ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΜΟΝΑΔΩΝ ΥΓΕΙΑΣ ΚΑΙ ΠΡΟΝΟΙΑΣ
ΑΚΑΔΗΜΑΙΚΟ ΕΤΟΣ 2018-2019

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Κοινωνικά Δίκτυα

&

Προστασία Προσωπικών Δεδομένων

ΣΠΟΥΔΑΣΤΗΣ:ΜΠΑΣΔΕΚΗΣ ΔΗΜΗΤΡΙΟΣ (Α.Μ. D2014084)

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: κος Κοτσιλιέρης Θεόδωρος

Πρόλογος

Διανύουμε την εποχή μιας νέας οικουμενικής ψηφιακής πολιτείας όπου αυτή, έχει χαρακτηρισθεί ως «ψηφιακή εποχή» από τη χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου. Τα ανωτέρω συνετέλεσαν στην αλματώδηανάπτυξη και χρήση των ιστοσελίδων κοινωνικής δικτύωσης,όπου με τη δυναμική «εισβολή» τους στην καθημερινότητά μαςπροωθούν έναν νέο τρόπο επικοινωνίας, μετάδοσης και διαμοιρασμού των πληροφοριών παγκοσμίως. Και ενώ οι ιστοσελίδες κοινωνικής δικτύωσης αποτελούν πλέον ένα μεγάλο μέρος της καθημερινής μας ζωής, εμφανίζεται όμως μεγάλος ο «κίνδυνος» για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων όλων των απανταχού χρηστών αυτών. Χρειάζεται λοιπόν αφενός να ληφθούν τα κατάλληλα μέτρα ώστε να προστατευθεί η προσωπική ζωή των χρηστών και αφετέρου να αλλάξει η στάση τους, προσεγγίζοντας τη χρήση τους με μεγαλύτερη σύνεση και στοχεύοντας στην καλύτερη ενημέρωσή τους για την επίτευξη της αυτοπροστασία τους.

Είναι σημαντικό να ευχαριστήσω τον επιβλέποντα καθηγητή κοΚοτσιλιέρη Θεόδωρο, που μου υπέδειξε χρήσιμη βιβλιογραφία και με καθοδήγησε με τις σημαντικές παρατηρήσεις του, ώστε να ολοκληρώσω την εκπόνηση της πτυχιακής μου εργασίας.

«Υπεύθυνη Δήλωση και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο «ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΑΝΘΡΩΠΙΝΩΝ ΔΙΚΑΙΩΜΑΤΩΝ» αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφιών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο δηλών

Μπασδέκης Δημήτρης

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Ιστορική Ανασκόπηση

Η εμφάνιση των μέσων κοινωνικής δικτύωσης (social networks) αποτελεί το νέο κοινωνικό φαινόμενο που συνεχώς εξελίσσεται και το οποίο άρχισε να διαδραματίζεται πολλά χρόνια πριν. Πρόκειται για τη φυσική εξέλιξη των παραδοσιακών μέσων μαζικής επικοινωνίας (ΜΜΕ) που αφορούν την παροχή-μετάδοση των πληροφοριών μέσω της έντυπης, ακουστικής και οπτικής μορφής, όπως είναι η εφημερίδα, το ραδιόφωνο, η τηλεόραση, αποτελώντας ένα εξελιγμένο μέσο το οποίο συνδυάζει δύο κριτήρια, αυτό της μαζικής ενημέρωσης με εκείνο της επικοινωνίας.

Και ενώ τα παραδοσιακά μέσα μαζικής επικοινωνίας δημιουργούν κανάλια επικοινωνίας με την παροχή πληροφορίας μιας κατεύθυνσης, η έλευση του Web 2.0 έδωσε το πρωταρχικό στοιχείο της διαδραστικότητας και της αλληλεπίδρασης στον τρόπο επικοινωνίας και ενημέρωσης σε διαδικτυακό περιβάλλον, αποτελώντας έτσι το χαρακτηριστικό σημείο αιχμής για την ανάπτυξη των κοινωνικών δικτύων. Από την άλλη πλευρά το internet από μόνο του αποτέλεσε ένα ξεχωριστό κοινωνικό δίκτυο έχοντας καταφέρει να φέρει σε επαφή ανθρώπους από διαφορετικά σημεία και τοποθεσίες του πλανήτη, ξεπερνώντας τα γεωγραφικά σύνορα.

Η δημιουργία των κοινωνικών δικτύων βασίστηκε στην ιδέα της ηλεκτρονικής σύνδεσης μεμονωμένων ηλεκτρονικών υπολογιστών και κατά τις αρχικές προσπάθειες δημιουργήθηκαν τα USENET,APRANET όπως και υπηρεσίες bulletin (BBS). Μερικά χαρακτηριστικάορόσημα (milestones) των μέσων κοινωνικής δικτύωσης είναι τα εξής:

το 1971 στάλθηκε το πρώτο e-mail, το 1985 εμφανίστηκε ένα από τα πρώτα chat-rooms (THEWELL) και το 1994εμφανίζεται η εταιρία διαδικτυακών υπηρεσιών YAHOO. Αργότερα, το 2003 κάνει εμφάνιση στο διαδίκτυο ο ιστοχώρος LINKEDIN, το 2004 ιδρύεται ένα δημοφιλές διαδικτυακό μέσο επικοινωνίας, ενημέρωσης και κοινωνικής δικτύωσης το FACEBOOK, οποίο μέχρι αυτή τη στιγμή χρησιμοποιείται από εκατομμύρια χρήστες σε όλο το πλανήτη.

Ένα χρόνο αργότερα το 2005, δημιουργείται ο διαδικτυακός τόπος YouTube, για την αναπαραγωγή και αποθήκευση βίντεο, ταινιών, μουσικής. Το 2006 εμφανίζεται το TWITTER, με κύριο χαρακτηριστικό την ενημέρωση.

Παγκοσμιοποίηση και Πληροφορία

Η παγκοσμιοποίηση σε συνδυασμό με το διαδίκτυο έφερε τεράστιες αλλαγές στην επικοινωνία, η οποία επηρέασε την ίδια την πληροφόρηση αλλά και τους χρήστες αυτής.

Η προμήθεια της πληροφορίας ξεκίνησε να διαδίδεται σε ένα ευρύ φάσμα κοινού στο παγκόσμιο στερέωμα. Η διαδραστικότητα των χρηστών μέσω κοινωνικών δικτύων επέτρεψε τη διάδοση της πληροφορίας σε παγκόσμιο επίπεδο όπου, εκατομμύρια χρήστες χρησιμοποιούν το διαδίκτυο για διαφορετικές ανάγκες ο καθένας όπως: την επικοινωνία, ενημέρωση, εκπαίδευση, οικονομία αλλά και για διάφορους επαγγελματικούς λόγους που αποφέρει έσοδα. Στην πορεία του χρόνου όμως, με την αυξημένη συχνότητα χρήσης και την απανταχού χρήση των Κοινωνικών Δικτύων, η ποσότητα και η ευαισθησία των δεδομένων του κάθε χρήστη που είναι αποθηκευμένα αλλά και στη συνέχεια αποθηκεύονται σε αυτά, αυξήθηκε επίσης σε τρομερό βαθμό, εγείροντας ανησυχίες και διλήμματα για την προστασία, ασφάλεια που παρέχεται και τη χρήση τους.

Το γεγονός αυτό από μόνο του, αλλά και σε συνδυασμό με την εξέλιξη και αναβάθμιση των κοινωνικών δικτύων προς κάλυψη των αναγκών των χρηστών, έχει οδηγήσει στην αύξηση των θεμάτων που αφορούν τους κινδύνους και τις απειλές που εγκυμονούν σχετικά με την ιδιωτικότητα (privacy risks and threats) των χρηστών, αλλά και τα αντίστοιχα μέτρα που θα πρέπει να ληφθούν ώστε να μετριαστούν, να αποτραπούν και να ελεγχθούν οι ανωτέρω (κίνδυνοι, απειλές) και να προστατευτούν τόσο οι διακινούμενες πληροφορίες όσο και τα δεδομένα των ίδιων των χρηστών.

Δομή Εργασίας

Το περιεχόμενο της εργασίας παρουσιάζεται σε πέντε (5) Κεφάλαια. Συγκεκριμένα, η δομή της έχει ως εξής:

Στο εισαγωγικό κομμάτι της πτυχιακής εργασίας γίνεται αναφορά για το διαδίκτυο, τη παγκοσμιοποίηση, την πληροφορία και των μέσων κοινωνικής δικτύωσης τα οποία θα τα αναλυθούν στα επόμενα κεφάλαια.

Στο **Κεφάλαιο 1**, γίνεται αναφορά στην ιστορικότητα των κοινωνικών δικτύων, τη κατηγοριοποίηση αυτών με παρουσίαση και αναφορά στα συγκεκριμένα παραδείγματα μέσων κοινωνικής δικτύωσης όπως:Facebook,Twitter,LinkedIn,YouTube.

Στο **Κεφάλαιο 2**, αναλύονται οι επιδράσεις των κοινωνικών δικτύων στην κοινωνία με αναφορά στις τάσεις, τα πλεονεκτήματα και μειονεκτήματα που έχει η χρήση τους, την ασφάλεια και τους κινδύνους που ελλοχεύουν, καθώς και τη χρήση και εφαρμογή τους στον εργασιακό χώρο και τις επιχειρήσεις.

Στο **Κεφάλαιο3**, αναλύεται η προστασία ιδιωτικότητας, περιγράφονται τα προσωπικά δεδομένα, παρουσιάζεται το πλαίσιο των ισχύον κανονισμών – νομοθεσιών στο διεθνή και ευρωπαϊκό χώρο με αναφορά στον νέο «Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων» (GDPR), την Αρχή Προστασίας Προσωπικών Δεδομένων (DPA) και τέλος, τις προβλέψεις που ισχύουν από το Ελληνικό Δίκαιο.

Στο **Κεφάλαιο 4**, παρουσιάζονται τα παγκόσμια σκάνδαλα που συγκλόνισαν την εμπιστοσύνη των χρηστών των μέσων κοινωνικής δικτύωσης, οι διαρροές των δεδομένων και πληροφοριών από αυτά, η υποκλοπή τους (Hacking), οι επιπτώσεις του "bullying"στα παιδιά, εφήβους, οικογένεια και η θέση – στάση της παγκόσμιας κοινότητας στα θέματα προστασίας αναφορικά με την κοινωνική δικτύωση.

Στο **Κεφάλαιο 5**, παρουσιάζονται θέματα που αφορούν τη στάση, συμπεριφορά των χρηστών επί των κοινωνικών δικτύων, τις αλληλεπιδράσεις των χρηστών σε αυτά και πως τα χρησιμοποιούν, θέματα πεποιθήσεων για την αποκάλυψη και παρουσίαση προσωπικών πληροφοριών καθώς και τον έλεγχο που εφαρμόζεται για αυτά, θέματα ιδιωτικότητας και αντίληψης των κινδύνων περί αυτών, τα θέματα της προστασίας και τα μέτρα πρόληψης που λαμβάνουν οι χρήστες και οι εφαρμογές (applications) των μέσων κοινωνικών δικτύων και τέλος, θέματα που αφορούν στην ασφάλεια (security) και αξιοπιστία τους ως μέσων επικοινωνίας.

ΚΕΦΑΛΑΙΟ 1 –ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

1.1 Εισαγωγή

Η κοινωνική δικτύωση έχει αποτέλεσει ένα ευρέως διαδεδομένο φαινόμενο στον τρόπο επικοινωνίας και ενημέρωσης, όπου τα μέσα κοινωνικής δικτύωσης (social media) και τα κοινωνικά δίκτυα (ή ψηφιακά κοινωνικά δίκτυα) (social networks), κατακτούν με εκπληκτικά αυξανόμενους ρυθμούς όλο και περισσότερους χρήστες (Zhang, 2010).

Οι όροι «social media» και «social networks» χρησιμοποιούνται ευρύτατα στο χώρο της Τεχνολογίας Πληροφορίας και Επικοινωνίας (ΤΠΕ) και συχνά ταυτίζονται στα ελληνικά κάτω από τον όρο «κοινωνική δικτύωση».

Ωστόσο, κατά τη διερεύνησή τους διαπιστώνεται σημαντική διαφοροποίηση. Σε μια πρώτη ανάγνωση, ο όρος «social media» αναφέρεται στα μέσα (εργαλεία) διαμοιρασμού της πληροφορίας, των δεδομένων και της επικοινωνίας στο κοινό ενώ ο όρος «social networking» αναφέρεται στη δημιουργία και την αξιοποίηση κοινοτήτων για τη διασύνδεση ανθρώπων με κοινά ενδιαφέροντα. Θα μπορούσε να ειπωθεί δηλαδή ότι ο όρος «social media» αναφέρεται στα εργαλεία-μέσα ενημέρωσης και κοινωνικής δικτύωσης, ενώ ο όρος «social networking» στη διαδικασία της κοινωνικής δικτύωσης.

Στο Κεφάλαιο 1, θα εξετάσουμε το θέμα εξέλιξης της κοινωνικής δικτύωσης, την κατηγοριοποίηση των κοινωνικών δικτύων και θα αναλύσουμε με παραδείγματα μερικά από τα πιο δημοφιλή μέσα διαδικτυακής κοινότητας στον κόσμο.

1.2 Κοινωνική Δικτύωση και Ιστορική Εξέλιξη

Η εφεύρεση του παγκόσμιου διαδικτυακού ιστού (World Wide Web) το 1991, είναι η μεγαλύτερη πληροφοριακή βάση δεδομένων όπου ο Tim Berners-Lee κατόρθωσε να συνδέσει την hypertext τεχνολογία στο διαδίκτυο (Internet) και δημιούργησε τη βάση ενός νέου τύπου δικτυακής επικοινωνίας. Οι υπηρεσίες μέσω των Weblogs, διακομιστών (listservers) και τα e-mail,βοήθησαν στη δημιουργία της απευθείας σύνδεσης (online) κοινοτήτων ή την υποστήριξη των ομάδων σε επίπεδο εκτός σύνδεσης (offline).

Το Web 1.0 (τεχνολογία πρώτης γενιάς) ήταν η πρώτη υλοποίηση του διαδικτύου και διήρκεσε από το 1989 έως το 2005 και ορίστηκε ως ιστός των συνδέσεων πληροφοριών.Η εμφάνισή του, ήταν η "ευανάγνωστη" (readable) φράση του Παγκόσμιου Ιστού με επίπεδα δεδομένα.

Έτσιμε το Web 1.0, υπήρχε μόνο περιορισμένη αλληλεπίδραση μεταξύ ιστότοπων και χρηστών του διαδικτύου, όπου αυτό είναι απλώς μια πύλη πληροφοριών όπου οι χρήστες

λαμβάνουν παθητικά πληροφορίες χωρίς να έχουν τη δυνατότητα να δημοσιεύουν κριτικές και σχόλια.

Με την εμφάνιση του Web 2.0, οι υπηρεσίες απευθείας σύνδεσης μεταβλήθηκαν από απλά κανάλια δικτυακής επικοινωνίας σε αμφίδρομης διαδραστικής επικοινωνίας μέσα για κοινωνική δικτύωση (Castells 2007, Manovich 2009). Με την εξέλιξη-ωρίμανση του Web 2.0 σε πιο λειτουργική υποδομή, οι χρήστες προχώρησαν και αυτοί ένα βήμα περισσότερο, μεταφέροντας τις καθημερινές τους δραστηριότητες σε περιβάλλοντα απευθείας σύνδεσης (online), όπου οι δραστηριότητες αυτές απλά, δεν διοχετεύονται μέσω των διαφόρων πλατφορμών αλλά, προγραμματίζονται με ένα πιο συγκεκριμένο αντικειμενικό στόχο.

Το γεγονός αυτό μετατόπισε την έμφαση αναφορικά με τη χρησιμότητα της παρεχόμενης υπηρεσίας από μια απλή υποστηρικτική σε μια προσαρμοσμένη(customized) υπηρεσία. Οι περισσότερες Web 2.0 πλατφόρμες ξεκίνησαν ως «ενδιάμεσες» υπηρεσίες για την ανταλλαγή επικοινωνικού ή δημιουργικού περιεχομένου (content) μεταξύ των διαφόρων φίλων (π.χ. ομάδες φοιτητών, λάτρεις φωτογραφίας, θιασώτες video) που υιοθέτησαν ένα "niche" για απευθείας σύνδεση (online) αλληλεπίδρασης όπου και έτσι ανέπτυξαν μια πρακτική επαναλαμβανόμενης μεσολάβησης. Έτσι λοιπόν, τα μέσα κοινωνικής δικτύωσης άρχισαν να αξιοποιούν τεχνολογίες που βασίζονται στο διαδίκτυο (web-based) με στόχο την επικοινωνία και την ενεργοποίηση του ευρύτερου κοινωνικού διαλόγου.

Οι Kaplan & Haenlein (2010 οπ. αναφ. στηWikipedia) ορίζουν τα μέσα κοινωνικής δικτύωσης ως εφαρμογές που βασίζονται στο διαδίκτυο και αξιοποιούν τόσο τις τεχνολογίες της δεύτερης γενιάς του διαδικτύου (Web 2.0), όσο και τη φιλοσοφία τους, που δίνει έμφαση στη δημιουργία και την ανταλλαγή περιεχομένου από τους χρήστες. Τα social media είναι δηλαδή απόρροια της δεύτερης γενιάς του διαδικτύου, στην οποία ο κάθε χρήστης έχει τηδυνατότητα όχι μόνο να δημοσιεύει το περιεχόμενο που επιθυμεί άμεσα, αλλά και νααλληλεπιδρά με άλλους χρήστες Ωστόσο, ούτε το Web 1.0 ούτε το Web 2.0 με τη γενική έννοια αρκούσαν για να κατανοήσουν οι μηχανές τις πληροφορίες στον Ιστό. Το Web 3.0 ήταν εκείνο που αποτέλεσε ένα από τα σύγχρονα και επαναστατικάκεφάλαιαπου ακολούθησε τις αρχικές πρωτοβουλίες του Web 2.0 (δεύτερη γενιά διαδικτύου). Σχεδιάστηκε για πρώτη φορά από τον John Markoff των New York Times ο οποίος το πρότεινε ως την τρίτη γενιά του ιστού το 2006.
ToWeb 3.0 μπορείεπίσηςναδηλωθείως "εκτελέσιμοWeb.

Το Web 3.0 είναι ωστόσο γνωστό και ως Σημασιολογικός Ιστός (SemanticWeb), όπου ορίστηκε από τον δημιουργό του Tim Berners-Lee ως «... μια επέκταση του τρέχοντος ιστού στον οποίο δίδεται η πληροφορία σαφώς καθορισμένη σημασία, επιτρέποντας

καλύτερα στους υπολογιστές και τους ανθρώπους να δουλεύουν σε συνεργασία»

Ηύπαρξη του Web 4.0 στην πορεία, μπορεί να θεωρηθεί ως ο εξαιρετικά ευφυής (ultra– intelligent) συμβιωτικός (symbiotic)και «πανταχού παρών» ιστός, όπου η αλληλοεπίδραση μεταξύ των ανθρώπων και μηχανών κατά τη συμβίωση αποτελούσε πάντα εκείνο το κίνητρο πίσω από τον συμβιωτικό ιστό.

Απλά, τα μηχανήματα θα μπορούν να είναι έξυπνα κατά την ανάγνωση του περιεχομένου του ιστού, να αντιδρούν με τη μορφή εκτέλεσης αποφασίζοντας τι να εκτελέσουνπρώτα, φορτώνοντας γρήγορα τις ιστοσελίδες με ανώτερη ποιότητα και απόδοση και χτίζοντας περισσότερες διεπαφές. Έτσι λοιπόν το Web 4.0 θα μπορεί να διαβάζει και να γράφει με συγχρονισμό διασφαλίζοντας την παγκόσμια διαφάνεια, διακυβέρνηση, διανομή, συμμετοχή, συνεργασία εντός βασικών κοινοτήτων, όπως αυτή της πολιτικής, κοινωνικής, οικονομικής, εκπαίδευσης καθώς και άλλων κοινοτήτων

1.3 Κατηγοριοποίηση Μέσων Κοινωνικής Δικτύωσης

Καθώς οι χρήσεις των μέσων κοινωνικής δικτύωσης αλλά και τα ίδια τα μέσακοινωνικής δικτύωσης πολλαπλασιάζονται με ταχύτατους ρυθμούς και εξαπλώνονται σε πάρα πολλούς χώρους, υπάρχουν διαφόρων ειδών κατηγοριοποιήσεις. Στησυνέχεια παρουσιάζονται τριών ειδών κατηγοριοποιήσεις: η κατηγοριοποίηση κατά Bard, η κατηγοριοποίηση κατά Zhang και η κατηγοριοποίηση των μέσων ως προς τις δυνατότητες που αυτά παρέχουν, η οποία ανήκει στον Owyang.

1.3.1 Κατηγοριοποίηση κατά Bard

Ενδιαφέρουσα αλλά αρκετά περίπλοκη και λεπτομερής είναι η κατηγοριοποίηση της MirnaBard (2010), η οποία οργανώνει τα μέσα κοινωνικής δικτύωσης σε 23κατηγορίες, όπως φαίνονται στο **Σχήμα 1**, αναφερόμενη κυρίως στο χώρο τωνεπιχειρήσεων.

Σχήμα 1 – Social Media (Κατηγοριοποίησηκατά Mirna Bard)

Με αφορμή αυτή την κατηγοριοποίηση και λαμβάνοντας υπόψη ότι υπάρχουν 1,2 εκατομμύρια ανακοινώσεις σε ιστολόγια (blogs, microblogs κλπ.) ενώ κάθε μέρα το 45% των ενήλικων χρηστών του διαδικτύου δημιουργεί κάποιο δικό του «προϊόν» στο διαδίκτυο, ο χώρος των μέσων κοινωνικής δικτύωσης είναι ένα δυναμικό και ταχύτατο αναπτυσσόμενο πεδίο, ιδιαίτερα ελκυστικό και για τις επιχειρήσεις, καθώς ανοίγει νέες πολύπλευρες δυνατότητες για τους καταναλωτές και αλλάζει το χάρητης αγοράς.

1.3.2 Κατηγοριοποίηση κατά Zhang

Μια πιο συνοπτική κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης (Zhang,2010) είναι η ακόλουθη:

- Ιστολόγια (blogging / micro-blogging): Σήμερα, ιδιαίτερα δημοφιλή είναι ταBlogger, WordPress, Twitter, στα οποία μπορεί κανείς να διαβάσει ζητήματα με οποιοδήποτε περιεχόμενο, π.χ. απόψεις-σχόλια, προσωπικές καταχωρήσεις για κάθεείδους θέμα π.χ.τεχνολογία, μόδα, καλλιτέχνες, εθελοντικές οργανώσεις κ.ά.

- Κοινωνικά δίκτυα (social networking), με γνωστότερα τα Facebook, Myspace, Linkedin, Ning, τα οποία επιτρέπουν στους χρήστες να αναζητήσουν και να συνδεθούν με άλλους χρήστες με παρόμοια ενδιαφέροντα και χαρακτηριστικά, π.χ.φίλους, συνεργάτες κ.ά. και να επικοινωνήσουν άμεσα μεταξύ τους, να ενημερωθούν, να ανταλλάξουν πληροφορίες, αρχεία, σκέψεις κ.ά.
- Κοινωνική σελιδοσήμανση (Social bookmarking), όπως τα: Delicious, Diggo,Faves, StumbleUpon, BlogMarks, τα οποία επιτρέπουν στον χρήστη όχι μόνο ναεπισημαίνει κάθε φορά τις ιστοσελίδες που τον ενδιαφέρουν αλλά και να τημοιράζεται με τους ανθρώπους που επιθυμεί.
- Συνεργατική συγγραφή (Collaborative authoring), με γνωστότερα τα ακόλουθα:Wikipedia, Googledocs, Zohoofficesuite κ.ά.
- Διαμοιρασμός πολυμέσων (multimedia sharing), όπως τα: Flickr, YouTube, Qik,Snapfish, Jumpcut, Vimeo, Decianart, με τα οποία οι χρήστες δημιουργούν και διαμοιράζονται αρχεία ήχου, εικόνας, video.
- Διαδικτυακές τηλεδιασκέψεις (web-conferencing), όπως τα: WebEx,Go To Meeting, DimDim.
- Σε αυτή την κατηγοριοποίηση πρέπει να προστεθεί και η κατηγορία των Ειδήσεων (NewsSite ή SocialNews) με δικτυακούς τόπους όπως τα Digg, Sphinn, Newsvine, και BallHype που δίνουν τη δυνατότητα να διαβάσει κανείς ζητήματα-άρθρα της επικαιρότητας και στη συνέχεια να τα ψηφίζει ή να τα σχολιάζει. Η συμμετοχή τωνχρηστών στα άρθρα αλλάζει και τη θέση τους στο site.Μπορεί δηλαδή ένα άρθροπου έχει ψηφιστεί πολλές φορές να προωθηθεί σε μια πιο «εξέχουσα» θέση.

1.3.3 Κατηγοριοποίηση των μέσων με βάση τις δυνατότητές τους (Owyang)

Η ενσωμάτωση των δυνατοτήτων των μέσων κοινωνικής δικτύωσης θα γίνεισύμφωνα με τον Owyang (2009) σε πέντε διαδοχικά επίπεδα ή περιόδους:

- Επίπεδο ή Περίοδος Κοινωνικών Σχέσεων, στο οποίο οι άνθρωποι συνδέονται και επικοινωνούν με άλλους ανθρώπους.
- Επίπεδο ή Περίοδος Κοινωνικής Λειτουργικότητας, στο οποίο τα κοινωνικά δίκτυα παίζουν το ρόλο ενός λειτουργικού συστήματος σε έναν Η/Υ.
- Επίπεδο ή Περίοδος Κοινωνικής Επίκοισης, στο οποίο η κάθε εμπειρία έχει νόημασε κοινωνικό επίπεδο.

- Επίπεδο ή Περίοδος Κοινωνικού Περιεχομένου, όπου αποδίδεται-παρουσιάζεταιακριβές προσωπικό περιεχόμενο από τους χρήστες.
- Επίπεδο ή Περίοδος Κοινωνικής Αγοράς, στο οποίο οι διαδικτυακές κοινότητες καθορίζουν τα μελλοντικά προϊόντα και τις υπηρεσίες.

1.4 Παραδείγματα Μέσων Κοινωνικής Δικτύωσης

Με τον όρο «Μέσα Κοινωνικής Δικτύωσης» αναφερόμαστε στον μηχανισμό (πλατφόρμα) που συνδέει χιλιάδες ίσως και δισεκατομμύρια χρήστες από όλο τον κόσμο οι οποίοι μοιράζονται, ανταλλάσουν πληροφορίες, ιδέες μέσα από τα κοινωνικά δίκτυα. Αποτελούν σημαντικό ρόλο όχι μόνο μεμονωμένα σε κάθε άτομο αλλά και σε ολόκληρες επιχειρήσεις χρησιμοποιώντας ορισμένα από τα Μέσα Κοινωνικής Δικτύωσης για τη προώθηση και τη διαφήμιση τους. Επιπλέον σου δίνουν τη δυνατότητα να δημιουργήσεις αυτόνομα κανάλια επικοινωνίας, video ακόμη και blog με αποτέλεσμα να συγκεντρώνει πληροφορίες αλλά και να μαθαίνεις το ενδιαφέρον του κοινού σου χωρίς να υπάρχουν επιπλέον δαπάνες.

Τα social media εμφανίζονται σε διάφορες μορφές όπως:

1.4.1 LINKEDIN

Το LinkedIn ιδρύθηκε το Δεκέμβριο του 2002 αλλά ξεκίνησε επίσημα το 2003 με ιδρυτή τον Reid Hoffman, ενώ το 2016 πουλήθηκε στη Microsoft έναντι του ποσού $26,4 (USD) δισεκατομμυρίων δολαρίων περίπου, αποτελώντας την πιο ακριβή απόκτηση – επένδυση για λογαριασμό της Microsoft. Είναι το μεγαλύτερο κοινωνικό δίκτυο επαγγελματικής δικτύωσης με περισσότερο από 562εκατομμύρια χρήστες (στοιχεία: Σεπτέμβριος 2018), με παρουσία σε πάνω από 200 χώρες παγκοσμίως.Θεωρείταιτο πιο δημοφιλές με αναφορά τους ενεργούς χρήστες (monthly active users)- ήτοι με στοιχεία Σεπτέμβριος 2018 (Γ’ τρίμηνο 2018 Q3-2018) ο συνολικός αριθμός τους έφτασε τα 260 εκατομμύριασε παγκόσμιο επίπεδο. Είναι διαθέσιμο σε πάνω από 24 γλώσσες όπως (αγγλικά, ιταλικά, γαλλικά κ.λπ.) και στοχεύει στις επαγγελματικές και επιχειρηματικές επαφές για τους εργοδότες και τους επαγγελματίες εργαζόμενους, παρέχοντας στις μεν επιχειρήσεις τη δυνατότητα να παρουσιάσουν εαυτές μέσω των online σελίδων στους δε χρήστες, να βρουν εργασιακή απασχόληση από τις αναρτήσεις (joblistings), προάγοντας με τις διεπαφές τους την ειδικότητά τους.

Σε σύγκριση με πολλά άλλα κοινωνικά δίκτυα, το LinkedIn, παρέχει στους χρήστες τη δυνατότητα να δουν, ποιος χρήστης "είδε" το προσωπικό τους profile, ένα τεχνικό χαρακτηριστικό το οποίο οι χρήστες αξιολογούν ως πολύ βοηθητικό στην προώθηση των δικτυακών τους επαφών.

Τα έσοδά του, προέρχονται από τρεις κυρίως πηγές: τις λύσεις πρόσληψης, που αποτελούν το μεγαλύτερο τμήμα συνεισφοράς στα εταιρικά έσοδα, ακολουθούμενες από τις διαφημίσεις και τις συνδρομές – εγγραφές (premium subscriptions). Το 2015 τα ετήσια έσοδα ανήλθαν στο άνω του ποσού των $2.99 δισεκατομμυρίων (USD)δολαρίων με την πλειονότητα να προέρχονται από το πεδίο των πωλήσεων.

1.4.2 FACEBOOK

Το Facebook ιδρύθηκε στις 4 Φεβρουαρίου 2004 με ιδρυτή τον Mark Zukerberg, ως μέλος του πανεπιστημίου του Harvard. Αρχικά, δικαίωμα συμμετοχής είχαν μόνο οι φοιτητές του πανεπιστημίου Harvard. Το 2005 δικαίωμα πρόσβασης απέκτησαν και ορισμένα λύκεια και ορισμένες μαθητικές κοινότητες, ενώ το 2006 έγινε προσβάσιμο σε όλο το πλανήτη, με τα καθαρά έσοδα το 2016 να φτάνουν το ποσό των $12.427 (USD) εκατομμυρίων δολαρίων.

Το Facebook, είναι ένας ιστοχώρος στον οποίο όλοι οι χρήστες έχουν ελεύθερη πρόσβαση αφού δημιουργήσουν τον σχετικό προσωπικό λογαριασμό τους. Επίσης, έχουν τη δυνατότητα να επικοινωνούν μέσω μηνυμάτων, να κάνουν ανάρτηση (upload) φωτογραφίες, βίντεο αλλά και να ειδοποιούνται όταν ανανεώνουν τις προσωπικές τους πληροφορίες με άτομα που έχουν ήδη διασυνδεθεί ως "φίλοι"(friends) στον προσωπικό τους λογαριασμό. Ακόμη παρέχει τη δυνατότητά χρήσης παιχνιδιών ενώ μπορεί να χρησιμοποιηθεί ως μέσο ενημέρωσης αλλά και εργαλείο του "marketing" από τις επιχειρήσεις.Είναι μακράν το πιο δημοφιλές κανάλι διαφήμισης στα κοινωνικά μέσα δικτύωσης. Σύμφωνα με το "*Social Media Examiner's 2017 Social Media Industry Report*", το 93% των διαφημιστών των κοινωνικών μέσων δικτύωσης, χρησιμοποιούν τις διαφημίσεις του Facebook. Το επόμενο δίκτυο το οποίο πλησιάζει είναι το Instagram με 24%, αλλά αυτό είναι επίσης τμήμα της πλατφόρμας του Facebook. Το Facebook θεωρείται ως το κορυφαίο σε επισκεψιμότητα μέσο κοινωνικής δικτύωσης καθώς το 2008 ξεπέρασε το Myspace, ενώ μέχρι το 2013 είχε φθάσει να έχει πάνω από 1 δισεκατομμύριο ενεργούς χρήστες. Σύμφωνα με το *comScore*, το Facebook έχει προσβασιμότητα οκτώ (8) φορές κατά μέσο την ημέρα, ακολουθούμενο από το Instagram (έξι), Twitter (πέντε) και το Facebook Messenger (τρεις).

Με βάσει τα οικονομικά αποτελέσματα (Facebook Q3-2018 Results, investor.fb.com), το Γ' τρίμηνο 2018 (Q3-2018) οι μηνιαίοι χρήστες (Monthly Active Users) σε παγκόσμιο επίπεδο ήταν 2.271 εκατομμύρια, με τα συνολικά έσοδα (Revenues) για την ίδια περίοδο να έχουν ανέλθειστο ποσό των $13.727 (USD) εκατομμυρίων δολαρίων. Η χρηματιστηριακή κεφαλαιοποίηση (MarketCap) με βάση τα στοιχεία FB: USNASDAQGS – FacebookInc (Bloomberg 31-10-2018), ανήρχετο στο ποσό των 436.852 ($ USD) εκατομμυρίων δολαρίων.

1.4.3 YouTube

Δημιουργήθηκε το Φεβρουάριο του 2005 και το Νοέμβριο του 2006 ονομάστηκε από το περιοδικό Time ως "*Invention of the Year 2006*". Τον Οκτώβριο του 2006, η εταιρεία αγοράστηκε από την Google με ανταλλαγή μετοχών αξίας $1,65 δισεκατομμυρίων (USD) δολαρίων και σήμερα λειτουργεί ως θυγατρική της Google με ιδρυτές τους Steven Chen, Jawed Karim και Chad Hurley, πρώην υπαλλήλους της PayPal.

Το YouTube είναι η μεγαλύτερη διαδικτυακή πλατφόρμα (online) παγκοσμίως που χαρακτηρίζεται από μια ποικιλία μέσων περιεχομένου που δημιουργούν οι χρήστες και οι επιχειρήσεις και περιλαμβάνει μουσικά βίντεο, τηλεοπτικά κλιπ (TVclips), video blogs, βίντεο παιγνίδια, εκπαιδευτικά βίντεο κ.λπ.

Όλοι έχουν το δικαίωμα να βλέπουν αποθηκευμένα τραγούδια και ψηφιακές ταινίες ενώ οι εγγεγραμμένοι χρήστες δημιουργώντας λογαριασμό έχουν το πλεονέκτημα να κάνουν ανεβάζουν ("up-load") βίντεο, μουσικά βίντεο το οποία δημιούργησαν οι ίδιοι, ή ακόμη και κάποιο ιστολόγιο (blog) με αποτέλεσμα να λαμβάνουν σχόλια, κριτικές αλλά και μηνύματα από διάφορους επαγγελματίες, ερασιτέχνες κ.λπ.Ωστόσο, ενώ το περιεχόμενο μέχρι σήμερα είναι ελεύθερο για προβολή, εντούτοις υπάρχουν περιπτώσεις όπως η εντοπιότητα περιοχής (regional) όπου υπόκειται σε κάποιους περιορισμούς για λόγους πνευματικής ιδιοκτησίας.

Οι χρήστες του ανέρχονται στο 1,5 δισεκατομμύριο σε παγκόσμιο επίπεδο με πρόβλεψη για αύξησή τους στο 1,86 δισεκατομμύρια μέχρι το 2021 καιτην εταιρεία να στοχεύει στην χρηματική εξαργύρωση του διαφημιστικού της περιεχομένου. Η αύξηση της χρήσης των smartphones και των άλλων κινητών συσκευών επικοινωνίας, βοήθησε στην κατανάλωση των βίντεο του YouTube εν κινήσει (onthego), όπου αυτό κατατάσσεται μεταξύ των πιο δημοφιλών κινητών πλατφορμών και στο GooglePlay και Apple,AppStore, παγκοσμίως.

1.4.4 TWITTER

Το Twitter είναι ένας ιστοχώρος κοινωνικής δικτύωσης μέσου του οποίου οι χρήστες έχουν το δικαίωμα να διαβάζουν κείμενα μέχρι 140χαρακτήρων τα λεγόμενα (tweets) χωρίς να δεσμεύονται δημιουργώντας λογαριασμό, ωστόσο, μόνο οι συνδεδεμένοι χρήστες έχουν το δικαίωμα το δημοσιεύουν κάποιο κείμενο.
Ιδρύθηκε 21 Μαρτίου 2006 από τους JackDorsey, NoahGlass, BizStone και EvanWilliams, έχοντας αποκτήσει 335 εκατομμύρια ενεργούς χρήστες με βάσει στοιχεία του Β' Τριμήνου 2018.

Σε μόνιμη βάση έχει χαρακτηρισθεί ως ένα από τα πιο δημοφιλή κοινωνικά δίκτυα για τους νέους στις ΗΠΑ. Ωστόσο, από πρόσφατες έρευνες που διενεργήθηκαν φάνηκε ότι απώλεσε ένα μερικό μερίδιο της αγοράς από τους ανταγωνιστές (mobile competitors) του, το Instagram και το Snapchat. Πρόσφατα δεδομένα κοινωνικών μέσων επίσης αποδεικνύουν ότι η χρήση του, είναι προεξέχουσα αυξανόμενη κατά την διάρκεια διαφόρων εκδηλώσεων. Έτσι, σε ζωντανές εκδηλώσεις «τιτιβίσματος» (live-tweeting happenings), όπως αθλητικές εκδηλώσεις ή παρουσίας νέων τηλεοπτικών προγραμμάτων, η online συμμετοχή-διασύνδεση των χρηστών με άλλους, διαμοιράζοντας σκέψεις για τρέχουσες εμπειρίες, έχει γίνει πολύ δημοφιλής.

Τα έσοδα της εταιρίας το 2017, ανήλθαν στο ποσό των $2.44 δισεκατομμυρίων (USD) δολαρίων με την καθαρή ζημία (netloss) να ανέρχεται στο ποσό των 108 εκατομμυρίων (USD) δολαρίων, με το κύριο έσοδό της να προέρχεται μέσω της διαφήμισης.
Η εταιρία δημοσιοποιήθηκε το Νοέμβριο 2013 και κατατάσσεται ως μία από τις μεγαλύτερες αμερικάνικες εταιρίες του διαδικτύου με τη χρηματιστηριακή αξία τον Ιούνιο 2018 που να αγγίζει τα $30 δισεκατομμύρια δολάρια.

ΚΕΦΑΛΑΙΟ 2 – ΕΠΙΔΡΑΣΕΙΣ ΣΤΗΝ ΚΟΙΝΩΝΙΑ

2.1 Εισαγωγή

Το φαινόμενο της κοινωνικής δικτύωσης μέσω διαδικτύου στην εποχή μας έχει πάρει τεράστιες διαστάσεις και έχει αποκτήσει μεγάλη ισχύ σχεδόν σε όλους τους τομείς της καθημερινότητάς μας (ενημέρωση, διασκέδαση, πολιτική, οικονομία, εμπόριο, εκπαίδευση ιατρικές εφαρμογές, κ.α.).

Στο Κεφάλαιο 2, θα εξετάσουμε το θέμα της κοινωνικής υπηρεσίας που προσφέρουν τα μέσα κοινωνικής δικτύωσης και τις τάσεις που υπάρχουν και έχουν διαμορφωθεί με τη χρήση τους, τα μειονεκτήματα και τα πλεονεκτήματα από τη χρήση τους, τα μέτρα ασφάλειας που πρέπει να υιοθετούν οι χρήστες και τους κινδύνους που ελλοχεύουν σε περίπτωση μη εφαρμογής τους. Τέλος, θα εξετάσουμε πως η χρήση τους έχει επιδράσει στο εργασιακό περιβάλλον και στις επιχειρήσεις.

2.2 Κοινωνική Υπηρεσία των Μέσων Κοινωνικής Δικτύωσης– Εφαρμογές

Τα μέσα κοινωνικής δικτύωσης έχουν γίνει αναπόσπαστο κομμάτι του σύγχρονου πολιτισμού μας. Πρόκειται για έναν τομέα επικοινωνίας που έχει συμβάλει καθοριστικά στη ριζική αλλαγή των σημερινών κοινωνικών αλληλεπιδράσεων που έχουν σημειωθεί τα τελευταία χρόνια. Το αποτέλεσμα αυτό οφείλεται στην ραγδαία εξέλιξη της τεχνολογίας σε συνδυασμό με τον ολοένα και αυξανόμενο αριθμό των οραματιστών της εποχής μας, οι οποίοι με την εφευρετικότητα που τους διακατέχει έχουν δημιουργήσει τεράστιες παγκόσμιες και πετυχημένες πλατφόρμες κοινωνικής δικτύωσης.

Οι εφαρμογές τους εντοπίζονται στα κατωτέρω :

- **Πηγή Ειδήσεων**

Τα μέσα κοινωνικής δικτύωσης έχουν γίνει μια σημαντική πηγή ειδήσεων. Παρ' όλα αυτά η αξιοπιστία ορισμένων πηγών μπορεί σαφώς να αμφισβητηθεί. Η διαθεσιμότητά τους στα κοινωνικά δίκτυα καθιστά τα νέα και τις ειδήσεις πιο προσιτά στο ευρύ κοινό. Επιπλέον, τα νέα ταξιδεύουν με ιλιγγιώδη ταχύτητα και κάνουν το γύρο του κόσμου μέσα σε λίγα δευτερόλεπτα.

- **Πολιτική**

Τα κοινωνικά μέσα μαζικής ενημέρωσης επέτρεψαν (και επιτρέπουν) τη δημιουργία μεγαλύτερης πολιτικής ευαισθητοποίησης και οργάνωσης, η οποία έχει σε ορισμένες περιπτώσεις ξαναγράψει ολόκληρο το πολιτικό τοπίο από την αρχή. Διαδραμάτισαν μεγάλο ρόλο στις εκλογές του Ιράν, στην επανεκλογή του Ομπάμα για δεύτερη θητεία (Νοέμβριος 2012) ως Προέδρου των ΗΠΑ, στη συνταγματική αναθεώρηση στην Ισλανδία (Facebook), καθώς και ενέπνευσε τις πολιτικές αναταραχές στην Αίγυπτο (Ιανουάριος 2011).

- **Εκπαίδευση**

Τα μέσα κοινωνικής δικτύωσης και τα κοινωνικά δίκτυα κατακτούν με εκπληκτικά αυξανόμενους ρυθμούς όλο και περισσότερους χρήστες, έτσι και στην εκπαίδευση, η εφαρμογή νέων αναβαθμισμένων και ποιοτικότερων μεθόδων, σχετίζεται άμεσα με το φαινόμενο αυτό. Οι Douglas & Seely-Brown (2011), διατείνονται πως η χρήση των κοινωνικών δικτύων στην εκπαίδευση οδηγεί σε μια νέα κουλτούρα, σε μια μάθηση που στηρίζεται στις αρχές της συλλογικής ανακάλυψης. Πιο συγκεκριμένα, οι φοιτητές των έχουν τη δυνατότητα να αναπτύξουν κριτική και αναλυτική σκέψη με στόχο την οικοδόμηση νέας γνώσης μέσα από το αλληλεπιδραστικό, κοινωνικό και πολύ συμμετοχικό χαρακτήρα των κοινωνικών δικτύων (Selwyn, 2012).

- **Επιχειρήσεις**

Πολλές επιχειρήσεις αξιοποιούν τις δυνατότητες διασύνδεσης που προσφέρουν τα κοινωνικά δίκτυα για να ενισχύσουν την παραγωγικότητα, την καινοτομία, τη φήμη, τη συνεργασία και τη δέσμευση των εργαζομένων τους με την εταιρεία. Είναι σημαντικό να σημειωθεί πως πολλές επιχειρήσεις χρησιμοποιούν τα κοινωνικά μέσα αποκλειστικά ως μάρκετινγκ εργαλεία. Παγκόσμιοι κολοσσοί που χρησιμοποιούν επιτυχημένα τα νέα μέσα κοινωνικής δικτύωσης είναι η Coca-cola, η στρατηγική της οποίας αναπτύχθηκε με κύριο γνώμονα την προσέγγιση των fans μέσω κοινωνικών, photo-sharingvideo-sharing, δικτύων, η Ford, τα Starbucks, η Dell.

- **Επιστήμη**

Σημαντική χρήση των κοινωνικών δικτύων διαφαίνεται και από την επιστημονική κοινότητα. Σύμφωνα με τους Liebeskind & al (1996)«η κοινωνική δικτύωση επιτρέπει στις επιστημονικές ομάδες να επεκτείνουν τις γνώσεις τους και να διαμοιράσουν καινούριες ιδέες μεταξύ των μελών, σε σημείο τέτοιο ώστε αν δεν υπήρχε αυτή(κοινωνική δικτύωση) οι θεωρίες τους να χαρακτηρίζονταν "απομονωμένες και ανομοιόμορφες".

Η Ιατρική επιστήμη προσπαθώντας να ενισχύσει το έργο της μέσα από τα μέσα κοινωνικής δικτύωσης έχει δημιουργήσεις ιστοσελίδες για ασθενείς με παρόμοια προβλήματα όπως για παράδειγμα το κοινωνικό δίκτυο Sober Circle που απευθύνεται σε αλκοολικούς και τοξικομανείς, ενώ παράλληλα μέσα από αυτά ενημερώνει τους χρήστες για τις ιατρικές εξελίξεις.

2.3 Η Εξέλιξη των Μέσων Κοινωνικής Δικτύωσης: Πώς θα είναι το Μέλλον

Σχεδόν για μια δεκαετία, οι πλατφόρμες των μέσων κοινωνικής δικτύωσης μετασχηματίζουν τις επιχειρήσεις και τις κοινωνικές ζωές διαμέσου της δικτύωσης των ανθρώπων και παρέχοντας την δυνατότητα σε κάθε άτομο να επικοινωνεί και να συνεργάζεται. Η διασπαστική δύναμή τους (disruptive power) στις επιχειρήσεις και στις κοινωνικές διεργασίες προέρχεται από την ικανότητά τους, να εγκαθιδρύουν συνεργατικές δικτυακές δομές κατά τον ίδιο τρόπο όπως συμβαίνει και με τους ανθρώπους που έρχονται κοντά και συνεργάζονται στον πραγματικό κόσμο.

Κατά τη δεκαετία αυτή, τα κοινωνικά δίκτυα έχουν αναπτυχθεί όχι μόνο σε κλίμακα και ευρωστία αλλά περισσότερο έχουν εμπλουτισθεί με χαρακτηριστικά συμπεριλαμβάνοντας νέους κύκλους ζωής περιεχομένων (content lifecycles) καθώς και τρόπους προσέγγισης. Το τελευταίο, έχει οδηγήσει στην βαθμιαία εμφάνιση διαφόρων τύπων πλατφορμών όπως επαγγελματικών δικτύων (π.χ. LinkedIn, ResearchGate), δίκτυα που στοχεύουν στα video και image sharing (π.χ. Instagram), όπου πλέον είναι εμφανές ότι τα κοινωνικά δίκτυα διαρκώς εξελίσσονται καθώς εμφανίζονται νέες πλατφόρμες. Η εξέλιξη αυτή εκμεταλλεύεται τις νέες τάσεις τεχνολογίας βελτιώνοντας τις εμπειρίες των χρηστών, ενεργοποιώντας έξυπνες υπηρεσίες και αναπτύσσοντας την αυτοματοποίηση.

Κλείνοντας αυτή τη δεκαετία οι τάσεις που δημιουργούνται στην εξέλιξη των κοινωνικών δικτύων για το μέλλον είναι οι ακόλουθες:

α) Artificial Intelligence (AI)

Μία από τις κύριες τάσεις των κοινωνικών δικτύων θα είναι η ενσωμάτωσή τους με τα συστατικά στοιχεία και τις υπηρεσίες της τεχνητής νοημοσύνης (Artificial Intelligence) ως μέσων ανάπτυξης της αυτοματοποίησης και την νοημοσύνης.

Ήδη έχουμε τα πρώτα δείγματα αυτής της σύγκλισης μέσω των chatbots τα οποία σταδιακά γίνονται αναπόσπαστα τμήματα των εφαρμογών μηνυμάτων εντός και εκτός των

πλατοφορμών των κοινωνικών δικτύων, όπου τα chat bots, παρέχουν τη δυνατότητα για γρήγορη, έξυπνη και αυτοματοποιημένη αλληλεπίδραση με τους τελικούς χρήστες.

β) Augmented Reality (AR)

Η επόμενη τάση αφορά την βελτίωση της εμπειρίας των χρηστών με την ενσωμάτωση της «επαυξημένης πραγματικότητας» (AR) εντός των πλατφορμών των κοινωνικών δικτύων και των εφαρμογών τους. Η ενσωμάτωση της «επαυξημένης πραγματικότητας» σκοπεύει στο να επιτρέπει την περισσότερο ευχάριστη, αποτελεσματική και εργονομική αλληλεπίδρασή του διευκολύνοντας τους τελικούς χρήστες να έχουν μεγαλύτερη απόλαυση όταν χρησιμοποιούν τις εφαρμογές των κοινωνικών δικτύων. Διακεκριμένο παράδειγμα αποτελεί το Instagram που πρόσφατα πρόσθεσε AR φίλτρα προσώπου τα οποία παρέχουν τη δυνατότητα στους χρήστες να χαρτογραφήσουν και να εφαρμόσουν "κινούμενα σχέδια" για το πρόσωπό τους. Είναι σημαντικό να αναφερθεί ότι και η πλατφόρμα του Facebook έχει μια πλήρη και φιλόδοξη στρατηγική για την ενσωμάτωση AR, όπως ο Δ/νων Σύμβουλος αυτού Mark Zuckerberg ανέφερε στο συνέδριο της εταιρίας το 2017 (F8 Developer Conference), όπου το AR θα είναι το «μέλλον» των έξυπνων τηλεφώνων (smartphones).

γ) Social Internet of Things (IoT)

Σκεπτόμενοι πέρα από τις πρόσθετες βελτιώσεις πάνω στα υπάρχοντα παραδείγματα των κοινωνικών δικτύων, αναμένεται ότι οι «μηχανές» θα αρχίσουν να σχηματίζουν ή να συμμετέχουν στα κοινωνικά δίκτυα. Δισεκατομμύρια πράγματα είναι ήδη διασυνδεδεμένα στο διαδίκτυο συμπεριλαμβάνοντας μερικά έξυπνα αντικείμενα (smartobjects), π.χ. αντικείμενα με ημι-αυτόνομη συμπεριφορά, όπου ήδη αυτά έχουν τη δυνατότητα να ενασχολούνται με ομότιμους χρήστες (π.χ. Machine-to-Machine), αλληλεπιδρώντας.

Αυτό δύναται να αποτελέσει τη θεμέλια βάση για να πραγματοποιούνται αυτές οι γνωστικές αλληλεπιδράσεις διαμέσου της πρόσθεσης νοημοσύνης και της κοινωνικής διάστασης.

Σαν παράδειγμα αντίστοιχων αλληλεπιδράσεων μπορούν να κατονομαστούν αυτές στις έξυπνες εφαρμογές μεταφορών, όπου διάφοροι συσκευές αισθητήρων και ελέγχου εντός των οχημάτων συμπλέκουν διάφορους τύπους εφαρμογών όπως V2I (Vehicle-to-Infrastructure), V2P (Vehicle-to-Pedestrian), V2G (Vehicle-to-Grid) και V2V (Vehicle-to-Vehicle) αλληλεπιδράσεις.

Στα επόμενα χρόνια, αναμένεται οι εφαρμογές να αυξηθούν σε κλίμακα και εξέλιξη ανάπτυξης καθώς θα συμπεριλαμβάνεται και ο ανθρώπινος παράγοντας, όπου μαζί άνθρωποι

και μηχανές θα συμμετέχουν από κοινού στην επίλυση κοινωνικών προβλημάτων σε διάφορους τομείς όπως οι μεταφορές, η βιομηχανία, η ενέργεια και η διαχείριση εφοδιασμού.

δ) "Block chain"-based Social Media Network

Η τεχνολογία διανεμημένης πληροφορίας (distributed ledger technology – DLT), γνωστή και ως "block chain", είναι πιθανό να διαδραματίσει ένα σημαντικό ρόλο στο μέλλον των κοινωνικών δικτύων. Η λογική πίσω από αυτή την πρόβλεψη βασίζεται στο γεγονός της προσφοράς καθαρών πλεονεκτημάτων που προσφέρονται σε διάφορες περιοχές οι οποίες καταγράφονται κατωτέρω:

- Μη ανάγκη ύπαρξης ενός αξιόπιστου Τρίτου Μέρους (No-need for Trusted Third Party)

  Η τεχνολογία Block chain παρέχει τη δυνατότητα της αποκεντρωμένης αποθήκευσης δεδομένων και της επεξεργασίας τους χωρίς να υπάρχει η ανάγκη της ύπαρξης αξιόπιστου τρίτου μέρους. Αυτό όμως δύναται να μειώσει το απόρρητο και τα σχετικά εμπόδια εμπιστοσύνης για τη συμμετοχή των χρηστών στα κοινωνικά δίκτυα.
- Συνεργασία σε αντίθεση με Συγκέντρωση (Collaboration vs Centralization)

  Η τεχνολογία Block chain επιτρέπει τον σχηματισμό συνεργασιών κοινοτήτων των ανθρώπων και μηχανών, ωθώντας στην συνεργατική επίλυση προβλημάτων χωρίς την ύπαρξη ελέγχου.
- Επεκτασιμότητα και Αξιοπιστία (Scalability and Reliablility)

  Η αποκέντρωση παρέχει χώρο για την αύξηση της επεκτασιμότητας και αξιοπιστίας. Αν και τα υπάρχοντα κοινωνικά δίκτυα επιδεικνύουν μια τρομερή επεκτασιμότητα, εντούτοις περιορίζονται όταν είναι στο να υποστηρίξουν τα δισεκατομμύρια των συνδεδεμένων δικτυακών αντικειμένων, όπου σε αυτή την περίπτωση η τεχνολογία Blockchain μπορεί να προσφέρει μια συναρπαστική εναλλακτική στην σύγχρονη τεχνολογική υποδομή των "clouds".

Συνολικά, η εξέλιξη των κοινωνικών δικτύων είναι σε πολλές περιπτώσεις καθοδηγούμενη από μερικές βασικές ψηφιακές τάσεις, οι οποίες με τη σειρά τους διαμορφώνουν τις ανάγκες των χρηστών σε σχέση με τους τρόπους που αυτοί επιζητούν την πρόσβαση και χρήση στις ηλεκτρονικές υπηρεσίες.

2.4 Μειονεκτήματα και Πλεονεκτήματα Χρήσης των Κοινωνικών Δικτύων

Τα κοινωνικά δίκτυα έχουν πραγματοποιήσει μια διαρκή εξέλιξη τα πρόσφατα χρόνια, δίνοντας την ισχυρή αντανάκλαση της δομής και δυναμικής της κοινωνίας του 21ου αιώνα και της αλληλεπίδρασης της γενιάς του διαδικτύου μαζί με την τεχνολογία και τον υπόλοιπο κόσμο. Η δραματική αυτή ανάπτυξη των κοινωνικών πολυμέσων και του περιεχομένου που γεννάται από τους χρήστες είναι πράγματι επαναστατική, επηρεάζοντας όλες τις φάσεις της αλυσίδας αξίας περιεχομένου, συμπεριλαμβάνοντας την παραγωγή, επεξεργασία, διανομή και τέλος, την κατανάλωση. Ωστόσο, το περιβάλλον των κοινωνικών δικτύων έχει αντίστοιχα πλεονεκτήματα και μειονεκτήματα τα κυριότερα από οποία θα επιδείξουμε εδώ.

Τα πλεονεκτήματα των κοινωνικών διακτύων μπορούν να κατηγοριοποιηθούν ως ακολούθως:

(i) Παγκόσμια Διασύνδεση(Worldwide Connectivity)

Προσφέρουν ταχύτητα διασύνδεσης του ανθρώπινου πληθυσμού ανεξάρτητα σε ποιο σημείο του πλανήτη ευρίσκεται, διευκολύνοντας την επικοινωνία για π.χ. εύρεση εργασίας, δημιουργία φιλίας, αναζήτηση υποστήριξης – βοήθειας, αναζήτηση συμβουλών σε διάφορα θέματα.

(ii) Κοινότητες Ιδίων Ενδιαφερόντων (Commonality of Interest)

Επιτρέπουν τη συμμετοχή των ατόμων σε κοινότητες που έχουν τα ίδια ενδιαφέροντα κτίζοντας σχέσεις ψηφιακές αντί διαμέσου της φυσικής παρουσίας τους, παρέχοντας τη δυνατότητα να αναπτύσσεται η κάθε κοινότητα με ομάδες από άλλες κοινότητες ή ομάδες.

(iii) Διάδοση Πληροφοριών σε Πραγματικό Χρόνο (Real-Time Sharing of Information

Ανταλλαγή πληροφοριών σε πραγματικό χρόνο μέσω της συνομιλίας (chat), διευκολύνοντας συναντήσεις ομάδων, συζητήσεις στελεχών επιχειρήσεων, πελατών, φοιτητών, κ.α.

(iv) ΕλεύθερηκαιΕστιασμένηΔιαφήμιση(Free of Cost Targed Advertising)
Μεταφορά-διάδοση του «μηνύματος» σε παγκόσμια κλίμακα χωρίς την ύπαρξη κόστους, όπου προωθείται είτε κάποιο προϊόν είτε κάποια υπηρεσία με εστίαση σε ένα πιο συγκεκριμένο κοινό.

(v) Ταχύτητα Χρόνου Μετάδοσης Νέων (Increased News Cycle Speed)

Αύξηση της ταχύτητας του παραδοσιακού κύκλου διάδοσης των διαφόρων νέων, όπου η συλλογή και διανομή τους πραγματοποιείται σε ελάχιστο χρόνο σε παγκόσμια κλίμακα.

(vi) Εγγυημένος Τόπος Συνάντησης

Η πρόσβαση στα κοινωνικά δίκτυα παρέχει αυξημένες δυνατότητες για τον τόπο και χρόνο που λαμβάνουν χώρα οι συναντήσεις, με το να μην απαιτείται η πραγματοποίηση ταξιδιών και διευκολύνοντας τους συμμετέχοντες στη διαχείριση του διαθέσιμου χρόνου τους.

Τα μειονεκτήματα των κοινωνικών διακτύων μπορούν επίσης να κατηγοριοποιηθούν ως ακολούθως:

(i) Κυβερνο-εκφοβισμός και Έγκλημα (Cyber-Bullying and Crime)

Η απόκρυψη πίσω από την οθόνη του διαδικτύου παρέχει νέες δυνατότητες σε κάποιους από τους χρήστες που στην πραγματικότητα, δεν μπορούν να έχουν.

Η παρενόχληση μέσω του κυβερνοχώρου δύναται να καθοριστεί ο εκφοβισμός μέσω των κοινωνικών δικτύων που περιλαμβάνει: δημοσιεύσεις αρνητικών σχολίων, αναρτήσεις υβριστικών μηνυμάτων, χρήση εικόνων ή video για γελοιοποίηση κ.α.

(ii) Κίνδυνοι Απάτης και Κλοπής Ταυτότητας (Riskof Fraudand IdentityTheft)

Η κλοπή ταυτότητας χρήστη, επηρεάζει εκατομμύρια άτομα κάθε χρόνο, κοστίζοντας στα θύματα αμέτρητες ώρες και χρήματα για την επαναφορά και τη επιδιόρθωσή της.

Το 2012 μόνο, υπολογίζεται ότι 12 εκατομμύρια άτομα έγιναν θύματα κλοπής ταυτότητας και απάτης με το κόστος τους να υπολογίζεται σε ύψος στα $21 δισεκατομμύρια (USD) δολάρια ζημιά του έτους μόνο, αποδεικνύοντας ότι αποτελεί ένα από τα αυξανόμενα προβλήματα στις ΗΠΑ.

(iii) Ελάττωση Παραγωγικότητας (Decreased Productivity)

Σύμφωνα με μελέτη που διεξήγαγε η εταιρεία ερευνών Πληροφορικής Nucleus Research (ITresearchco) σε 237 υπαλλήλους, οι επιχειρήσεις που επιτρέπουν τη χρήση του Facebook κατά το χρόνο εργασίας, ζημιώνονται με 1.5% κατά μέσο όρο στην αποδοτικότητα των υπαλλήλων τους.

Η Δ/νουσα Σύμβουλος της Nucleus Research, Rebecca Wettermann, σε δήλωσή της ανέφερε ότι, «*αν η εταιρεία σου έχει περιορισμένα περιθώρια κέρδους και χαμηλής κερδοφορίας, τότε πως είναι δυνατόν να ανεχθείς οποιαδήποτε απόσπαση προσοχής που εξαντλεί την παραγωγικότητα?*»

(iv) Επίδραση στην Ψυχική και Φυσική Υγεία (Impact on Mental and Physical Health)

Αναμφισβήτητα, το μεγαλύτερο μειονέκτημα της κοινωνικής δικτύωσης αποτελεί η επίδραση που διαδραματίζει στην νοητική και την φυσική υγεία, με την εμφάνιση θεμάτων υγείας που σχετίζονται με κατάθλιψη, απομόνωση, σύνδρομο προσκόλλησης, μείωση φυσικής άσκησης, ανησυχία, χρήση ναρκωτικών και αλκοόλ, αϋπνία κ.α.

(v) Εκτενή Διάδοση Λανθασμένων Πληροφοριών (Extensive Spread of Misinformation)

Η διάδοση και μετάδοση λανθασμένων ή ψεύτικων πληροφοριών, φήμες κ.α. οι οποίες μπορούν να προκαλέσουν πανικό και σύγχυση. Η δημοτικότητα που απολαμβάνουν τα κοινωνικά δίκτυα, αποτελεί «πρόκληση»στον εντοπισμό τέτοιου είδους πληροφοριών όπου η σύζευξή τους,

τους δίνει τη δυνατότητα στο να μεταδίδουν την λανθασμένη είδηση-πληροφορία, σε πολύ γρήγορο χρόνο.

(vi) Χαμηλή Επάρκεια Γλώσσας και Γραμματικής (Poor Language and Grammar)

Η αυξανόμενη χρήση των διαφόρων πλατφορμών κοινωνικών δικτύων και ο υποχρεωτικός περιορισμός της χρήσεως χαρακτήρων έχουν οδηγήσει στην συντομογραφία λέξεων, παράλειψη σημείων στίξης και τη δημιουργία γραμματικών λαθών και μείωση της γλωσσικής επάρκειας. Σε σχετική αναφορά από το Πανεπιστήμιο του Waterloo (UK)στην απαιτούμενη δοκιμασία για την επάρκεια Αγγλικής γλώσσας,

η γενική διευθύντρια των εξετάσεων Αγγλικών (Ann Barrett) διαπιστώνει ότι «το 30% των σπουδαστών που εισέρχονται σε αυτό, δεν είναι ικανό για να περάσει ούτε με τη μικρότερη βαθμολογία».

2.5 Κοινωνικά Δίκτυα: Ασφάλεια και Κίνδυνοι (Security Risks)

Η χρήση των κοινωνικών δικτύων παρ' ότι όπως αναφέραμε στη ανωτέρω παράγραφο παρουσιάζει πολλά πλεονεκτήματα, εντούτοις "κρύβει" ακόμη περισσότερους κινδύνους οι οποίοι όταν υλοποιηθούν, δύναται να καταστρέψουν ολόκληρη τη ζωή (π.χ. χρηστών, επιχειρήσεων, ομάδων) σε περίπτωση μη-λήψης των αναγκαίων μέτρων ασφαλείας (πρόληψη) για την προφύλαξη από αυτούς.

Στην εποχή την οποία ζούμε είμαστε "περικυκλωμένοι" από τα κοινωνικά δίκτυα με αποτέλεσμα, να υπάρχει η ανάγκη-ευκαιρία να τα χρησιμοποιήσουμε δημιουργώντας αντίστοιχους "λογαριασμούς" είτε στο Facebook, στο Twitter, ή στο Instagram, αγνοώντας όμως τους "κινδύνους" που συχνά διατρέχουμε. Ειδικότερα, οι "λογαριασμοί" που δημιουργούμε, απαιτούν τη συνεχή εγρήγορση και παρακολούθησή μας. Είναι πολύ εύκολο όταν για παράδειγμα γίνει μια κυβερνο-επίθεση (cyber-attack)και αυτή να μεταδοθεί και στους επονομαζόμενους "followers" με αποτέλεσμα και αυτοί να προσβληθούν, "χάνοντας" έτσι - μεταξύ και των άλλων προβλημάτων που δημιουργούνται - την εμπιστοσύνη προς τους συνδέσμους που ακολουθούν, είτε είναι φίλοι, ομάδες, κοινότητες, επιχειρήσεις κ.λπ.

Οι απειλές – κίνδυνοι (cyber-threats) που διακατέχει τη χρήση των κοινωνικών δικτύων, είναι τριών (3) κατηγοριών, ήτοι: (1) της εφαρμογής (platform related), (2) του χρήστη (user related), και (3) κυβερνο-επίθεση (cyber-attack). (*E. Fokes and Lei Li - 2014*).Αυτοί (κίνδυνοι) που σχετίζονται με τις εφαρμογές, περιλαμβάνουν τις διαδικτυακές πληροφορίες της ιστοσελίδας του κοινωνικού δικτύου, πολιτικές απορρήτου και ασφάλειας, τρωτότητες όπως η επιλογή επαλήθευσης (verification options), διαδικασίες αυθεντικότητας (authentication processes), και παραβίαση δεδεομένων (data breach).

Οι αντίστοιχοι που αφορούν τους χρήστες αφορούν πρακτικές τρωτότητας που περιλαμβάνουντην ανταλλαγή πληροφοριών, συμπεριφορές αντιγραφής απορρήτου, ρυθμίσεις απορρήτου του χρήστη και έλλειψη επαρκούς ενημέρωσης.

Τέλος, οι κυβερνο-απειλές, επιθέσεις, αφορούν μια πληθώρα κινδύνων όπως η αγνόηση των κινδύνων από τον ίδιο τον χρήστη όπως για παράδειγμα η πλαστογραφία (spoofing), "click jacking", και επιθέσεις από κακόβουλο λογισμικό (malware) και Trojans

Όπως συμβαίνει με κάθε τι το τεχνολογικό, έτσι και τα κοινωνικά δίκτυα έχουν τα δικά τους μειονεκτήματα και κινδύνους. Το Κέντρο Δικτυακών Παραπόνων Εγκλήματος (Internet Crime Complaint Center - IC3), έδειξε ότι το 12% από τα υποβληθέντα παράπονα το 2014, αφορούσαν θέμα με τα κοινωνικά δίκτυα.

Έτσι, τα παράπονα έχουν τετραπλασιαστεί σε σχέση με τα αντίστοιχα το 2009, όπως αναφέρει το IC3 (2014).

Στις περισσότερες των περιπτώσεων, η κοινωνική μηχανική ή οι "hacked accounts" προσέβαλαν το απόρρητο των θυμάτων τους. Το 2010, υπολογίζεται ότι έγιναν 2.322 συλλήψεις για σεξουαλικά εγκλήματα με βάσει το διαδίκτυο σε βάρος ανηλίκων όπου περιλάμβαναν ιστότοπους κοινωνικών δικτύων κατά κάποιο τρόπο, συμπεριλαμβάνοντας και 503 συλλήψεις με ανεγνωρισμένα θύματα με τη χρήση των κοινωνικών δικτύων από τους παραβάτες. *(Mitchell, Finkelhor, Jones, & Wolak, 2010).*

2.6 Εργασιακός Χώρος – Επιχειρήσεις

Από την πλευρά των επιχειρήσεων, μία στις τρεις πλέον χρησιμοποιούν πλατφόρμες κοινωνικής δικτύωσης. Η χρήση των κοινωνικών δικτύων από τους εργαζομένους στο πλαίσιο της εργασίας τους έχει τη δυναμική να μεταμορφώσει συνολικά τον κόσμο της εργασίας. Πολλές γνωστές εταιρείες αξιοποιούν τις δυνατότητες διασύνδεσης που προσφέρουν τα social media για να ενισχύσουν την παραγωγικότητα, την καινοτομία, τη φήμη, τη συνεργασία και τη δέσμευση των εργαζομένων τους με την εταιρεία.

Χωρίς αμφιβολία τα μέσα μαζικής δικτύωσης αποτελούν σημαντικό ρόλο στην καθημερινή ζωή των ανθρώπων, ενώ μπορεί κάποιος να τα καθορίσει ως απαραίτητα μέσα στον επιχειρηματικό χώρο αλλά και από τους πιο αποτελεσματικούς τρόπους διαφήμισης-marketing ενός προϊόντος σε μια επιχείρηση. Τα πρώτα χρόνια λειτουργίας του διαδικτύου - από τα μέσα ως και τα τέλη του 1990 - υπήρχε μια επιφυλακτικότητα από τις επιχειρήσεις προς τα μέσα κοινωνικής δικτύωσης.

Πίστευαν ότι ορισμένοι εργαζόμενοι θα τα χρησιμοποίησαν για προσωπική τους χρήση αποσπώντας τους την προσοχή, ενώ αντιθέτως πολλοί εργαζόμενοι το θεώρησαν αναγκαίο εργαλείο της δουλειάς, αξιοποιώντας την δύναμή του διαδικτύου με στόχο να αποφέρουν καλύτερα αποτελέσματα στις επιχειρήσεις και να γίνουν αποδοτικότεροι.

Η δυναμική των Social Media είναι πολύ μεγάλη και έχει τη δυνατότητα να μεταμορφώσει τον εργασιακό χώρο ενώ επίσης μπορεί να ενισχύσει την αποδοτικότητα παραγωγικότητα, την καινοτομία, τη φήμη, τη συνεργασία και τη δέσμευση των εργαζομένων τους με την εταιρεία. Το 75% των επιχειρήσεων διεθνώς δεν διαθέτουν επίσημη πολιτική για τη χρήση ιστοχώρων κοινωνικής δικτύωσης σε ώρα εργασίας.

Στην Ελλάδα το ποσοστό αυτό ανέρχεται στο 86%, στην περιοχή EMEA είναι στο 87% και στην Αμερική στο 69Τα Social Media μπορεί να θεωρηθούν ως ένας τρόπος επικοινωνίας, ανταλλαγής απόψεων, διαφήμισης (Social Media Marketing), προώθησης, ενημέρωσης που πολλές επιχειρήσεις χρησιμοποιούν. Με βάση τα κέρδη που επιφέρει το Social Media Marketing αποτελεί βασικό ρόλο στις επιχειρήσεις ως μέσω προώθησης σε

συνδυασμό με την άμεση επικοινωνία ανάμεσα σε εταιρίες και πελάτες χωρίς εμπόδια αλλά και της παγκοσμιοποίησης της αγοράς.

Αυτό το αποτέλεσμα προκύπτει από την χρήση εκατοντάδων εκατομμυρίων χρηστών των Social Media με διαφορετικές ιδέες, τάσεις και ανάγκες οι οποίοι έχουν. Έχοντας ως αποτέλεσμα οι επιχειρήσεις να δημιουργήσουν μια σχέση εμπιστοσύνης μεταξύ των online καταναλωτών.

ΚΕΦΑΛΑΙΟ 3 - ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ-ΝΟΜΟΘΕΣΙΑ

3.1 Εισαγωγή

Στο Κεφάλαιο 3, θα εξετάσουμε τις βασικές έννοιες για την πληροφοριακή ιδιωτικότητα και τα προσωπικά δεδομένα, με αναφορά στην προστασία αυτών και του απορρήτου. Στη συνέχεια θα αναφερθούμε και θα παραθέσουμε το διεθνές & ευρωπαϊκό νομικό και κανονιστικό πλαίσιο για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων, πως διενεργείται η εποπτεία και η εφαρμογή αυτού και πως τα μέσα κοινωνικής δικτύωσης ενσωματώνουν τους κανόνες για την προστασία των προσωπικών που ισχύουν. Τέλος, θα αναφερθούμε και θα παραθέσουμε το νομοθετικό πλαίσιο που ισχύει σε εθνικό επίπεδο, πως και ποιο τρόπο εποπτεύεται η εφαρμογή του.

3.2 Προστασία Ιδιωτικότητας – Απορρήτου

Η ραγδαία τεχνολογική εξέλιξη που παρατηρείται τα τελευταία χρόνια, είχε ως αποτέλεσμα την ανάπτυξη πρωτοποριακών εφαρμογών σε όλους τους τομείς της καθημερινότητάς μας. Η εξέλιξη της κινητής τηλεφωνίας, το διαδίκτυο και η πληθώρα των προσφερόμενων ηλεκτρονικών υπηρεσιών, δίνουν πολλαπλές δυνατότητες ηλεκτρονικής επικοινωνίας, μέσα σε ένα ολοένα και περισσότερο δικτυωμένο περιβάλλον. Η αυξανόμενη χρήση κινητών συσκευών – διαρκώς συνδεδεμένων μέσω του διαδικτύου – προσφέρει νέες δυνατότητες επικοινωνίας οπουδήποτε, ανεξαρτήτως χρόνου, θέσης και κίνησης.

Όμως, η ανάπτυξη και η εξέλιξη αυτή, στη χρήση των ηλεκτρονικών επικοινωνιών, εγείρει ταυτόχρονα και σημαντικά ζητήματα σχετικά με την ασφάλεια, την ιδιωτικότητα και το απόρρητο της επικοινωνίας, τα οποία οι χρήστες συχνά αγνοούν ή τείνουν να υποβαθμίζουν. Κίνδυνοι υποκλοπών και παραβίασης του απορρήτου των επικοινωνιών υφίστανται τόσο για τους χρήστες των τηλεπικοινωνιακών δικτύων όσο και για τους χρήστες του διαδικτύου (κυβερνοχώρου), ενώ συχνά περιστατικά υποκλοπών βλέπουν το «φως» της δημοσιότητας.

Μία από τις συνηθέστερες θεωρήσεις της έννοιας της ιδιωτικότητας είναι ότι συνίσταται στον απόρρητο χαρακτήρα ορισμένων ζητημάτων και υπό αυτήν την έννοια η ιδιωτικότητα προσβάλλεται με την αποκάλυψη απόρρητης πληροφορίας. Ιδίως η «κλασική» προσέγγιση της ιδιωτικότητας ως καταφυγίου (Refugium) παρουσιάζει στοιχεία ταύτισης ή και σύγχυσης με την έννοια του απορρήτου (Secrecy) και της εμπιστευτικότητας (Confidentiality). Οι όροι αυτοί, αν και συχνά γίνονται αντιληπτοί και χρησιμοποιούνται ως

ισοδύναμοι, εκφράζοντας σε τελευταία ανάλυση παρεμφερείς αξιώσεις προστασίας, εντούτοις δεν ταυτίζονται:

Η έννοια του απορρήτου (Secrecy) αναφέρεται είτε στη μη προσπελασιμότητα ορισμένων πληροφοριών που εμπίπτουν στη σφαίρα επιρροής ενός ατόμου είτε στο καθήκον ή την υποχρέωση προσώπων ή οργανισμών να διαφυλάσσουν πληροφορίες, που είτε ένα άτομο έχει εμπιστευτεί σε αυτά, στο πλαίσιο μιας γενικότερης σχέσης εμπιστοσύνης (όπως το ιατρικό απόρρητο ή το τραπεζικό απόρρητο), είτε τις κατέχουν επί τη βάσει της θέσης και της αρμοδιότητάς τους (όπως το υπηρεσιακό απόρρητο). Εάν μάλιστα πρόκειται για πληροφορία που εμπίπτει στη δημόσια σφαίρα δεν είναι νοητή η προστασία από το απόρρητο. Για να είναι απόρρητη / εμπιστευτική η πληροφορία θα πρέπει να είναι σε μία κατάσταση περιορισμένης προσβασιμότητας από πρόσωπα, ομάδες κ.λπ.

3.3 Πληροφοριακή Ιδιωτικότητα και Προσωπικά Δεδομένα

(α) Πληροφοριακή Ιδωτικότητα

Η έννοια της ιδιωτικότητας «αναφέρεται στη θέσπιση του κατάλληλου νομικού πλαισίου και στην εφαρμογή ειδικών τεχνικών και τεχνολογιών για την προφύλαξη του πολίτη από την αποκάλυψη, σε μη εξουσιοδοτημένες οντότητες, πληροφοριών και δεδομένων που τον αφορούν, αλλά μπορεί επίσης να προσδιοριστεί και ανάλογα με το πλαίσιο στο οποίο αυτή εξετάζεται. Έτσι, έχουμε τις ακόλουθες παραλλαγές της:

- Πληροφοριακή Ιδιωτικότητα: σχετίζεται με τη συγκέντρωση, την αποθήκευση, την επεξεργασία και τη διάδοση των πληροφοριών που αποτελούν προσωπικά δεδομένα ενός ανθρώπου (προσώπου).
- Χωρική Ιδιωτικότητα: σχετίζεται με την προστασία της φυσικής περιοχής στην οποία βρίσκεται ένα πρόσωπο (π.χ. οικία, εργασιακός χώρος κλπ.).
- Σωματική Ιδιωτικότητα: σχετίζεται με την προστασία ενός του σώματος ενός προσώπου από αδικαιολόγητη παρέμβαση (π.χ. σωματικός έλεγχος κλπ.).
- Επικοινωνιακή Ιδιωτικότητα: σχετίζεται με την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.

Ο πιο κοινά αποδεκτός ορισμός της Πληροφοριακής Ιδιωτικότητας προτάθηκε το 1967 από τον Alan F. Westin και αναφέρει ότι:

«Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους». Επίσης η πληροφοριακή ιδιωτικότητα πολλές φορές προκαλεί

αντιθέσεις με άλλους μηχανισμούς ασφαλείας γι αυτό όλοι οι μηχανισμοί ασφαλείας που δημιουργούνται θα πρέπει να είναι συμβατοί με τις βασικές αρχές μιας δημοκρατικής κοινωνίας, όπως ορίζεται από τον ΟΟΣΑ:

«Η ασφάλεια πρέπει να εφαρμόζεται με τρόπο σύμφωνο με τις αξίες που αναγνωρίζονται από τις δημοκρατικές κοινωνίες, όπως η ελευθερία ανταλλαγής σκέψεων και ιδεών, η ελεύθερη ροή πληροφοριών, ο εμπιστευτικός χαρακτήρας της πληροφόρησης και επικοινωνίας, η κατάλληλη προστασία των προσωπικών πληροφοριών, το άνοιγμα και η διαφάνεια» - ("Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency").

Το σημαντικότερο σημείο της έννοιας της Ιδιωτικότητας Πληροφοριών αποτελεί ο διαχωρισμός των πληροφοριών που είναι δημόσια διαθέσιμες και αυτών που χαρακτηρίζονται ως ιδιωτικές και πρέπει να προστατευτούν. Ο προσδιορισμός της κατηγορίας στην οποία εντάσσεται κάθε είδος πληροφορίας, εξαρτάται από διάφορους παράγοντες και συνήθως βασίζεται στο ισχύον νομικό και κανονιστικό πλαίσιο.

Η έννοια της Ιδιωτικότητας των Πληροφοριών καθίσταται εξαιρετικά σημαντική σε Πληροφοριακά Συστήματα Ηλεκτρονικής Διακυβέρνησης, εξαιτίας τόσο του χαρακτήρα των πληροφοριών που αξιοποιούνται όσο και του σημαντικού όγκου που συλλέγεται, επεξεργάζεται και αποθηκεύεται.

Παραδείγματα τέτοιων πληροφοριών δεδομένων αποτελούν τα διάφορα αναγνωριστικά (τομεακά ή μη) που αξιοποιεί ο κάθε χρήστης: οικονομικά – φορολογικά στοιχεία, δημογραφικά στοιχεία, ποινικό μητρώο, ιατρικά αρχεία και δεδομένα που σχετίζονται με θρησκευτικές και πολιτικές πεποιθήσεις. Επιπρόσθετα, η ιδιαιτερότητα των υπηρεσιών που προσφέρονται από τη Δημόσια Διοίκηση έγκειται στην υποχρέωση παροχής όλων των απαιτούμενων πληροφοριών –δεδομένων, σε αντίθεση με τις ηλεκτρονικές υπηρεσίες σε Πληροφοριακά Συστήματα ηλεκτρονικού εμπορίου ή ηλεκτρονικής μάθησης, όπου ο χρήστης μπορεί να επιλέξει να μην παρέχει κάποιες πληροφορίες αλλά παρόλα αυτά να καταστεί δυνατή η παροχή της υπηρεσίας.

(β) Προσωπικά Δεδομένα

«Δεδομένο προσωπικού χαρακτήρα» μπορεί να συνιστά κάθε πληροφορία που αναφέρεται σε ένα ορισμένο πρόσωπο (το υποκείμενο των δεδομένων). Τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα. Ο νομοθέτης παρέχει στα ευαίσθητα προσωπικά δεδομένα διευρυμένη προστασία, ορίζοντας αυστηρότερες προϋποθέσεις για την πρόσβαση σε αυτά και την τήρηση αρχείων που να τα εμπεριέχουν. Τα δεδομένα προσωπικού χαρακτήρα μπορούν, στα πλαίσια διαμόρφωσης αποθετηρίων και τήρησης των

σχετικών αρχείων, είτε να συνίστανται σε στοιχεία αναγνώρισης είτε να αναφέρονται σε ενδιαφέροντα - συνήθειες/ δεδομένα ακαδημαϊκής δραστηριότητας/ δεδομένα θέσης κλπ τα οποία να συνδέονται με συγκεκριμένο πρόσωπο. Ευαίσθητα προσωπικά δεδομένα είναι τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του «Γενικού Κανονισμού Προστασίας Δεδομένων» (ΓΚΠΔ). Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα.

Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη. Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή.

Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- όνομα και επώνυμο
- διεύθυνση κατοικίας
- ηλεκτρονική διεύθυνση, π.χ. όνομα.επώνυμο@εταιρεία.com·
- αναγνωριστικός αριθμός κάρτας
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)
- αναγνωριστικό cookie
- το αναγνωριστικό διαφήμισης του τηλεφώνου σας
- δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει αποκλειστικά ένα άτομο.

(Ευρωπαϊκή Επιτροπή – Νομοθεσία ανά θεματικό πεδίο: Προσωπικά Δεδομένα)

3.4 Νομικό Πλαίσιο (Διεθνές & Ευρωπαϊκό Δίκαιο)

(α) Κυβερνο-έγκλημα

Η προστασία των προσωπικών πληροφοριών αποτελεί βασικό δομικό στοιχείο μιας δημοκρατικής κοινωνίας. Το γεγονός ότι διανύουμε την "Εποχή της Πληροφορίας", δηλαδή στην ελεύθερη διακίνησή της, κάνει επιτακτική την ανάγκη για προάσπιση της πληροφοριακής ιδιωτικότητας.

Η εποχή της πληροφορίας θέτει σε κίνδυνο την ιδιωτικότητα και τα προσωπικά δεδομένα του ατόμου λόγω της μεγάλης και εύκολης διακίνησης των πληροφοριών. Η χρήση της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ), έχοντας αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί η σύγχρονη κοινωνία, κατέστησε δυνατή, τη διάπραξη ενός μεγάλου αριθμού εγκληματικών πράξεων, οι οποίες προϋποθέτουν εξειδίκευση και τεχνολογική κατάρτιση.

Η παραβατική συμπεριφορά η οποία και αναπτύχθηκε στην πορεία, από την ανθρώπινη δραστηριότητα με τη χρήση και υιοθέτηση των τεχνολογικών εργαλείων και μέσων, δημιούργησε το επονομαζόμενο, "ηλεκτρονικό έγκλημα" ή "κυβερνο-έγκλημα" (cyber-crime). Ο όρος "Ηλεκτρονικό Έγκλημα", περιλαμβάνει όλες εκείνες τις αξιόποινες πράξεις που τελούνται με τη χρήση υπολογιστών και δικτύων επικοινωνίας.

Λόγω της πολυπλοκότητας των ΤΠΕ, αλλά και των πολλών διαφορετικών τεχνολογιών που εμπλέκονται, είναι δύσκολο να κατηγοριοποιήσουμε το ηλεκτρονικό έγκλημα σε σχέση με την τεχνολογία που χρησιμοποιείται. Ανάλογα με το περιεχόμενο της επίθεσης τα κυβερνο-εγκλήματα διακρίνονται σε:

- Εγκλήματα κατά της προσωπικότητας και της ιδιωτικότητας
- Εγκλήματα κατά της περιουσίας
- Διακίνηση παράνομου και αθέμιτου / επιβλαβούς περιεχομένου

Υπάρχουν διάφοροι τρόποι με τους οποίους είναι δυνατό να εμπλακούν οι ΤΠΕ στο ηλεκτρονικό έγκλημα, άλλοτε αποτελώντας στόχο και άλλοτε εργαλείο, όπου με τον παράγοντα της "ανωνυμίας", ενισχύεται και αυξάνεται η συχνότητα τέλεσης αυτών.

(β) Νομικό Πλαίσιο

Το Νομικό Πλαίσιο και οι σχετικοί κανόνες που έχει αναπτύξει και διαθέτει η παγκόσμια κοινότητα και οι οποίοι έχουν εκδοθεί για την προστασία των χρηστών, μπορούν να κατηγοριοποιηθούν σε τέσσερις ενότητες, που αφορούν τα ακόλουθα:

- Προστασία της προσωπικότητας και ιδιωτικότητας
- Καταστολή οικονομικού ηλεκτρονικού εγκλήματος
- Προστασία πνευματικής ιδιοκτησίας
- Προστασία από παράνομο και αθέμιτο περιεχόμενο

Από τα τέλη της δεκαετίας του 1960 καταγράφεται η ανάγκη νομοθετικής προστασίας της ιδιωτικότητας. Η διασυνοριακή ροή προσωπικών πληροφοριών, δηλ. η ανταλλαγή και διαβίβαση πληροφοριών από χώρασε χώρα, οδήγησε σε μια πρώιμη παγκοσμιοποίηση της πληροφορίας. Γι'αυτό το λόγο, μεγάλο μέρος των κανονιστικών κειμένων που αφορούν την προστασία προσωπικών δεδομένων αναφέρεται στη ρύθμιση της νόμιμης διασυνοριακής κυκλοφορίας των προσωπικών πληροφοριών. Η ανάγκη προστασίας της ιδιωτικότητας διατυπώνεται ήδη στη Σύμβαση της Ρώμης της 4ης Νοεμβρίου 1950 για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών.

Στο άρθρο 8 της Σύμβασης ρυθμίζεται το δικαίωμα κάθε ανθρώπου να γίνεται σεβαστή η ιδιωτική και οικογενειακή του ζωή, η κατοικία και η αλληλογραφία του.

Στα πρώτα σχετικά κείμενα κατατάσσεται επίσης η απόφαση 2450/19.12.1968 της Γ.Σ. των Ηνωμένων Εθνών, η οποία αφορά τα προβλήματα που ανακύπτουν σχετικά με τα ανθρώπινα δικαιώματα από την ανάπτυξη της επιστήμης και της τεχνολογίας και ειδικότερα από τη χρήση των ηλεκτρονικών μέσων.

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) είναι ο δεύτερος διεθνής οργανισμός που ασχολήθηκε με την προστασία προσωπικών δεδομένων εκδίδοντας τις λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων».

Οι Αρχές αυτές περιλαμβάνουν:

- Την αρχή της περιορισμένης συγκέντρωσης και συλλογής δεδομένων
- Την αρχή της ποιότητας των δεδομένων
- Την αρχή του προσδιορισμένου σκοπού
- Την αρχή της περιορισμένης χρήσης των προσωπικών δεδομένων
- Την αρχή μέτρων ασφάλειας των προσωπικών δεδομένων
- Την αρχή της διαφάνειας
- Την αρχή της συμμετοχής του ατόμου
- Την αρχή της ευθύνης

(γ) Ηνωμένες Πολιτείες Αμερικής – Η.Π.Α.

Στις ΗΠΑ, δεν υπάρχει ενιαίος, περιεκτικός ομοσπονδιακός (εθνικός) νόμος που να ρυθμίζει τη συλλογή και χρήση προσωπικών δεδομένων. Αντ' αυτού, οι ΗΠΑ έχουν ένα συνονθύλευμα σύστημα ομοσπονδιακών και κρατικών νόμων και κανονισμών που μπορεί μερικές φορές να επικαλύπτονται, να συμπλέκονται και να αντιβαίνουν ο ένας στον άλλο. Επιπλέον, υπάρχουν πολλές κατευθυντήριες γραμμές που αναπτύσσονται από κυβερνητικούς οργανισμούς και βιομηχανικές ομάδες που δεν έχουν ισχύ νόμου αλλά αποτελούν μέρος κατευθυντήριων γραμμών και πλαισίων αυτορρύθμισης που θεωρούνται «βέλτιστες πρακτικές». Αυτά τα πλαίσια αυτορρύθμισης έχουν στοιχεία λογοδοσίας και επιβολής, τα οποία χρησιμοποιούνται όλο και περισσότερο ως μέσο επιβολής από τις ρυθμιστικές αρχές.

Μερικοί από τους σημαντικούς ομοσπονδιακούς νόμους για το απόρρητο περιλαμβάνουν – χωρίς να εξαντλούν τη νομοθεσία – τους κατωτέρω:

- The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act), είναι ο ομοσπονδιακός νόμος για την προστασία καταναλωτών, ο οποίος απαγορεύει τις αθέμιτες και παραπλανητικές πρακτικές και έχει εφαρμοστεί για εκτός και με σύνδεση (offline and online) πολιτικές απορρήτου και ασφάλειας δεδομένων.
- The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827), ο οποίος ρυθμίζει την συλλογή, χρήση και διάθεση των χρηματοοικονομικών πληροφοριών.
- Εφαρμόζεται ευρέως στα χρηματοπιστωτικά ιδρύματα, ήτοι τράπεζες, χρηματιστηριακές εταιρίες και ασφαλιστικές εταιρίες καθώς κα σε άλλες επιχειρήσεις που παρέχουν χρηματοοικονομικές υπηρεσίες και προϊόντα.
- The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) οοποίος ρυθμίζει τις ιατρικές πληροφορίες. Εφαρμόζεται ευρέως στους παρόχους υγείας, φαρμακεία, και άλλες οντότητες που χειρίζονται ιατρικού περιεχομένου πληροφορίες.
- The HIPAA Omnibus Rule που επίσης αναθεωρήθηκε από the Security Breach Notification Rule (45 C.F.R. Part 164), ο οποίος απαιτεί από τις καλυπτόμενες οντότητες να ενημερώσουν για παραβίαση προστατευόμενων πληροφοριών για την υγεία.
- The Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) που τροποιήθηκε από The Fair Credit Reporting Act), εφαρμόζεται στους οργανισμούς αναφοράς καταναλωτή, αυτοί που χρησιμοποιούν αναφορές καταναλωτών (όπως δανειστές) και σε αυτούς που παρέχουν πληροφορίες για καταναλωτές (όπως εταιρίες πιστωτικών καρτών).

- The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.), που ρυθμίζουν τη συλλογή και τη χρήση διευθύνσεων ηλεκτρονικού ταχυδρομείου και αριθμών τηλεφώνου, αντίστοιχα.
- The Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) ρυθμίζουν την παρακολούθηση των ηλεκτρονικών επικοινωνιών και την παραβίαση του ηλεκτρονικού υπολογιστή, αντίστοιχα.

Το 2016, το Κογκρέσο ενέκρινε το νόμο περί δικαστικής αποκατάστασης, δίνοντας στους πολίτες ορισμένων συμμάχων (κυρίως κρατών μελών της ΕΕ) το δικαίωμα να ζητήσουν αποζημίωση στα αμερικανικά δικαστήρια για παραβιάσεις της ιδιωτικής ζωής, όταν οι προσωπικές πληροφορίες τους μοιράζονται με τις υπηρεσίες επιβολής του νόμου.
Παρόλο που οι ΗΠΑ έχουν ορισμένους ομοσπονδιακούς νόμους περί απορρήτου δεδομένων που διέπουν συγκεκριμένες κατακόρυφες καταστάσεις, όπως ο νόμος για την ασφάλεια φορητότητας και λογοδοσίας (HIPAA), δεν έχει έναν ενιαίο νόμο όπως τον Γενικό Κανονισμό Προστασίας Δεδομένων – "General Data Protection Regulation" (GDPR), που καλύπτει όλους τους πολίτες. Εάν δεν ψηφιστεί ένας ομοσπονδιακός νόμος περί απορρήτου δεδομένων, οι νόμοι κάθε πολιτείας θα έχουν αρμοδιότητα στους δικούς τους πολίτες.

(δ)Κατάλογος με Διεθνείς Νομοθεσίες, Κανονισμούς και Πράξεις για Προστασία Δεδομένων

δ1. Ευρωπαϊκή Ένωση (EU)

- Γενικός Κανονισμός Προστασίας Δεδομένων – General Data Protection Regulation (GDPR). (Αντικατέστησε την Ευρωπαϊκή Οδηγία 95/46/EC) με ισχύ από 25 Μαΐου 2018.
- Κανονισμός Ηλεκτρονικού Απορρήτου – (ePrivacy Regulation (PECR)), για το Απόρρητο των ηλεκτρονικών Επικοινωνιών.
- Πράξη Προστασίας Δεδομένων 2018 (Ιρλανδίας), η οποία αντικατέστησε την Πράξη Προστασίας Δεδομένων 1988
- Πράξη Προστασίας Δεδομένων 2001 (Μάλτα)
- Πράξη Προστασίας Δεδομένων 2018 (Ηνωμένο Βασίλειο – U.K), ο οποίος αντικατέστησε την Πράξη Προστασίας Δεδομένων 1988

δ2. Αμερική (Βόρεια, Νότια)

ΗΠΑ:

- Ειδικοί Νόμοι Προστασίας ανά τομέα (Sector-specific data protection laws)
- Πράξη Προστασίας Καταναλωτή (Καλιφόρνια)
- Νόμος περί Δικαιωμάτων Απορρήτου Καταναλωτών (CPBORA)
- EU – US Ασπίδα Προστασίας Ιδωτικής Ζωής (EU-US Privacy Shield)

Καναδάς:

- Καναδική Πράξη Απορρήτου
- Πράξη Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA)

Αργεντινή: Πράξη Προστασίας Προσωπικών Δεδομένων

Βραζιλία: Γενικό ς Νόμος Προστασίας Δεδομένων

Βερμούδα: Πράξη Προστασία ς Προσωπικών Πληροφοριών (PIPA)

δ3. Αφρική

Νότιος Αφρική: Πράξη Προστασίας Πορσωπικών Πληροφοριών (POPI Act)

Μαυριτανία: Πράξη Προστασίας Δεδομένων 2017 (αντικαθιστά αυτή του 2004)

δ4. Αυστραλία & Νέα Ζηλανδία

Αυστραλιανή Πράξη Προστασίας

Ν. Ζηλανδίας Πράξη Προστασίας

δ5. Ασία

Ινδία: Πρόγραμμα Προστασίας Προσωπικών Δεδομένων 2018

Πλαίσιο Απορρήτου (Asia Pacific Economic Cooperation APEC) και Οργανισμός Οικονομικής Συνεργασίας & Αναπτύξεως (OECD)

Ιαπωνία: Πράξη προστασίας Προσωπικών Πληροφοριών (PIPA)

Χονγκ-Κονγκ: Διάταξη Απορρήτου Προσωπικών Δεδομένων

δ6. Μέση Ανατολή

Ισραήλ: Νόμος Προστασίας Απορρήτου (2014)

3.5 Ελληνικό Δίκαιο – Ρυθμιστική Αρχή Προστασίας Προσωπικών Δεδομένων

3.5.1 Ελληνικό Δίκαιο

Γενική Νομοθεσία

Μετά την αναθεώρηση του Ελληνικού Συντάγματος το 2001, εισήχθη το άρθρο 9Α για την προστασία των προσωπικών δεδομένων ενός ατόμου από την παράνομη επεξεργασία. Έχει επίσης εισαγάγει για πρώτη φορά το δικαίωμα της «πληροφόρησης» ως ξεχωριστή πτυχή του δικαιώματος στην ιδιωτική ζωή, το οποίο ουσιαστικά σημαίνει το δικαίωμα του ατόμου να γνωρίζει, να ελέγχει και να αποφασίζει πότε και αν πρέπει να συλλέγονται τα προσωπικά του δεδομένα, επεξεργασία ή χρήση με οποιονδήποτε τρόπο.

Μέχρι την έναρξη ισχύος του κανονισμού (ΕΕ) 679/2016 για την προστασία των φυσικών προσώπων (Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων - GDPR) όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών μέχρι 25 Μαϊου του 2018, η συλλογή και χρήση δεδομένων προσωπικού χαρακτήρα στην Ελλάδα ρυθμίζετο από τον νόμο περί προστασίας δεδομένων (DPL) (νόμος 2472/1997), ο οποίος μετέφερε στην εθνική νομοθεσία την οδηγία 95/46 / ΕΚ για την προστασία των δεδομένων (οδηγία για την προστασία των δεδομένων).

Προς το παρόν, αναμένεται η έκδοση του ειδικού εφαρμοστικού νόμου για τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) που θα ισχύσει για την Ελληνική επικράτεια.

Τομεακή Νομοθεσία

Υπάρχουν επίσης ορισμένοι ειδικοί νόμοι που ρυθμίζουν συγκεκριμένους τομείς, όπως:

α) Νόμος 3471/2006. Αυτός ρυθμίζει τη συλλογή και χρήση δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των ηλεκτρονικών επικοινωνιών και μεταφέρει στην εθνική νομοθεσία την οδηγία 2002/58 / ΕΚ για την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

β) Νόμος 3917/2011. Ρυθμίζει τη διατήρηση δεδομένων προσωπικού χαρακτήρα που συλλέγονται / επεξεργάζονται και μεταφέρει στην εθνική νομοθεσία την οδηγία 2006/24 / ΕΚ σχετικά με τη διατήρηση δεδομένων που παράγονται ή υποβάλλοντα ι σε επεξεργασία

σε σχέση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών.

γ) Νόμος 4070/2012. Ο νόμος ρυθμίζει ότι απαιτούνται γενικές άδειες για την ανάληψη κάθε είδους δραστηριοτήτων ηλεκτρονικής επικοινωνίας που σχετίζονται με δίκτυα ή / και υπηρεσίες ηλεκτρονικών επικοινωνιών, σύμφωνα με τον Νόμο και τον "Κανονισμό Γενικών Αδειών" (Απόφαση ΕΕΤΤ 390/3 / 31-6-06).

3.5.2 Ρυθμιστική Αρχή Προστασίας Προσωπικών Δεδομένων

Για την προστασία του ατόμου στην κοινωνία της πληροφορίας δεν επαρκούν οι παραδοσιακές θεσμικές εγγυήσεις και ρυθμίσεις, αλλά χρειάζεται ειδική αντιμετώπιση. Για τον σκοπό αυτό στην στην Ελλάδα, ιδρύθηκε με τον Νόμο 2472/1997 ως ανεξάρτητος διοικητικός φορέας η ΑΠΔΠΧ, η οποία λειτουργεί από τον Νοέμβριο του του 1997. Άλλες αρχές που εποπτεύουν την επεξεργασία προσωπικών δεδομένων είναι στην Ελλάδα η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών και στην Ευρώπη ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), γνωστή (ανεπίσημα) και ως Αρχή Προστασίας Προσωπικών Δεδομένων, ξεκίνησε τη λειτουργία της στις 10 Νοεμβρίου 1997 και είναι συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική Αρχή.

Ιδρύθηκε με τον Νόμο 2472/1997 «για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ.

Η οδηγία αυτή θέτει κανόνες για την προστασία των προσωπικών δεδομένων σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης.

ΚΕΦΑΛΑΙΟ 4 –ΑΠΟΤΕΛΕΣΜΑ ΕΜΠΙΣΤΟΣΥΝΗΣ, ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΠΡΟΒΛΗΜΑΤΩΝ ΠΟΥ ΕΜΦΑΝΙΖΟΝΤΑΙ ΣΤΑ ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ

4.1 Εισαγωγή

Στο Κεφάλαιο 4, ενδεικτικά εξετάζουμε τα παγκόσμια σκάνδαλα που τελευταία εμφανίστηκαν και κλόνισαν την εμπιστοσύνη των χρηστών των κοινωνικών μέσων δικτύωσης, αναφορικά με τη διαρροή των πληροφοριακών τους δεδομένων. Στη συνέχεια, αναφερόμαστε στα θέματα ασφάλειας δεδομένων (data security issues) και ιδιωτικότητας (privacy concerns) που απασχολούν τους χρήστες των κοινωνικών μέσων δικτύωσης, επικεντρώνοντας την προσοχή στα προσωπικά τους δεδομένα. Τέλος, παραθέτουμε στοιχεία μελέτης για το πως αισθάνονται οι χρήστες από τον έλεγχο που ασκούν επί των κοινωνικών μέσων δικτύωσης και την προστασία των δεδομένων τους από αυτά.

4.2 Παγκόσμια Σκάνδαλα και Εμπιστοσύνη Χρηστών

Τα μέσα κοινωνικής δικτύωσης και γενικότερα το διαδίκτυο είναι ένα μέσο επικοινωνίας εκατομμυρίων ατόμων απ'όλο το κόσμο, ενημέρωσης τους. Στο διαδίκτυο καθημερινά εγγράφονται νέα άτομα τα οποία δίνουν τα προσωπικά τους στοιχεία κατά την ολοκλήρωση της εγγραφής τους, ενώ επίσης όλοι οι χρήστες των social media έχουν δώσει τα προσωπικά τους στοιχεία παλαιότερα. Το αποτέλεσμα αυτό δημιουργεί θετικές εντυπώσεις για την ιδιωτικότητα των προσωπικών στοιχείων. Από την άλλη όμως πλευρά δε πρέπει να είμαστε σίγουροι για τίποτα διότι έχουν υπάρξει και μεγάλα σκάνδαλα στο διαδίκτυο όπως π.χ. εκείνο της Cambridge Analytica και το Facebook (Μάρτιος 2018), του Instagram (Αύγουστος 2017) και του iPhone Tracking.

4.2.1 Cambridge Analytica και Facebook

Η Cambridge Analytica είναι μια Βρετανική συμβουλευτική εταιρία η οποία συνδύαζε εξόρυξη και ανάλυση δεδομένων αναφορικά με τη στρατηγική επικοινωνία κατά τη διάρκεια των εκλογικών διαδικασιών. Η εταιρεία έκλεισε τις δραστηριότητές της το 2018, παρόλο που συνέχισαν να υπάρχουν συναφείς επιχειρήσεις.

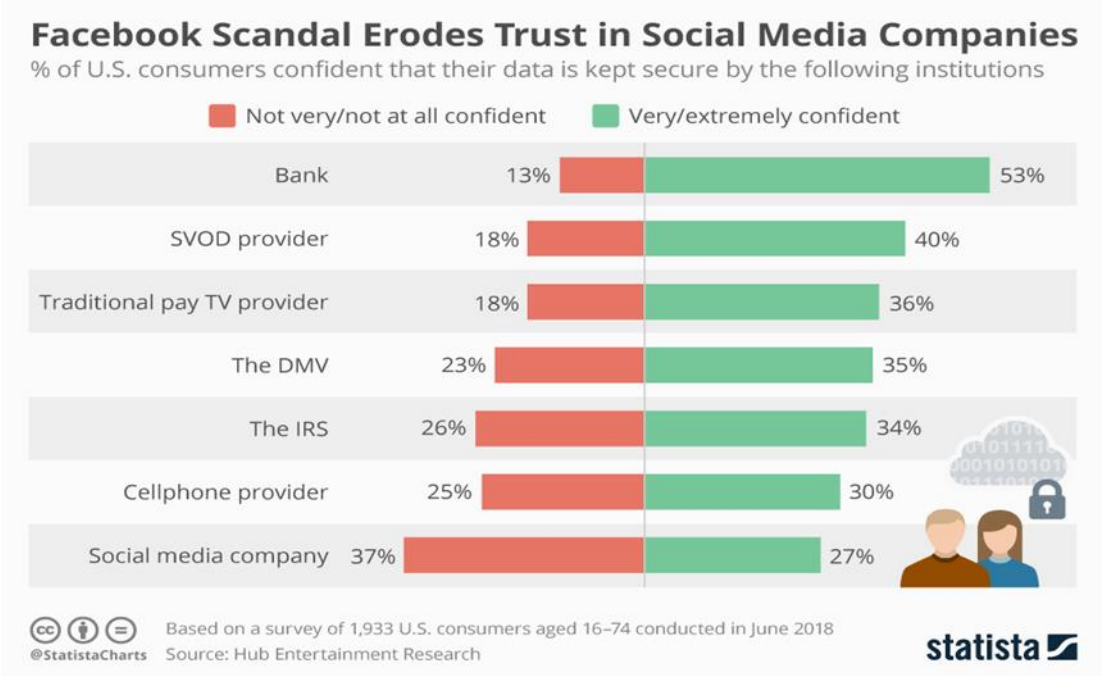
Στις 17 Μαρτίου του 2018 έγινε ένα από τα μεγαλύτερα διαδικτυακά σκάνδαλα όπου η Cambridge Analytica κατάφερε να διασπάσει πληροφορίες με τα προσωπικά στοιχεία των χρηστών μέσω μια εφαρμογής

"This Is Your Digital Life." Δίνοντας την άδεια αυτής της εφαρμογής τρίτου μέρους να αποκτήσει τα δεδομένα της, πίσω το 2015, αυτό έδωσε επίσης στην εφαρμογή πρόσβαση σε πληροφορίες σχετικά με το δίκτυο φίλων του χρήστη με αποτέλεσμα η Cambridge Analytica - χωρίς να της έχουν δώσει άδεια - να έχει πρόσβαση στα δεδομένα 87 εκατομμυρίων χρηστών. Με αφορμή αυτό το περιστατικό πολλοί απο τους χρήστες του Facebook να έχασαν την εμπιστοσύνη τους διαγράφοντας ακόμη και την εφαρμογή.

Η ανεξάρτητη αυτή εταιρεία κατόρθωσε να «περιμαζεύει» τις προσωπικές πληροφορίες από περίπου 50 εκατομμύρια λογαριασμούς Facebook χρησιμοποιώντας τις διεπαφές προγραμματισμού εφαρμογών (API) τους. Ακόμη χειρότερα, υπάρχει η εικασία ότι αυτές οι πληροφορίες θα μπορούσαν να έχουν επηρεάσει τις εκλογές στις ΗΠΑ, όπου ο Donald Trump έγινε πρόεδρος. Αυτή η τεράστια παραβίαση δεδομένων δεν ήταν το αποτέλεσμα ενός hack, αλλά απλά μια αδυναμία στο Facebook API. Πέραν της ίδιας της παραβίασης, το σκάνδαλο Cambridge Analytica είναι πιθανό να έχει σημαντικές επιπτώσεις όταν πρόκειται για τη ρύθμιση της ιδιωτικής ζωής με τον CEO του Facebook, Mark Zuckerberg, να έχει κληθεί να καταθέσει πολλές φορές ήδη.

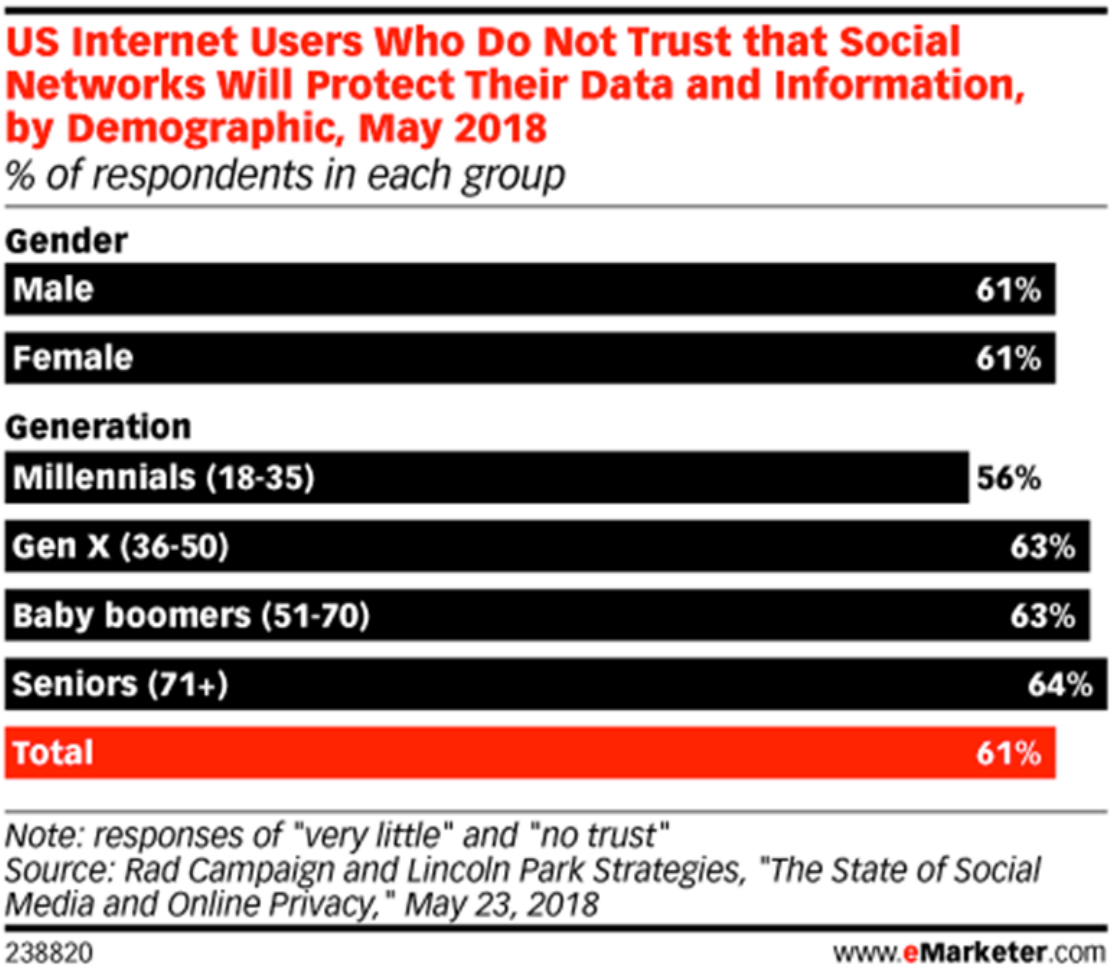
Σύμφωνα με πρόσφατη έρευνα που διεξήχθη από την Hub Entertainment Research, το 49% των Αμερικανών καταναλωτών δεν είναι πολύ σίγουροι ότι το Facebook θα κρατήσει τα δεδομένα τους ασφαλή.

Όπως δείχνει το παρακάτω διάγραμμα (Σχήμα 2), το σκάνδαλο Cambridge Analytica φαίνεται να έχει διαβρώσει την εμπιστοσύνη στις εταιρείες κοινωνικών μέσων ενημέρωσης γενικά. Σε σύγκριση με άλλες εταιρείες και ιδρύματα, οι εταιρίες κοινωνικών μέσων παραμένουν σε σημαντικό ποσοστό όσον αφορά το επίπεδο εμπιστοσύνης που έχει το κοινό των ΗΠΑ στην ικανότητά τους να διατηρούν τις πληροφορίες τους ασφαλή.



Σχήμα 2 – Ποσοστό αμερικανών καταναλωτών που είναι βέβαιοι ότι τα δεδομένα τους είναι ασφαλή από τα (συγκεκριμένα) ιδρύματα.

Σε έρευνα του Μαΐου 2018 (Σχήμα 3) που πραγματοποιήθηκε από την Rad Campaign αυτή διαπίστωσε ότι το 61% των ερωτηθέντων δεν είχε καμιά εμπιστοσύνη στα κοινωνικά δίκτυα. Αυτό συγκρίνεται με το 53% του 2016 και το 57% του 2014. Οι Millennials, που ορίζονται στην έκθεση ως οι ηλικίες 18 έως 35, ήταν οι λιγότερο επικριτικές σε σχέση με τις κοινωνικές πλατφόρμες, αλλά περισσότεροι από τους μισούς (56%) δήλωσαν ότι δεν εμπιστεύονται τα κοινωνικά δίκτυα για την προστασία των δεδομένων τους.



Σχήμα 3 – Ποσοστό αμερικανών καταναλωτών που δεν εμπιστεύονται ότι τα κοινωνικά δίκτυα προστατεύουν τα δεδομένα & πληροφορίες ανά δημογραφική κατηγορία.

Το Facebook πρέπει να βρει έναν τρόπο να ανακτήσει την εμπιστοσύνη του κοινού. Μετά από όλα, αν οι άνθρωποι δεν είναι πλέον πρόθυμοι να μοιραστούν πληροφορίες σχετικά με το Facebook, τότε ολόκληρο το επιχειρησιακό μοντέλο της εταιρείας είναι «διαρρηγμένο».

4.2.2 Instagram

Ένα άλλο σκάνδαλο εμφανίστηκε σχεδόν στα τέλη Αυγούστου 2017, όταν ανακαλύφθηκε ότι οι χάκερ κατάφεραν να παραβιάσουν το Instagram.

Μπόρεσαν να αποκτήσουν πρόσβαση στα ευαίσθητα δεδομένα (αριθμούς τηλεφώνου, ηλεκτρονικού ταχυδρομείου) των χρηστών υψηλού προφίλ εκμεταλλευόμενοι ένα σφάλμα στη διεπαφή προγραμματισμού εφαρμογών (API).

Ενώ το σφάλμα έσπασε γρήγορα και ενημερώθηκαν οι χρήστες, το θέμα των κλεμμένων δεδομένων εν τω μεταξύ, δεν μπορούσε να λυθεί.

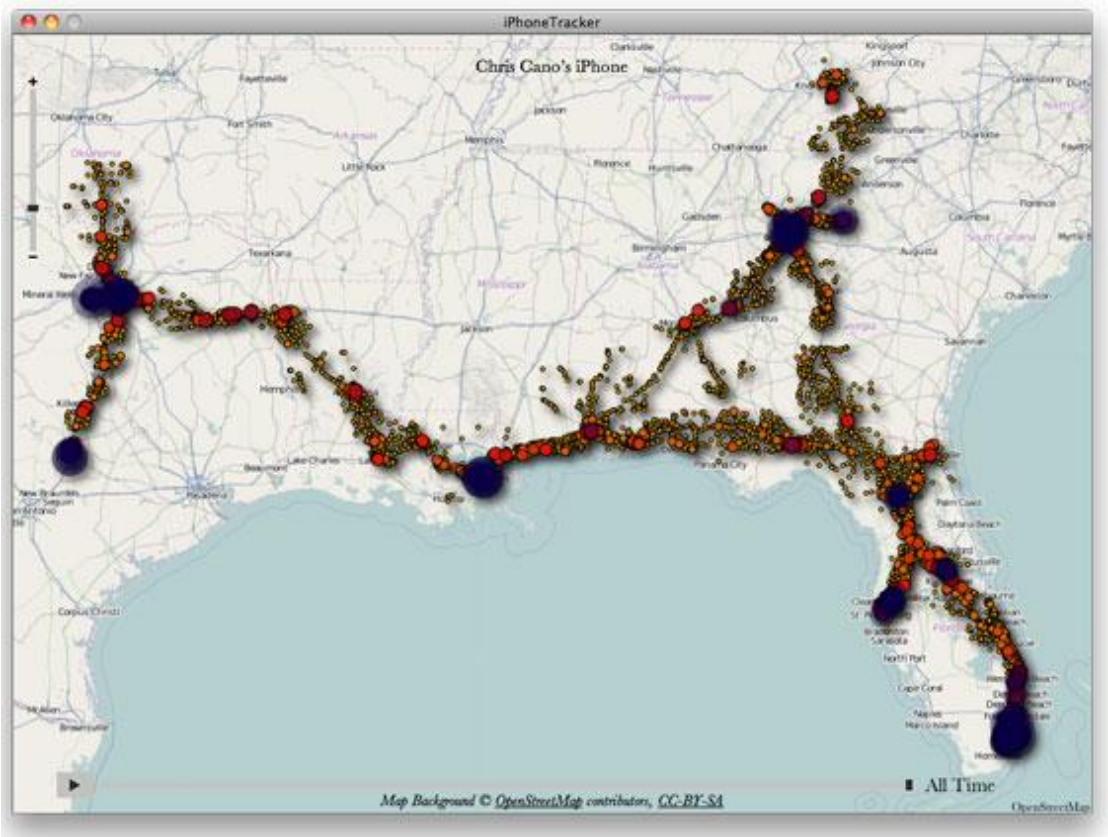
Από τη φωτεινή πλευρά, τουλάχιστον οι κωδικοί πρόσβασης λογαριασμού δεν διακυβεύονται. Το πρόβλημα εδώ είναι ότι οι ειδήσεις έρχονται στο φως μόλις δύο (2) ημέρες μετά από έναν χάκερ που κατάφερε να χάσει τον πιο αληθινό λογαριασμό Instagram - αυτόν που ανήκει στην ηθοποιό Selena Gomez.

4.2.3 Apple: I-phone Tracking

Επίσης ένα άλλο βασικό σκάνδαλο το οποίο είχε απασχολήσει το διαδίκτυο ήταν το "i-phone tracking", το οποίο χρησιμοποιούνταν σε συσκευή τηλεφώνου της εταιρίας Apple. Η Apple έλαβε πολλές κριτικές σχετικά με το πώς τα iPhones και τα iPads συλλέγουν και αποθηκεύουν δεδομένα θέσης χρηστών, τα οποία στη συνέχεια ανάγκασε τον CEO Steve Jobs σε μια σπάνια συγγνώμη τον Απρίλιο του 2011.

Το σκάνδαλο βγήκε στην δημοσιότητα μετά από έρευνες από εξειδικευμένους ερευνητές οι οποίοι ανακάλυψαν ότι ένα μη-κρυπτογραφημένο αρχείο μέσα στις συσκευές, περιείχε μια προσωρινή μνήμη των τοποθεσιών που επισκέφθηκαν οι χρήστες τους τελευταίους 12 μήνες. Το συγκεκριμένο αρχείο είχε την δυνατότητα να καταγράφει αλλά και να αποθηκεύει τη τοποθεσία-συντεταγμένες που βρισκόταν ο χρήστης του κινητού i-phone, ανεξάρτητα από το αν ο αυτός συμφωνεί ή όχι. Σε ορισμένα τηλέφωνα, θα μπορούσαν να αποθηκευτούν δεδομένα αξίας σχεδόν ενός έτους, καθώς η καταγραφή δεδομένων φαίνεται να έχει ξεκινήσει με την ενημέρωση της Apple iOS-4 στο λειτουργικό σύστημα του τηλεφώνου που κυκλοφόρησε τον Ιούνιο του 2010. Με τον τρόπο αυτό σε περίπτωση που κάποιος κλέψει το κινητό και το «χακάρει», μπορεί να έχει πολύ πιο εύκολη πρόσβαση στα στοιχεία του χρήστη που ανήκε η συσκευή αλλά και στις κινήσεις τις οποίες αυτός έχει κάνει. Η κρυπτογράφηση δεδομένων στον υπολογιστή είναι ένας τρόπος προστασίας από αυτό, ωστόσο εξακολουθεί να «αφήνει» το αρχείο στο τηλέφωνο.

Στο **Σχήμα 4**, απεικονίζεται μια σύνοψη των τοποθεσιών (i-phone tracker) χρήστη τον τελευταίο χρόνο, όπως αυτή αποθηκεύεται στον υπολογιστή.



Σχήμα 4 – Τοποθεσίες που βρισκόταν ο χρήστης του κινητού (i-phone tracker)

4.3 Κοινωνικά Μέσα Δικτύωσης: Θέματα Ασφάλειας Προσωπικών Δεδομένων

Ανεξάρτητα από το πώς επεκτείνονται οι ιστότοποι κοινωνικής δικτύωσης, τα ζητήματα ασφάλειας και ιδιωτικότητας ακολουθούν πάντα και παραμένουν ως μεγάλες προκλήσεις για τους χρήστες. Εδώ, εξετάζονται τα θέματα ασφάλειας των κοινωνικών δικτυακών ιστότοπων (SNS) επικεντρώνοντας στα προσωπικά δεδομένα των χρηστών.

Στην πράξη, τα SNS διασφαλίζουν ότι τα αποθηκευμένα δεδομένα είναι ασφαλή από μη-εξουσιοδοτημένη πρόσβαση και χρήση, τα δεδομένα των χρηστών είναι αξιόπιστα και ακριβή και είναι διαθέσιμα όταν απαιτείται. Η ασφάλεια των δεδομένων αποκαλείται επίσης ασφάλεια πληροφοριών.

Οι τεχνολογίες ασφάλειας δεδομένων εφαρμόζονται, για να διασφαλίσουμε ότι τα ψηφιακά δεδομένα, οι σκληροί δίσκοι, το υλικό και το λογισμικό των SNS δεν διαβάζονται από τους χάκερς και τους μη-εξουσιοδοτημένους χρήστες.

Συνήθως, οι στόχοι ασφαλείας (security objectives) των ιστότοπων κοινωνικών δικτύων (SNS), συνίστανται στην ακεραιότητα, τη διαθεσιμότητα και την προστασία της ιδιωτικής ζωής των δεδομένων. Ειδικότερα:

- **Η ακεραιότητα των δεδομένων** (data integrity) σημαίνει ότι τα δεδομένα χρήστη δεν έχουν τροποποιηθεί και ότι αυτά παραμένουν τα ίδια με τα αρχικά δεδομένα. Μια τυπική επίθεση ενάντια στην ακεραιότητα των δεδομένων είναι η επίθεση επονομαζόμενη "man-in-the-middle" (MITM). Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος "host" (ενδιάμεσος) ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.
- **Η διαθεσιμότητα δεδομένων** (data availability) διασφαλίζει ότι ο χρήστης μπορεί πάντα να έχει πρόσβαση στους πόρους και στις πληροφορίες του ιστότοπου. Είναι σημαντικό να βεβαιώνεται ότι οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε δεδομένα ανά πάσα στιγμή. Η άρνηση εξυπηρέτησης είναι ένας τύπος επίθεσης που μπορεί να εμποδίσει τους εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στα δεδομένα κανονικά, όπου αυτός ο τύπος επίθεσης σκοπεύει να διακόψει την υπηρεσία.
- **Το απόρρητο δεδομένων** (data privacy) σχετίζεται με την κατάλληλη χρήση των πληροφοριών. Με άλλα λόγια, τα άτομα, οι εταιρείες και οι τρίτοι θα πρέπει να χρησιμοποιούν τα δεδομένα που τους παρέχονται μόνο για τον νόμιμο σκοπό.

Το ιδιωτικό απόρρητο δεδομένων ονομάζεται επίσης προστασία προσωπικών δεδομένων.

Καθώς η δημοτικότητα των κοινωνικών δικτυακών ιστότοπων μεγαλώνει και αυτά «παράγουν» τεράστιο όγκο δεδομένων κάθε μέρα, τα προσωπικά δεδομένα αντιμετωπίζουν υψηλότερους κινδύνους και αποτελούν πιθανούς στόχους του εγκλήματος στον κυβερνοχώρο με το να υποκλέπτονται για παράνομους σκοπούς. Οι προσωπικές αναγνωρίσιμες πληροφορίες και άλλα είδη ευαίσθητων δεδομένων βρίσκονται υπό απειλές τόσο εσωτερικά όσο και εξωτερικά με το ενδεχόμενο να διαρρεύσουν, να χαθούν, να κλαπούν ή να προσβληθούν από παράνομη πρόσβαση. Όλες οι πληροφορίες σχετικά με αυτά, βρίσκονται υπό απειλή για την ασφάλεια ακόμη και σε καλά προστατευμένες περιοχές.

Οι στατιστικές για το έγκλημα στον κυβερνοχώρο σε ολόκληρο τον κόσμο (σύμφωνα με έρευνα της Symantec – "10 countries that were the source of the most cybercrime in 2016"), η οποία εξέτασε ποιες χώρες ήταν οι μεγαλύτερες πηγές κακόβουλων προγραμμάτων, ανεπιθύμητων μηνυμάτων και επιθέσεων ηλεκτρονικού "ψαρέματος" καταγράφοντας ότι η Αμερική με 23.96%, η Κίνα με 9.63% η Βραζιλία με 5.84%, η Ινδία με 5.11% και η Γερμανία με 3.35%, βρίσκονται στην κορυφή της λίστας με κυβερνο-εγκλήματα στον κυβερνοχώρο. Οι στατιστικές δεν σταματούν εδώ. Η Cybersecurity Ventures προέβλεψε αρχικά ότι οι ζημιές στον κυβερνοχώρο θα κοστίζουν στον κόσμο σε 6 τρισεκατομμύρια δολάρια μέχρι το 2021 στην έκθεση "Hackerpocalypse: A Cybercrime Revelation" που δημοσιεύθηκε τον Αύγουστο του 2016.

4.4 Θέματα Ιδιωτικότητας στα Κοινωνικά Μέσα Δικτύωσης

Εκτός από τα προφανή πλεονεκτήματα από την άποψη της γρήγορηςανάπτυξης της διαδικτυακής κοινότητας, την ταχεία ανταλλαγή πληροφοριών σε επαγγελματικό και ιδιωτικό επίπεδο, οι επίκαιρες πλατφόρμες δικτύων εγείρουν διάφορα ζητήματα σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια των χρηστών τους, όπου αυτοί ανησυχούν για την ιδιωτικότητα και τη χρήση των προσωπικών τους πληροφοριών. Ενώ υπάρχουν στοιχεία ότι τα κοινωνικά μέσα δικτύωσης λειτουργούν με μερικούς σημαντικούς τρόπους για τους ανθρώπους, οι μελέτες του Pew Research Center έχουν δείξει ότι οι άνθρωποι ανησυχούν για όλες τις προσωπικές πληροφορίες που συλλέγονται και μοιράζονται και για την ασφάλεια των δεδομένων τους.

Σε έρευνά του το 2014 συνολικά, το Pew Research Center διαπίστωσε ότι το 91% των Αμερικανών "συμφωνούν" ή "συμφωνούν έντονα" ότι οι άνθρωποι έχουν χάσει τον έλεγχο του τρόπου συλλογής και χρήσης προσωπικών πληροφοριών από κάθε είδους οντότητες.

Περίπου το 80% των χρηστών των κοινωνικών μέσων ενημέρωσης δήλωσαν ότι ανησυχούν για τους διαφημιζόμενους και τις επιχειρήσεις που έχουν πρόσβαση στα δεδομένα που μοιράζονται σε πλατφόρμες κοινωνικών μέσων δικτύωσης και το 64% δήλωσε ότι η αμερικάνικη κυβέρνηση πρέπει να κάνει περισσότερα για να ρυθμίσει τους διαφημιστές. Σε μια άλλη προηγούμενη έρευνά του διαπίστωσε ότι μόνο το 9% των χρηστών των κοινωνικών μέσων ήταν "πολύ σίγουροι" ότι οι εταιρείες κοινωνικών μέσων ενημέρωσης θα προστατεύσουν τα δεδομένα τους. Περίπου οι μισοί χρήστες δεν ήταν καθόλου ή δεν ήταν σίγουροι ότι τα δεδομένα τους ήταν σε ασφαλή χέρια. Επιπλέον παρατηρήθηκε ότι οι άνθρωποι, αγωνίζονται να κατανοήσουν τη φύση και το εύρος των δεδομένων που συλλέγονται για αυτά. Μόνο το 9% πιστεύει ότι έχουν «πολύ έλεγχο» πάνω στις πληροφορίες που συλλέγονται για αυτούς, ακόμη και όταν η συντριπτική πλειοψηφία (74%) δηλώνει ότι είναι πολύ σημαντικό για αυτούς να ελέγχουν ποιος μπορεί να συλλέξει πληροφορίες για αυτούς.

Κατά την τελευταία δεκαετία, παρατηρήσαμε την ταχεία διάδοση των ιστότοπων κοινωνικής δικτύωσης (Social Network Sites - SNS). Ενώ μαθαίνουμε πράγματα για τους ανθρώπους στον κόσμο μας μέσω των κοινωνικών δικτυακών τόπων, μαθαίνουν και αυτοί για εμάς, μέσω του ίδιου καναλιού επίσης.

Για παράδειγμα, το Facebook, το πιο δημοφιλές SNS με πάνω από 1,4 δισεκατομμύρια ενεργούς χρήστες από τον Μάρτιο του 2015, ενθαρρύνει τους χρήστες του να χρησιμοποιήσουν τις πραγματικές τους πληροφορίες ταυτότητας και να ανεβάσουν τα προσωπικά τους στοιχεία στις σελίδες του προφίλ τους. Μια τυπική σελίδα προφίλ στο Facebook περιλαμβάνει γενέθλια, διευθύνσεις, αριθμούς τηλεφώνου και πιο οικεία στοιχεία όπως ενδιαφέροντα, χόμπι, κατάσταση σχέσεων και σεξουαλική προτίμηση του ιδιοκτήτη. Βλέπουμε εικόνες από τα παιδιά τους, τις οικογένειές τους, τα αυτοκίνητά τους, τις διακοπές τους και τα σπίτια τους. Μαθαίνουμε για τις ευπάθειές τους. Όλη αυτή η κοινή χρήση μπορεί να συμβάλει στη δημιουργία στενότερων σχέσεων μεταξύ τους αλλά επίσης «καταστρέφει» (ενδεχομένως) το ιδιωτικό απόρρητο των πληροφοριών των χρηστών του SNS's. Είναι σαφές ότι υπάρχουν πολλοί άνθρωποι εκτός από φίλους και τους γνωστούς που ενδιαφέρονται για τις πληροφορίες που οι διάφοροι χρήστες μοιράζονται στο προφίλ τους σελίδες (π.χ. κλέφτες ταυτότητας, scammers, συλλέκτες χρεών, πωλητές που αναζητούν πλεονέκτημα αγοράς), οι οποίοι χρησιμοποιούν τα SNS για τη συλλογή πληροφοριών σχετικά με τους χρήστες.

Λόγω της πολυπλοκότητας της έννοιας της ιδιωτικής ζωής, είναι δύσκολο να καταλάβουμε πώς τα άτομα ορίζουν την ιδιωτικότητά τους στον εικονικό κόσμο. Οι συζητήσεις σχετικά με τα ζητήματα απορρήτου σε απευθείας σύνδεση των πολιτών συνεχίζονται.

Για παράδειγμα, η συζήτηση μεταξύ Europe-vs-Facebook και το Facebook έχουν διαρκέσει αρκετά χρόνια χωρίς σαφή λύση ακόμα. Από τη μια πλευρά, ορισμένοι

υποστηρίζουν ότι ο κανόνας για την ανταλλαγή προσωπικών πληροφοριών αλλάζει και οι άνθρωποι γίνονται πιο ανοικτοί με την προσωπική τους ζωή.

Για παράδειγμα, ο Mark Zukerberg, Διευθύνων Σύμβουλος του Facebook, δήλωσε: «Οι άνθρωποι αισθάνονται άνετα όχι μόνο να μοιράζονται περισσότερες πληροφορίες και διαφορετικά είδη, αλλά πιο ανοιχτά και με περισσότερους ανθρώπους. Αυτός ο κοινωνικός κανόνας είναι κάτι που εξελίχθηκε με την πάροδο του χρόνου». Ο Pete Cashmore, Διευθύνων Σύμβουλος της Mashable, μοιράστηκε μια παρόμοια άποψη και είπε: «Η ιδιωτικότητα είναι νεκρή». Από την άλλη πλευρά, ορισμένοι ερευνητές εξακολουθούν να πιστεύουν ότι η ιδιωτικότητα στο διαδίκτυο είναι εξίσου σημαντική με την ιδιωτική ζωή. Υποστηρίζουν ότι η υπονόμευσή της (ιδιωτικότητας) σε απευθείας σύνδεση ιδιωτικού απόρρητου των ανθρώπων είναι να στερήσει τους ανθρώπους την λευτεριά και την ελευθερία (freedom and liberty). Ο Danah Boyd, ανώτερος ερευνητής της Microsoft Research, δήλωσε: «Οι άνθρωποι θα πρέπει - και κάνουν - να φροντίσουν βαθιά για το ιδιωτικό απόρρητο στο διαδίκτυο».

Αν και δεν υπάρχει αμφιβολία ότι οι άνθρωποι και η κοινωνία θα προσαρμοστούν τελικά στο τεχνολογικό περιβάλλον, η κατανόηση και προστασία της ιδιωτικότητας των χρηστών του Διαδικτύου εξακολουθεί να είναι κρίσιμη για τις κυβερνήσεις και τις επιχειρήσεις.

ΚΕΦΑΛΑΙΟ 5 –ΣΤΑΣΗ ΧΡΗΣΤΩΝ ΚΟΙΝΩΝΙΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΜΕΤΡΑ

5.1 Εισαγωγή

Στο Κεφάλαιο 5, εξετάζουμε μερικά θέματα που αφορούν τη συμπεριφορά και την ψυχολογία που υιοθετούν οι Χρήστες των μέσων κοινωνικής δικτύωσης από τη χρήση και την σύνδεσή τους σε αυτά, παραθέτοντας σχετικά στοιχεία από μελέτη για το προφίλ που αυτοί παρουσιάζουν. Στη συνέχεια, αναφερόμαστε στα θέματα της στάσης – αντίληψης των χρηστών αναφορικά με τα μέτρα προστασίας για την ασφάλεια και το απόρρητο που διαλαμβάνουν με τις διεπαφές τους (άλλους χρήστες) των κοινωνικών δικτύων και την έκθεσή τους σε κινδύνους. Τέλος, παρατείθεται βασικά μέτρα ως τμήμα μιας γενικότερης στρατηγικής μέτρων πρόληψης που οι χρήστες πρέπει να ακολουθούν, ώστε να προστατεύονται με γνώμονα την ασφάλεια και το απόρρητο των πληροφοριών τους και των προσωπικών δεδομένων κατά την χρήση των κοινωνικών μέσων δικτύωσης.

5.2 Συμπεριφορά (Mindset) και Ψυχολογία των Χρηστών Κοινωνικών Δικτύων

Σύμφωνα με το ερευνητικό κέντρο Pew Research, η πλειοψηφία των ενήλικων χρηστών που χρησιμοποιούν τα social media, είναι συνδεδεμένοι σε παραπάνω από ένα κοινωνικά δίκτυα. Και σύμφωνα με έρευνα η οποία πραγματοποιήθηκε από το Βασιλικό Κολέγιο του Λονδίνου και το Πολιτειακό Πανεπιστήμιο της Πενσυλβάνια, οι χρήστες των κοινωνικών δικτύων υιοθετούν εντός του καθενός εξ αυτών ένα άλλο πρόσωπο, μία διαφορετική “persona” από αυτήν που τους χαρακτηρίζει στην πραγματική τους ζωή.

Οι ερευνητές εικάζουν ότι οι διαφορετικές περσόνες των χρηστών αναλόγως του social media που χρησιμοποιούν, πηγάζουν από μία εσωτερική επιθυμία του καθενός να ταιριάζει με την "ξεχωριστή, διακριτή κουλτούρα ή τους άγραφους κανόνες συμπεριφοράς" του κάθε κοινωνικού δικτύου.

Για παράδειγμα, όπως αναφέρουν, μία φωτογραφία ενός πολύχρωμου ποτού μπορεί να είναι δημοφιλής στο Instagram, αλλά καθόλου αποδεκτή στο LinkedIn. Ως εκ τούτου, οι χρήστες παρουσιάζουν τους εαυτούς τους διαφορετικά σε κάθε “online” περιβάλλον.

Για να καταλήξει σε συμπεράσματα, η ερευνητική ομάδα συγκέντρωσε στοιχεία από περισσότερους από 100,000 άτομα μέσω του site About.me, στο οποίο οι χρήστες με τη θέλησή τους δίνουν το προφίλ τους στα social, γεγονός που το καθιστά μία αξιόπιστη πηγή δεδομένων, σύμφωνα με δηλώσεις στο σχετικό δελτίο τύπου από τον Dongwon Lee, έναν εκ των ερευνητών. Η ερευνητική ομάδα προχώρησε σε ανάλυση των προφίλ των χρηστών στις πλατφόρμες κοινωνικής δικτύωσης Facebook, Instagram, Twitter και Linkedln και ειδικότερα, των φωτογραφιών προφίλ και των βιογραφικών πληροφοριών τους. Πρόκειται για πληροφορίες οι οποίες παρέχονται από τους ίδιους τους χρήστες και όπως εξήγησε ο καθηγητής Lee, "οι χρήστες έχουν την τάση να παρουσιάζουν τους εαυτούς τους με διαφορετικούς τρόπους σε αυτούς τους διαφορετικούς κόσμους". Το εντυπωσιακότερο είναι ότι κατά την περίοδο της μελέτης και ανάλυσης, οι ερευνητές διαπίστωσαν πως οι χρήστες όχι μόνο παρουσιάζονται διαφορετικοί στα social media, αλλά και ότι υπάρχουν συγκεκριμένα κοινά στον τρόπο που υιοθετούν και προβάλλουν την εικόνα τους οι διάφορες δημογραφικές ομάδες. Για παράδειγμα, οι γυναίκες είναι πολύ λιγότερο πιθανό να εμφανίζονται στα social media με φωτογραφίες στις οποίες φοράνε μυωπικά γυαλιά σε σχέση με τους άνδρες. Παρομοίως, οι χρήστες κάτω των 25 ετών, ήταν λιγότερο πιθανό να χαμογελούν στις φωτογραφίες προφίλ τους.

Οι τάσεις αναλόγως κοινωνικού δικτύου και ομάδας πληθυσμού ήταν τόσο συνεπείς, ώστε οι ερευνητές αναφέρουν ότι μόνο από την περιγραφή κάθε προφίλ και τη συνοδευτική "profile picture" του, ένα σχετικό μοντέλο που δημιούργησαν ήταν ικανό να αναγνωρίσει σωστά για ποιο social media είχε δημιουργηθεί το εκάστοτε προφίλ, με ποσοστό επιτυχίας έως και **80%.**

Οι ερευνητές πάντως δεν πιστεύουν ότι η αλλαγή "persona" των χρηστών είναι τόσο συνειδητή όσο είναι μία υποσυνείδητη προσαρμογή της συμπεριφοράς τους. Ο Nisanth Sastry από το Βασιλικό Κολέγιο του Λονδίνου και ένας εκ των ερευνητών εξηγεί πως οι χρήστες τροποποιούν το προφίλ τους μάλλον υποσυνείδητα, προσαρμόζοντας τη συμπεριφορά τους στο εκάστοτε κοινωνικό δίκτυο. "Παρά τις προσπάθειές μας, ακόμα ταιριάζουμε με τα στερεότυπα του φύλου και της ηλικίας μας, στον τρόπο που προσαρμόζουμε τις "persona" μας [στον ψηφιακό κόσμο των social]", εξηγεί ο Sastry.

"Τα μέσα κοινωνικής δικτύωσης αποτελούν μεγάλο μέρος της ζωής μας.

Ως εκ τούτου, η κατανόης η της αλληλεπίδρασης μεταξύ μας όταν τα χρησιμοποιούμε είναι σημαντική για την κατανόηση του ποιοι είμαστε στον

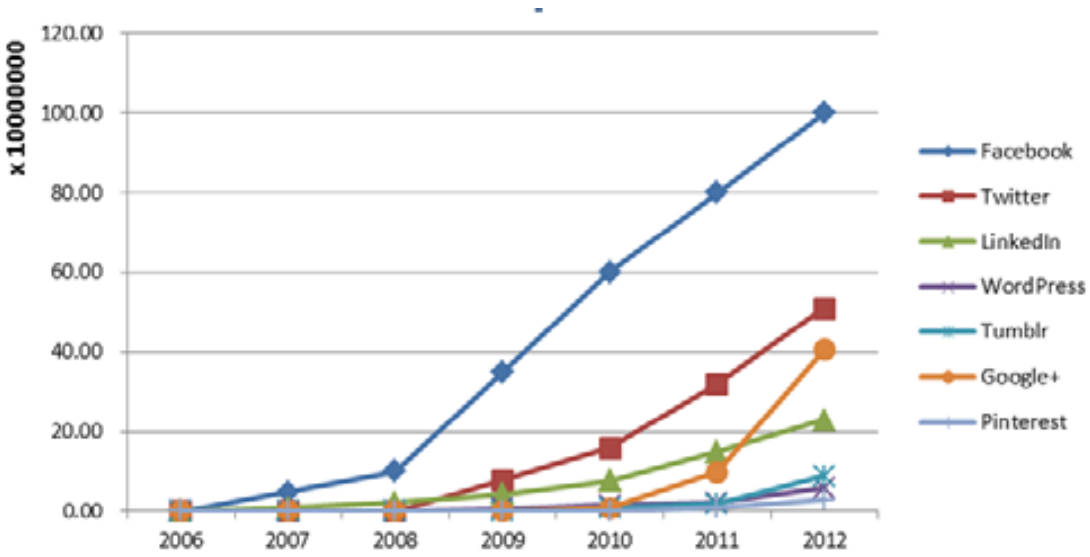
“online” κόσμο και του πώς μπορούμε να σχετιζόμαστε μεταξύ μας με τρόπους ουσιαστικούς", σημειώνουν οι ερευνητές. “Στην εποχή των κοινωνικών μέσων μαζικής ενημέρωσης, χωρίς να το συνειδητοποιούμε, αφήνουμε τα σημάδια μας. Αν μπορούμε να αξιοποιήσουμε αυτά τα ψηφιακά ίχνη, τότε μπορούμε να μάθουμε πολλά για την συμπεριφορά μας”.

5.3 Στάση των Χρηστών και τα Μέτρα Προστασίας

5.3.1 Επίγνωση Χρηστών για Απόρρητο κ Ασφάλεια

Εξετάζοντας τους χρήστες ως διακριτές οντότητες (individuals) - και όχι στο αντίστοιχο πλαίσιο όπου ως «χρήστης» ορίζεται η επιχείρηση ή ένας οργανισμός - είναι διαπιστωμένο ότι το κάθε άτομο χρησιμοποιεί τα κοινωνικά δίκτυα, έχοντας έναν διαφορετικό προσωπικό σκοπό ή / και στόχο.

Με τη δημιουργία «Λογαριασμού Χρήστη» (User Account) σε ένα συνδεδεμένο κοινωνικό δίκτυο (Online Social Network - OSN), ανοίγεται ένας δρόμος προς τις ευκαιρίες αλλά ταυτόχρονα επιφυλάσσει και ορισμένους σημαντικούς κινδύνους. Οι χρήστες των κοινωνικών δικτύων μπορούν να εκφοβιστούν, οι φωτογραφίες τους μπορούν να κλαπούν ή οι θέσεις κατάστασής τους (status post) να φτάσουν σε ανεπιθύμητο κοινό. Ακόμη και όταν τα προφίλ δεν περιέχουν καμία πληροφορία, τα κοινωνικά γραφήματα μπορεί να αναλυθούν για να εξαχθούν προσωπικές πληροφορίες. Παρ’ όλα αυτά, τα κοινωνικά δίκτυα έχουν εκατοντάδες εκατομμύρια χρήστες, επειδή οι χρήστες πιστεύουν ότι τα θετικά υπερισχύουν των αρνητικών και διατηρούν έτσι την παρουσία τους στο διαδίκτυο. Ωστόσο, αυτή η συμπεριφορά των χρηστών δεν είναι ανέμελη. Οι μεμονωμένες περιπτώσεις παραβίασης της ιδιωτικής ζωής και οι συνέπειές τους, έχουν συζητηθεί ευρέως στα κοινωνικά μέσα ενημέρωσης και οι κίνδυνοι για την προστασία της ιδιωτικής ζωής έχουν αυξηθεί και αυτοί στην πάροδο του χρόνου, καθώς τα κοινωνικά δίκτυα έχουν αυξηθεί εκθετικά σε μέγεθος **(Σχήμα 5)**.



Σχήμα 5 – Ανάπτυξη Κοινωνικών Δικτύων (2006 – 2012)

Αρκετές ερευνητικές προσπάθειες έχουν διεξαχθεί για την ανακούφιση από αυτά τα προβλήματα, με τα αποτελέσματα ορισμένων εργαλείων που βοηθούν τους χρήστες για να είναι περισσότερο ενήμεροι για την προστασία της ιδιωτικής τους ζωής. Ωστόσο, εμπειρικές μελέτες δείχνουν ότι οι χρήστες των κοινωνικών δικτύων, δεν συνηθίζουν να χρησιμοποιούν τις καθορισμένες ρυθμίσεις απορρήτου και πολύ συχνά δεν αλλάζουν τις προεπιλεγμένες (by default), ρυθμίσεις απορρήτου οι οποίες είναι πολύ «συναινετικές». Κατά συνέπεια, η δημιουργία νέων σχέσεων – επαφών (φιλίας), χωρίς να προσλαμβάνονται (ειδικεύονται) οι κατάλληλες ρυθμίσεις απορρήτου, ενδέχεται να εκθέσουν τον κάθε χρήστη στον κίνδυνο απώλειας προσωπικών δεδομένων χωρίς καν να το αντιληφθεί. Στο γεγονός αυτό οφείλεται ότι σχεδόν σε όλα τα συνδεδεμένα κοινωνικά δίκτυα (OSN) οι χρήστες μπορούν να αναφέρουν (παραθέσουν) πληροφορίες – πόρους άλλων χρηστών στο κοινωνικό γράφημά τους όπου γενικά, δεν είναι δυνατό ή είναι πολύ δύσκολο για τον κάθε χρήστη να ελέγχει τις πληροφορίες - πόρους που δημοσιεύονται από κάποιο άλλον χρήστη. Κατά αυτό τον τρόπο, αυτή η ανεξέλεγκτη ροή πληροφοριών υπογραμμίζει το γεγονός ότι η δημιουργία μιας νέας «σχέσης» (επαφής) με άλλους χρήστες, εκθέτει κάποιον σε κάποιους από τους κινδύνους απορρήτου.

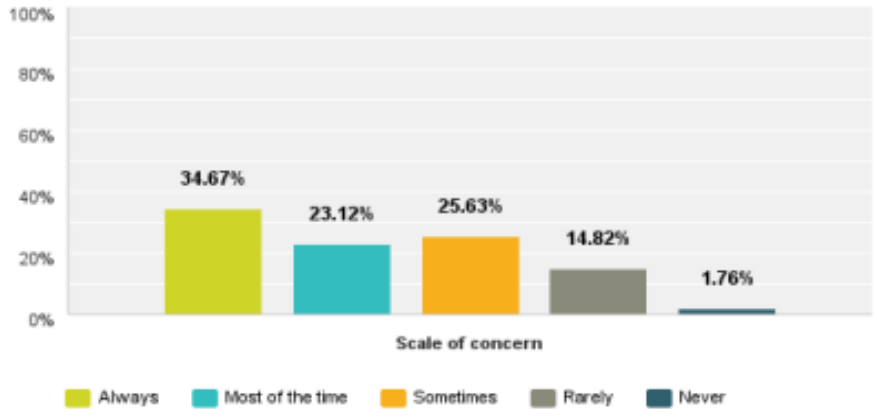
Παρά τις πιθανές σοβαρές συνέπειες της εγκαθίδρυσης νέων σχέσεων (επαφών), η σημερινή κατάσταση είναι ότι οι χρήστες των κοινωνικών δικτύων δεν είναι καλά ενημερωμένοι για τους εικονικούς φίλους τους και με τους οποίους οι φίλοι τους, διατηρούν επικοινωνία.

Τα εξαιρετικά δημοφιλή κοινωνικά δίκτυα εξακολουθούν να πιστεύουν ότι ένας «φίλος» είναι κάποιος με τον οποίο ένας χρήστης μπορεί να μοιραστεί τα πάντα, και επιπλέον, ότι ο χρήστης μπορεί ακόμη και να μοιράζεται τα περισσότερα από τα στοιχεία του προφίλ του με τους φίλους των φίλων του (friends of friends). Οι συνιστώμενες ρυθμίσεις απορρήτου είναι σύμφωνες με αυτήν την έννοια του φίλου. Για παράδειγμα, στο Facebook, οι φίλοι φίλων, επιτρέπονται από προεπιλογή να βλέπουν τα περισσότερα μέρη ενός προφίλ χρήστη.

Σχετική έρευνα (Edith Cowan University Researh Online - 2016) διεξήχθη, για την εξακρίβωση του επιπέδου αποκάλυψης των προσωπικών πληροφοριών από τα μέλη ιστοσελίδας κοινωνικής δικτύωσης κατά τη στιγμή της προσχώρησής τους και τις επακόλουθες ενημερώσεις τους στην ιστοσελίδα αναφορικά τις ρυθμίσεις για την ασφάλεια της ιδιωτικότητας.

Στην ερώτηση: "Είναι η ιδιωτικότητα των πληροφοριών σας σε ιστότοπους κοινωνικής δικτύωσης μια μεγάλη ανησυχία για σας;" όπου σκοπό είχε να προσδιοριστεί η αξία της ιδιωτικότητας (privacy) στο διαδίκτυο για τον χρήστη, προέκυψε ότι εάν κάποιοι δεν ανησυχούν πολύ για την προστασία της ιδιωτικής ζωής των πληροφοριών τους στο διαδίκτυο, δεν θα είναι τόσο αυστηροί στην εφαρμογή προστατευτικών ρυθμίσεων ιδιωτικότητας και ασφάλειας για να αποφευχθεί η διαρροή πληροφοριών. Επιπλέον, τα άτομα που εκτιμούν την ιδιωτικότητά τους και ανησυχούν περισσότερο για τις πληροφορίες τους, (δεδομένα) πιθανότατα δεν θα μοιράζονται τόσα προσωπικά στοιχεία τους σε σχέση με όσους ανησυχούν λιγότερο για την ιδιωτικότητα.

Με βάσει τα ανωτέρω προαναφερόμενα σε σχέση με την τεθείσα ερώτηση, η διαβάθμιση για το σχετικό ενδιάφερον (concern) των χρηστών αναφορικά με το θέμα της ιδιωτικότητα (των συμμετεχόντων στην έρευνα) ήτοι δηλ. του “Scale of concern over Privacy”, απεικονίζεται στο Σχήμα 6, ως κατωτέρω:



Σχήμα 6 – Κλίμακα ενδιαφέροντος για την ιδιωτικότητα "Scale of concern over Privacy"

Τα αποτελέσματα (σύμφωνα με τη μελέτη) έδειξαν ότι υπήρξε τελικά έλλειψη εμπιστοσύνης προς τους παρόχους κοινωνικών δικτύων όσον αφορά την αποθήκευση και την προστασία των χρηστών, καθώς το 66,3% των ερωτηθέντων απάντησε ότι δεν εμπιστεύτηκαν τους παρόχους τους με τις πληροφορίες (δεδομένα) τους.

5.3.2 Ενέργειες Χρηστών - Απαιτήσεις για Ασφάλεια, Απόρρητο

Η βασική αρχή για την ασφάλεια και το απόρρητο είναι ότι τα δεδομένα των χρηστών πρέπει να προστατεύονται όπου υπάρχουν, είτε σε εφαρμογή βάσεων δεδομένων ή σε άλλα μέρη. Η ασφάλεια των μέσων κοινωνικών δικτύωσης είναι εξαιρετικά σημαντική και αφορά την προστασία από τις κάθε είδους «επιθέσεις» για την ενίσχυση της αξιοπιστίας των υπό διαχείριση πληροφοριών. Σε αυτό συμβάλλει η ύπαρξη μιας καλής ηθικής ενημέρωσης – πληροφόρησης (good information ethics) πολιτική ασφάλειας, η οποία να ενδυναμώνει την ενημέρωση των χρηστών αναφορικά με την ασφάλεια των πληροφοριών τους και να βελτιώνει τα συστήματα και διαδικασίες διαχείρισης των πληροφοριών χρηστών για την προστασία του απορρήτου αυτών. Αναφορικά με τη συλλογή των πληροφοριών και τη χρήση τους, πρέπει να υπάρχουν περιοριστικοί κανόνες με τη διαφάνεια του σκοπού για τη συλλογή και τη χρήση αυτών.

Για όσον αφορά δε το απόρρητο, θα πρέπει να τίθεται υψηλότερο επίπεδο ασφάλειας και αυστηρή στη διαχείριση πρόσβασης και χρήσης πληροφοριών των χρηστών.

Στο περιβάλλον δικτύωσης που βασίζεται στην τεχνολογία των πληροφοριών, η συνειδητοποίηση των χρηστών σχετικά με την ασφάλεια των πληροφοριών είναι πολύ σημαντική. Η ευημερία και η ανάπτυξη των κοινωνικών δικτύων βασίζονται στην εμπιστοσύνη μεταξύ των χρηστών. Τα περισσότερα μέσα κοινωνικής δικτύωσης, απαιτούν από τους χρήστες να εγγραφούν με τα πραγματικά ονόματά τους, ώστε να παρέχεται υψηλή ακρίβεια των πληροφοριών των χρηστών. Επιπλέον, ο κατάλογος διεπαφών είναι βασικά οι πραγματικοί φίλοι στη ζωή και η ενημερότητα των χρηστών για την ασφάλεια δεν επαρκεί. Σε πολλές περιπτώσεις, οι χρήστες επαναστρέφουν εύκολα κάποιες φαινομενικά δόλιες (fraudulent) πληροφορίες από φίλους, οι οποίες τείνουν να διευκολύνουν τους χάκερς να επιτύχουν το στόχο τους. Οι χρήστες που ενδιαφέρονται για κοινωνικά δίκτυα, συχνά δημοσιεύουν τμήματα της καθημερινής

ζωής τους και «ανεβάζουν» πολλές φωτογραφίες και βίντεο για να μοιραστούν με άλλους χρήστες με τις ενέργειες αυτές να δημιουργούν υψηλό κίνδυνο διαρροής πληροφοριών.

Για τα ζητήματα ασφάλειας και προστασίας απορρήτου κατά τη χρήση των κοινωνικών δικτύων, ο κάθε χρήστης πρέπει να βελτιώσει τις γνώσεις του σχετικά με θέματα της ασφάλειας των πληροφοριών αλλά και του απορρήτου. Σε συνέχεια, για να αποφευχθούν τα θύματα του εγκλήματος στον κυβερνοχώρο, οι χρήστες πρέπει να λάβουν ορισμένες προφυλάξεις. Μερικές βοηθητικές και χρήσιμες υποδείξεις είναι οι ακόλουθες:

- Προσεκτική ρύθμιση των «ρυθμίσεων απορρήτου», για εξασφάλιση ότι μόνο τα άτομα που εμπιστεύεστε έχουν πρόσβαση στα προφίλ σας και στις πληροφορίες που δημοσιεύετε. Περιορισμός της δυνατότητας των άλλων να δημοσιεύουν πληροφορίες στις σελίδες σας, για την προστασία από τις περιπτώσεις όπου οι άλλοι δημοσιεύουν ορισμένες πληροφορίες «σκουπίδια» ή κακόβουλα links. Οι προεπιλεγμένες ρυθμίσεις για ορισμένους ιστότοπους ενδέχεται να επιτρέπουν σε οποιονδήποτε να δει τις πληροφορίες μας ή να δημοσιεύσει πληροφορίες στη σελίδα μας.
- Προσεκτικός έλεγχος της πολιτικής απορρήτου του μέσου κοινωνικής δικτύωσης. Μπορούμε να αξιολογήσουμε τον ιστότοπο και να διασφαλίσουμε ότι κατανοούμε την πολιτική απορρήτου. Ορισμένοι ιστότοποι ενδέχεται να μοιράζονται πληροφορίες χρηστών, όπως προτιμήσεις, διευθύνσεις ηλεκτρονικού ταχυδρομείου και αριθμούς τηλεφώνου. Εάν μια πολιτική απορρήτου είναι κακό-σχεδιασμένη ή δεν μπορεί να προστατεύσει σωστά τις πληροφορίες μας, μπορούμε να αρνηθούμε να χρησιμοποιήσουμε τον ιστότοπο.
- Προσεκτική επιλογή σχετικά με την εγκατάσταση ορισμένων συγκεκριμένων εφαρμογών. Ειδικότερα, ορισμένα μέσα κοινωνικής δικτύωσης παρέχουν τις εφαρμογές τρίτων κατασκευαστών, όπως τα παιχνίδια όπου η πλατφόρμα κοινωνικής δικτύωσης να ενδέχεται να μην έχει προβεί σε έλεγχο ποιότητας ή αναθεώρησης αυτών των εφαρμογών και αυτές να ενδέχεται να έχουν πλήρη πρόσβαση στο λογαριασμό του χρήστη και τις πληροφορίες που μοιράζεται. Οι κακόβουλες εφαρμογές μπορούν να έχουν πρόσβαση στα δεδομένα μας για να αλληλεπιδρούν με τους φίλους μας για λογαριασμό μας, να υποκλέπτουν και να καταχρώνται τα προσωπικά μας δεδομένα. Ως εκ τούτου, θα πρέπει να γίνεται εγκατάσταση μόνο εφαρμογών που προέρχονται από αξιόπιστους, γνωστούς ιστότοπους και αν δεν χρειάζεται πλέον να χρησιμοποιείται μια εφαρμογή, θα

πρέπει να αφαιρεθεί. Η εγκατάσταση ορισμένων εφαρμογών ενδέχεται να τροποποιήσει τις ρυθμίσεις ασφαλείας και απορρήτου από την αρχική προεπιλογή.

- Αποφυγή παροχής της διεύθυνσης του ηλεκτρονικού ταχυδρομείου ή των αριθμών τηλεφώνων των φίλων μας.
- Μη παραχώρηση έγκρισης στα κοινωνικά δίκτυα να σαρώσουν το βιβλίο διευθύνσεων ηλεκτρονικού ταχυδρομείου ή το βιβλίο διεπαφών. Αναλυτικότερα, όταν εισερχόμεθα σε έναν νέο ιστότοπο κοινωνικού δικτύου, ίσως χρειαστεί να εισαγάγουμε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον κωδικό πρόσβασης, για να ελέγξουμε αν οι επαφές μας βρίσκονται στο ίδιο δίκτυο.
- Ο ιστότοπος όμως, μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να στείλει μηνύματα ηλεκτρονικού ταχυδρομείου σε όλους στη λίστα επαφών μας, γεγονός που οδηγεί σε μεγάλο αριθμό ανεπιθύμητων μηνυμάτων.
- Ιδιαίτερη προσοχή σχετικά με συγκεκριμένους συνδέσμους. Αν ένας σύνδεσμος φαίνεται ύποπτος ή φαίνεται πολύ καλός για να είναι αληθινός ("too good to be true"), να μη γίνει προσπάθεια σύνδεσης σε αυτόν, ακόμα κι αν ο σύνδεσμος είναι από τη σελίδα του πιο αξιόπιστου «φίλου» μας. Ο λογαριασμός του «φίλου» ενδέχεται να έχει μολυνθεί ή να πειραματιστεί και τώρα να μεταδίδει κάποιο κακόβουλο λογισμικό.
- Είναι προτιμότερη η συνήθεια να χρησιμοποιείτε τους προσωπικούς σελιδοδείκτες (bookmarks) ή να πληκτρολογείτε τη διεύθυνση (URL) του κοινωνικού διαδικτύου απευθείας στον περιηγητή (explorer). Εάν κάνουμε κλικ σε έναν σύνδεσμο σε έναν ψεύτικο ιστότοπο κοινωνικής δικτύωσης μέσω ανεπιθύμητης αλληλογραφίας ή άλλου ιστότοπου, ενδεχομένως να εισάγουμε το όνομα λογαριασμού και τον κωδικό πρόσβασης στον πλαστό ιστότοπο και τότε τα προσωπικά μας στοιχεία θα μπορούσαν να κλαπούν.
- Για τη διαγραφή του λογαριασμού (User Account), να αφαιρεθούν πρώτα όλα τα δεδομένα και να γίνει βεβαίωση ότι ο λογαριασμός πρέπει να διαγραφεί αντί να απενεργοποιηθεί.
- Χρησιμοποίηση «ισχυρών» και μοναδικών κωδικών πρόσβασης (password). Οι σύντομοι, απλοί και «αφελείς» κωδικοί πρόσβασης είναι εύκολο να υποτιμηθούν από λογισμικό υπολογιστή.
- Προσεκτική επιλογή των «φίλων» και των «ομάδων» συμμετοχής στα κοινωνικά δίκτυα. Όσο αυξάνει ο αριθμός των «φίλων» και των «ομάδων» που ο χρήστης συμμετέχει, διευρύνεται περισσότερο οι σύνδεσμοι (χρήστες) που έχουν πρόσβαση στις πληροφορίες μας. Με την υποκλοπή «ταυτότητας» χρήστη οι

κλέφτες ταυτότητας μπορεί να δημιουργήσουν ψεύτικα προφίλ για να αντιγράψουν τις πληροφορίες μας μόλις προστεθεί ο ψεύτικος «φίλος» στις διεπαφές, τμήμα ή σύνολο του προφίλ χρήστη οδηγεί στη διαρροή των προσωπικών του πληροφοριών.

- Να μην θεωρείται βέβαιο το απόρρητο σε ένα μέσο κοινωνικής δικτύωσης. Για το λόγο αυτό, δεν πρέπει να μοιράζονται οι εμπιστευτικές μας πληροφορίες ούτε για προσωπική ούτε για επαγγελματική χρήση.
- Μη δημοσίευση των προσωπικών στοιχείων - όπως η διεύθυνση, το χρονοδιάγραμμα και η καθημερινή «ρουτίνα» - γεγονός που καθιστά τους χρήστες ευάλωτους.
- Πριν τη δημοσίευση πληροφοριών ή σχολίων, να υπάρχει σκέψη αναφορικά με τη διακριτικότητα. Αφού δημοσιευθούν κάποιες πληροφορίες, ενδεχομένως να μην μπορούν να αποσυρθούν αργότερα.
- Διαγραφή των meta-data κατά την ανάρτηση εικόνων. Υπάρχει το ενδεχόμενο αυτά να περιέχουν την ημερομηνία και την ώρα της εικόνας.

Έχοντας αποδεχθεί ότι τα κοινωνικά δίκτυα έχουν εγκατεστηθεί στις ζωές των ανθρώπων και θεωρούμενα ως αναπόσπαστο κομμάτι της ζωής τους, αυτό έχει ως αποτέλεσμα - παρόλα τα πλεονεκτήματα που μπορεί να προσφέρουν - να θέτει τη ζωή τους σε κίνδυνο οπότε, οι ίδιοι οι χρήστες αυτών - αλλά γενικώς και του παγκόσμιου διαδικτύου (internet) – είναι επιβεβλημένο λόγω των αυξανόμενων "προκλήσεων" (κυρίως των τεχνολογικών) που εμφανίζονται, να προσλαμβάνουν ορισμένα συγκεκριμένα μέτρα για την προστασία τους. Δεδομένου ότι όλοι οι χρήστες των μέσων κοινωνικής δικτύωσης μπορούν πολύ εύκολα να γίνουν «θύμα» ενός «κυβερνο-εγκληματία», σκοπός του κάθε χρήστη είναι να υιοθετήσει ορισμένες πολύ βασικές στρατηγικές ώστε, να ελαχιστοποιήσει τις πιθανότητες, να αποτελεί στόχο.-

Επίλογος

Τα κοινωνικά δίκτυα συνεχώς εξελίσσονται όλο και περισσότερο διότι με την αύξηση των χρηστών οι ανάγκες-απαιτήσεις μεγαλώνουν. Ποτέ άλλοτε τόσοι πολλοί άνθρωποι δεν είχαν την ευκαιρία να έρθουν σε επαφή, διαμοιράζοντας πληροφορίες.

Με την αυξανόμενη χρήση των μέσων κοινωνικής δικτύωσης (social media) και την εμφάνιση τους ως ένα νέο φαινόμενο στις ανθρώπινες ζωές, δεν μπορεί κανείς να είναι απόλυτα σίγουρος για την «ασφαλή» προστασία των προσωπικών του δεδομένων.Ως εκ τούτου οι εμφανίζόμενοι διαρκώς όλο και περισσότεροι «κίνδυνοι» - οι οποίοι και αυξάνονται πολλαπλασιαστικά με την ανάπτυξη της τεχνολογίας – και τους οποίους προσπαθεί να διαχειριστεί επαρκώς η παγκόσμια κοινότητα ώστε να μειώσουν τις επιπτώσεις και τον αντίκτυπό τους, αντιμετωπίζονται με την υιοθέτηση συγκεκριμένων μέτρων προστασίας στα οποία συμπεριλαμβάνονται οι παγκόσμιοι κανονισμοί και η ανάπτυξη διεθνών και εθνικών ή και τοπικών νομοθεσιών που εποπτεύονται από τις αντίστοιχες αρμόδιες αρχές.

Στα ανωτέρω μέτρα προστασίας, έρχονται να προστεθούν και οι ανελλιπώς δημοσιευόμενες προτάσεις και συμβουλές της παγκόσμιας κοινότητας για την ορθότερη χρήση των ιστοσελίδων κοινωνικών δικτύων σε θέματα ασφάλειας και απορρήτου αλλά και τρόπων διαχείρισης και συμπεριφορών των χρηστών. Αποτελεί ωστόσο υποχρέωση η υιοθέτηση μιας υπεύθυνης στάσης όλων των χρηστών που χρησιμοποιούν τις ιστοσελίδεςτων κοινωνικών δικτύων να ενημερώνονται προσεκτικάγια τα δικαιώματά τους και για την ανάγκη προστασίας της προσωπικής τους ζωής, τόσο σε αυτά όσο και και για όλο το διαδίκτυο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΚΕΦΑΛΑΙΟ 1^{ο}

- https://sites.google.com/site/koinonikidiktyosi/istorike-anadrome
- http://imu.ntua.gr/static/courses/strategicISmanagement/lectures/11-Social%20Networks.pdf
- **.(Κοινωνικά δίκτυα και μέσα κοινωνικής δικτύωσης στην εξ αποστάσεως τριτοβάθμια εκπαίδευση – Ε. Μανούσου – Τ. Χαρτοφύλακα 2ο Πανελλήνιο Συνέδριο – «'Ενταξη και Χρήση των ΤΠΕ στην Εκπαιδευτική Διαδικασία, Πάτρα 2011).**

ΚΕΦΑΛΑΙΟ 2^{ο}

- https://www.ukessays.com/essays/internet/advantages-and-disadvantages-of-social-networks.php
- https://socialnetworksgoodsandbads.weebly.com/kappaalphataualpha-kappaomicroniotanuomeganuiotakappaomeganu-deltaiotakappatauupsilonomeganu.html
- https://futureofworking.com/10-advantages-and-disadvantages-of-social-networking/
- http://www.bbc.co.uk/schoolreport/22065333
- https://www.statista.com/topics/1164/social-networks/
- http://www.kathimerini.com.cy/gr/geek/geek-nea/236871/?ctype=ar
- http://www.divico.gr/kindinoi-sta-social-media-kai-to-internet/2855
- http://www.contentmarketing.gr/%CE%BA%CE%AF%CE%BD%CE%B4%CF%85%CE%BD%CE%BF%CE%B9-%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B1%CF%82-%CF%83%CF%84%CE%B1-social-media-%CE%BA%CE%B1%CE%B9-%CF%80%CF%89%CF%82-%CE%BD%CE%B1-%CF%84%CE%BF/
- https://academic.oup.com/jcmc/article/19/1/38/4067499
- https://www.sciencedirect.com/science/article/pii/S0007681314000974
- https://el.wikibooks.org/wiki/%CE%9A%CE%BF%CE%B9%CE%BD%CF%89%CE%BD%CE%B9%CE%BA%CE%AC_%CE%94%CE%AF%CE%BA%CF%84%CF%85%CE%B1_(Social_Networks)_%CF%83%CE

%B5_%CE%BC%CE%B9%CE%B1_%CE%B5%CF%80%CE%B9%CF%87%CE%B5%CE%AF%CF%81%CE%B7%CF%83%CE%B7._%CE%97_%CF%80%CE%B5%CF%81%CE%AF%CF%80%CF%84%CF%89%CF%83%CE%B7_%CF%84%CE%BF%CF%85_FaceBook

- http://www.novelwebdesigns.com/social-media-marketing
- http://www.simplyesty.com/adevertising-and-marketing/brands/excellent-coca-cola-social-media-strategy-presentation/
- **(Storberg-Walker & Gubbin, "Introducing Social Networks as a Theoretical and Empirical Tool to Understand and "Do" HRD").**
- https://www.itexchangeweb.com/blog/the-evolution-of-social-networks-what-will-the-future-look-like/
- **(International Journal of Advance Research in Computer Science and Management Studies – V3, Issue 5, May 2015 – Impacts of Social Networks: A Comprehensive Study on Positive and Negative Effects on Different Age Groups in a Society)**
- **.(The Paradox of Social Media Security: Users' Perceptions versus Behavior -Zahra Alqubaiti - 2016).**
- **(Κοινωνικά Δίκτυα (Social Networks) σε μια επιχείρηση. Η περίπτωση του FaceBook – el.wikibooks.org**
- **%.(The Contradictory Influence of Social Media Affordances on Online Communal Knowledge Sharing – Ann Majchrzak, Samer Faraj, Gerald C. Kane, Bigan Azad - 2013).**

ΚΕΦΑΛΑΙΟ 3^{ο}

- **(Μήτρου, Λ. Προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες. - 2010)**
- **(Αναστάσιος Χ. Παπαναστασίου – Ασφάλεια, ιδιωτικότητα και προστασία απορρήτου στις ηλεκτρονικές επικοινωνίες - 2013)**
- **(Vrakas, N., Kalloniatis, C., Tsohou, A. &Lambrinoudakis, C., 2010. Privacy Requirements Engineering for Trustworthy e-Government Services. Berlin, Springer LNCS)**
- https://legal.heal-link.gr/index.php/sensitive-personal-data
- **Κάτσικας Σ. – Γκρίτζαλης Δ. – Γκρίτζαλης Σ.,(2004) Ασφάλεια Πληροφοριακών Συστημάτων, Αθήνα, Εκδόσεις Νέων Τεχνολογιών**

- **Data protection in the United States: overview by Ieuan Jolly, Loeb & Loeb** **https://www.ibm.com/security/solutions/protect-critical-assets?cm_mmc=Search_Google-_-Security_Security+Brand+and+Outcomes-_-WW_NA-_-%2Bdata%20%2Bprotection_b&cm_mmca1=000034XN&cm_mmca2=10009272&cm_mmca7=9061582&cm_mmca8=kwd-18855659289&cm_mmca9=_k_Cj0KCQiAkfriBRD1ARIsAASKsQJXmmYYn1EefHQ9VW1CMljcOe4GweLEHP_GDp1P0pVg0PJ7YlZ078UaAiQ-EALw_wcB_k_&cm_mmca10=326196896615&cm_mmca11=b&gclid=Cj0KCQiAkfriBRD1ARIsAASKsQJXmmYYn1EefHQ9VW1CMljcOe4GweLEHP_GDp1P0pVg0PJ7YlZ078UaAiQ-EALw_wcB**
- **http://www.el.wikipedia.org**
- **http://www.uk.practicallaw.thomsonreuters.com**
- **(Data protection in the United States: overview by Ieuan Jolly, Loeb & Loeb)**
- **http://www.greeklawdigest.gr/index.php**

ΚΕΦΑΛΑΙΟ 4ο

- **https://www.statista.com/chart/15246/confidence-in-institutions-to-keep-data-secure/**
- **https://www.technadu.com/worst-internet-privacy-scandals/30236/**
- **https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.**
- **https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears**
- **https://el.wikipedia.org/wiki/Apple**
- **http://www.appleiphonereview.com/issues/apple-location-tracking-scandal/**
- **https://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html**
- **https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/**
- **Zilpelwar, R. A., Bedi, R. K. and Wadhai, V., An overview of privacy and security in sns.**
- **International Journal of P2P Network Trends and Technology, 2,1(2012).**

ΚΕΦΑΛΑΙΟ 5ο

- **Penn State University – Who are you on social Media? New research examines norms of online personas by Erin Cassidy Hendrick/ Communications Strategist at Penn State University – April 2017)**
- **https://news.psu.edu/story/460855/2017/04/06/research/who-are-you-social-media-new-research-examines-norms-online**
- **(Adam Alter, psychologist at New York University and author of Irresistible: The Rise of Addictive Technology And The Business Of Getting Us Hooked.)**
- **(Privacy in Social Networks: How Risky is Your Social Graph? CuneytGurcanAkcora, Barbara Carminati, Elena Ferrari DICOM, Universit`adegliStudidell'InsubriaVia Mazzini 5, Varese, Italy)**

- **(Edith Cowan University Resaerch Online "A Survey of Social Media Users Privacy Settings & Information Disclosure" - MashaelAljohani, Alastair Nisbet, Kelly Blincoe, Security & Forensic Research Group, Auckland University of Technology Auckland, New Zealand – Australian Information Security Management Conference - 2016)**

- **(Shun Yang, Helsinki September 10, 2015. M.Sc. Thesis UNIVERSITY OF HELSINKI, Department of Computer Science)**
-
- **(Becker, J. L. and Chen, H., Measuring privacy risk in online social networks. Ph.D. thesis, University of California, Davis, 2009)**
-
- **(Franchi, E., Poggi, A. and Tomaiuolo, M., Information attacks on online social networks. Journal of Information Technology Research (JITR) - 2014).**