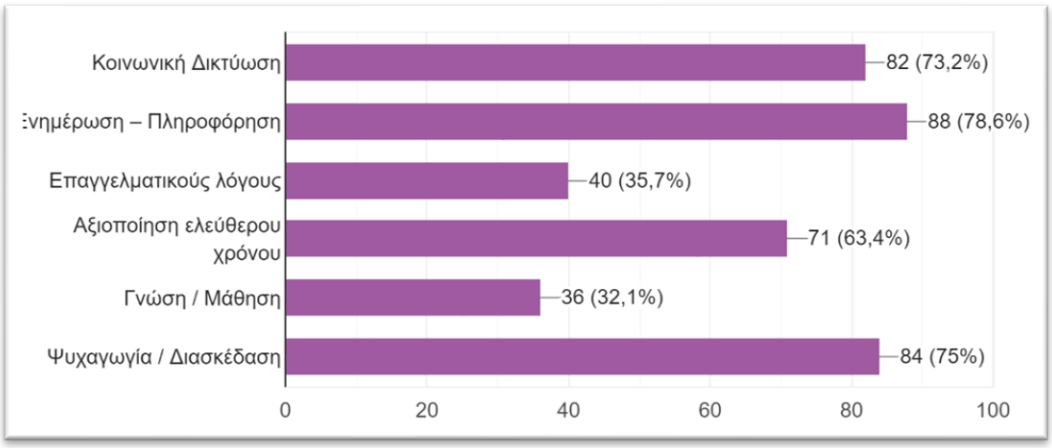
Ερώτηση 8: Τι πιστεύετε ότι μπορούν να προσφέρουν τα Social Media;

Η πλειοψηφία των ερωτηθέντων δήλωσε ότι είναι εξοικειωμένοι στη χρήση των ιστοσελίδων κοινωνικής δικτύωσης. Το 39,5% απάντησε ότι μπορούν να τις χειριστούν αρκετά ικανοποιητικά, το 29,8% ικανοποιητικά, το 24,6% δήλωσε άριστα ενώ μόνο το 6,1% μπορεί να τις χειριστεί σε μικρό βαθμό.



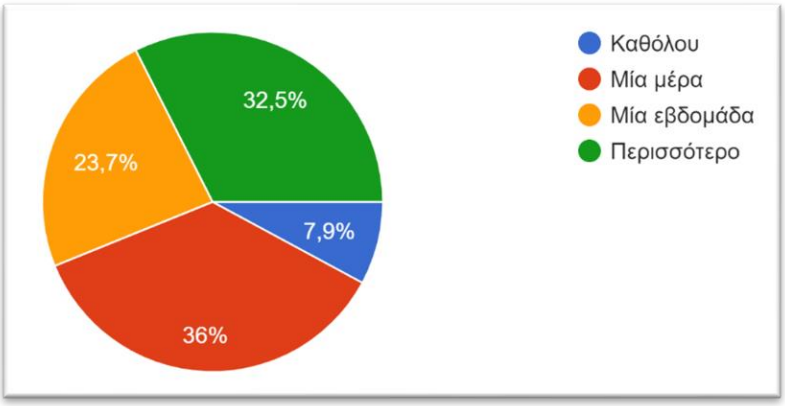
Ερώτηση 9: Σε τι βαθμό μπορείτε να χειριστείτε τις ιστοσελίδες των Social Media;

Στην επόμενη ερώτηση ζητήθηκε από τους ερωτηθέντες να προσδιορίσουν τους λόγους για τους οποίους επισκέπτονται τα μέσα κοινωνικής δικτύωσης. Το παρακάτω σχήμα δείχνει ότι οι χρήστες χρησιμοποιούν τα μέσα κυρίως για λόγους ενημέρωσης και πληροφόρησης (88 απαντήσεις), ψυχαγωγίας και διασκέδασης (84 απαντήσεις), κοινωνικής δικτύωσης (82 απαντήσεις) και τέλος για την αξιοποίηση του ελεύθερου χρόνου (71 απαντήσεις).



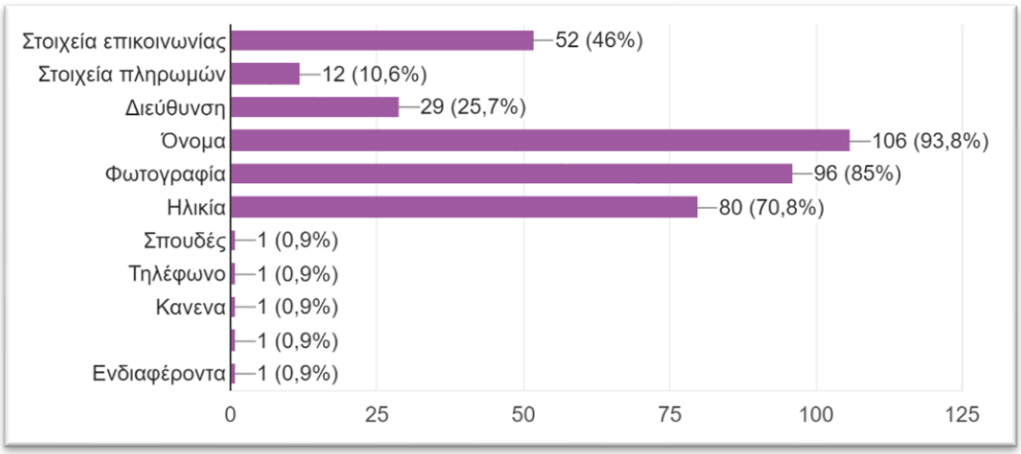
Ερώτηση 10: Ποιοι είναι συνήθως οι λόγοι για τους οποίους επισκέπτεστε τα Social Media;

Συνεχίζοντας την έρευνα, οι χρήστες ρωτήθηκαν πόσο εκτιμούν ότι θα μπορούσαν να μην χρησιμοποιήσουν τα μέσα κοινωνικής δικτύωσης. Τα ποσοστά δείχνουν ότι το 36% θα μπορούσε μόνο μία μέρα, ενώ ακολουθεί αρκετά κοντά το 32% των χρηστών που θα μπορούσαν να μην τα χρησιμοποιήσουν περισσότερο από μία εβδομάδα. Το 23,7% αποκρίθηκε μία εβδομάδα, ενώ ήταν εξαιρετικά λίγοι οι χρήστες (7,9%) οι οποίοι δεν θα μπορούσαν να μην κάνουν χρήση των μέσων κοινωνικής δικτύωσης. Τα ποσοστά της ανάλυσης αυτής δείχνουν ότι τα μέσα κοινωνικής δικτύωσης είναι πλέον αναπόσπαστο κομμάτι της καθημερινότητας των χρηστών καθώς και σε προηγούμενη ανάλυση παρατηρήθηκε η σχετικά υψηλή χρήση τους με το 50% των χρηστών να αφιερώνουν πάνω από 3 ώρες καθημερινά σε αυτά.



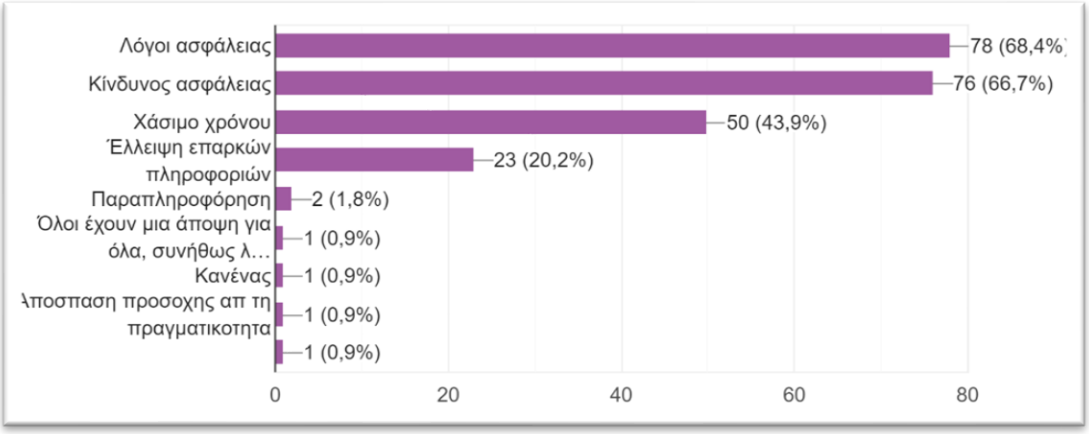
Ερώτηση 11: Πόσο καιρό πιστεύετε θα μπορούσατε να μην χρησιμοποιείτε τα Μέσα Κοινωνικής Δικτύωσης;

Μετέπειτα, ζητήθηκε από τους χρήστες να επιλέξουν τα προσωπικά τους στοιχεία που έχουν δώσει στα μέσα κοινωνικής δικτύωσης. Οι ερωτηθέντες μοιράζονται μεγάλο αριθμό πληροφοριών σχετικά με τον εαυτό τους. Το παρακάτω σχήμα εξηγεί ότι 106 χρήστες έχουν δώσει το όνομά τους, δηλαδή μόνο οι 7 χρήστες δεν έχουν εμφανιστεί με το πραγματικό τους όνομα στα μέσα. Τα προσωπικά στοιχεία που έχουν μοιραστεί η πλεοψηφία των χρηστών, μετά το όνομά τους, είναι φωτογραφίες (85%) και η ηλικία τους (70,8%). Σημαντικό αποτελεί το γεγονός ότι μόνο ένας χρήστης απάντησε ότι δεν έχει μοιραστεί κανένα από τα προσωπικά του στοιχεία. Τα ευρήματα δείχνουν ότι οι ερωτηθέντες είναι κυρίως πρόθυμοι να δώσουν βασικές πληροφορίες και ορισμένα προσωπικά δεδομένα.



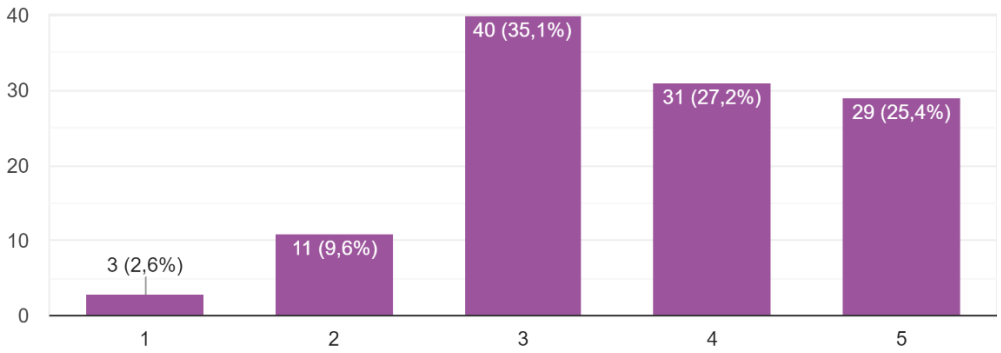
Ερώτηση 12: Ποιο/ποια από τα παρακάτω προσωπικά στοιχεία έχετε δώσει στα Μέσα Κοινωνικής Δικτύωσης;

Προχωρώντας στην έρευνα, διερευνάται η συμπεριφορά των χρηστών σε ζητήματα ιδιωτικότητας και διαχείρισης των προσωπικών τους δεδομένων κατά την επίσκεψή τους στα Social Media. Αναφορικά με τους ενδοιασμούς για την χρήση των κοινωνικών μέσων, οι χρήστες ταυτίστηκαν με τις επιλογές που αφορούν τους λόγους ασφάλειας (68,4%), τον κίνδυνο ασφάλειας (66,7%), καθώς και ένα μεγάλο ποσοστό (43,9%) συμφώνησε στο ότι η χρήση των Social Media πρόκειται για χάσιμο χρόνου.



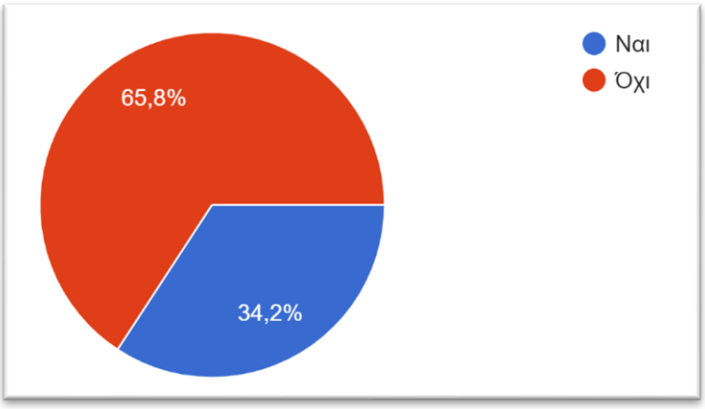
Ερώτηση 13: Ποιοι είναι οι ενδοιασμοί σας για την χρήση των Social Media;

Ο βαθμός ανησυχίας των χρηστών σχετικά με την προστασία της ιδιωτικής τους ζωής εμφανίζεται σχετικά υψηλός, καθώς τα μεγαλύτερα ποσοστά τείνουν προς την υψηλή ανησυχία. Σε κλίμακα από το 1 (χαμηλή ανησυχία) έως το 5 (υψηλή ανησυχία) οι περισσότεροι χρήστες (το 35,1%) απάντησαν το 3, έπειτα το 27,2% επέλεξε το 4 και το 25,4% επέλεξε το 5 (υψηλή ανησυχία), γεγονός που αποδεικνύει ότι οι χρήστες έχουν γνώση των κινδύνων που απειλούν την ιδιωτικότητά τους.Οι υπόλοιποι ερωτηθέντες ανησυχούσαν σε μικρό βαθμό.



Ερώτηση 14: Σε κλίμακα από το 1 έως το 5, σε τι βαθμό εκφράζετε την ανησυχία σας για την προστασία της ιδιωτικής σας ζωής;

Εν συνεχεία, στην ερώτηση για το αν έχουν διαβάσει την πολιτική ασφάλειας των Social Media που χρησιμοποιούν, μεγάλος αριθμός των χρηστών, το 65,8%, δήλωσε όχι. Παρατηρείται ότι παρ' όλη τη μεγάλη ανησυχία που υπάρχει σχετικά με την προστασία της ιδιωτικής τους ζωής, οι χρήστες δεν ενημερώνονται για θέματα ασφάλειας των προσωπικών τους δεδομένων και με αυτό τον τρόπο εκφράζουν την εμπιστοσύνη τους απέναντι στην προστασία των δικαιωμάτων τους.

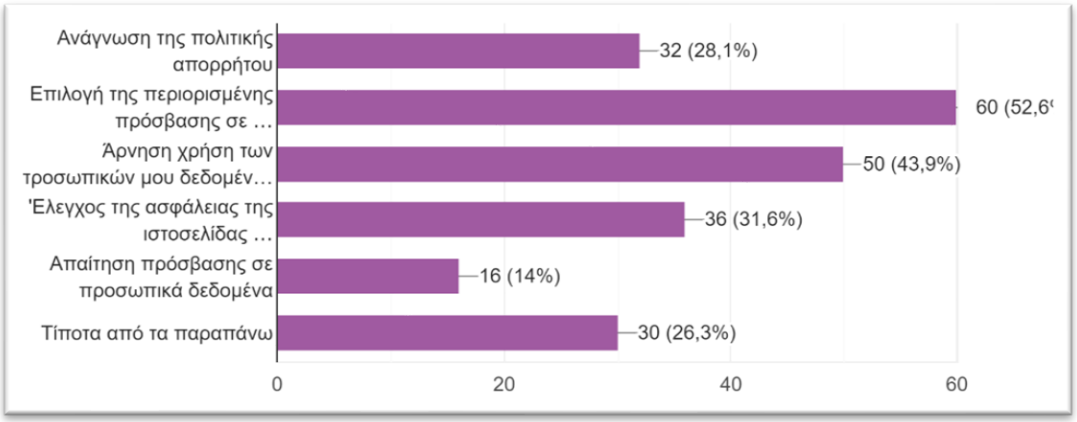


Ερώτηση 15: Έχετε διαβάσει ποτέ την πολιτική ασφάλειας των Social Media που χρησιμοποιείτε;

Στο εν λόγο γράφημα οφείλουμε να δηλώσουμε την ανησυχία μας, καθώς στην ερώτηση αν διαβάζονται οι όροι και οι προϋποθέσεις πριν την χρήση των μέσων βλέπουμε ότι άνω του μισού ποσοστού (50,9%) απάντησε ‘πατάω «Δέχομαι» χωρίς να διαβάσω το κείμενο. Έπειτα με ποσοστό 36% ακουσθούν εκείνοι ο ποιοι απλά περνούν το κείμενο χωρίς κάποιο ουσιαστικό διάβασμα και το λιγότερό ποσοστό κατά 13,2 % διαβάζει όλο το κείμενο.

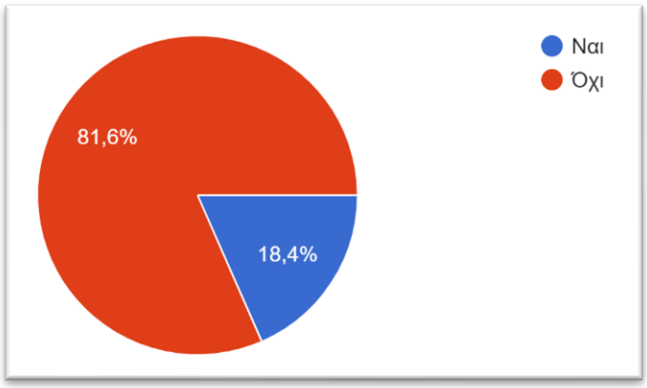
Ερώτηση 16: Διαβάζετε τους όρους και τις προϋποθέσεις πριν την χρήση των μέσων που θα χρησιμοποιήσετε;

Μία πολύ σημαντική ερώτηση στην οποία οφείλουμε να δώσουμε προσοχή, αναφέρετε στο ποιες ενέργειες έχουν προβεί οι χρήστες για να διαχειριστούν τις ρυθμίσεις πρόσβασης σε προσωπικά τους δεδομένα. Βλέπουμε το ότι το μεγαλύτερο ποσοστό 52,6% απάντησε ότι η ενέργεια που κάνει είναι επιλογή της περιορισμένης πρόσβασης σε προσωπικά στοιχεία. Συμπεραίνουμε από αυτό ότι οι περισσότεροι χρήστες έχουν την συνείδηση ότι μπορούν εύκολα να εκτεθούν στον κίνδυνο. Έπειτα με ποσοστό 43,9% έρχεται η απάντηση ότι οι χρήστες επιλέγουν την Άρνηση χρήση των προσωπικών μου δεδομένων για διαφημιστικούς λόγους. Μετά με ποσοστό 31,6% οι χρήστες απάντησαν ότι επιλέγουν τον έλεγχο της ασφάλειας της ιστοσελίδας προτού δώσω τα προσωπικά μου στοιχεία. Μετά ακολουθεί με ποσοστό 28,1% η ανάγνωση της πολιτικής απορρήτου. Και τέλος τα μικρότερα ποσοστά αφορούν την απαντήσεις τίποτα παραπάνω αλλά και την απαίτηση πρόσβασης σε προσωπικά δεδομένα με ποσοστά 26,3% και 14% αντίστοιχα.



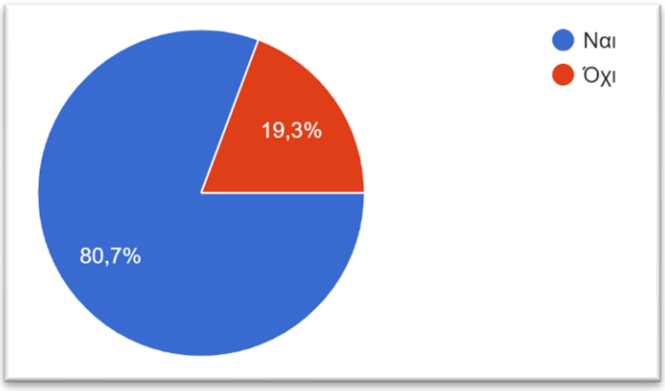
Ερώτηση 17: Σε ποια/ποιες από τις παρακάτω ενέργειες έχετε προβεί για να διαχειριστείτε τις ρυθμίσεις πρόσβασης σε προσωπικά σας δεδομένα;

Το παρακάτω σχήμα παρουσιάζει τα αποτελέσματα στην ερώτηση εάν τα προσωπικά στοιχεία των χρηστών είναι δημόσια κοινοποιημένα στον λογαριασμό τους. Βλέπουμε ότι το μεγαλύτερο ποσοστό έχει απαντήσει πως τα προσωπικά τους στοιχεία δεν είναι δημόσια με ποσοστό 81,6% κάτι το οποίο είναι αρκετά σημαντικό για την αποφυγή κλοπής προσωπικών στοιχείων. Έπειτα η απάντηση 'Ναι' με ποσοστό 18,4% μπορούμε να πούμε πως είναι αρκετά σημαντική όταν οι κίνδυνοι στο διαδίκτυο είναι μεγάλοι.



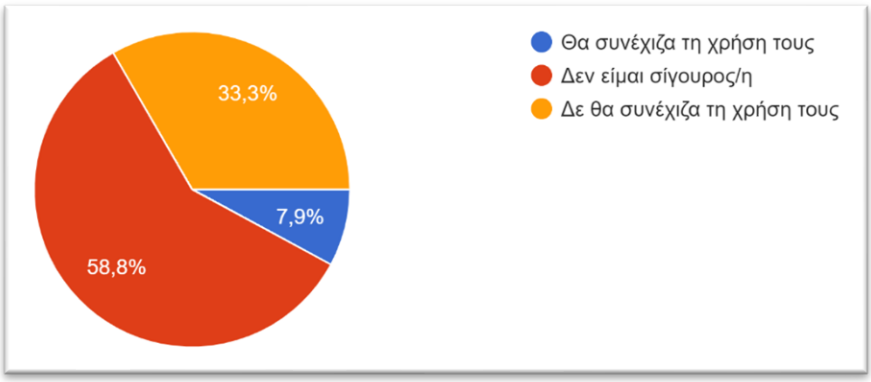
Ερώτηση 18: Τα προσωπικά σας στοιχεία είναι δημόσια κοινοποιημένα στον λογαριασμό σας;

Στην ερώτηση αναφορικά με τις απαραίτητες ρυθμίσεις που έχουν προβεί οι χρήστες ώστε να ελέγχουν σε ποιους είναι ορατά τα στοιχεία που αναρτούν, βλέπουμε ότι το μεγαλύτερο ποσοστό (80,7%) έχει απαντήσει θετικά, πράγμα που σημαίνει ότι εν μέρη μπορούν κατά ένα ποσοστό να ελέγχουν τα προσωπικά τους στοιχεία και νιώθουν μια στοιχειώδη ασφάλεια. Βέβαια δεν είναι μικρό και το ποσοστό που απάντησαν αρνητικά καθώς το 19,3% δεν έχει εκτελέσει τις απαραίτητες ενέργειες και αφήνει τα προσωπικά του στοιχεία εκτεθειμένα.



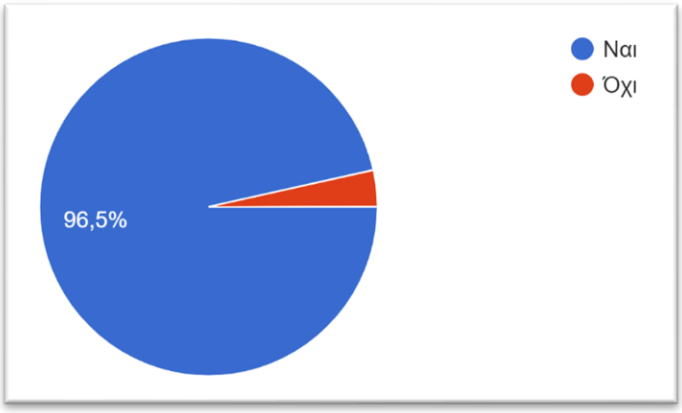
Ερώτηση 19: Έχετε κάνει τις απαραίτητες ρυθμίσεις ώστε να ελέγχετε σε ποιους είναι ορατά τα στοιχεία που αναρτάτε;

Θέλωντας να γνωρίσουμε την στάση των χρηστών απέναντι στο θέμα της ιδιωτιότητας στο διαδίκτυο, τέθηκε η απορία για το αν θα συνέχιζαν να χρησιμοποιούν τα μέσα σε περίπτωση που μάθαιναν ότι παραβιάστηκε η ιδιωτικότητά τους. Ανησυχία εκδηλώνει η απάντηση «Δεν είμαι σίγουρος/η» καθώς κατέχει το μεγαλύτερο και άνω του μισού ποσοστό 58,8%. Έπειτα το 33,3% του ποσοστού απάντησε πως δεν θα συνέχιζαν την χρήση του και τέλος ένα μικρό ποσοστό ,το 7,9%, δηλώνει ότι δεν παύει την χρήση των μέσων.



Ερώτηση 20: Αν μαθαίνατε ότι παραβιάζεται η ιδιωτικότητά σας από τα ίδια τα μέσα, θα συνεχίζατε να τα χρησιμοποιείτε;

Τέλος, εξίσου σημαντική ερώτηση στην οποία οι ερωτηθέντες απάντησαν με την δική τους κριτική σκέψη και άποψη, αφορά τον εθισμό στα Μέσα Κοινωνικής Δικτύωσης και αν θεωρούν ότι επηρεάζει την κρίση των χρηστών σχετικά με την διαχείριση των προσωπικών τους στοιχείων. Με μεγάλη διαφορά η θετική απάντηση των ερωτηθέντων σε ποσοστό 96,5%, μας επιβεβαιώνει τον εθισμό των χρηστών αλλά και τον φόβο έλλειψης ορθής κρίσης τους για την διαχείριση των προσωπικών δεδομένων. Ένα 3,5% των ερωτώμενων απάντησε αρνητικά στην ερώτηση.



Ερώτηση 21: Πιστεύετε ότι ο εθισμός στα Μέσα Κοινωνικής Δικτύωσης που παρατηρείται τελευταία, επηρεάζει την κρίση σχετικά με την διαχείριση των προσωπικών δεδομένων;

Τα αποτελέσματα της έρευνας δείχνουν υψηλό ποσοστό χρήσης των μέσων κοινωνικής δικτύωσης, αλλά οι τρέχουσες ρυθμίσεις απορρήτου χρειάζονται βελτίωση. Αν και δεν υπάρχει πρότυπο για τον έλεγχο των ρυθμίσεων απορρήτου προσωπικών πληροφοριών, συνιστάται οι πάροχοι κοινωνικών δικτύων να σχεδιάσουν ένα σύστημα που προστατεύει τους χρήστες από διαφορετικούς τύπους απειλών και κινδύνων. Επιπλέον, έπειτα από την παρατήρηση ότι οι χρήστες δεν δίνουν ιδιαίτερη σημασία στους όρους και τις προϋποθέσεις χρήσης των κοινωνικών δικτύων, είναι αναγκαίο η παρουσίασή τους να γίνει πιο προσιτή και να απλοποιηθεί για να παρέχει στους χρήστες μία σαφή εικόνα των δεδομένων που θα κοινοποιούνται σε άλλους.

ΚΕΦΑΛΑΙΟ 6 : ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΠΡΟΤΑΣΕΙΣ

Με την τεχνολογία να έχει επηρεάσει την κοινωνία με εκπληκτικούς και καινοτόμους τρόπους, η κοινωνική δικτύωση είναι πλέον μία από τις μεγαλύτερες επιρροές του 21ου αιώνα. Όπως παρουσιάστηκε στην εργασία αυτή, η ανάπτυξη της τεχνολογίας Web 2.0 έφερε ίσως τη μεγαλύτερη επανάσταση στη διαδικτυακή επικοινωνία μέσω της δημιουργίας των μέσων και των ιστότοπων κοινωνικής δικτύωσης. Με συνδυασμό τη σύγχρονη και ασύγχρονη επικοινωνία, οι άνθρωποι τα χρησιμοποιούν για αλληλεπίδραση με άλλους ανθρώπους, με την δημοσίευση προσωπικών φωτογραφιών, βίντεο, πληροφοριών και κειμένων.

Ενώ η χρήση μέσων κοινωνικής δικτύωσης έχει αυξηθεί σημαντικά, οι ανησυχίες σχετικά με το απόρρητο και την ασφάλεια των πληροφοριών του χρήστη έχουν επίσης αυξηθεί. Τέτοιες ανησυχίες δημιουργούνται εξαιτίας της παραβίασης ορισμένων ιστότοπων κοινωνικής δικτύωσης (hacking) οπότε κρίνεται σημαντικό η αντιμετώπισή τους.

Συνέπεια όλων των πλεονεκτημάτων που επιφέρει η τεχνολογία είναι η καταπάτηση της ιδιωτικότητας του σύγχρονου ανθρώπου. Στις μέρες μας, δίνεται μεγάλη προσοχή σε θέματα προστασίας πνευματικής ιδιοκτησίας και εμπιστευτικών δεδομένων. Η προσοχή αυτή επιβάλλεται λόγω των συνεχόμενων επιθέσεων των δεδομένων προσωπικού χαρακτήρα που παρατηρείται σε όλους τους χώρους. Καθώς οι ιστοσελίδες κοινωνικής δικτύωσης απαιτείται να ακολουθούν βασικές αρχές προστασίας των προσωπικών δεδομένων, παρ' όλα αυτά, οι κίνδυνοι της παράνομης χρήσης των δεδομένων αυτών συνεχίζουν να υπάρχουν και είναι ικανοί να βλάψουν το άτομο που τα φέρει. Τέτοιοι κίνδυνοι αφορούν την κλοπή της ταυτότητας του χρήστη και καταλήγουν στην επεξεργασία των προσωπικών του δεδομένων για οποιαδήποτε κακόβουλη χρήση τους.

Λόγω της εμφάνισης όλο και περισσότερων κινδύνων, από την αυξανόμενη χρήση των μέσων κοινωνικής δικτύωσης, η παγκόσμια κοινότητα προσπαθεί όλο και πιο πολύ να μειώσει τις επιπτώσεις τους και να δημιουργήσει μία ασφαλή προστασία των προσωπικών δεδομένων. Αυτό επιτυγχάνεται μέσα από την υιοθέτηση μέτρων προστασίας που περιλαμβάνουν την ανάπτυξη παγκόσμιων κανονισμών και διεθνών, εθνικών ή και τοπικών νομοθεσιών. Παρ' όλα αυτά, είναι απαραίτητο να παρθούν και αντίμετρα προστασίας της ιδιωτικότητας και των προσωπικών δεδομένων και από την μεριά του χρήστη. Για τον λόγο αυτό, έρχονται να προστεθούν συμβουλές για την ορθότερη χρήση των ιστοσελίδων κοινωνικής δικτύωσης πάνω σε θέματα ασφάλειας και απορρήτου.

Παρακάτω αναφέρεται ένας δεκάλογος συμβουλών για την σωστή χρήση και τον έλεγχο των προσωπικών δεδομένων στα μέσα κοινωνικής δικτύωσης:

1. Μη δημοσιεύετε ευαίσθητες πληροφορίες, όπως για παράδειγμα: διεύθυνση κατοικίας, αριθμό τηλεφώνου, φωτογραφίες της κατοικίας σας, επωνυμία της εταιρείας που εργάζεστε κ.ά..

2. Συχνή αλλαγή και χρήση ισχυρού κωδικού πρόσβασης/συνθηματικού στους προσωπικούς λογαριασμούς (π.χ. email, Facebook, e-banking κ.λπ.).

3. Κατά τη σύνδεση σε προσωπικό λογαριασμό με τη χρήση συνθηματικών, μην παραλείπετε έπειτα την αποσύνδεσή σας από τις ιστοσελίδες και κυρίως από ηλεκτρονικές συσκευές τρίτων ατόμων.

4. Διαβάστε προσεκτικά τις πολιτικές των εφαρμογών που χρησιμοποιείτε οι οποίες ζητούν την πρόσβαση στην τοποθεσία σας.

5. Σημαντικό παράγοντα αποτελεί ο έλεγχος της πολιτικής απορρήτου που χρησιμοποιεί κάθε ιστοσελίδα που επισκέπτεστε. Ενημερωθείτε για τις ενέργειες που πρόκειται να κάνουν οι σελίδες αυτές χρησιμοποιώντας τα προσωπικά σας δεδομένα. Τέτοιες ενέργειες μπορεί να είναι η αποθήκευση αρχείων cookies, η χρήση των δεδομένων για στατιστικά αποτελέσματα ερευνών, ακόμα και η προώθησή τους σε διαφημιστικές εταιρείες.

6. Αποφυγή επικοινωνίας με άγνωστα άτομα μη γνωρίζοντας τον απώτερο σκοπό τους. Ενώ οι ιστότοποι κοινωνικής δικτύωσης είναι ιδανικοί για δημιουργία νέων φίλων και τη διατήρηση της επικοινωνίας τους, είναι επίσης ένα όφελος για όσους θέλουν να συλλέξουν προσωπικές πληροφορίες, για οποιονδήποτε σκοπό.

7. Σε περίπτωση αμφιβολίας, απορρίψτε το: Οι σύνδεσμοι σε email, tweets, δημοσιεύσεις και διαφημίσεις στο διαδίκτυο είναι συχνά ο τρόπος με τον οποίο οι κυβερνο-εγκληματίες προσπαθούν να κλέψουν τα προσωπικά σας στοιχεία. Ακόμα κι αν γνωρίζετε την πηγή, αν κάτι φαίνεται ύποπτο, διαγράψτε το.

8. Μείνετε ενήμεροι σε θέματα χρήσης των μέσων κοινωνικής δικτύωσης. Εκμεταλλευτείτε οποιαδήποτε ενέργεια ρύθμισης απορρήτου, προσαρμόστε το κοινωνικό μέσο όπως επιθυμείτε έτσι ώστε να νιώθετε ασφαλείς κατά τη χρήση του.

9. Σκεφτείτε το καλά πριν δημοσιεύσετε κάποια πληροφορία ή φωτογραφία στον προσωπικό σας λογαριασμό. Ακόμα και αν διαγράψετε κάτι, αυτό παραμένει στο διαδίκτυο για καιρό ή να έχει χρησιμοποιηθεί ήδη από κάποιον τρίτο χρήστη.

10. Διαβάστε προσεκτικά τα “ψιλά γράμματα”. Πολλοί είναι αυτοί που διαλέγουν να αναφέρουν τους όρους χρήσης των δεδομένων με αυτόν τον τρόπο. Αυτό κυρίως παρατηρείται κατά τη χρήση πληροφοριών για διαφημιστικούς σκοπούς όπου η συγκατάθεσή σας επιβάλλεται.

Βιβλιογραφία

Άρθρο 4 – Γενικός Κανονισμός για την Προστασία Δεδομένων – Ορισμοί. Ανακτήθηκε: 12/10/2020 από https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-4-genikos-kanonismos-gia-tin-prostasia-dedomenon-orismoi

Αστανάστας, Ε. (2015). Τα 4 είδη Malware (κακόβουλα λογισμικά) που κυκλοφορούν σήμερα. Ανακτήθηκε την 9η Οκτωβρίου 2020 από https://www.safer-internet.gr/ta-4-eidi-malware-pou-kukloforoun/

Βικιπαίδεια (2019). Ιδιωτικότητα. Ανακτήθηκε την 12η Οκτωβρίου 2020 από https://el.wikipedia.org/wiki/Ιδιωτικότητα

Βικιπαίδεια. Ασφάλεια πληροφοριακών συστημάτων. Ανακτήθηκε την 13η Οκτωβρίου 2020 από https://el.wikipedia.org/wiki/Ασφάλεια_πληροφοριακών_συστημάτων.

Γεωργιάδης, Χ. Κ. (2015). Κεφάλαιο 3: Ασφαλείς Συναλλαγές στον Παγκόσμιο Ιστό. Ανακτήθηκε την 25η Αυγούστου 2020 από http://repfiles.kallipos.gr/html_books/9536/Chapter%203/Chapter03.html

Γρίβας, Α. (2018). GDPR: Τι Είναι Και Σε Ποιους Απευθύνεται. Ανακτήθηκε την 23η Αυγούστου 2020 από https://grillmagazine.gr/2018/08/11/gdpr-τι-είναι-και-σε-ποιους-απευθύνεται/

Δεμερτζής, Ν., Μανδενάκη, Κ., Τσέκερης, Χ. (2020). Ιδιωτική ζωή και επιτήρηση στο Διαδίκτυο: Η εποχή της μετα-ιδιωτικότητας (Private life and surveillance in the internet: The age of post privacy). Τεύχος 32, 1-40.

Δρογκάρης, Κ. Π. (2013). Ασφάλεια και Προστασία της Ιδιωτικότητας σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης (Διδακτορική Διατριβή). Πανεπιστήμιο Αιγαίου, Σάμος.

Δροσανάκης, Γ. (2018). Μέσα Κοινωνικής Δικτύωσης (Social Media): πλεονεκτήματα και μειονεκτήματα των μέσων κοινωνικής δικτύωσης και ο εθισμός σε αυτά (Πτυχιακή εργασία). Τ.Ε.Ι. Κρήτης.

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Ανακτήθηκε: 15/10/2020 από https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679

Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης. Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου. Ανακτήθηκε: 15/10/2020 από https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&

Θεοδωρίδου, Δ. (2018). Τι είναι ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (General Data Protection Regulation). Τεύχος 30. Ανακτήθηκε την 16η Οκτωβρίου 2020 από https://www.accountancygreece.gr/τι-είναι-ο-γενικός-κανονισμός-προστασ/

Θεοδώρου, Α. (2016). Μέθοδοι ανίχνευσης προσωπικών δεδομένων στο Διαδίκτυο και τεχνικές για την προστασία τους από κακόβουλους χρήστες (Πτυχιακή εργασία). Τ.Ε.Ι. Κρήτης, Ηράκλειο.

Καρφοπούλου, Κ. (2012). Τα κοινωνικά δίκτυα και η ιδιωτικότητά τους. Αλεξάνδρειο Τ.Ε.Ι. Θεσσαλονίκης.

Κοτσώνη, Μ. (2018). Η προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση: η διατήρηση μιας online ιδιωτικότητας. Ανακτήθηκε την 22η Σεπτεμβρίου 2020 από https://thesafiablog.com/2018/12/10/analysis_kotsoni/.

Κουμτζής, Μ. (2016). Προστασία προσωπικών δεδομένων στις υπηρεσίες κοινωνικής δικτύωσης. Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

Κυριάκης, Σ. (2015). Προστασία της Ιδιωτικότητας στα Κοινωνικά Δίκτυα. Πανεπιστήμιο Πειραιά.

Κωνσταντινίδου, Μ. (2017). Η ασφάλεια των προσωπικών δεδομένων στα κοινωνικά δίκτυα στην Ελλάδα. Πανεπιστήμιο Πελοποννήσου.

Λαχανά, Φ. (2019). Διεθνείς νομοθεσίες του 2019 για την ιδιωτικότητα και τα προσωπικά δεδομένα. Ανακτήθηκε την 25η Νοεμβρίου 2020 από https://dpo.ert.gr/blog/deontologia/arthrografia/diethneis-nomothesies-toy-2019-gia-tin-idiotikotita-kai-ta-prosopika-dedomena/

Μανούσου, Ε. & Χαρτοφύλακα, Τ. (2011). Κοινωνικά δίκτυα και μέσα κοινωνικής δικτύωσης στην εξ αποστάσεως τριτοβάθμια εκπαίδευση. Ένταξη και Χρήση των ΤΠΕ στην Εκπαιδευτική Διαδικασία. 2ο Πανελλήνιο Συνέδριο, Πάτρα.

Μήτρου, Λ. (2010). Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες : Η νομική διάσταση. Πανεπιστήμιο Αιγαίου.

Νέφρου, Δ. & Ντούσσα, Β. & Παππά, Π. (2017). Από το Web 1.0 στο Web 3.0 (Πτυχιακή εργασία). Τ.Ε.Ι. Δυτικής Ελλάδας, Πάτρα.

Νικήτα, Ν. (2018). Το νομικό και ρυθμιστικό πλαίσιο προστασίας των προσωπικών δεδομένων: ζητήματα προστασίας στον τομέα της υγείας (Διδακτορική Διατριβή). Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, Αθήνα.

Ντράχας, Δ. (2019). Η Χρήση των μέσων κοινωνικής δικτύωσης κατά την διάρκεια της εργασίας αίτια και αποτέλεσμα (Μεταπτυχιακή εργασία). Πανεπιστήμιο Θεσσαλίας, Βόλος.

Παναγιωτοπούλου, Φ. Ν. (2015). Η ψηφιακή τεχνολογία, το διαδίκτυο και η κοινωνική δικτύωση: Η διάδραση μεταξύ των ιστοτόπων, των μέσων κοινωνικής δικτύωσης και των κοινωνικών κινημάτων (Διπλωματική εργασία). Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα.

Παπαδοπούλου, Γρ. Β. & Μονιάς, Ν. (2018). WEB 2. Τεχνολογική ή κοινωνική επανάσταση;. Εφαρμοσμένη Παιδαγωγική, Περιοδική Ηλεκτρονική Έκδοση του Ελληνικού Ινστιτούτου Εφαρμοσμένης Παιδαγωγικής και Εκπαίδευσης (ΕΛΛ.Ι.Ε.Π.ΕΚ.), Τεύχος 9.

Παπαποστόλου, Α. Σ. (2017). Κατηγοριοποίηση με μηχανές διανυσμάτων υποστήριξης (Διπλωματική εργασία). Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Θεσσαλονίκη

Ρίκας, Ι. (2015). Προστασία της ιδιωτικότητας σε Social Networks και πλατφόρμες όπως το Facebook κ.λπ.. Πανεπιστήμιο Πειραιώς.

Ρουμελιώτη, Μ. Μέσα κοινωνικής δικτύωσης: Η σύγχρονη δημοκρατία των νέων τεχνολογιών. Academia. Ανακτήθηκε την 19η Οκτωβρίου 2020 από https://www.academia.edu/1639955/Μέσα_κοινωνικής_δικτύωσης_Η_σύγχρονη_συμμετοχική_δημοκρατία_των_νέων_τεχνολογιών_

Σουλούκου, Δ. (2019). Επίδραση των κοινωνικών μέσων δικτύωσης στις ευκαιρίες απασχόλησης στην Ελλάδα (Μεταπτυχιακή εργασία). Ανοικτό Πανεπιστήμιο Κύπρου.

Σχέδιο Νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα. ΚΕΦΑΛΑΙΟ Α'- Γενικές Διατάξεις – Άρθρο 1 Σκοπός του νόμου. Υπουργείο Δικαιοσύνης. Ανακτήθηκε την 24η Οκτωβρίου 2020 από http://www.opengov.gr/ministryofjustice/?p=10647

Σωφρονάς, Η. (2015). Τεχνικές Εξόρυξης Δεδομένων. Μελέτη Εφαρμογής της Εξόρυξης Δεδομένων στον Αθλητισμό με Χρήση του Λογισμικού Weka (Διπλωματική εργασία). Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα.

Τζικόπουλος, Α. (2013). Ηλεκτρονικά μέσα κοινωνικής δικτύωσης (social media). Εκδόσεις Γενικής Γραμματείας Διά Βίου Μάθησης.

Τικπασανούδη, Α. (2019). Αξιοποίηση των κοινωνικών δικτύων στην παιδαγωγική διαδικασία από εκπαιδευτικούς της πρωτοβάθμιας εκπαίδευσης (Διπλωματική εργασία). Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Θεσσαλονίκη.

Το κακόβουλο botnet Emotet ξαναχτυπά και μάλιστα αυτή τη φορά οι επιθέσεις αφορούν μεγάλο αριθμό χρηστών στην Ελλάδα. (2020, 29 Οκτωβρίου). Ανακτήθηκε από https://www.eset.com/gr/about/newsroom/press-releases-gr/to-kakoboylo-botnet-emotet-xanachtypa-kai-malista-ayti-ti-fora-oi-epitheseis-aforoyn-megalo-arithmo-chri/

Τσίτσικα, Κ. Α. (2014). Προτάσεις και λύσεις για την ασφαλή χρήση του διαδικτύου. Ανακτήθηκε την 17η Νοεμβρίου 2020 από http://youth-health.gr/thematikes-

enotites/genika-gia-tin-efibeia/protaseis-kai-luseis-gia-tin-asfali-xrisi-tou-diadiktuou/#.X6EwS5BxeM8

Abhishek, K. & Subham, K. G. & Animesh, K.R. & Sapna, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4).

Ajami, R. & Ramadan, N. & Mohamed, N. & Al-Jaroodi, J. (2011). Security Challenges and Approaches in Online Social Networks: A Survey. IJCSNS International Journal of Computer Science and Network Security Manuscript, Vol 11.

Alalawi, N. & Al-Jenaibi, B. (2016). Social Network and Privacy. J Mass Communicat Journalism, 6(1).

Aldhafferi, N. & Watson, C. & Sajeev, A.S.M. (2013). Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. International Journal of Security, Privacy and Trust Management (IJSPTM), 2(2).

Almarabeh, H., & Sulieman, A. (2019). The impact of cyber threats on social networking sites. International Journal of Advanced Research in Computer Science, 10(2).

Barnes, S. B. (2006). A Privacy Paradox: Social networking in the United States. First Monday, 11(9). https://doi.org/10.5210/fm.v11i9.1394

Blasbalg, J. & Cooney, R. & Fulton, S. (2012). Defining and exposing privacy issues with social media. Consortium for Computing Sciences in Colleges, 28(2), 6-14.

Choudhury, N. (2014). World Wide Web and Its Journey from Web 1.0 to Web 4.0. International Journal of Computer Science and Information Technologies. 5(6).

Cohn, M. (2011). Social Media vs Social Networking. Ανακτήθηκε την 20η Σεπτεμβρίου 2020 από https://www.compukol.com/social-media-vs-social-networking/

Crosman, P. (2020) Coronavirus phishing scams proliferate. Ανακτήθηκε την 19η Οκτωβρίου 2020 από https://www.americanbanker.com/news/coronavirus-phishing-scams-proliferate

Davis, M. (2007). Semantic Social Computing. Network Centric Operations Industry Consortium.

Dean, B. (2020). Social Network Usage & Growth Statistics: How Many People Use Social Media in 2020? Ανακτήθηκε την 26η Νοεμβρίου 2020 από https://backlinko.com/social-media-users#most-popular-social-media-platforms-in-2020

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. IEEE Communications Surveys & Tutorials, 16(4), 2019-2036.

Garton, L. & Haythornthwaite, C. & Wellman, B. (1997). Studying Online Social Networks. Journal of Computer-Mediated Communication. 3(1).

Hiat, D., Young, B. (2016). Role of Security in Social Networking. International Journal of Advanced Computer Science and Applications, Vol 7.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56-59.

Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizon, 53(1), 59-68.

Kaplan, A. M. & Haenlein, M. (2014). Collaborative projects (social media application): About Wikipedia, the free encyclopedia. Business Horizon, 57(5), 617-626.

Kekulluoglu, D., Kokciyan, N., & Yolum, P. (2018). Preserving privacy as social responsibility in online social networks. ACM Transactions on Internet Technology (TOIT), 18(4), 1-22.

Kenton, Will. (2021, February 23). Social Networking. Ανακτήθηκε από https://www.investopedia.com/terms/s/social-networking.asp

Key Social Media Privacy Issues for 2020. Ανακτήθηκε από https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020

Kozlowska, Iga (2018). Facebook and Data Privacy in the Age of Cambridge Analytica. Ανακτήθηκε την 15η Ιανουαρίου 2021 από https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 39(5), 22-31.

Lindsey, N. (2019). New Research Study Shows That Social Media Privacy Might Not Be Possible, CPO Magazine, Ανακτήθηκε την 3η Σεπτεμβρίου 2020 από https://www.cpomagazine.com/data-privacy/new-research-study-shows-that-social-media-privacy-might-not-be-possible/

Naughton, J. (2016). The evolution of the Internet: from military experiment to General Purpose Technology. Journal of Cyber Policy, 1(1), 5-28.

Obiniyi, A. A., Oyelade, O. N., & Obiniyi, P. (2014). Social network and security issues: Mitigating threat through reliable security model. International Journal of Computer Applications, 103(9).

Perrin, A. (2018). Americans are changing their relationship with Facebook. Pew Research Center. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Quinn, K., & Epstein, D. (2018, July). # MyPrivacy: how users think about social media privacy. In Proceedings of the 9th International Conference on Social Media and Society (pp. 360-364).

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. Information sciences, 421, 43-69.

Rehman, Ikhlaq ur (2019). Facebook-Cambridge Analytica data harvesting: What you need to know. Library Philosophy and Practice (e-journal). 2497.

Romansky, R. (2014). Social Media and Personal Data Protection. International Journal on Information Technologies and Security, 6(4), 65-80.

Schneier, B. (2010). A Taxonomy of Social Networking Data. Ανακτήθηκε την 30η Οκτωβρίου 2020 από https://www.schneier.com/essays/archives/2010/07/a_taxonomy_of_social.html

Social Media. Merriam-Webster.com Dictionary, Merriam-Webster. Ανακτήθηκε την 27η Οκτωβρίου 2020 από https://www.merriam-webster.com/dictionary/social%20media

Statista (2020). Social media - Statistics & Facts. Ανακτήθηκε την 29η Οκτωβρίου 2020 από https://www.statista.com/topics/1164/social-networks/

Statista (2020). Most popular social networks worldwide as of July 2020, ranked by number of active users. Ανακτήθηκε την 29η Οκτωβρίου 2020 από https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Sykora, M. (2017). Web 1.0 to Web 2.0: an observational study and empirical evidence for the historical r(evolution) of the social web. International Journal of Web Engineering and Technology, 1(12), 70-94.

Twitter Inc. (2020, July 18). An update on our security incident. Ανακτήθηκε από https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

Tyagi, R. (2020). Twitter Breach: Massive Cyber Attack of 2020. Ανακτήθηκε την 10η Δεκεμβρίου από https://www.teceze.com/twitter-breach-massive-cyber-attack-of-2020?fbclid=IwAR0fzLBUmg8e71OLjQZkZsY4WI1t3X4OIK3zWDvd1qcbtoYSsdJfhXMwxxA

Vogt, P., Nentwich, F., Jovanovic, N., Kirda, E., Kruegel, C., & Vigna, G. (2007). Cross site scripting prevention with dynamic data tainting and static analysis. In NDSS, p. 12.

Weisman, S. (2020). What is a distributed denial of service attack (DDoS) and what can you do about them? Ανακτήθηκε από https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

Wikipedia (2020). Internet Privacy. Ανακτήθηκε την 21η Οκτωβρίου 2020 από https://en.wikipedia.org/wiki/Internet_privacy

Zhang, J. (2010). Social media and distance education.

Zuckerberg, M. (2018, March 21). I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue. We have a responsibility to protect your data, and if we can't then we [Facebook status update]. https://www.facebook.com/zuck/posts/10104712037900071?pnref=story