

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ



Πτυχιακή εργασία

ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΑ
ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ

ΚΥΡΙΑΚΗΣ ΣΤΕΦΑΝΟΣ

ΠΕΙΡΑΙΑΣ 2015

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΑ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πτυχιακή εργασία

ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΑ
ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ

ΚΥΡΙΑΚΗΣ ΣΤΕΦΑΝΟΣ

E/08071

Σύμβουλος καθηγητής
κος Κωνσταντίνος Λαμπρινουδάκης

ΠΕΙΡΑΙΑΣ 2015

Πνευματικά δικαιώματα

Copyright © Στέφανος Κυριάκης, 2014

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιά δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΠΕΡΙΛΗΨΗ

Αντικείμενο της παρούσας εργασίας αποτελεί η μελέτη των υπηρεσιών κοινωνικής δικτύωσης. Πρόκειται για τη νέα μορφή επικοινωνίας και κοινωνικοποίησης των ανθρώπων που έχει εξελιχθεί ραγδαία τα τελευταία χρόνια.

Αρχικά θα γίνει αναφορά σε κάποια εισαγωγικά και γενικά σημεία του Διαδικτύου και συγκεκριμένα, θα δοθεί έμφαση στις σελίδες κοινωνικής δικτύωσης. Έπειτα θα αναφερθούν κάποιοι ορισμοί, θα παρουσιαστούν ορισμένα σημαντικά ιστορικά και στατιστικά στοιχεία για τα κοινωνικά δίκτυα. Καθώς επίσης, θα παρουσιαστούν και κάποιες τεχνολογίες που βασίζονται τα σημερινά, αλλά και τα παλιότερα κοινωνικά δίκτυα. Θα αναλυθούν δύο από τα «μεγαλύτερα» και «διασημότερα» κοινωνικά δίκτυα, το Facebook και το Twitter. Θα αναλυθούν οι σημαντικές λειτουργίες των σελίδων αυτών, τα ιστορικά στοιχεία, αλλά και η πολιτική προστασίας που ακολουθούν και οι «παγίδες» που κρύβουν.

Θα μελετηθούν και θα προσδιοριστούν οι κίνδυνοι και οι απειλές που παρουσιάζουν τα κοινωνικά δίκτυα, δίνοντας ιδιαίτερη βαρύτητα στους κινδύνους εκείνους που αφορούν στα προσωπικά τους δεδομένα. Σημαντικό κεφάλαιο της εργασίας αποτελεί η ενότητα 5, στην οποία παρουσιάζονται όλα τα νομοθετικά και ρυθμιστικά πλαίσια, οι αναθεωρήσεις και οι τροποποιήσεις που αφορούν στα προσωπικά δεδομένα των χρηστών στο Διαδίκτυο, σε παγκόσμια κλίμακα, στην Ευρώπη αλλά και συγκεκριμένα στην Ελλάδα. Στο τέλος θα αναφερθούν κάποια γενικά συμπεράσματα και παρατηρήσεις.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Η αρίθμηση των πρώτων σελίδων είναι λατινική (i, ii, iii, iv, v, vi, ...), ενώ η αραβική αρίθμηση ξεκινά από το πρώτο κεφάλαιο.

ΠΕΡΙΛΗΨΗ	iii
ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ	iv
ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ	vi
ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ	vii
1 ΕΝΟΤΗΤΑ 1: Τεχνολογική εξέλιξη και Πληροφορία	1
1.1 Εισαγωγή	1
1.2 Η πληροφορία	2
2 ΕΝΟΤΗΤΑ 2: Ορισμοί και Ιστορική εξέλιξη των ΙΚΔ	3
2.1 Ορισμός των ΙΚΔ	3
2.2 Ανάπτυξη του web 2.0	4
2.3 Ιστορική εξέλιξη των ΙΚΔ	5
2.4 Στατιστικά χρήσης των ΙΚΔ	10
3 ΕΝΟΤΗΤΑ 3: Facebook, Twitter & Πολιτικές Προστασίας	15
3.1 Το Facebook	15
3.1.1 Εισαγωγή	15
3.1.2 Υπηρεσίες & Δυνατότητες	15
3.1.3 Δημιουργία προφίλ στο Facebook	16
3.1.4 Πολιτική Προστασίας του Facebook	19
3.1.4.1 Πολιτική χρήσης δεδομένων	19
3.1.4.2 «Παγίδες» στην πολιτική χρήσης δεδομένων	20
3.1.5 Προστασία της Ιδιωτικότητας στο Facebook	21

3.2	Το Twitter	24
3.2.1	Εισαγωγή	24
3.2.2	Ιστορική αναδρομή - Υπηρεσίες & Δυνατότητες	24
3.2.3	Δημιουργία προφίλ στο Twitter.....	25
3.2.4	Πολιτική Προστασίας του Twitter	26
4	ΕΝΟΤΗΤΑ 4: Κίνδυνοι, Απειλές & Μέτρα Αντιμετώπισης.....	26
4.1	Κίνδυνοι και απειλές των ΙΚΔ.....	28
4.2	Κίνδυνοι με τα Προσωπικά Δεδομένα	30
4.3	Μέτρα και Νόμοι Αντιμετώπισης κινδύνων.....	31
5	ΕΝΟΤΗΤΑ 5: Νομοθεσίες και Πολιτικές Προστασίας	42
5.1	Ορισμοί	42
5.2	Κανονιστικές Προσεγγίσεις	43
5.2.1	Ευρωπαϊκή Νομοθεσία.....	43
5.2.2	Ελληνική Νομοθεσία.....	44
5.2.3	Διεθνής Νομοθεσία.....	45
5.3	Πολιτικές Προστασίας Προσωπικών Δεδομένων	46
5.3.1	Η Πολιτική της Ευρώπης	46
5.3.2	Πολιτική για την Προστασία των παιδιών και μέτρα στην εκπαίδευση ...	47
6	ΕΝΟΤΗΤΑ 6	49
6.1	Συμπεράσματα	49
6.1.1	Θετικές επιδράσεις	49
6.1.2	Αρνητικές επιδράσεις	50
6.2	Επίλογος.....	50
	ΒΙΒΛΙΟΓΡΑΦΙΑ	52

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1: Ένα σύννεφο ετικετών (ένα τυπικό φαινόμενο Web 2.0 από μόνο του) που παρουσιάζει θέματα του Web 2.0.....	4
Εικόνα 2: Χρονοδιάγραμμα με ημερομηνίες έναρξης πολλών μεγάλων ΙΚΔ (Danah m. Boyd, University of California-Berkeley & Nicole B. Ellison, Michigan State University)	8
Εικόνα 3: Χρήστες ΙΚΔ, ανάλογα με τον αριθμό των εγγεγραμμένων χρηστών (σε εκατ.)	10
Εικόνα 4: Χάρτης των κοινωνικών δικτύων, που δείχνει τις πιο δημοφιλείς τοποθεσίες κοινωνικής δικτύωσης με βάση τη χώρα, σύμφωνα με την Alexa	11
Εικόνα 5: Στατιστικά χρήσης των ΙΚΔ	12
Εικόνα 6: Στατιστικά υψηλότερων και χαμηλότερων χρηστών των ΙΚΔ στην Ευρώπη	13
Εικόνα 7: Εγγεγραμμένοι Έλληνες χρήστες σε Facebook, Twitter και Blogs	14
Εικόνα 8: Χάρτης με χώρες στις οποίες έχουν αποκλειστεί και απαγορευτεί τα κοινωνικά δίκτυα σε περιόδους κρίσης, Facebook, Twitter, YouTube.....	18
Εικόνα 9: Παρουσιάζεται ένας χάρτης με τα tweets παγκοσμίως που είχαν ως δημοφιλέστερο hashtag το #twitterisblockedinturkey	26
Εικόνα 10: Στατιστικά στοιχεία Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, Φεβρουάριος 2014	28

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Παρουσιάζονται συνοπτικά όλες οι σημαντικές συντομογραφίες που έχουν χρησιμοποιηθεί στο κείμενο της πτυχιακής:

ΙΚΔ: Ιστοσελίδες Κοινωνικής Δικτύωσης

ΕΕ: Ευρωπαϊκή Ένωση

Η/Υ: Ηλεκτρονικός Υπολογιστής

ΕΝΟΤΗΤΑ 1^Η

Τεχνολογική εξέλιξη και Πληροφορία

1.1 Εισαγωγή

Στις μέρες μας παρατηρείται μια συνεχής και διαρκής τεχνολογική εξέλιξη. Η ραγδαία εξάπλωση του Διαδικτύου ώθησε και κατέστησε δυνατή την άμεση επικοινωνία σε όλο τον κόσμο. Μέσα σε ένα παγκόσμιο φαινόμενο οι σελίδες κοινωνικής δικτύωσης (*social network*), έχουν πάρει τεράστιες κοινωνικές, πολιτικές, ψυχολογικές διαστάσεις και έχουν προκαλέσει ποικίλες αντιδράσεις. Αποτελούν μια νέα μορφή επικοινωνίας, η οποία έχει ιντριγκάρει και σαγηνεύσει τόσο τους νέους, όσο και ανθρώπους μεγαλύτερων ηλικιών. Τα κοινωνικά δίκτυα έχουν κατακτήσει την καθημερινότητα μας. Η απόκτηση φίλων, η συνομιλία, η ανταλλαγή απόψεων και εμπειριών, η χρήση τους για επαγγελματικούς σκοπούς μέσα σε ένα ευρύτερο πλαίσιο, καθώς και η γρήγορη και εύκολη επικοινωνία και ενημέρωση σε κάθε μεριά του πλανήτη τις έχει καταστήσει πλέον απαραίτητες.

Υπάρχει βέβαια και η αρνητική στάση και καχυποψία, στο κατά πόσο διασφαλίζεται η προστασία της ιδιωτικότητας στις σελίδες κοινωνικής δικτύωσης. Αν είναι εφικτή η πλήρης και ουσιαστική προστασία και ασφάλεια των προσωπικών δεδομένων των χρηστών, κατά πόσο η εγκυρότητα των σελίδων αυτών και τα νομοθετικά πλαίσια τους καλύπτουν και σε ποιές περιπτώσεις. Το σίγουρο όμως είναι ότι τα κοινωνικά δίκτυα έχουν επηρεάσει την σύγχρονη κοινωνία. Η ασφαλή και με προστασία χρήση και αξιοποίηση των δικτύων αυτών οδηγεί σε μια καινοτόμα διαδικτυακή επικοινωνία.



1.2 Η πληροφορία

Η τεχνολογική εξέλιξη αποτελεί όχι μόνο τεχνολογικό, αλλά κοινωνικό και οικονομικό φαινόμενο. Αυτή η ανάπτυξη επέφερε αλλαγές στην διακίνηση των προσωπικών πληροφοριών και απόψεων, κι έτσι αποτέλεσε επιτακτική ανάγκη η δημιουργία νομικών κανόνων, έτσι ώστε να εξασφαλίζεται και να διασφαλίζεται η προστασία και προάσπιση των προσωπικών στοιχείων. Η ελεύθερη διακίνηση πληροφοριών και ο γοργός ρυθμός εξέλιξης της τεχνολογίας, οδήγησε και κατέστησε αναγκαία την δημιουργία ενός νομικού πλαισίου. Όμως με την περαιτέρω ανάπτυξη της τεχνολογίας και την εξέλιξή της, οδηγηθήκαμε στην χρήση του ατομικού υπολογιστή. Όπως επίσης και με την ανάπτυξη των δικτύων οδηγηθήκαμε σε αλματώδη αύξηση των χρηστών, συνεπώς η μετάδοση και η συλλογή δεδομένων γίνεται πλέον ατομικά και μεμονομένα. Στους χρήστες παρέχεται πλέον μια πληθώρα εργαλείων και δυνατοτήτων που μπορούν να εκμεταλλευτούν μέσα από διαδραστικές υπηρεσίες. Όμως η αλόγιστη και χωρία όρια χρήση, η μεταβίβαση μεγάλου όγκου πληροφοριών μπορεί να οδηγήσει σε περιορισμό της ιδιωτικής τους ζωής. Έτσι συνεπάγεται και η σωστή διαμόρφωση νέων πλαισίων επεξεργασίας των πληροφοριών.

Πρόκληση αποτελεί το γεγονός, κατά πόσο μπορούν τα νομοθετικά πλαίσια αυτά να εφαρμοστούν, να ανταποκριθούν στις ανάγκες και τις απαιτήσεις της εποχής, καθώς επίσης και πόσο συχνά μπορούν να αναθεωρούνται και να τροποποιούνται με βάση τις ανάγκες. Η επικοινωνία και η ανταλλαγή πληροφοριών και δεδομένων γίνεται σε μια παγκόσμια κλίμακα, καθιστώντας αδύνατο τον νομικό έλεγχο και την ασφάλεια των προσωπικών δεδομένων. Οι εταιρίες στεγάζονται εντός και εκτός Ε.Ε, ως εκ τούτου είναι δύσκολο να γίνει αντιληπτό σε ποιές αρχές και ποιούς νόμους συμμορφώνονται, καθώς δεν υπάρχουν όλες οι χώρες σε ενιαίο δίκαιο.

Επιπλέον, με την τεχνολογική αυτή ανάπτυξη και εξέλιξη των σελίδων κοινωνικής δικτύωσης παρατηρείται η «εμπορευματοποίηση της πληροφορίας». Οι εταιρίες μπορούν μέσα από νέες τεχνολογίες να εγκαθιστούν cookies και pixel στους φυλλομετρητές και στην διεύθυνση IP των χρηστών, καταγράφοντας διάφορες πληροφορίες για τους χρήστες. Οι χρήστες παράλληλα, με την αποδοχή των όρων χρήσης των σελίδων, χάνουν κάθε δικαίωμα για έλεγχο των προσωπικών δεδομένων που έχουν παραχωρήσει και δίνουν την συγκατάθεση στις εταιρίες να παραχωρήσουν τα προσωπικά τους δεδομένα σε διαφημιστικές εταιρίες. Οι διαφημιστικές εταιρίες επεξεργάζονται και καταγράφουν τα δεδομένα αυτά και παρέχουν στους χρήστες διαφημίσεις ανάλογα με τις ανάγκες και τις επιθυμίες τους.

ΕΝΟΤΗΤΑ 2^Η

Ορισμοί και Ιστορική εξέλιξη των ΙΚΔ

2.1 Ορισμός των ΙΚΔ

Καθημερινά, ολοένα και περισσότεροι άνθρωποι προστίθενται στην λίστα των ενεργών μελών των σελίδων κοινωνικής δικτύωσης. Οι ιστοσελίδες, γνωστές και ως κοινωνικά δίκτυα χρησιμοποιούνται καθημερινά από εκατομμύρια χρήστες. Ορίζουμε ως ιστότοπους κοινωνικής δικτύωσης, διαδικτυακές υπηρεσίες που επιτρέπουν στους ανθρώπους να δημιουργήσουν ένα δημόσιο ή ημι-δημόσιο προφίλ με προσωπικά δεδομένα και την δημιουργία λιστών επαφής. Προσφέροντάς τους εύκολη επικοινωνία μέσω του διαδικτύου και ανταλλαγή πληροφοριών και πόρων μέσα από το σύστημα. Δεκάδες, χιλιάδες άνθρωποι παγκοσμίως καθημερινά γίνονται χρήστες, ακόμα και άνθρωποι μεγαλύτερων ηλικιών με ελάχιστες γνώσεις χρήσης των Ηλεκτρονικών Υπολογιστών και του διαδικτύου. Ένας άλλος ορισμός για τα κοινωνικά δίκτυα είναι εκείνος που τα «ονομάζει ως άτυπα εργαλεία διαχείρισης της ταυτότητας που επιτρέπουν, μέσω κοινωνικών σχέσεων, την πρόσβαση σε περιεχόμενο που καταχωρείται από τους ίδιους τους χρήστες».¹

Η δημιουργία καταλόγων με επαφές και η επικοινωνία με αγνώστους, δεν είναι αυτή που κάνει τις ιστοσελίδες κοινωνικής δικτύωσης μοναδικές, αλλά μάλλον η δυνατότητα που τους δίνεται να εκφράσουν και να κάνουν ορατή την προσωπικότητα τους. Ενώ οι ΙΚΔ έχουν υλοποιήσει μια ποικιλία εφαρμογών, το κύριο χαρακτηριστικό τους είναι ότι αποτελούνται από ορατά προφίλ και λίστα φίλων που είναι χρήστες τους συστήματος. Με την είσοδο των χρηστών στο σύστημα, για την δημιουργία του προφίλ τους, συμπληρώνονται κάποιες φόρμες με ερωτήματα, όπως η ηλικία, ο τόπος διαμονής, η επαγγελματική κατάρτιση, γενικές περιγραφές του κάθε χρήστη κ.α. Επιπλέον, πολλές σελίδες επιτρέπουν στους χρήστες να διαμορφώσουν το προφίλ τους με την προσθήκη περιεχομένου πολυμέσων ή την τροποποίηση εμφάνισης του προφίλ τους και το πώς αισθάνονται. Η εμφάνιση και η ορατότητα κάθε προφίλ εξαρτάται από την πολιτική που ακολουθεί κάθε σελίδα.

Ενώ οι περισσότερες σελίδες κοινωνικής δικτύωσης σχεδιάστηκαν για να είναι ευρέως προσβάσιμες από όλους, πολλές διαχωρίστηκαν και προσέλκυσαν διαφορετικές ομάδες ατόμων (ηλικία, εθνικότητα, θρησκεία, μορφωτικό επίπεδο κ.α.) έστω και αν αυτό δεν ήταν η πρόθεση των σχεδιαστών. Κατά κύριο λόγο, η ανάπτυξη των ΙΚΔ οφείλεται στην εφαρμογή του web 2.0.

¹ Ευρωπαϊκός Οργανισμός Ασφάλειας Πληροφοριακών Συστημάτων (ENISA)

2.2 Ανάπτυξη του Web 2.0

Το Web 2.0 είναι μια φράση που εφευρέθηκε από τον Tim O'Reilly της O'Reilly Media (O'Reilly, 2005), για να αναφερθεί και περιγράψει μια προτεινόμενη δεύτερη γενιά υπηρεσιών οι οποίες βασίζονται στο διαδίκτυο, όπως οι σελίδες κοινωνικής δικτύωσης, τα wiki, τα εργαλεία που δίνουν έμφαση στην ηλεκτρονική συνεργασία και ανταλλαγή μεταξύ των χρηστών.

Το Web 2.0 είναι ένα σύνολο νέων δικτυακών υπηρεσιών, που επιτρέπουν στους χρήστες να συνεργάζονται, να ανταλλάσσουν δεδομένα και να επικοινωνούν ζωντανά. Ο όρος Web 2.0, «χρησιμοποιείται για να περιγράψει τη "δεύτερη γενιά" υπηρεσιών του Παγκόσμιου Ιστού. Η τεχνολογία web 2.0 διευκολύνει την αλληλεπίδραση μεταξύ των χρηστών και τη συνεργασία για τον διαμοιρασμό περιεχομένου». ²



Εικόνα 1: Ένα σύννεφο ετικετών (ένα τυπικό φαινόμενο Web 2.0 από μόνο του) που παρουσιάζει θέματα του Web 2.0. (πηγή: http://el.wikipedia.org/wiki/Web_2.0)

² Τεχνολογίες web 2.0, Εθνικό Πληροφοριακό Σύστημα Έρευνας & Τεχνολογίας (ΕΠΣΕΤ)

Η παρουσίαση των πληροφοριών αποκτά έναν δυναμικό και διαδραστικό ρόλο, και επίσης θέτει ως επίκεντρο τον χρήστη, ο οποίος μπορεί να παρεμβαίνει και να διαμορφώνει το περιεχόμενο ιστοσελίδων μέσω διαδραστικών εφαρμογών. Χαρακτηριστικές εφαρμογές του Web 2.0 είναι τα κοινωνικά μέσα (youtube), οι πλατφόρμες κοινωνικής δικτύωσης (facebook, twitter κ.ά.), τα wiki (όπου είναι ιστοσελίδες που ο χρήστης διαμορφώνει, να τροποποιεί και να διαγράφει το περιεχόμενό τους), τα blogs (που είναι σελίδες που περιέχουν πληροφορίες, απόψεις, προσωπικές καταχωρήσεις, φωτογραφίες κ.ά.) και πλήθος άλλων εφαρμογών. Μέσα από εξειδικευμένα εργαλεία και διάφορες εκφράσεις όπως είναι, η αναζήτηση (search), το tag, η παράθεση links ή το authoring. Οι εφαρμογές αυτές ενδυναμώνουν τον ρόλο του χρήστη στη διαμόρφωση και διακίνηση της πληροφορίας.

Επέκταση των τεχνολογιών web 2.0 θα είναι οι τεχνολογίες web 3.0, όπου θα δίνεται η δυνατότητα στον χρήστη να εξατομικεύει δεδομένα και πληροφορίες, αφού οι μηχανές αναζήτησης θα γίνουν «εξυπνότερες».

2.3 Ιστορική Εξέλιξη των ΙΚΔ

Η πρώτη ΙΚΔ άρχισε να λειτουργεί και προωθήθηκε το 1997, ήταν η www.sixdegrees.com. Επέτρεπε στον χρήστη να δημιουργήσει το δικό του προφίλ και έναν κατάλογο από φίλους, με τους οποίους μπορούσε να έρθει σε επικοινωνία. Το 1998 δόθηκε η δυνατότητα στους χρήστες να πλοηγηθούν στις λίστες των φίλων τους. Η ιστοσελίδα www.classmates.com η οποία δημιουργήθηκε το 1995 είχε τα ίδια χαρακτηριστικά με την SixDegrees.com, οι χρήστες συνδέονταν απλά μέσω διευθύνσεων ηλεκτρονικού ταχυδρομίου, αλλά δεν τους δινόταν η δυνατότητα επικοινωνίας και η δημιουργία συνδέσεων με άλλους χρήστες. Το 1999 εμφανίστηκε το **LiveJournal**, ένα κοινωνικό δίκτυο το οποίο ενθάρρυνε τους χρήστες του, να δημιουργούν ομάδες και να αλληλεπιδρούν μεταξύ τους. Επίσης, την ίδια χρονιά άρχισε να λειτουργεί η κορεάτικη παγκόσμια ιστοσελίδα **Cyworld**, με χαρακτηριστικά κοινωνικής δικτύωσης. Το 2000 ο σουηδικός κοινοτικός ιστός **LunarStorm** παρουσίασε μια υπηρεσία κοινωνικής δικτύωσης, η οποία περιείχε καταλόγους φίλων και ημερολόγιο. Το 2001 εμφανίστηκε μια άλλη ιστοσελίδα η www.ryze.com, η οποία είχε ως στόχο και σκοπό να προωθήσει και να βοηθήσει τους ανθρώπους να ενδυναμώσουν τα επιχειρησιακά δίκτυα τους. Ο ιδρυτής της εισήγαγε μέλη από την επιχειρηματική κοινότητα του Σαν Φρανσίσκο, επιχειρηματίες και επενδυτές. Οι ιστοσελίδες www.tribe.net, www.linkedin.com και www.friendster.com συνδέθηκαν στενά, προσωπικά και επαγγελματικά με την Ryze. Πίστευαν και στόχευαν, ότι θα μπορούσαν να υποστηρίξουν η μια την άλλη χωρίς ανταγωνισμό. Η **Friendster** άρχισε να λειτουργεί το 2002 και κατασκευάστηκε από την ίδια εταιρία, που κατασκευάστηκε και η Ryze. Σχεδιάστηκε με σκοπό την γνωριμία φίλων και πολύ σύντομα κατάφερε να πολλαπλασιάσει τους χρήστες της, πριν την επίσημη παρουσίαση του. Η Friendster προσέλκυσε και παρουσίασε ιδιαίτερη αύξηση σε τρεις τύπους διαφορετικών ομάδων τους bloggers, τους καλλιτέχνες και τους ομοφυλόφιλους άνδρες. Εξαιτίας όμως, της απότομης αύξησης της ιστοσελίδας,

λόγω της “εισβολής” νέων μελών που ενημερώθηκαν από την συνέντευξη τύπου στα μέσα ενημέρωσης, αναστατώθηκαν οι ισορροπίες και δυσαρεστήθηκαν οι διαφορετικές ομάδες χρηστών που ήταν ήδη ενεργές. Ο αρχικός σχεδιασμός της Friendster απαγόρευε στους χρήστες να βλέπουν το προφίλ άλλων χρηστών, οι οποίοι δεν ήταν μεγαλύτερη από τέσσερις βαθμούς, δηλαδή φίλος-φίλου-φίλου-φίλου. Αυτοί οι περιορισμοί, ανάγκασαν πολλούς χρήστες να δημιουργήσουν ψεύτικα προφίλ, έτσι ώστε να διευρύνουν τα κοινωνικά τους δίκτυα και αυξήσουν την δημοτικότητα τους. Ο αριθμός των χρηστών άρχισε να μειώνεται, όταν η εταιρία άρχισε να διαγράφει τα ψεύτικα προφίλ και γενικά χρήστες οι οποίοι δεν είχαν ρεαλιστικές φωτογραφίες. Μεγαλύτερο πλήγμα δέχτηκε, όταν δημιουργήθηκαν προβλήματα με τους χρήστες από την παλιά ομάδα χρηστών, λόγω των τεχνικών δυσκολιών και των κοινωνικών συγκρούσεων, με αποτέλεσμα να χαθεί η εμπιστοσύνη ανάμεσα σε εκείνους και την ιστοσελίδα με σκοπό να αποχωρήσουν.

Η Ryze δεν απέκτησε ποτέ μαζική δημοτικότητα και η Friendster χαρακτηρίστηκε ως, αν όχι η σημαντικότερη “μια από τις μεγαλύτερες απογοητεύσεις της ιστορίας του διαδικτύου”.³

Το 2003, η εταιρία της ιστοσελίδας www.MySpace.com συνειδητοποίησε την ανάγκη για δημιουργία μια σελίδας κοινωνικής δικτύωσης, που είχε στόχο να αντικαταστήσει, να προσελκύσει και να φιλοξενήσει τους χρήστες που είχαν αποχωρήσει από την σελίδα Friendster. Το MySpace ξεκίνησε από τον Brad Greenspan, ο οποίος ήταν ο ιδρυτής και Διευθύνων Σύμβουλος της eUniverse. Οι πρώτοι χρήστες του ήταν υπάλληλοι της eUniverse . Αρχικά, προσέλκυσε το ενδιαφέρον πολλών καλλιτεχνών και κυρίως μουσικών συγκροτημάτων διαφημίζοντας την δουλειά τους και στην συνέχεια, χρήστες που ήθελαν να τους ακολουθήσουν και να τους πλησιάσουν. Το MySpace έδινε την δυνατότητα στους χρήστες του να επεμβαίνουν και να προσαρμόζουν το προφίλ τους ανάλογα με τις ανάγκες τους, επίσης δεν υπήρχε όριο στο να εγγραφεί ένας νέος χρήστης, έτσι το 2004 άρχισαν να το χρησιμοποιούν μαζικά οι έφηβοι. Το 2006 MySpace ήταν η πιο δημοφιλής ιστοσελίδα κοινωνικής δικτύωσης στις ΗΠΑ, το 2007 και το 2008 έκανε πολλές αλλαγές στη διάρθρωση και τη λειτουργία του. Η “Αρχική Σελίδα” του χρήστη ήταν η πρώτη λειτουργία που ξανασχεδιάστηκε, ενώ το 2008 σχεδιάστηκε σε μια απλούστερη διάταξη που ήταν πιο ελκυστικό στο μάτι.

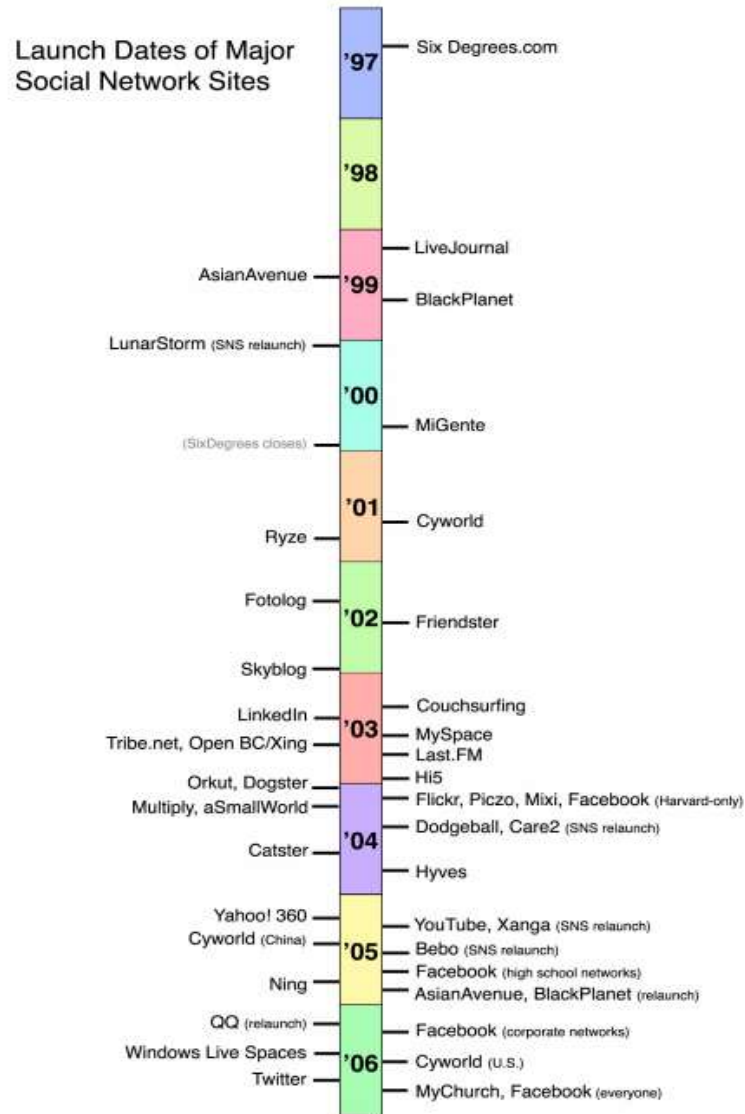


³ *Social Network Sites: Definiton, History and Scholarship, Danah m. Boyd, Nicole B. Ellison*

Επίσης το 2008, επανασχεδιάστηκε η σελίδα “μουσική” προσθέτοντας νέα χαρακτηριστικά για όλους τους μουσικούς. Αυτά τα νέα χαρακτηριστικά περιλαμβάνουν την ικανότητα των χρηστών να δημιουργήσουν λίστες αναπαραγωγής, που μοιάζουν με τις λειτουργίες άλλων κοινωνικών ιστοσελίδων μουσικής, μαζί με το δημοφιλές ProjectPlaylist που είναι δημοφιλές στα προφίλ.

Η νέα μουσική διαθέτει επίσης, «τραγούδια αρχείο» από πολλούς δημοφιλείς καλλιτέχνες, που μοιάζουν με τις υπηρεσίες του iTunes και του Napster. Το MySpace Music προτείνει επίσης τραγούδια με βάση τα τραγούδια που ακούνε ή τα τραγούδια που είχαν προστεθεί στη λίστα αναπαραγωγής οι χρήστες, καθιστώντας το ένα εργαλείο ανακάλυψης μουσικής. Τον Σεπτεμβρίου 2012, ένας νέος επανασχεδιασμός ανακοινώθηκε κάνοντας το Myspace πιο οπτικό και προφανώς βελτιστοποιημένο για δισκία (tablets).

Από το 2003 και μετά, πολλές νέες ΙΚΔ δημιουργήθηκαν και προωθήθηκαν, άλλες προσπαθώντας να αυξήσουν τους χρήστες της, άλλες βασισμένες στην διανομή πολυμέσων και άλλες στοχεύοντας σε ένα συγκεκριμένο κοινό. Το www.flickr.com, ήταν αρχικά μια υπηρεσία που φιλοξενούσε [chat rooms](#) με δυνατότητα ανταλλαγής φωτογραφιών μεταξύ των χρηστών και τον Μάρτιο του 2005 αγοράστηκε από την Yahoo!. Το 2007, οι χρήστες που δημιούργησαν λογαριασμό θα έπρεπε να δημιουργήσουν λογαριασμό στο Yahoo!, έτσι ώστε να μπορέσουν να εγγραφούν. Αυτό οδήγησε στην αποχώρηση πολλών χρηστών του Flickr. Όπως η Flickr, έτσι και το www.instagram.com το οποίο ξεκίνησε τον Οκτώβριο του 2010, είναι μια υπηρεσία που επιτρέπει στους χρήστες της να τραβήξουν φωτογραφίες και βίντεο, να τα επεξεργαστούν με ψηφιακά [φίλτρα](#), και να τα μοιραστούν και με άλλες υπηρεσίες κοινωνικής δικτύωσης. Ένα χαρακτηριστικό του είναι ότι περιορίζει τις φωτογραφίες των χρηστών σε ένα τετράγωνο σχήμα. Τον Ιανουάριο του 2011, το Instagram πρόσθεσε [hashtags](#) για να μπορέσει να βοηθήσει τους χρήστες να ανακαλύπτουν φωτογραφίες και βίντεο περισσότερων χρηστών. Το www.youtube.com δημιουργήθηκε το Φεβρουάριο του 2005 και είναι ένας διαδικτυακός τόπος, που επιτρέπει την αποθήκευση, την αναζήτηση και την αναπαραγωγή μουσικών ταινιών και ψηφιακών βίντεο. Το www.hi5.com ξεκίνησε το 2003, οι χρήστες μπορούν να δημιουργήσουν ένα προφίλ με πληροφορίες, όπως τα ενδιαφέροντα, την ηλικία και την πατρίδα. Επίσης οι χρήστες μπορούν να ανεβάσουν φωτογραφίες και να δημιουργήσουν φωτογραφικά άλμπουμ, όπου άλλοι χρήστες μπορούν να δημοσιεύουν σχόλια. Στις αρχές του 2010, το Hi5 άρχισε να εξελίσσεται από ένα κοινωνικό δίκτυο σε ένα δίκτυο gaming. Η www.tumblr.com ξεκίνησε το 2006 και επέτρεπε στους χρήστες να δημιουργούν μια σύντομη μορφή [blog](#) με σκοπό την δημοσίευση πολυμέσων και άλλων περιεχομένων. Οι χρήστες μπορούν να ακολουθήσουν τα blogs των άλλων χρηστών, καθώς και να κάνουν τα blogs τους ιδιωτικά. Στις 20 Μαΐου του 2013, η Yahoo! ανακοίνωσε την απόκτηση της Tumblr με αποτέλεσμα πολλοί από τους χρήστες να δυσανεστηθούν.



Εικόνα 2: Χρονοδιάγραμμα με ημερομηνίες έναρξης πολλών μεγάλων ΙΚΔ (Danah m. Boyd, University of California-Berkeley & Nicole B. Ellison, Michigan State University)

Το www.pinterest.com είναι ένας “πίνακας ανακοινώσεων”, ξεκίνησε τον Δεκέμβριο του 2009. Είναι μια σελίδα ανταλλαγής φωτογραφιών και επιτρέπει στους χρήστες να δημιουργούν και να διαχειρίζονται συλλογές εικόνων με βάση τα ενδιαφέροντα, εκδηλώσεις, χόμπι κ.α. Οι χρήστες μπορούν επίσης, να περιηγηθούν και σε άλλους “πίνακες ανακοινώσεων”. Το **Google+** είναι μια υπηρεσία κοινωνικής δικτύωσης που ανήκει στην εταιρία της Google. Είναι ο δεύτερος μεγαλύτερος ιστοχώρος κοινωνικής δικτύωσης στον κόσμο μετά το Facebook. Ένα από τα κύρια πλεονεκτήματα του Google+ ήταν το χαρακτηριστικό "Hangout", που λίγο αργότερα μια αντίστοιχη εφαρμογή εφαρμόστηκε στο Facebook και η εγκατάσταση της γινόταν σε πιο απλά βήματα.

Το www.qqzone.qq.com είναι μια κινέζικη σελίδα κοινωνικής δικτύωσης, η οποία δημιουργήθηκε το 2005 και είναι μια ταχέως αναπτυσσόμενη και πιο ενεργή κοινότητα σε ολόκληρη την βιομηχανία. Το <http://vk.com> είναι η δεύτερη μεγαλύτερη σελίδα κοινωνικής δικτύωσης στην Ευρώπη μετά το Facebook. Είναι ευρέως διαδεδομένο και ιδιαίτερα δημοφιλές μεταξύ των ρωσόφωνων χρηστών σε όλο τον κόσμο.

Σήμερα υπάρχουν πάρα πολλές σελίδες κοινωνικής δικτύωσης, οι οποίες συνεχίζουν να πολλαπλασιάζονται και συνεχώς να εμφανίζονται νέες με γοργούς ρυθμούς, ως αποτέλεσμα να καθίσταται δύσκολη η παρουσίαση όλων αυτών. Στην παρούσα ενότητα αναφέρθηκαν οι πρώτες σελίδες που εμφανίστηκαν, κάποιες από τις οποίες δεν είναι σε λειτουργία πια. Αναφέρθηκαν οι σημαντικότερες και γνωστότερες σελίδες και εκείνες που πρωτοτύπησαν.

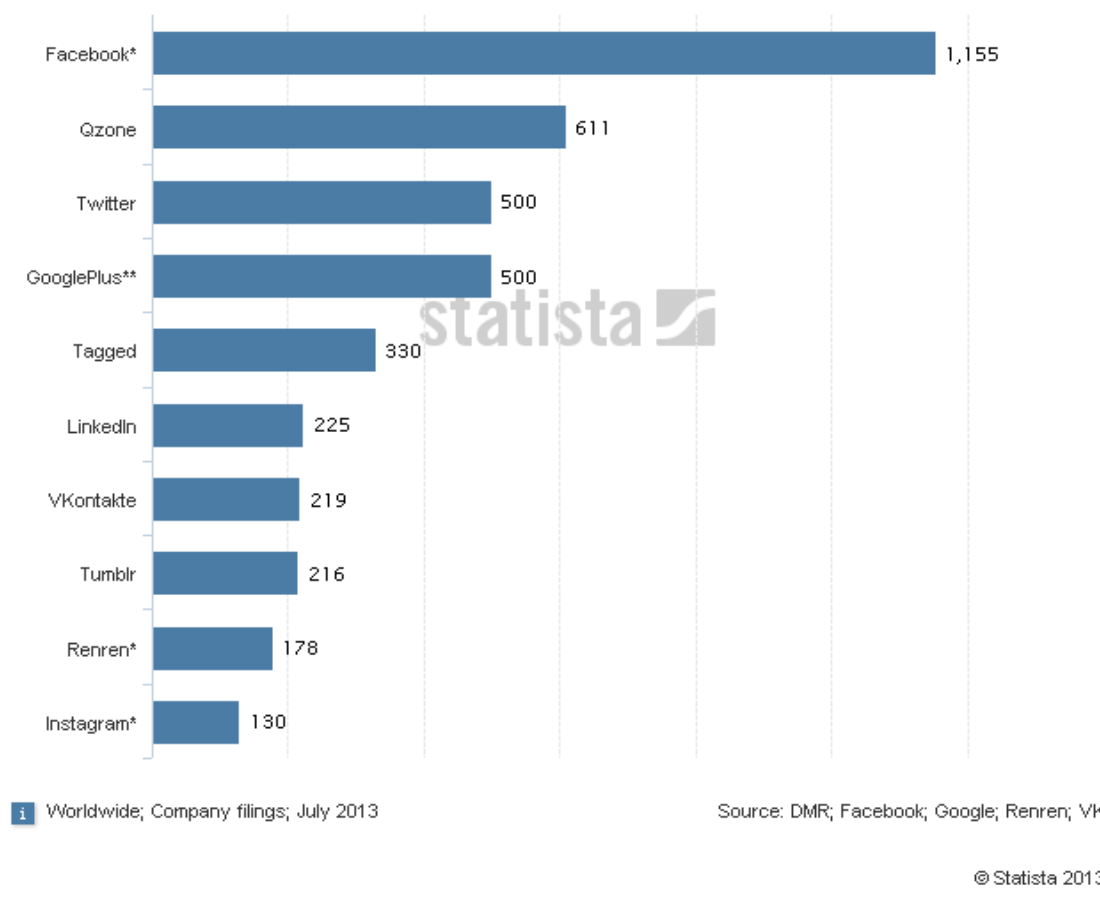


2.4 Στατιστικά χρήσης των ΙΚΔ

Τα πιο δημοφιλή κοινωνικά δίκτυα απαρτίζονται και εμφανίζουν μεγάλο αριθμό χρηστών. Τα στοιχεία δείχνουν ότι αποτελούν σημαντικό κομμάτι στην καθημερινότητα, συνέχεια κερδίζουν έδαφος και εξελίσσονται συνεχώς. Το 2012, πάνω από 1,4 δισεκατομμύρια χρήστες του Διαδικτύου είχαν πρόσβαση στα κοινωνικά δίκτυα και οι αριθμοί αυτοί να αναμένεται να αυξηθούν, όσο αυξάνεται η χρήση των κινητών συσκευών και εφαρμογών για κοινωνικά δίκτυα.

GLOBAL SOCIAL NETWORKS RANKED BY NUMBER OF REGISTERED USERS IN 2013

Leading social networks worldwide as of July 2013, ranked by number of registered users (in millions)

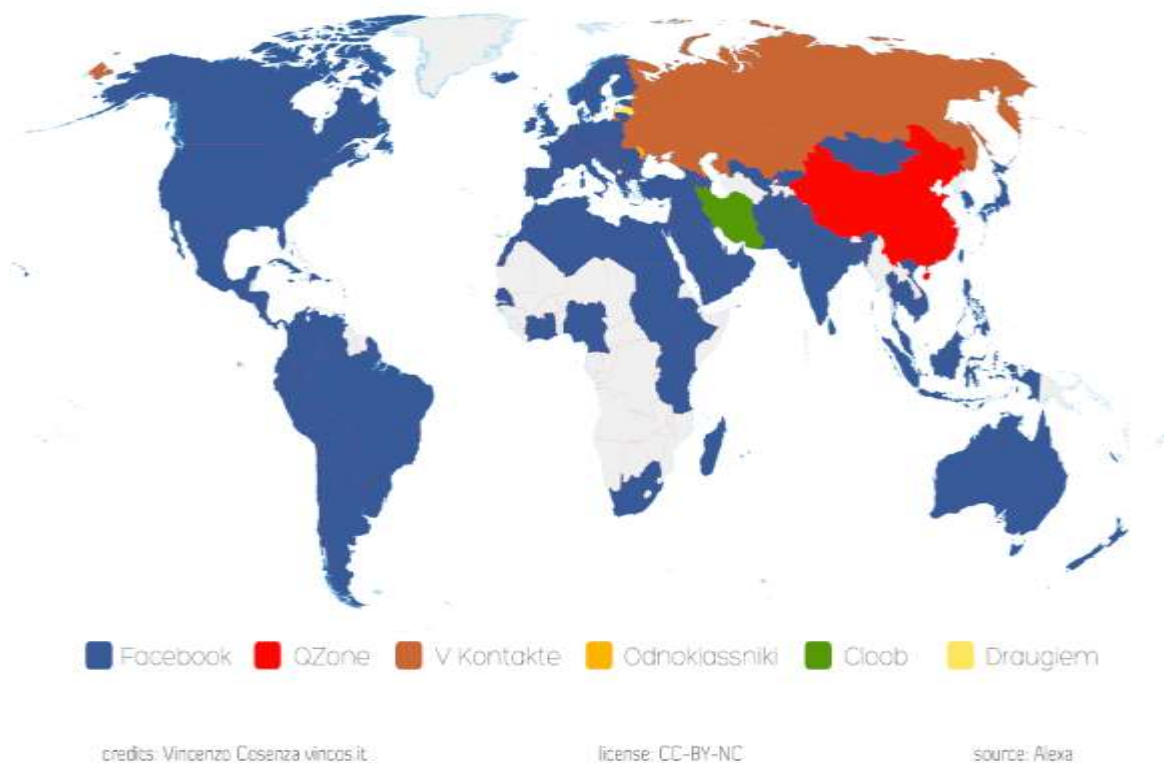


Εικόνα 3: Χρήστες ΙΚΔ, ανάλογα με τον αριθμό των εγγεγραμμένων χρηστών (σε εκατ.) (**πηγή:** <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-registered-users/>)

Σύμφωνα με την έρευνα του Διαγράμματος 1, η οποία διεξήχθη τον Ιούλιο του 2013 το **Facebook** ήταν το πρώτο κοινωνικό δίκτυο, το οποίο ξεπέρασε το 1 δισεκατομμύριο καταχωρημένους λογαριασμούς. Τρίτο, κατετάγη το δίκτυο **Twitter**, το οποίο είχε πάνω από 500 εκατομμύρια εγγεγραμμένους λογαριασμούς. Ενώ, πρόσφατα το νεοεισερχόμενο **Pinterest** έφτασε 10 εκατομμύρια μοναδικούς επισκέπτες, χωρίς κάποια βοήθεια. Η πλειοψηφία με περισσότερους από 100 εκατομμύρια χρήστες προέρχεται από τις Ηνωμένες Πολιτείες, αλλά και από τις ευρωπαϊκές χώρες, ενώ το **VK** στην Ρωσία ή τα κινέζικα κοινωνικά δίκτυα **Qzone** και **Renren** έχουν κερδίσει μεγάλη απήχηση στις περιοχές τους.

WORLD MAP OF SOCIAL NETWORKS

June 2013



Εικόνα 4: Χάρτης των κοινωνικών δικτύων, που δείχνει τις πιο δημοφιλείς τοποθεσίες κοινωνικής δικτύωσης με βάση τη χώρα, σύμφωνα με την Alexa ([πηγή: http://vincos.it/world-map-of-social-networks/](http://vincos.it/world-map-of-social-networks/))

Στην Εικόνα 3, απεικονίζονται με διάφορα χρώματα στον παγκόσμιο χάρτη τα διασημότερα κοινωνικά δίκτυα σε κάθε χώρα, σύμφωνα με την Alexa. Παρατηρούμε ότι το *Facebook* είναι το διασημότερο και ευρύτερο κοινωνικό δίκτυο παγκοσμίως. Καλύπτει την μεγαλύτερη έκταση στον χάρτη, εκτός των χωρών που είναι Ρωσόφωνοι και στα Ρωσικά εδάφη όπου η έκταση χρωματίζεται με με καφέ. Εκεί το

διασημότερο κοινωνικό δίκτυο είναι το *V Kontakte* που εξακολουθεί να συναγωνίζεται με το *Odnoklassniki* για το πιο θα κατακτήσει την αγορά.

Επίσης, στις Ασιατικές περιοχές που χρωματίζονται με κόκκινο επικτατεί ως διασημότερο κοινωνικό δίκτυο το *Qzone* με 623 εκατ. χρήστες. Στο Ιράν, επικρατεί κρατική λογοκρισία και είναι δύσκολο από τους χρήστες του Διαδικτύου να αποκτήσουν πρόσβαση στο Facebook γι' αυτό ο «ηγέτης» των κοινωνικών δικτύων είναι το *Cloob*.

Παρακάτω παρουσιάζονται κάποια στατιστικά χρήσης των κοινωνικών δικτύων ανα τον κόσμο.

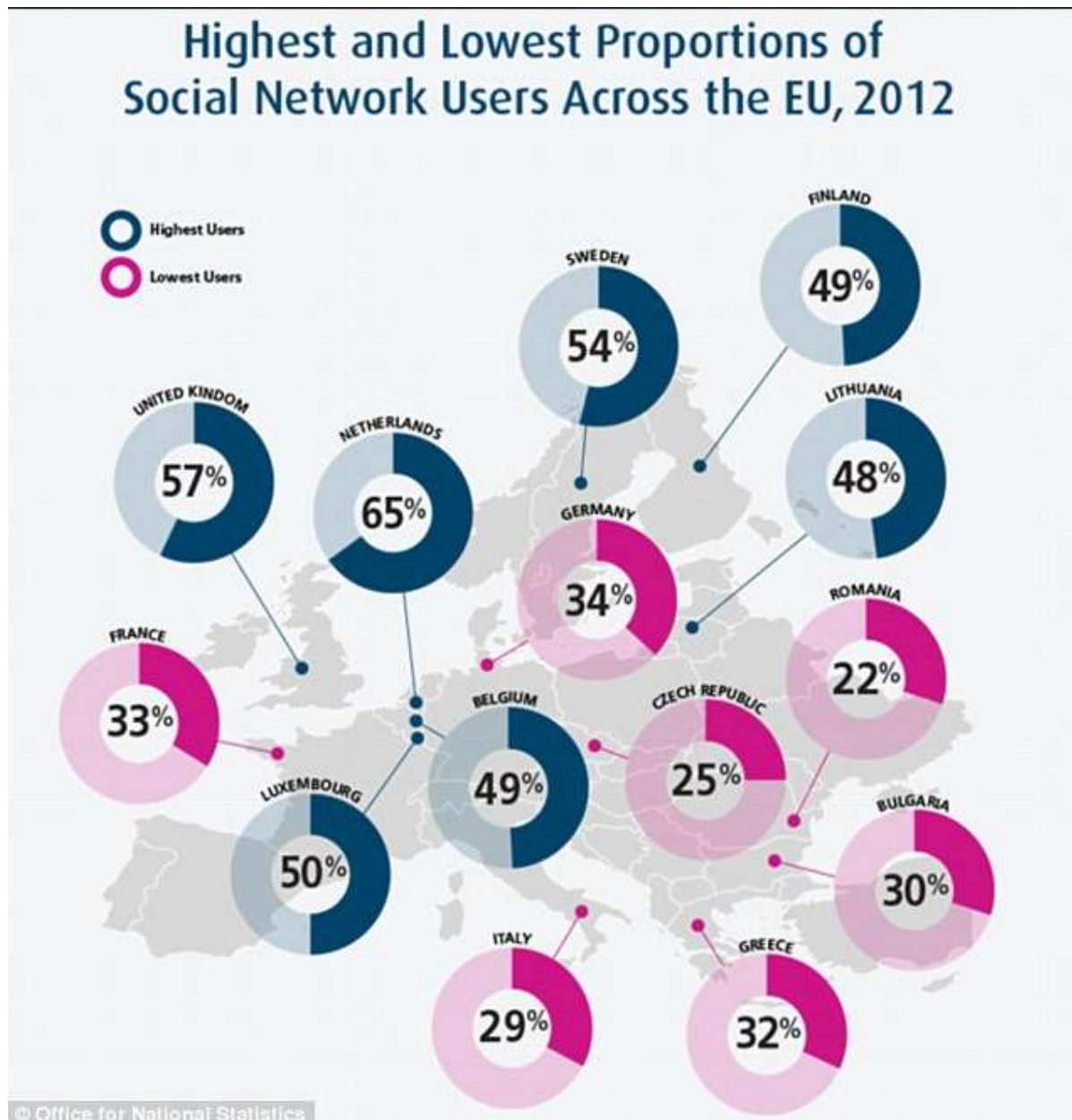
Social Network Statistics	Data
Total number of Facebook users worldwide	1.4 Billion
Total percentage of 18-24 year olds who already use social media	98%
Total percentage of people on Earth who use Facebook	11%
Total amount of minutes people spend on Facebook every month	700 billion
Average amount of time a person uses Facebook per month	15 hours 33 minutes
Total amount of people who access Facebook with phone	250 million
Total amount of websites that have integrated with Facebook	2.5 million
Total pieces of content shared on Facebook each month	70 billion
Total amount of unique YouTube users per month	490 million
Total amount of YouTube page views per month	92 billion
Total amount hours spent on YouTube per month	2.9 billion
Total amount of articles hosted by Wikipedia	17 million
Average pictures uploaded to Flickr per minute	3,000
Total amount of pictures hosted by Flickr	5 billion
Average amount of tweets per day	190 million
Percent of teenagers who log on to Facebook over 10 times per day	22%
Percent of Facebook users under the age of 10	25%
Percent of teens that view social networks as unsafe	59%
Percent of Americans who aren't confident in their ability to use privacy settings	24%

Εικόνα 5: Στατιστικά χρήσης των ΙΚΔ (πηγή: Browser Media, Socialnomics, MacWorld)

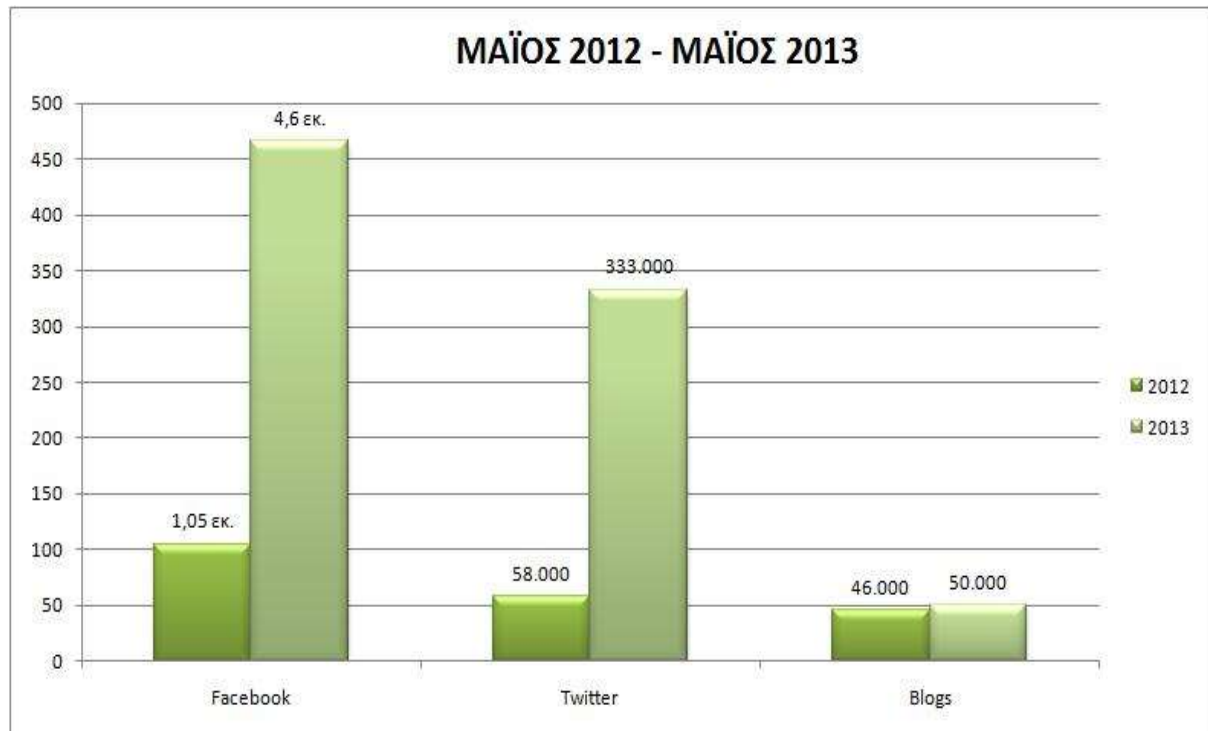
Στον πίνακα, τα στατιστικά αυτά έχουν προκύψει από έρευνα που έγινε στη 1 Ιανουαρίου του 2014, από τις Browser Media, Socialnomics και Macworld. Η έρευνα δείχνει τον τρόπο με τον οποίο οι άνθρωποι συνδέονται στα κοινωνικά δίκτυα, με την μέτρηση να "βγάζει" πρώτο το Facebook αριθμώντας 1,4 δισεκατομμύρια μέλη. Το 98 τοις εκατό των νέων, ηλικίας 18-24 έχει χρησιμοποιήσει τα κοινωνικά δίκτυα. Επίσης, περίπου 250 εκατομμύρια χρήστες χρησιμοποιούν τα κινητά τους τηλέφωνα για να εισαχθούν στο Facebook. Σημαντική ένδειξη στην έρευνα αποτελεί το γεγονός ότι το 25 τοις εκατό των χρηστών του Facebook είναι παιδιά, κάτω των 10 ετών, με την πλειοψηφία των νέων να δείχνει την τάση να μην νοιώθουν ασφάλεια στα

κοινωνικά δίκτυα. Ακόμα, το 24 τοις εκατό των αμερικάνων πολιτών δείχνει ανικανότητα στο κατά πόσο μπορεί να χρησιμοποιήσει τις ρυθμίσεις απορρήτου του Facebook.

Η Εθνική Στατιστική Υπηρεσία και η Eurostat μελέτησαν τον αριθμό των ανθρώπων σε όλη την Ευρώπη που χρησιμοποιούν τα κοινωνικά δίκτυα. Η Ολλανδία βρίσκεται στην κορυφή με 65 τοις εκατό και το Ηνωμένο Βασίλειο στην δεύτερη θέση.



Εικόνα 6: Στατιστικά υψηλότερων και χαμηλότερων χρηστών των ΙΚΔ στην Ευρώπη (πηγή: National Statistics & Eurostat)



Εικόνα 7: Εγγεγραμμένοι Έλληνες χρήστες σε Facebook, Twitter και Blogs (πηγή: Sidebar Monitor: <http://monitor.sidebar.gr/>)

Στην Εικόνα καταγράφεται η μεταβολή των κοινωνικών δικτύων στην Ελλάδα, από μια ελληνική ιστοσελίδα, την Monitor. Αυτή η μεταβολή μετράται από τον Μάιο του 2012 εως τον ίδιο μήνα του 2013. Στην εικόνα παρατηρείται μια θεαματική αύξηση των νέων Ελλήνων χρηστών που εγγράφηκαν μέσα σε ένα έτος. Οι Έλληνες χρήστες του Facebook αυξήθηκαν μέσα σε ένα έτος κατα 3.5 εκατ. και στο Twitter πάνω από 250 χιλιάδες.


ΕΝΟΤΗΤΑ 3^Η

Facebook, Twitter & Πολιτικές Προστασίας

3.1 Το Facebook

3.1.1 Εισαγωγή

Το Facebook είναι ένας από τους μεγαλύτερους και κερδοφόρους ιστότοπους κοινωνικής δικτύωσης. Ξεκίνησε τον Φεβρουάριο του 2004, με στόχο να λειτουργήσει ως εργαλείο σύνδεσης των ανθρώπων, επιδιώκοντας να αποτελέσει ένα είδος γέφυρας μεταξύ ψηφιακού και πραγματικού κόσμου. Ιδρύθηκε από τον Mark Zuckerberg, ως μέλος του πανεπιστημίου του Harvard. Αρχικά, συμμετείχαν μόνο φοιτητές του Harvard, το 2005 δόθηκε το δικαίωμα πρόσβασης σε μαθητές συγκεκριμένων λυκείων και μέλη ορισμένων μαθητικών κοινοτήτων, ενώ το 2006 η υπηρεσία έγινε προσβάσιμη σε κάθε άνθρωπο του πλανήτη που η ηλικία του ξεπερνούσε τα 13 χρόνια. Σύμφωνα με την επίσημη έκθεση του Α' Τριμήνου του 2013 για το μήνα Μάρτιο, η οποία δημοσιεύεται στην σελίδα του Facebook, αναφέρεται ότι έχει καθημερινά 665 εκατομμύρια ενεργούς χρήστες κατά μέσο όρο, αύξηση της τάξης του 26% από έτος σε έτος. Ενώ σύμφωνα με την εταιρία Monitor οι Έλληνες χρήστες του Facebook αριθμούν πάνω από 4,5 εκατομμύρια.



Ελληνες χρήστες Facebook: 4,663,095

Το Facebook σε αντίθεση με άλλα κοινωνικά δίκτυα, επιδιώκει την επικοινωνία με πραγματικούς φίλους της πραγματικής ζωής και όχι την δημιουργία εικονικών επαφών με αγνώστους. Με αποτέλεσμα σχεδόν όλοι οι χρήστες να χρησιμοποιούν τα πραγματικά τους στοιχεία, ονοματεπώνυμο, επάγγελμα, ημερομηνία γέννησης, σπουδές κ.α. Αυτό το γεγονός αποτελεί μεγάλη ανησυχία για την προστασία των προσωπικών δεδομένων των χρηστών σε παγκόσμιο επίπεδο.

3.1.2 Υπηρεσίες & Δυνατότητες

Το Facebook μέσα από την σελίδα του παρέχει πολλές υπηρεσίες και διάφορες δυνατότητες στους εγγεγραμμένους χρήστες του. Επιτρέπει την δημιουργία **προσωπικού προφίλ**, δίνοντας την δυνατότητα στον χρήστη να δημιουργήσει μέσα από κάποια εργαλεία την προσωπική του σελίδα. Μπορεί να καταχωρήσει το ονοματεπώνυμο του, την ηλικία του και γενικά στοιχεία της ταυτότητας του, τα επαγγελματικά και μορφωτικά στοιχεία του, στοιχεία επικοινωνίας, όπως τηλέφωνο,

ηλεκτρονική διεύθυνση. Επίσης, μπορεί να καταχωρήσει τα ενδιαφέροντα του, τις ασχολίες του, τις πολιτικές και θρησκευτικές του πεποιθήσεις, και να ανεβάσει μια φωτογραφία του με την εγγραφή. Κάθε χρήστης έχει την δυνατότητα να επιλέξει ποιόν «φίλο» θα καλέσει και ποιόν θα αποδεχτεί, να εκφράσει τις σκέψεις, τις ιδέες, την συναισθηματική του κατάσταση και ότι άλλο τον απασχολεί με την υπηρεσία δημοσίευσης. Έτσι προκύπτει ότι, το Facebook δίνει την δυνατότητα στους χρήστες του να δημιουργούν ένα κοινωνικό προφίλ με «φίλους», ένα χρονικό δραστηριοτήτων με σκέψεις, δημοσιεύσεις και καταχωρήσεις φωτογραφικού υλικού, βίντεο και μουσικής. Στον χρήστη, δίνεται επίσης και η δυνατότητα διαγραφής και αλλαγής οποιασδήποτε δημοσίευσης ή προσωπικού στοιχείου δεν τον αντιπροσωπεύει πια.

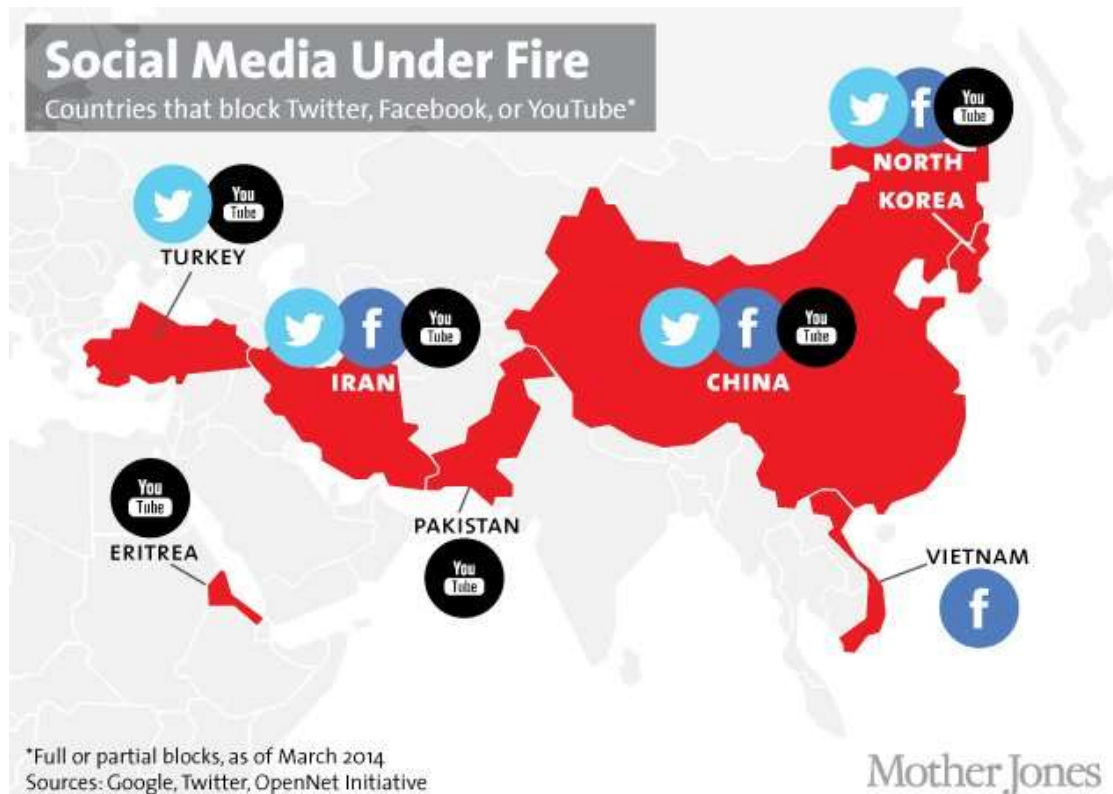
Στις 5 Σεπτεμβρίου 2006 στο Facebook προστέθηκαν δύο νέες υπηρεσίες, το **News Feed** και το **Mini-Feed**. Το **News Feed** ήταν μια υπηρεσία που εμφανίζε ως είδηση στην αρχική σελίδα του κάθε χρήστη τις αλλαγές στο προφίλ των «φίλων», η υπηρεσία συνέχισε να εξελίσσεται. Τον Φεβρουάριο του 2010, πρόσθεσαν νέες επιλογές στο μενού, έτσι ώστε οι χρήστες να βρίσκουν γρήγορα τις νέες και πιο πρόσφατες ενημερώσεις. Μέχρι και σήμερα, στην «Αρχική σελίδα» του κάθε χρήστη, εμφανίζονται οι **πιο πρόσφατες ή οι σημαντικές ενημερώσεις** των «φίλων» του κάθε χρήστη. Εμφανίζονται όλες οι ενέργειες, δημοσιεύσεις και κοινοποιήσεις του χρήστη και του κάθε «φίλου» του, την ακριβή ώρα και ημερομηνία που έγιναν. Το **Mini-Feed** δείχνει τι άλλαξε πρόσφατα στο προφίλ και το περιεχόμενο του κάθε χρήστη. Στις 18 Αυγούστου του 2010 εγκαινιάστηκε μια νέα υπηρεσία, οι χρήστες μπορούν να μοιραστούν με τους «φίλους» τους τις αγαπημένες τους τοποθεσίες μέσω του Facebook Places, η υπηρεσία αυτή ονομάζεται «**Κοινοποίηση παρουσίας (Check-in)**». Στις 22 Σεπτεμβρίου του 2011 παρουσιάστηκε το «**Χρονολόγιο (Timeline)**», αυτή η υπηρεσία δίνει την δυνατότητα στον χρήστη να μετακινηθεί στο παρελθόν και να δει γεγονότα, φωτογραφίες και μηνύματα την χρονική στιγμή που συνέβησαν στο παρελθόν. Μπορεί να επιλέξει τι θα εμφανίζεται στο χρονολόγιο του, να επιλέξει τα αγαπημένα γεγονότα και να τους διπλασιάσει το μέγεθος και μπορεί να κρύψει κάποια άλλα γεγονότα τελείως. Υπάρχει και η υπηρεσία **ανταλλαγής γραπτών και ηχογραφημένων μηνυμάτων, εικόνων και αρχείων**, δηλαδή δίνεται η δυνατότητα επικοινωνίας μεταξύ των χρηστών. Η επικοινωνία μπορεί να γίνει και σε πραγματικό χρόνο με χρήστες από την λίστα των «φίλων» που είναι συνδεδεμένοι στο σελίδα την ίδια χρονική στιγμή. Παρέχεται και η δυνατότητα επικοινωνίας με «βίντεοκλήση» με τους συνδεδεμένους «φίλους». Μια άλλη δυνατότητα που δίνει το Facebook είναι το «**Σκούντημα (Poke)**», όταν σκουντάτε κάποιον, ειδοποιείται ότι τον σκουντήσατε. Οι χρήστες του Facebook σκουντάνε τους «φίλους» τους για διάφορους λόγους, όπως για παράδειγμα, για να τους χαιρετήσουν. Επίσης, η σελίδα αποτελείται από **παιχνίδια** και **εφαρμογές** για τους χρήστες, όπως να ακούσουν μουσική με «φίλους» τους, να κοινοποιήσουν ό,τι διαβάζουν κ.α.

3.1.3 Δημιουργία Προφίλ στο Facebook

Οι σελίδες κοινωνικής δικτύωσης δίνουν την δυνατότητα στους χρήστες να δημιουργούν την δική τους ιστοσελίδα στο διαδίκτυο, καταγράφοντας τις σκέψεις, τις επιθυμίες, τα ενδιαφέροντα και τις σχέσεις με άλλους χρήστες. Παλιότερα μόνο γνωστοί και ισχυροί χαρακτήρες είχαν την δυνατότητα να εκφράζονται και να καταγράφουν δημόσια τις σκέψεις και την βιογραφία τους. Πλέον, δίνεται σε όλους τους χρήστες του διαδικτύου η ευκαιρία να εκφραστούν δημόσια δημιουργώντας προφίλ σε σελίδες κοινωνικής δικτύωσης. Οι χρήστες καταχωρούν στοιχεία όπως, όνομα, επώνυμο, ηλικία, ημερομηνία γέννησης, τόπος καταγωγής, τόπος διαμονής, στοιχεία της προσωπικότητάς τους κ.α, αλλά και στοιχεία επικοινωνίας όπως ηλεκτρονική διεύθυνση, τηλέφωνο κ.α. Κάθε χρήστης μπορεί να έχει τον έλεγχο στις πληροφορίες που δημοσιεύει και μπορεί να επιλέξει ποιές από αυτές θα εμφανίζονται δημόσια στο προσωπικό του προφίλ. Οι περισσότεροι χρήστες δημιουργούν ένα κοινωνικό προφίλ με σκοπό την δυνατότητα επικοινωνίας και φιλίας, την απόκτηση νέων «φίλων» ή την αναζήτηση παλιότερων μέσω της μηχανής αναζήτησης. Οι χρήστες μπορούν να δημοσιεύουν σκέψεις, φωτογραφίες, να σχολιάζουν, να στέλνουν και να αποδέχονται αιτήματα φιλίας, να επικοινωνούν κ.α. Εκτός όμως από το κοινωνικό προφίλ, οι χρήστες μέσα από την δημιουργία σελίδων (Pages) και ομάδων (Groups) μπορούν να εκφράζουν τις αντιδράσεις τους, τις διαφωνίες τους σε πολιτικά και κοινωνικά φαινόμενα παγκοσμίως. Η δημιουργία τέτοιων σελίδων και ομάδων αποτελεί έναν τρόπο συλλογικής ψηφιακής διαμαρτυρίας. Τα κοινωνικά μέσα αποτελούν βοηθήματα για κινήματα. Είναι χρήσιμα για την κινητοποίηση γύρω από έναν σκοπό, για το συντονισμό μεγάλων και ανομοιογενών ομάδων ανθρώπων και δίνουν τη δυνατότητα σε κινήματα να καθορίσουν το δικό τους μήνυμα.⁴ Πολλά είναι αυτά τα παραδείγματα όπως, το 2008 στην Αίγυπτο που δημιουργήθηκε μια ομάδα στο Facebook για να διαμαρτυρηθεί για την αύξηση των τροφίμων, η ομάδα συγκέντρωσε 75.000 μέλη και λίγο αργότερα ο δημιουργός της συνελήφθη. Επίσης το 2009, στην Κίνα απαγορεύτηκαν τα κοινωνικά δίκτυα όταν μια ειρηνική διαμαρτυρία κατά των Ουιγούρων, της μουσουλμανικής μειονότητας της Κίνας, κατέληξε σε θανατηφόρες ταραχές στην Xinjiang. Την ίδια χρονιά το Ιράν μπλοκάρει τα κοινωνικά δίκτυα μετά από τις αμφισβητούμενες προεδρικές εκλογές. Στο Βιετνάμ τα τελευταία δύο χρόνια, υπήρξαν εκτεταμένες αναφορές για αποκλεισμό του Facebook και τον Σεπτέμβριο του 2013, ψήφισε ένα νόμο που απαγορεύει στους πολίτες του να δημοσιεύουν αντικυβερνητικό περιεχόμενο στο κοινωνικό δίκτυο.

Στην παρακάτω εικόνα παρουσιάζονται χώρες που τα κοινωνικά δίκτυα έχουν υποστεί λογοκρισία από κυβερνητικά στελέχη σε περιόδους κοινωνικών και πολιτικών εξελίξεων.

⁴ Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου, Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας



Εικόνα 8: Χάρτης με χώρες στις οποίες έχουν αποκλειστεί και απαγορευτεί τα κοινωνικά δίκτυα σε περιόδους κρίσης, Facebook, Twitter, YouTube (πηγή: MotherJones: <http://www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked>)

Το Facebook σχηματίζει και το καταναλωτικό προφίλ κάθε χρήστη. Οι σελίδες κοινωνικής δικτύωσης δίνουν την δυνατότητα στις διαφημιστικές εταιρίες μέσα από εφαρμογές (applications) να δημιουργούν το προφίλ κάθε χρήστη. Οι δημιουργοί έχουν πρόσβαση στο προφίλ κάθε χρήστη προσπαθώντας έτσι να μετρήσουν την επίδραση των εφαρμογών και να προσωποποιήσουν το ανάλογο διαφημιστικό περιεχόμενο, μπορούν ακόμα να αποκτήσουν πρόσβαση και στο προφίλ κάθε καταχωρισμένου «φίλου» του χρήστη. Οι διαφημιστικές εταιρίες με αυτόν τον τρόπο στοχεύουν ανάλογα με την συμπεριφορά κάθε χρήστη να παρέχουν την ανάλογη διαφήμιση. Η τακτική αυτή ονομάζεται «συμπεριφορική διαφήμιση (behavioural advertise)». Αυτή η μέθοδος έχει ως στόχο την άμεση στοχευμένη διαφήμιση και την πιθανότητα εμφάνισης ενός προϊόντος που ο χρήστης θα είχε περισσότερη ανάγκη.

3.1.4 Πολιτική Προστασίας του Facebook

3.1.4.1 Πολιτική Χρήσης Δεδομένων

Κάθε χρήστης με την είσοδο και εγγραφή του στο σύστημα οφείλει να αποδεχτεί τους όρους χρήσης, τους περιορισμούς και την πολιτική προστασίας της ιδιωτικότητας του δικτύου. Τον Νοέμβριο του 2008, έγινε μια σημαντική τροποποίηση που παρέιχε στους χρήστες την δυνατότητα να διατηρούν «ανοιχτό» ή «κλειστό» προφίλ και να ελέγχουν την πρόσβαση σε αυτό μέσα από μια πολιτική χρήσης δεδομένων. Σύμφωνα και με την τελευταία ενημέρωση στην πολιτική χρήση των δεδομένων τον Νοέμβριο του 2013, οι χρήστες μπορούν να διαχειρίζονται, να διαγράφουν, να τροποποιούν, να δημοσιεύουν, να κοινοποιούν τις πληροφορίες στο χρονολόγιό τους. Οι πληροφορίες είναι τα στοιχεία με τα οποία γράφετε στον ιστότοπο ένας χρήστης και οι πληροφορίες που επιλέγει να κοινοποιήσει. Πληροφορίες, όπως είναι το όνομά, η διεύθυνση email, η ημερομηνία γέννησης και το φύλο, αλλά και πληροφορίες, όπως είναι ο αριθμός του κινητού. Επιπλέον, περιλαμβάνονται οι πληροφορίες που έχει επιλέξει ο χρήστης να κοινοποιεί όταν επικοινωνεί (π.χ. μέσω μιας διεύθυνσης email) ή όταν κάνει μια ενέργεια. Η ημερομηνία γέννησης είναι απαραίτητη και υπάρχει όριο για την εγγραφή ενός νέου χρήστη για να ελέγχεται το περιεχόμενο και οι διαφημίσεις που είναι κατάλληλα για την ηλικία τους. Είναι από τις πληροφορίες που αργότερα, ο χρήστης μπορεί να αποκρύψει από το χρονολόγιό του. Τα δεδομένα που παρέχει και οι πληροφορίες που κοινοποιεί ένας χρήστης μπορεί να είναι δημόσια ή προσαρμοσμένα ανάλογα με την κρίση του. Δημόσιες πληροφορίες είναι αυτές επιλέγει να εμφανίζονται δημόσια όσο και εκείνες που είναι πάντοτε δημόσια διαθέσιμες. Πάντοτε δημόσια διαθέσιμες θεωρούνται το Όνομα, οι εικόνες προφίλ και φωτογραφίες εξωφύλλου, τα Δίκτυα, το Φύλο και αναγνωριστικό και όνομα χρήστη. Τις πληροφορίες αυτές μπορεί να τις δει οποιοσδήποτε, ακόμη και άτομα εκτός Facebook.

Η εταιρία στην εγγραφή και ασφάλεια λογαριασμού αναφέρει ότι οι χρήστες του Facebook θα πρέπει να παρέχουν τα αληθινά τους ονόματα και πραγματικά στοιχεία, καθώς επίσης και να τηρούν κάποιες δεσμεύσεις. Σε αντίθετη περίπτωση, οι διαχειριστές μπορούν να προχωρήσουν σε απενεργοποίηση του λογαριασμού των χρηστών αυτών.

Η εταιρία έχει ως βασικό στόχο και μέλημα ο χρήστης να έχει τον έλεγχο των προσωπικών πληροφοριών που καταχωρεί και κοινοποιεί. Να επιλέγει και να προσαρμόζει τις σχετικές ρυθμίσεις για τον λογαριασμό του και τις ρυθμίσεις για το απόρρητο. Η εταιρία συλλέγει και αποθηκεύει τα δεδομένα των χρηστών, τα οποία μπορούν να ελεγχθούν και από εξωτερικούς συνεργάτες για την βελτίωση των υπηρεσιών της, αλλά και να παρέχει πληροφορίες σε διαφημιστικές εταιρίες.

3.1.4.2 «Παγίδες» στην Πολιτική Χρήσης Δεδομένων

Κάθε χρήστης με την είσοδο και εγγραφή του στην πλατφόρμα του Facebook δίνει αυτόματα την άδεια και το δικαίωμα στους διαχειριστές της σελίδας αυτής, να χρησιμοποιούν τις πληροφορίες που παρέχουν οι χρήστες αυτοί. Τους δίνει την δυνατότητα να προσπελάσουν, να διατηρήσουν ή να κοινοποιήσουν τις πληροφορίες, όταν λάβουν σχετικό νομικό αίτημα (π.χ. ένταλμα έρευνας, δικαστική εντολή ή κλήτευση) ή όταν θεωρήσουν ότι κάτι τέτοιο είναι νομικά επιβεβλημένο. Επίσης, έχουν την δυνατότητα να έχουν πρόσβαση σε πληροφορίες, να τις διατηρούν και να τις κοινοποιούν όταν «θεωρούν» ότι είναι απαραίτητες για τον εντοπισμό, την αποτροπή και την αντιμετώπιση απάτης ή άλλων παράνομων δραστηριοτήτων (π.χ. αν αποτελούν μέρος ερευνών), καθώς και για την αποτροπή θανάτων ή επικείμενης σωματικής βλάβης. Μετα από νομικές άδειες, μπορούν να κοινοποιήσουν και να αποκαλύψουν πληροφορίες και δεδομένα χρηστών, όπως επιβάλλει η ισχύουσα νομοθεσία για να προασπίσουν τα συμφέροντά της εταιρίας τους ή στην περίπτωση που θα χρειαστεί στο να αποτρέψουν κάποια παράβαση και απάτη.

Επίσης, έχουν το δικαίωμα να διατηρήσουν για τουλάχιστον ένα έτος πληροφορίες από λογαριασμούς που έχουν απενεργοποιηθεί για παραβιάσεις των όρων χρήσης, προκειμένου να αποτρέψουν την επανειλημμένη κατάχρηση του ιστοτόπου ή περαιτέρω παραβιάσεις των όρων χρήσης. Μπορούν να χρησιμοποιήσουν τα στοιχεία επικοινωνίας των χρηστών (email, αριθμός κινητού) για να στείλουν ειδοποιήσεις και διάφορα μηνύματα. Άρα δίνει το δικαίωμα στην εταιρία να χρησιμοποιεί τα στοιχεία και τις πληροφορίες ανα πάσα στιγμή και για μεγάλο χρονικό διάστημα. Παλιότερα οι χρήστες δεν μπορούσαν να διαγράψουν το προφίλ από την πλατφόρμα, αλλά μόνο να το απενεργοποιήσουν. Όταν ο λογαριασμός απενεργοποιείται, μπαίνει σε κατάσταση αδράνειας και οι πληροφορίες δεν διαγράφονται. Πλέον ο χρήστης μπορεί να διαγράψει τον λογαριασμό του, αλλά με όρους, όπως ότι η διαγραφή θα διαρκεί συνήθως γύρω στον ένα μήνα και κάποιες πληροφορίες θα παραμένουν συχνά σε αντίγραφα ασφαλείας και σε αρχεία καταγραφής για τουλάχιστον 90 ημέρες.

Δύσκολος είναι και ο έλεγχος των πληροφοριών καθώς είναι πολύ εύκολο να δηλώσει ένας χρήστης ψευδή στοιχεία. Στην πολιτική του αναφέρει ότι δεν μπορούν να χρησιμοποιούν το Facebook άτομα εάν είναι κάτω των 13 ετών, όπως επίσης και άτομα τα οποία έχουν καταδικαστεί για σεξουαλικό αδίκημα. Πολλοί χρήστες δηλώνουν ψευδή ή ελλιπή στοιχεία θέτοντας σε κίνδυνο άλλους χρήστες ή σε χειρότερη περίπτωση παιδιά που βρίσκονται σε ηλικία κάτω των 13 είναι εύκολο να παγιδευτούν δηλώνοντας αναληθή στοιχεία.

Η ιστοσελίδα αναφέρει στην πολιτική της ότι εγκαθιστά cookie στους φυλλομετρητές και στην διεύθυνση IP των χρηστών, χωρίς όμως εκείνοι να γνωρίζουν την λειτουργία τους. Τα cookie είναι δεδομένα που αποθηκεύονται στον υπολογιστή, στο κινητό τηλέφωνο ή σε άλλη συσκευή των χρηστών. Επίσης, παράλληλα χρησιμοποιούνται και τα pixel. Τα pixel είναι μικρά τμήματα κώδικα στις ιστοσελίδες, που επιτρέπουν σε κάποιον άλλο διακομιστή να μετρά τις προβολές της ιστοσελίδας. Η χρήση αυτών των τεχνολογιών γίνεται για εμπορικούς λόγους, όπως είναι οι

διαφημίσεις και για να αποθηκεύουν πληροφορίες και να παρακολουθούν τη χρήση των προϊόντων και των υπηρεσιών.

Ο χρήστης έχει την δυνατότητα να ελέγχει όπως αναφέραμε νωρίτερα, σε ποιούς θα επιτρέψει την πρόσβαση και την προβολή των πληροφοριών και των δεδομένων. Όμως, δεν μπορεί να γνωρίζει και να ελέγχει σε ποιόν θα γνωστοποιηθούν αυτά τα στοιχεία έπειτα, αφού η εταιρία επιτρέπει σε χρήστες να αντιγράφουν και να χρησιμοποιούν δεδομένα, πληροφορίες, φωτογραφίες κ.α. άλλων χρηστών. Η εταιρία δεν εγγυάται την ασφάλεια σε αυτήν την περίπτωση, όπως επίσης και στην περίπτωση της παράνομης απόκτησης και πρόσβασης σε προσωπικές πληροφορίες. Τέλος, αναφέρουν ότι αν αλλάξει ιδιοκτησία η επιχείρησή, έχουν το δικαίωμα να μεταφέρουν τα στοιχεία των χρηστών στον νέο ιδιοκτήτη, καθώς επίσης και ότι η πλατφόρμα μπορεί να αλλάζει την Πολιτική χρήσης δεδομένων, όποτε το θεωρεί απαραίτητο. Ακόμα ενημερώνει ότι, πρόσβαση στα δεδομένα και τις πληροφορίες των χρηστών αποκτούν άτομα και εταιρίες με σκοπό, σύμφωνα με την εταιρία να την βοηθήσουν να κατανοήσει και να βελτιώσει τις υπηρεσίες της.

Άρα συμπεραίνουμε ότι ο χρήστης ουσιαστικά είναι δύσκολο να ελέγχει τα στοιχεία και τις πληροφορίες που παρέχει στην πλατφόρμα κοινωνικής δικτύωσης. Μπορούν να παραβιαστούν τα δεδομένα, να συλλεχθούν και να διαμοιραστούν πληροφορίες, φωτογραφίες και άλλα στοιχεία χρηστών από τρίτους. Καθώς επίσης και το ότι η εταιρία αποθηκεύει, καταχωρεί και διατηρεί φακέλους χρηστών, ακόμα και χρηστών που πάυουν να είναι χρήστες της σελίδας. Ενώ μπορεί ανα πάσα ώρα και στιγμή να αποκαλύψει πληροφορίες αν αυτό της ζητηθεί και εκείνη το θεωρεί απαραίτητο.

3.1.5 Προστασία της ιδιωτικότητας στο Facebook

Όπως αναφέρεται στην πολιτική του Facebook, με την εγγραφή νέων χρηστών στις Η.Π.Α δίνεται αυτόματα το δικαίωμα στην εταιρία να διαβιβάσει τις πληροφορίες και τα δεδομένα στις κρατικές και αστυνομικές αρχές των Ηνωμένων Πολιτειών. Στην Πολιτεία της Καλιφόρνια, όπου έχει έδρα η εταιρία του Facebook η νομοθεσία της επιτρέπει στους κατοίκους της Καλιφόρνιας να ζητάνε συγκεκριμένες λεπτομέρειες για όσα κοινοποιεί μια εταιρεία σε τρίτους με σκοπό την άμεση διαφημιστική προώθησή τους. Αμφισβητείται όμως το κατά πόσο το Αμερικάνικο δίκαιο θα δεχτεί τους όρους πολιτικής της εταιρίας Facebook.

Η εταιρία για να βελτιώσει το ρυθμιστικό πλαίσιο για την προστασία συμμετέχει στο πρόγραμμα απορρήτου Safe Harbor (ΗΠΑ), όπως ορίζεται από το Υπουργείο Εμπορίου των ΗΠΑ. Στο πλαίσιο της συμμετοχής της στο πρόγραμμα Safe Harbor, συμφώνησε να συνεργαστεί με την TRUSTe για την επίλυση διαφωνιών που αφορούν τη συμμόρφωσή της με τις αρχές απορρήτου του προγράμματος Safe Harbor. Με το πρόγραμμα αυτό προσπάθησε να εγγυηθεί την προστασία της ιδιωτικότητας και ασφάλειας των χρηστών, καθώς επίσης και να επιλύσει τα προβλήματα μεταξύ εταιρίας και χρήστη, αν και αργότερα αμφισβητήθηκε η αξιοπιστία του. Μια ακόμα ενέργεια που πραγματοποίησε η εταιρία ήταν η

προσχώρησή στις «αρχές ασφαλούς λιμένα», έπειτα από διαπραγματεύσεις μεταξύ Ε.Ε και Η.Π.Α. Η εταιρία είναι σύμφωνη με τις «αρχές» παρέχοντας ικανοποιητικό επίπεδο προστασίας προσωπικών δεδομένων και επιτρέποντας τη διαβίβαση δεδομένων από κράτη μέλη της Ευρωπαϊκής ένωσης προς αυτήν. Επίσης, η εταιρεία υπάγεται στην δικαιοδοσία του κρατικού φορέα της Ομοσπονδιακής Επιτροπής Εμπορίου των Η.Π.Α με σκοπό να διερευνά καταγγελίες και λαμβάνει μέτρα κατά των αθέμιτων πρακτικών, όπως και για να φροντίζει για την αποζημίωση θιγόμενων ανεξαρτήτου χώρας και ιθαγένειας σε περίπτωση μη συμμόρφωσης στις «αρχές».

Στο Δουβλίνο της Ιρλανδίας το 2008, εγκαθιστάτε η έδρα της επιχείρησης για τις περιοχές της Ευρώπης, της Μέσης Ανατολής και της Ασίας. Η εταιρία υποστηρίζει ότι δεν αποθηκεύει, δεν επεξεργάζεται και δεν κοινοποιεί τα προσωπικά δεδομένα των χρηστών, αλλά όπως αναφέραμε και παραπάνω στην πολιτική χρήσης είδαμε ότι εγκαθιστά cookie στους φυλλομετρητές και στην διεύθυνση IP των χρηστών και χρησιμοποιεί pixel. Όπως επίσης, ότι αποθηκεύει για μεγάλο χρονικό διάστημα τις πληροφορίες των χρηστών. Άρα συνεπάγεται ότι η εταιρία συλλέγει τα δεδομένα των χρηστών, με αποτέλεσμα να έρχεται σε αντίθεση με την Οδηγία 95/46/ΕΚ της Ε.Ε. η οποία εφαρμόζεται για τα δεδομένα που αποτελούν αντικείμενο επεξεργασίας. Η κοινοτική οδηγία εφαρμόζεται υπό προϋποθέσεις ακόμα και αν η εταιρία έχει έδρα εκτός Ε.Ε. Την Οδηγία 95/46/ΕΚ θα αναλύσουμε εκτενέστερα σε επόμενο κεφάλαιο.

Στο Ελληνικό πλαίσιο για την έρευνα σε προσωπικά προφίλ απαιτείται απόφαση Εισαγγελέα. Οι ελληνικές αρχές έχουν την δυνατότητα να ζητήσουν στοιχεία χρηστών από την εταιρία σε περιπτώσεις εξακρύβωσης παράνομων και σοβαρών εγκληματικών πράξεων. Για την πρόσβαση σε προσωπικά δεδομένα απαιτείται η άρση του απορρήτου και συγκεκριμένα σύμφωνα με τις διατάξεις: άρθρα 19, 25 του συντάγματος ν.2225/1194, ν.3115/2003, ν.3471/2006, ν.3674/2008. Στις περιπτώσεις που υπάρχουν καταγγελίες, όπως απειλές, επεξεργασία δεδομένων κ.α σε χρήστες με τα πραγματικά τους στοιχεία, δεν απαιτείται η άρση του απορρήτου, αφού μπορεί να γίνει επώνυμα η οποιαδήποτε καταγγελία. Άρση απορρήτου απαιτείται στις περιπτώσεις χρηστών που εκκρεμούν καταγγελίες εις βάρος τους και χρησιμοποιούν ψεύτικα ή πλαστά στοιχεία ή σε σοβαρές περιπτώσεις εγκληματικών πράξεων.

Στις 21 Σεπτεμβρίου 2012, στην Ελλάδα συλλαμβάνεται ο κάτοχος μιας σελίδας στο Facebook. Ένα γεγονός που δόθηκε μεγάλη έμφαση και δίχασε τις ελληνικές αρχές, το κράτος, τους νομικούς και γενικά το σύνολο της κοινωνίας σε Ελλάδα και εξωτερικό. Το αδίκημα του χρήστη κατατάσσεται στα αδικήματα της κακόβουλης βλασφημίας, της καθύβρισης θρησκευμάτων και της εξύβρισης νεκρού. Το συγκεκριμένο αδίκημα ανήκει στα πλημμελήματα, οπότε σύμφωνα με την πολιτική χρήση δεν αποτελεί σοβαρό αδίκημα και δεν επιτρέπεται η άρση απορρήτου. Σύμφωνα με τον κάτοχο της σελίδας, υποστηρίζει ότι τα στοιχεία του δόθηκαν στη Δίωξη Ηλεκτρονικού Εγκλήματος από το Facebook.⁵

⁵ <http://www.koutipandoras.gr/article/26337/facebook-niptei-ta-heiras-toy-gia-ton-pastitsio>

Σε δηλώσεις του ο πανευρωπαϊκός διευθυντής επικοινωνιών του Facebook, Iain Mackenzie ανέφερε ότι, «το Facebook παρέδωσε τα στοιχεία του συγκεκριμένου χρήστη στις Ελληνικές Εισαγγελικές Αρχές χωρίς να εξετάσει καν για ποιο λόγο ζητείται η άρση του απορρήτου των επικοινωνιών». ⁶

Στο δελτίο τύπου της ελληνικής αστυνομίας αντίθετα, αναφέρεται ότι «από την αστυνομική ψηφιακή έρευνα, που πραγματοποιήθηκε στο πλαίσιο διενέργειας προκαταρκτικής εξέτασης, διακριβώθηκαν τα αρχεία καταγραφής (logfiles) και τα ηλεκτρονικά ίχνη του διαχειριστή - χρήστη της επίμαχης σελίδας». ⁷

Ο κάτοχος της σελίδας καταδικάστηκε με 10 μήνες φυλάκιση για εξύβριση θρησκευμάτων κατ' εξακολούθηση, απόφαση που πυροδότησε σωρεία αντιδράσεων στα κοινωνικά δίκτυα και τα μέσα ενημέρωσης ακόμα και σε διεθνές επίπεδο, καθώς και του νομικούς κύκλους.



⁶ <http://www.csmonitor.com/World/Europe/2012/1002/Blasphemy-in-democracy-s- birthplace-Greece-arrests-Facebook-user>

⁷ 24-09-2012: Η Δίωξη Ηλεκτρονικού Εγκλήματος συνέλαβε 27 χρόνο ημεδαπό για κακόβουλη βλασφημία και καθύβριση θρησκευμάτων, μέσω του Facebook (πηγή: http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=20338&Itemid=965&lang=)


3.2 Το Twitter

3.2.1 Εισαγωγή

Το Twitter είναι ένας χώρος κοινωνικής δικτύωσης και παρέχει υπηρεσίες micro - ιστολογιών στους χρήστες του, που τους επιτρέπει να στέλνουν και να διαβάζουν “*tweets*”. Τα Tweets είναι μηνύματα κειμένου που περιορίζονται μέχρι 140 χαρακτήρες σε μέγεθος. Οι εγγεγραμμένοι χρήστες μπορούν να γράφουν και να διαβάζουν tweets άλλων χρηστών, αλλά οι μη εγγεγραμμένοι έχουν την δυνατότητα μόνο να διαβάζουν τα tweets των χρηστών. Δημιουργήθηκε τον Μάρτιο του 2006 από τους Jack Dorsey, Evan Williams, Biz Stone και Noah Glass.



Είναι μια πλατφόρμα επικοινωνίας που αριθμεί 400 εκατομμύρια μηνιαίους επισκέπτες και περισσότερα από 200 εκατομμύρια ενεργούς χρήστες κάθε μήνα σε όλο τον κόσμο. Στην Ελλάδα, σύμφωνα με την Monitor οι εγγεγραμμένοι χρήστες αριθμούν πάνω από τους 380 χιλιάδες.

 Έλληνες χρήστες Twitter: **380,271**

3.2.2 Ιστορική Αναδρομή - Υπηρεσίες & Δυνατότητες

Το Twitter παρέχει στους χρήστες του περιορισμένο αριθμό λειτουργιών σε σχέση με άλλα κοινωνικά δίκτυα, όπως για παράδειγμα το Facebook. Αυτός ίσως είναι ένας σημαντικός παράγοντας που βοήθησε στην ταχύτατη ανάδειξή του. Με την είσοδο και εγγραφή στην σελίδα, ο χρήστης μπορεί να δημιουργήσει ένα προσωπικό προφίλ, με το όνομα ή το ψευδώνυμο του, λεγόμενο ως «*handle*». Το όνομα αυτό είναι κάτι σαν μια διεύθυνση επικοινωνίας και ένας τρόπος αναγνώρισης και αλληλεπίδρασης του, με τους υπόλοιπους χρήστες. Με την δημιουργία λογαριασμού ο χρήστης μπορεί να προσθέσει μια φωτογραφία προφίλ, μια εικόνα κεφαλίδας και να συμπληρώσει ένα βιογραφικό σημείωμα που τον αντιπροσωπεύει και τον χαρακτηρίζει. Από τον Σεπτέμβριο μέχρι τον Οκτώβριο του 2010, η εταιρία άρχισε να αναπτύσσει μια ανανεωμένη έκδοση του νέου Twitter. Οι αλλαγές παρείχαν την δυνατότητα στους χρήστες να βλέπουν εικόνες και βίντεο χωρίς να φεύγουν από την πλατφόρμα. Στις 8 Δεκεμβρίου του 2011, εκτός από την καρτέλα «*Home*» προστέθηκαν και οι καρτέλες «*Connect*» και «*Discover*». Επιπλέον, επανασχεδιάστηκε και το χρονολόγιο στο οποίο εμφανίζονται τα «*tweets*» των χρηστών. Στις 5 Ιουνίου του 2012, αφαιρέθηκε το κείμενο από το λογότυπο και ανασχεδιασμένο παρουσιάστηκε το πουλί ως το κύριο λογότυπο και σύμβολο του

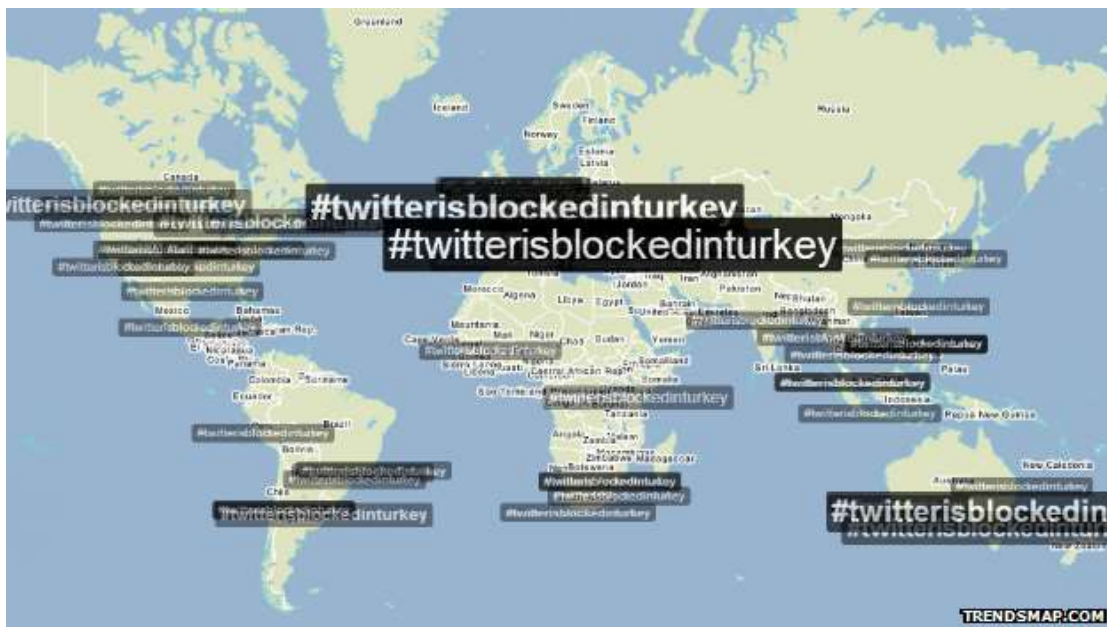
Twitter. Στις 18 Δεκεμβρίου 2012, το Twitter ανακοίνωσε ότι κατάφερε να ξεπεράσει τα 200 εκατομμύρια ενεργούς χρήστες κάθε μήνα. Στις 18 του Απριλίου του 2013, το Twitter ξεκίνησε μια εφαρμογή μουσικής που ονομάζεται «*Twitter Music*» για iPhone. Τον Απρίλιο του 2014 ανακοίνωσε νέες αλλαγές στο προφίλ των χρηστών. Το νέο προφίλ έχει σχεδιαστεί και μοιάζει με εκείνο του Facebook, μεγαλύτερο προφίλ με φωτογραφία και μια προσαρμοσμένη εικόνα κεφαλίδας. Το προφίλ θα δίνει έμφαση σε συγκεκριμένα tweets και θα επιτρέπει στους χρήστες να ψάχνουν μέσα από τις σελίδες προφίλ για να βρουν το είδος των tweets που θέλουν. Επίσης, ένας χρήστης θα μπορεί να καρφιστώσει ένα αγαπημένο tweet στην κορυφή της σελίδας του προφίλ του, ενώ τα tweets με τα περισσότερα retweets και οι απαντήσεις θα εμφανίζονται ελαφρώς μεγαλύτερα, έτσι ώστε να είναι πιο εύκολο για τους άλλους να τα βρουν. Τα tweets είναι μηνύματα τα οποία μπορούν να περιέχουν το πολύ 140 χαρακτήρες, τα μηνύματα αυτά θα εμφανίζονται στους followers. Οι followers είναι οι χρήστες που ακολουθεί ένας άλλος χρήστης.

3.2.3 Δημιουργία Προφίλ στο Twitter

Στο Twitter οι χρήστες δεν δημιουργούν ένα προφίλ με την πλέον διαδεδομένη έννοια όπως είδαμε και στο Facebook. Είναι ένα μέσο κοινωνικής δικτύωσης με το οποίο οι χρήστες αλληλεπιδρούν μέσω σύντομων μηνυμάτων, μέχρι 140 χαρακτήρες. Κυρίως λειτουργεί, ως ένα μέσο με το οποίο οι χρήστες ανακαλύπτουν τις τελευταίες ή δημοφιλέστερες πληροφορίες και ειδήσεις για το τί συμβαίνει σχετικά με θέματα που τους ενδιαφέρουν. Μέσω των hashtags τα οποία είναι λέξεις ή φράσεις χωρίς κενά, με το σύμβολο αριθμού ("#") μπορεί κανείς να αναζητήσει ένα σύνολο μηνυμάτων.

Όπως παρατηρήσαμε νωρίτερα (βλ. Εικόνα 5), τις επιδράσεις του Facebook στην πολιτικές και κοινωνικές εξελίξεις των χωρών, αντίστοιχα εντοπίζουμε ότι και το Twitter έχει επιρεάσει τις εξελίξεις των κοινωνιών και έχει δεχτεί επίσης λογοκρισία. Σημαντικά και αξιοσημείωτα γεγονότα είναι το 2011 που το Twitter χρησιμοποιήθηκε ως εργαλείο για την οργάνωση διαδηλώσεων κατά τη διάρκεια της Αραβικής Άνοιξης. Με αποτέλεσμα να μπλοκαριστεί ή να κλείσει πλήρως σε χώρες της Μέσης Ανατολής και της Βόρειας Αφρικής. Την ίδια χρονιά είχε μπλοκαριστεί και στην Λευκορωσία για να καταστείλει τις αντικυβερνητικές διαδηλώσεις. Πρόσφατο γεγονός αποτελεί και ο αποκλεισμός του Twitter που συνέβη τον Μάρτιο του 2014 στην Τουρκία, το 2010 στην Τουρκία είχαν δεχθεί ξανά λογοκρισία τα κοινωνικά δίκτυα από την κυβέρνηση. Το Youtube είχε αποκλειστεί δύο χρόνια και δεν επιτρεπόταν η πρόσβαση στην ιστοσελίδα διότι θεωρούνταν ότι υπήρχαν προσβλητικά βίντεο για τον ιδρυτή της χώρας, Μουσταφά Κεμάλ Ατατούρκ. Το Μάρτιο η Τουρκική κυβέρνηση ξανά λογοκρίνει ένα κοινωνικό δίκτυο, το Twitter αυτή την φορά. Οι χρήστες αντίκρισαν ένα πρωτοφανές μήνυμα στην σελίδα, μια δήλωση από την ρυθμιστική αρχή τηλεπικοινωνιών της Τουρκίας, η οποία αναφέρεται σε δικαστικές αποφάσεις για την προφανή κλείσιμο του site. Αιτία σύμφωνα με την κυβέρνηση της Τουρκίας για τον αποκλεισμό της ιστοσελίδας ήταν ότι κάποιοι χρήστες είχαν αναρτήσει φωνητικές εγγραφές και έγγραφα που εμφανίζαν ενδείξεις διαφθοράς μεταξύ του εσωτερικού

κύκλου της κυβέρνησης. Προφανές ήταν να ξεσπάσει ένα παγκόσμιο κύμα αντιδράσεων παγκοσμίως ενάντια στην απόφαση της κυβέρνησης της Τουρκίας για τον αυταρχικό και χωρίς προειδοποίηση αποκλεισμό ενός κοινωνικού δικτύου, καθώς και την απόφαση της να κινηθεί νομικά εναντίον της εταιρίας για το κλείσιμο της. Στην παρακάτω εικόνα παρουσιάζεται ένα παγκόσμιο trending topic (**trending topic**: αυτός είναι ένας ορισμός που χρησιμοποιείται στο Twitter και αναφέρεται στο δημοφιλέστερο hastag, το σύνολο των tweets σε ένα συγκεκριμένο θέμα που έχει συζητηθεί περισσότερο). Παράδειγμα ενός τέτοιου trending topic αποτελεί και το hastag, #twitterisblockedinturkey για τον αποκλεισμό των Τούρκων χρηστών από το Twitter με απόφαση της κυβέρνησής τους.



Εικόνα 9: Στην εικόνα παρουσιάζεται ένας χάρτης με τα tweets παγκοσμίως που είχαν ως δημοφιλέστερο hastag το #twitterisblockedinturkey (**πηγή:** BBC news EUROPE: <http://www.bbc.com/news/world-europe-26681236>)

3.2.4 Πολιτική Προστασίας του Twitter

Το Twitter συλλέγει προσωπικές πληροφορίες των χρηστών και έχει το δικαίωμα να τις μεταβιβάσει ως περιουσιακό στοιχείο, σε περίπτωση που η εταιρία αλλάξει χέρια. Σύμφωνα με την πολιτική του, αναφέρει ότι σε περίπτωση που οι χρήστες χρησιμοποιούν μια υπηρεσία του, αυτόματα δίνεται και η συγκατάθεση για την συλλογή, την αποθήκευση, τον χειρισμό και άλλων χρήσεων των δεδομένων αυτών. Επισημαίνοντας ότι τα στοιχεία και οι πληροφορίες αυτές ανεξαρτήτως χώρας, μπορούν να χρησιμοποιηθούν στις Ηνωμένες Πολιτείες και σε όποια άλλη χώρα δραστηριοποιείται η εταιρία. Με την υποβολή ή δημοσίευση οποιουδήποτε περιεχομένου μέσω της υπηρεσίας, παραχωρείται το **δικαίωμα για μια χωρίς δικαιώματα άδεια χρήσης** αντιγραφής, αναπαραγωγής, επεξεργασίας, τροποποίησης,

μετάδοσης, προβολής και διανομής του περιεχομένου αυτού σε όλα τα μέσα (ενημέρωσης, δικτύωσης κ.α) που υπάρχουν ή θα αναπτυχθούν στο μέλλον, σε άλλες εταιρίες ή σε οργανισμούς που συνεργάζονται με το Twitter, χωρίς να δωθεί κάποια αποζημίωση. Στις πολιτικές της αναφέρει ότι ένας εγγεγραμμένος χρήστης μπορεί να διαγράψει τον λογαριασμό του, ο λογαριασμός θα απενεργοποιηθεί για 30 ημέρες. Έπειτα από 30 ημέρες, ξεκινάει η διαδικασία διαγραφής του λογαριασμού από το σύστημα, η οποία μπορεί να διαρκέσει έως και μία εβδομάδα.

Το Twitter στις 21 Οκτωβρίου του 2013, στις πολιτικές ασφάλειας της σελίδας « *twitter.com/privacy* » αναφέρει ότι ενδέχεται στο μέλλον το περιεχόμενο και η παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων να αναθεωρηθεί ή να τροποποιηθεί. Επίσης, οι ίδιοι οι χρήστες είναι υπεύθυνοι για τις πληροφορίες και το περιεχόμενο που παρέχουν στην σελίδα, καθώς και για τις μετέπειτα επιπτώσεις χρήσης του περιεχομένου αυτού από τρίτους. Αναφέρει σχετικά ότι, το Twitter δεν θα είναι υπεύθυνο για οποιαδήποτε χρήση του περιεχομένου, σύμφωνα με τους παρόντες όρους. Οι χρήστες με την εγγραφή τους, δηλώνουν και εγγυώνται ότι παρέχουν όλα τα απαραίτητα δικαιώματα και εξουσίες για να παραχωρήσουν σε οποιονδήποτε το περιεχόμενο που υποβάλλουν.

Το Twitter όπως και το Facebook αναφέρει στην πολιτική του ότι χρησιμοποιεί τεχνολογίες cookies με τις οποίες έχει το δικαίωμα να συλλέγει δεδομένα και πληροφορίες των χρηστών, όπως επίσης της δίνεται το δικαίωμα να ελέγχει την χρήση του, από τους χρήστες με σκοπό την βελτίωση των υπηρεσιών της. Επίσης, αναφέρει ότι η εταιρία διατηρεί μια «Σύνδεση δεδομένων» η οποία περιλαμβάνει πληροφορίες που έχουν καταγραφεί από τους διακομιστές, όπως η διεύθυνση IP, ο τύπος browser, το λειτουργικό σύστημα, οι σελίδες που επισκέπτεται ένας χρήστης, η τοποθεσία, ο αριθμός του κινητού τηλεφώνου, η συσκευή και η εφαρμογές ταυτότητας και άλλες πληροφορίες που έχουν συλλεχθεί με την τεχνολογία των cookies. Σημαντικό είναι ότι επισημαίνει, ότι αλλάζοντας τις ρυθμίσεις σε έναν φυλλομετρητή, μπορεί να σταματήσουν να δέχονται cookies ή να ρωτά πριν την αποδοχή ενός cookie. Αυτό έχει ως ενδεχόμενο ορισμένες υπηρεσίες της να μην λειτουργούν σωστά εάν απενεργοποιηθούν τα cookies. Αυτές οι πληροφορίες παρέχονται στις διαφημιστικές εταιρίες που επιτρέπουν να προβάλλουν διαφημίσεις για πράγματα που μπορεί οι χρήστες να έχουν εκδηλώσει ενδιαφέρον.

Σοβαρό σημείο στην πολιτική της εταιρίας είναι ότι ο χρήστης με την εγγραφή του δίνει την συγκατάθεση του, ώστε η εταιρία να μοιράζεται τις ιδιωτικές προσωπικές πληροφορίες με παρόχους υπηρεσιών που υπόκεινται στις υποχρεώσεις τήρησης του απορρήτου σύμφωνα με την παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων και υπό την προϋπόθεση ότι οι τρίτοι χρησιμοποιούν ιδιωτικά τα προσωπικά σας δεδομένα μόνο για λογαριασμό και σύμφωνα με τις οδηγίες της. Τονίζει επίσης ότι μπορεί να αποκαλύψει πληροφορίες και δεδομένα που έχουν ως στόχο να περιορίσουν ενδεχόμενες νομικές άμυνες ή αντιρρήσεις. Ακόμα μπορεί να μεταβιβάσει και να αποκαλύψει πληροφορίες αν τις ζητήσει κάποια κυβέρνηση.

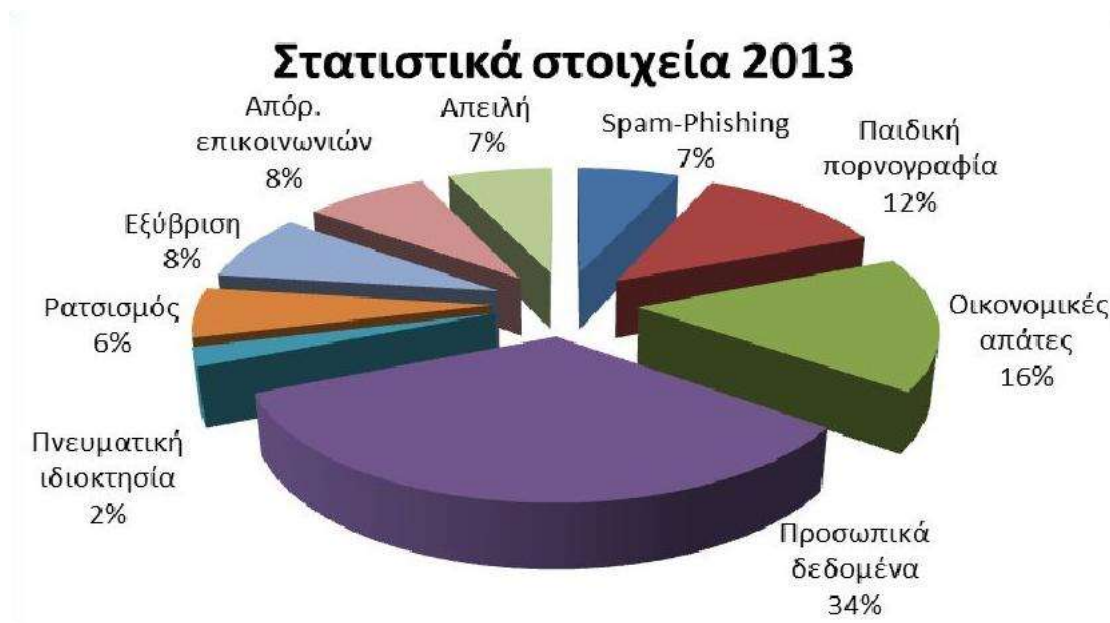
ΕΝΟΤΗΤΑ 4^Η

Κίνδυνοι, Απειλές & Μέτρα Αντιμετώπισης

4.1 Κίνδυνοι και απειλές των ΙΚΔ

Η χρήση των ΙΚΔ μπορεί να προκαλέσει πολλές αρνητικές συνέπειες, καθώς είναι πολύ εύκολο να «παγιδεύσει» τους χρήστες οι οποίοι καταχωρούν τα προσωπικά τους δεδομένα.

Σύμφωνα με στατιστικά στοιχεία της SafeLine⁸ το 2013 έλαβε συνολικά 3094 καταγγελίες, από τις οποίες οι 1551 αφορούσαν το Facebook, αριθμός που αυξήθηκε από το έτος 2012, αφού οι καταγγελίες ανερχόταν στις 845. Ο αριθμός αυτός σχεδόν διπλασιάστηκε, οι κυριότερες καταγγελίες που αφορούσαν το Facebook είχαν να κάνουν με την κλοπή κωδικών πρόσβασης και δημιουργία ψεύτικων προφίλ, παραβίαση προσωπικών δεδομένων, ηλεκτρονικός εκφοβισμός (cyberbullying) και προσέλκυση παιδιών για γενετήσιους λόγους (grooming). Επίσης, αναδημοσιεύεται φωτογραφικό υλικό χρηστών χωρίς την άδεια τους.



Εικόνα 10: Στατιστικά στοιχεία Ελληνικού Κέντρου Ασφαλούς Διαδικτύου, Φεβρουάριος 2014 (πηγή: www.safeline.gr)

⁸ Ελληνική Ανοικτή Γραμμή SafeLine για καταγγελίες παράνομου περιεχομένου που εντοπίζεται στο Διαδίκτυο.

Δηλαδή, φωτογραφίες χρηστών εμφανίζονται σε άλλες σελίδες, αφού πρώτα έχουν κλαπεί από το Facebook, χωρίς την έγκριση ή την άδεια των απεικονισμένων.

Η συλλογή, η επεξεργασία και ο διαμοιρασμός προσωπικών δεδομένων και αρχείων αποτελεί παραβίαση της ιδιωτικής ζωής του ανθρώπου, καθώς επίσης και κίνδυνο για την ατομική του ζωή. Η επεξεργασία και ο διαμοιρασμός των πληροφοριών αυτών, παραβιάζει τα δικαιώματα και τα συμφέροντα των προσώπων. Ελλοχεύει κινδύνους, όπως η παρενόχληση του, γνωστό παράδειγμα είναι το (spamming), όπου αποστέλλονται ηλεκτρονικά ανεπιθύμητα μηνύματα (spam) σε χρήστες, κυρίως για εμπορικούς σκοπούς. Η διαβίβαση προσωπικών δεδομένων για εμπορικούς λόγους παραβιάζει την αυτονομία του πολίτη, καταπατάει την ιδιωτική του ζωή και το δικαίωμα της οικονομικής του αυτοδιάθεσης.

Ένα σημαντικό ζήτημα που συνήθως δεν γνωρίζουν οι χρήστες όταν δημιουργούν ένα ηλεκτρονικό προφίλ σε ένα κοινωνικό δίκτυο είναι ότι αν αποφασίσουν να διαγράψουν το προφίλ τους δεν μπορούν. Υπάρχει η δυνατότητα απενεργοποίησης του προφίλ, το οποίο σημαίνει ότι τα δεδομένα παρόλο που δεν είναι προσβάσιμα υπάρχουν, όμως στους web servers των σελίδων. Ένας σημαντικός κίνδυνος είναι ο διαδικτυακός εκφοβισμός, ο οποίος αποτελεί μια εσκεμμένη, επαναλαμβανόμενη και εχθρική συμπεριφορά απέναντι σε κάποιο άτομο με σκοπό να το απομονώσει ή να το βλάψει. Μπορεί να έχει τη μορφή ενός εκφοβιστικού, ρατσιστικού ή προσβλητικού ηλεκτρονικού μηνύματος, φωτογραφίας ή βίντεο.⁹

Επίσης, μεγάλο κίνδυνο αποτελεί το **Social Networking phishing**, μια μέθοδος που αποσκοπεί στην απόκτηση ευαίσθητων προσωπικών δεδομένων και πληροφοριών. Είναι ένας κίνδυνος που αυξάνεται διαρκώς και έχει «κερδίσει» μεγάλο έδαφος στις Ιστοσελίδες Κοινωνικής Δικτύωσης. Μέσα από προσωπικά μηνύματα καλούν τον χρήστη να «επιβεβαιώσει» το όνομα χρήστη και τον κωδικό πρόσβασής τους λογαριασμούς κοινωνικής δικτύωσης. Έπειτα χρησιμοποιούν τις πληροφορίες αυτές για να στέλνουν ψευδείς μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα που μοιάζουν σαν να είναι από τον εγγεγραμμένο χρήστη για να ζητήσουν χρήματα ή να αποκτήσουν πρόσβαση σε λογαριασμούς άλλων χρηστών. Παρόμοιο κίνδυνο αποτελεί το **Social Networking spam**, οι spammers έχουν μια ποικιλία τρόπων για να διαδώσουν ανεπιθύμητα ηλεκτρονικά μηνύματα. Από τους πιο κλασσικούς είναι η κοινοποίηση ή η αποστολή ενός συνδέσμου(url) μετά από προτροπές όπως "κάντε κλικ εδώ", "δωρεάν" ή "wow", σε ψεύτικους λογαριασμούς ή κοινωνικών bots, ακόμα και σε εφαρμογές που υπόσχονται ειδικά χαρακτηριστικά, όπως αποκαλύπτουν τον αριθμό των χρηστών που έχουν δει το προφίλ σας στο Facebook, αλλά στην πραγματικότητα είναι spam εφαρμογές. Αυτοί οι τρόποι spam γίνονται κυρίως για διαφημιστικούς λόγους.

Το κακόβουλο λογισμικό, είναι ένας ακόμα κίνδυνος που κρύβουν τα μέσα κοινωνικής δικτύωσης. Οι ιστοσελίδες κοινωνικής δικτύωσης συνήθως αποτελούνται

⁹ Ασφάλεια στο Διαδίκτυο, http://www.pi.ac.cy/InternetSafety/sec_facebook.html

από μικρές εφαρμογές "widgets", οι δημιουργοί των οποίων δεν έχουν πάντα επαρκείς πιστοποιήσεις. Σε τέτοια περίπτωση, αυτές οι εφαρμογές ενδέχεται να περιέχουν κακόβουλο λογισμικό.

Τέλος, σοβαρό κίνδυνο στα κοινωνικά δίκτυα αποτελεί η περίπτωση της παρενόχλησης. Οι επιτήδριοι μπορούν να επικοινωνούν με ανυποψίαστους χρήστες μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης. Πολλές από τις εφαρμογές που φιλοξενούν αυτές οι πλατφόρμες ενδέχεται να διευκολύνουν περιστατικά παρενόχλησης. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό για την Ασφαλεία Δικτύων και Πληροφοριών, η απειλή της κλοπής ταυτότητας είναι επίσης ιδιαίτερα σημαντική, αφού ψεύτικα προφίλ δημιουργούνται με σκοπό την προσβολή και τον εξευτελισμό άλλων ατόμων. Ακόμη, δημιουργούνται προφίλ που χρησιμοποιούν ονόματα γνωστών εταιρειών ή προσωπικοτήτων με σκοπό την απόκτηση κέρδους από την εκμετάλλευση της φήμης τους.

4.2 Κίνδυνοι με τα Προσωπικά Δεδομένα

Όλα τα προσωπικά δεδομένα, οι πληροφορίες και τα στοιχεία ενός χρήστη είναι εκτεθειμένα μετά την εγγραφή και την «άδεια» του στα κοινωνικά δίκτυα. Έτσι μπορεί άμεσα να δωθεί πρόσβαση σε οποιονδήποτε να εισβάλει στην ιδιωτική του ζωή, χωρίς όμως να το γνωρίζει ο ίδιος ο χρήστης. Σύμφωνα με τον Ευρωπαϊκό Οργανισμό για την Ασφαλεία Δικτύων και Πληροφοριών, θα πρέπει οι χρήστες να προσέχουν ότι τα προσωπικά δεδομένα και στοιχεία μπορεί να αποθηκευτούν από τρίτους και να αποτελέσουν μέρος ψηφιακών φακέλων προσωπικών δεδομένων. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στα δευτερεύοντα δεδομένα, αφού εκτός των πληροφοριών που αναρτούν οι χρήστες με τη θέλησή τους, τα μέλη τέτοιου είδους ιστοσελίδων αποκαλύπτουν αυτόματα δευτερεύοντα στοιχεία, τα οποία αφορούν τον τρόπο που χρησιμοποιούν τις προσφερόμενες υπηρεσίες. Πολλές πλατφόρμες κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες τους να μαρκάρουν με μεταδεδομένα τις φωτογραφίες τους. Τα μεταδεδομένα μπορούν να είναι σύνδεσμοι σε προφίλ ή διευθύνσεις e-mail. Αυτό ενέχει κινδύνους για ανεπιθύμητη διασύνδεση των φωτογραφιών με προσωπικά δεδομένα.

Επίσης, η αποκάλυψη ευαίσθητων στοιχείων της προσωπικής του ζωής, όπως πολιτικά φρονήματα, θρησκείες, καταγωγή, προβλήματα υγείας, σεξουαλικές προτιμήσεις κ.α μπορεί να οδηγήσουν σε οικονομική, επαγγελματική, ψυχολογική, ακόμα και σε σωματική "κακοποίηση" ενός ατόμου. Παράδειγμα ενός τέτοιου κινδύνου είναι η περίπτωση των εταιριών, που "ψάχνουν" τους εργαζομένους ή καταφεύγουν στην συλλογή πληροφοριών για να ελέγξουν την προσωπικότητα, τις απόψεις και τις κινήσεις τους, παραβιάζοντας την σφαίρα της ιδιωτικής τους ζωής. Μέσα από τις πληροφορίες που σου παρέχουν τα κοινωνικά δίκτυα είναι εύκολο να εισβάλει ένας άγνωστος στην ιδιωτική σου ζωή και να σε εντοπίσει.

4.3 Μέτρα και Νόμοι Αντιμετώπισης κινδύνων

Η κλοπή ταυτότητας ή κωδικών πρόσβασης αποτελεί ένα συχνό πρόβλημα στο Διαδίκτυο και ειδικότερα τώρα, με την ανάπτυξη και την ραγδαία απήχηση των ΙΚΔ. Η πρακτική αυτή έχει ως στόχο τη χρήση της εικονικής ταυτότητας ενός άλλου ατόμου χρησιμοποιώντας, το όνομα χρήσης και τον κωδικό πρόσβασης του σε διάφορες διαδικτυακές υπηρεσίες. Με τον τρόπο αυτό οι επιτήδριοι επιχειρούν την οικονομική εξαπάτηση ή την προσβολή ενός ατόμου στο διαδικτυακό περιβάλλον. Απλοί τρόποι αντιμετώπισης είναι:

- Δημιουργία κωδικών πρόσβασης που δεν είναι εύκολο κανείς να φανταστεί, αποφυγή κωδικών με ημερομηνίες γέννησης κ.α.
- «**Google yourself!**» χρήση μιας μηχανής αναζήτησης ανά τακτά διαστήματα. Αναζήτηση με το όνομά ή το ψευδώνυμο που χρησιμοποιεί ο κάθε χρήστης στο Διαδίκτυο, έτσι ώστε για γίνεται έλεγχος στην εικονική παρουσία του.
- Επικοινωνία με τον πάροχο της υπηρεσίας όπου έχει γίνει η κλοπή ταυτότητας και η ενημέρωση του για το περιστατικό.
- Δημιουργία και αλλαγή e-mail, προφίλ, κωδικών πρόσβασης κλπ.
- Πρέπει να γίνεται αναφορά για περιστατικά στους διαχειριστές της ιστοσελίδας.

Ο ηλεκτρονικός εκφοβισμός (cyberbullying), είναι μια μορφή εκφοβισμού η οποία έχει συνδεθεί με την ανάπτυξη νέων τεχνολογιών και σύγχρονων τρόπων επικοινωνίας (social media). Ο ηλεκτρονικός εκφοβισμός *«αφορά παιδιά και εφήβους, τόσο ως θύματα, όσο και ως θύτες σε βίαιες, επικίνδυνες και απειλητικές ενέργειες στον κυβερνοχώρο. Σε αντίθεση με τον παραδοσιακό εκφοβισμό κατά τον οποίο ο θύτης έρχεται αντιμέτωπος πρόσωπο με πρόσωπο με το θύμα, επιτείνει τη ζημιά στο διαδικτυακό θύμα, λόγω της εικονικής φύσης του κυβερνοχώρου στον κυβερνοχώρο, ο θύτης μπορεί να κρυφτεί πίσω από μία οθόνη για να ταπεινώσει το θύμα και να διαδώσει ανώνυμα προσβλητικό υλικό σε ένα ευρύ κοινό, χωρίς να φοβάται ότι θα ανακαλυφθεί και θα τιμωρηθεί»*.¹⁰

Ο ηλεκτρονικός εκφοβισμός εμφανίζεται με διάφορες μορφές όπως **παρενόχληση, διαδικτυακή καταδίωξη, δυσφήμιση, πλαστοπροσωπία, ανάφλεξη** (αποστολή βίαιων, αγενών και χυδαίων ηλεκτρονικών μηνυμάτων), **εξαπάτηση, αποκλεισμός** (εσκεμμένος αποκλεισμός ενός ατόμου από την ομάδα των φίλων, από δωμάτια συζήτησης ή από διαδικτυακά ομαδικά παιχνίδια) κ.α. Για την ορθή πρόληψη και αντιμετώπιση του θα πρέπει να υπάρχει η απαραίτητη ενημέρωση και εκπαίδευση των παιδιών και των εφήβων, τόσο μέσα στο σχολικό, όσο και στο οικογενειακό περιβάλλον. Ο εκφοβισμός στο Διαδίκτυο θα πρέπει να αντιμετωπιστεί με

¹⁰ Ηλεκτρονικός εκφοβισμός: http://gre.tabby.eu/uploads/1/6/8/6/16865702/booklet_cyp.pdf

εκπαιδευτικά και επικοινωνιακά μέσα, από καταρτισμένους εκπαιδευτικούς και γονείς. Στην Ελλάδα υπάρχει και ανοιχτή γραμμή επικοινωνίας για καταγγελίες τέτοιων προβλημάτων. Η SafeLine δέχεται καταγγελίες για ιστοχώρους που περιέχουν εικόνες κακομεταχείρισης των παιδιών, οπουδήποτε στον κόσμο, ρατσιστικό και ξενοφοβικό περιεχόμενο που παραβαίνει την Ελληνική νομοθεσία ή άλλο παράνομο περιεχόμενο. Επίσης, υπάρχει και το Διεθνές Δίκτυο κατά του Διαδικτυακού Μίσους (INCHACH).

Σύμφωνα με την νομοθεσία το cyber bullying, εντάσσεται στις εγκληματικές πράξεις που μπορεί να βλάψουν τα παιδιά, είτε βλάπτοντας την σωματική, είτε την ψυχική τους υγεία. Στις εγκληματικές πράξεις κατατάσσεται και η προσέλευση παιδιών για γενετήσιους λόγους. Σύμφωνα με νόμο 3064/2002, για πρώτη φορά εισήχθη στον Ελληνικό Ποινικό Κώδικα το άρθρο 348Α, το οποίο αφορούσε στη «διακίνηση παιδικής πορνογραφίας μέσω Διαδικτύου». Επίσης, στους νόμους 3625/2007 και 3666/2008 συμπεριλήφθηκε το έγκλημα του 348Α, στις περιπτώσεις άρσης του απορρήτου των επικοινωνιών. Η προσβολή της γενετήσιας αξιοπρέπειας ποινικοποιείται βάσει του 337 άρθρο του Ποινικού Κώδικα και δυστυχώς λαμβάνει χώρα καθημερινά. Σύμφωνα με όσα ορίζει η διάταξη στην παράγραφο 3 που προστέθηκε με το Ν. 3727/2008: *«Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλου μέσου επικοινωνίας, αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα 15 έτη και, με χειρονομίες ή προτάσεις ασελγείς, προσβάλλει την αξιοπρέπεια του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν η πράξη τελείται κατά συνήθεια ή αν επακολούθησε συνάντηση, ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.»*

Όταν ένας ενήλικος πέραν της επικοινωνίας με κάποιον ανήλικο, προσποιείται επιπλέον τον ανήλικο με σκοπό να τον προσεγγίσει ευκολότερα και να έρθει σε σεξουαλική επαφή μαζί του, τότε γίνεται λόγος για το φαινόμενο «grooming». Παρά το γεγονός ότι δεν υπάρχει ο όρος «grooming» στον ελληνικό ποινικό κώδικα, παρ' όλα αυτά η πράξη αυτή τιμωρείται βάσει του άρθρου 348B Π.Κ., όπως αυτό προστέθηκε με τον νόμο 3727/2008. Κύριο στοιχείο της αντικειμενικής υπόστασης του 348 Π.Κ. είναι ο ενήλικας μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας να αποσκοπεί στην αποπλάνηση του παιδιού (339 Π.Κ.) και στο φυσικό κόσμο.

Το Social Networking phishing, είναι μηνύματα που έχουν ως στόχο να ξεγελάσουν τον χρήστη, έτσι ώστε να απαντήσει στον αποστολέα και να του δώσει κάποια προσωπικά στοιχεία, όπως αριθμούς λογαριασμού, πιστωτικής κάρτας κ.α. Ο κυριότερος τρόπος για να αντιμετωπιστεί το phishing είναι ο χρήστης να είναι υποψιασμένος, καταρτισμένος και πλήρως ενημερωμένος για τις απάτες που συμβαίνουν στο διαδίκτυο, τεχνικά μπορεί να γίνει χρήση λογισμικών περιήγησης που αναγνωρίζουν ιστοτόπους οι οποίοι σου παραπέμπουν παραπλανητικά μηνύματα μέσω διαφορετικού URL, επίσης μπορεί να γίνει χρήση antivirus με safe browsing advisor όπου παρέχονται αξιολογήσεις για κάθε σελίδα που θα αναζητήσει ο χρήστης στο διαδίκτυο και να χρησιμοποιηθούν προγράμματα κατασκοπείας (Anti-spyware). Όπως ακόμα και με την λήψη add-ons για ασφαλέστερη περιήγηση στο διαδίκτυο και τον εντοπισμό phishing script στις ιστοσελίδες. Παρόμοιο κίνδυνο με κοινά στοιχεία αποτελεί και το Social Networking spam, που είναι κυρίως ανεπιθύμητα ηλεκτρονικά μηνύματα. Στην Ελλάδα το spam ρυθμίζεται από τον νόμο 3471/2006, αρ. 11 ο οποίος ενσωμάτωσε με την Οδηγία 2002/58/ΕΚ για την

προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Τα ηλεκτρονικά μηνύματα που αποστέλλονται χωρίς την συγκατάθεση του χρήστη, δηλαδή τα μηνύματα spam, είναι παράνομα. Βέβαια, σύμφωνα με την παρ. 3 του αρ. 11, στην περίπτωση που η ηλεκτρονική διεύθυνση του χρήστη αποκτήθηκε από τον αποστολέα με την συγκατάθεση του, τα μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται με σκοπό την προώθηση προϊόντων ή υπηρεσιών ή για την εξυπηρέτηση παρόμοιων σκοπών. Όμως, τα μηνύματα αυτά που έχουν ως σκοπό την εμπορική προώθηση προϊόντων και υπηρεσιών, θα πρέπει να αναφέρεται η ταυτότητα του αποστολέα ή του προσώπου του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η διεύθυνση στην οποία ο χρήστης που έχει λάβει το μήνυμα να μπορεί να ζητήσει τον τερματισμό της επικοινωνίας. Γενικά, οι χρήστες πρέπει να προστατεύονται έτσι ώστε να μην γίνονται spammer άθελα τους. Θα πρέπει να προστατεύουν την ηλεκτρονική τους διεύθυνση και τον αριθμό του τηλεφώνου τους. Μια απλή λύση είναι η χρήση τεχνικών και λογισμικού φιλτραρίσματος (spyware). Το λογισμικό φιλτραρίσματος επιτρέπει το είδος του περιεχομένου που θα εμφανίζεται σε έναν υπολογιστή, μπορεί επίσης να χρησιμοποιηθεί και για την πλήρη παρεμπόδιση πρόσβασης στο διαδίκτυο. Μπορεί να βελτιώσει την ασφάλεια του και με την βοήθεια λογισμικών anti-spam για προστασία του ηλεκτρονικού ταχυδρομείου.

Στην Ενότητα 5^Η θα αναλύσουμε με εκτενή τρόπο όλο το νομοθετικό πλαίσιο που καλύπτει τους χρήστες και τις «παγίδες» που κρύβονται σε ότι αφορά τα προσωπικά τους δεδομένα. Εδώ θα παρουσιάσουμε κάποια προληπτικά μέτρα που θα πρέπει να ακολουθήσουν οι χρήστες για να προστατεύσουν τα προσωπικά τους δεδομένα. Πρώτον, σημαντικό είναι οι χρήστες να γνωρίζουν και να σκέφτονται που αποκαλύπτουν τα προσωπικά τους δεδομένα. Να διαβάζουν προσεκτικά τα «ψιλά γράμματα» των πολιτικών χρήσης κάθε εταιρίας και να προσέχουν, στο που μπορούν να μεταβιβάσουν τα δεδομένα αυτά απ' τις εκάστοτε εταιρίες. Θα πρέπει να γνωρίζουν που δίνουν την συγκατάθεση τους, κατά πόσο μπορεί να είναι ασφαλή τα δεδομένα και ποίος πρόκειται να τα χρησιμοποιήσει. Αν για παράδειγμα, οι εταιρίες εγκαθιστούν αρχεία cookies ή αν προωθούν τις πληροφορίες σε διαφημιστικές εταιρίες για εμπορικούς σκοπούς. Όπως αναφέραμε και νωρίτερα, η χρήση διαφορετικών συνθηματικών και η συχνή αλλαγή τους βοηθάει στην μεγαλύτερη ασφάλεια. Επίσης, δεν θα πρέπει, να ξεχνάνε να αποσυνδέονται από σελίδες που έχουν συνδεθεί με την χρήση συνθηματικών. Σημαντικό είναι οι χρήστες να κρατάνε τους Η/Υ ασφαλής. Τέτοια μέτρα για προστασία είναι, η χρήση προγραμμάτων τοίχους ασφαλείας (firewall) και προστασίας από ιούς (anti-virus). Το τείχος προστασίας εμποδίζει εισβολείς ή κακόβουλο λογισμικό (όπως ιούς τύπου worm) να αποκτήσουν πρόσβαση στον υπολογιστή μέσω δικτύου ή από το διαδίκτυο. Το τείχος προστασίας εμποδίζει επίσης και τον υπολογιστή, να στείλει λογισμικό κακόβουλης λειτουργίας σε άλλους υπολογιστές, όπως επίσης και τα αντιϊούς. Τα αντιϊικά προγράμματα είναι κυρίαρχη ασπίδα ασφάλειας εφόσον ελέγχουν σε πραγματικό χρόνο τις διεργασίες του υπολογιστή. Γι' αυτό θα πρέπει να είναι πάντα ενημερωμένα και ενεργοποιημένα. Ένα άλλο λογισμικό προστασίας είναι και οι σουίτες ασφαλείας (security suite), με την χρήση των λογισμικών αυτών ο χρήστης μπορεί να έχει μια αποτελεσματική κάλυψη.

Παρακάτω, παρουσιάζονται πίνακες με τις συχνότερες και πιο διαδεδομένες απειλές που παρουσιάζονται στα κοινωνικά δίκτυα. Παρουσιάζονται οι απειλές,

προτείνονται αντίμετρα και γίνεται σαφές, ποιός είναι ο τύπος του αντιμέτρου. Με τον όρο «τύπος αντιμέτρου» νοείται η κατηγορία στην οποία ανήκει το κάθε αντίμετρο. Ο τύπος των αντιμέτρων μπορεί να είναι **Νομικός** (δηλαδή, νομοθετικά πλαίσια, κανονιστικές οδηγίες και προσεγγίσεις), **Οργανωτικός** (συνεχής εκπαίδευση, επιμόρφωση, κατάρτιση και ενημέρωση), **Τεχνικός** (δηλαδή, την προστασία με την βοήθεια προγραμμάτων, εφαρμογών, άλλων λογισμικών κ.α.), **Διαδικαστικός** (τεχνικές, κανονισμούς και μέτρα ασφάλειας που προτείνουν οι ίδιες οι ΙΚΔ για την λειτουργία τους και για την προτασία των χρηστών).

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Διαμοιρασμός προσωπικών δεδομένων	<ul style="list-style-type: none"> • Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης εξέδωσε το 1992, κανονιστική ρύθμιση σύμφωνα με την οποία είναι <u>υποχρέωση</u> κάθε εταιρίας και οργανισμού η <u>διαμόρφωση πολιτικής ασφάλειας</u> με σκοπό την προστασία των πληροφοριών που βρίσκονται υπό την κατοχή της. 	<ul style="list-style-type: none"> • Νομικός
	<ul style="list-style-type: none"> • Ο χρήστης έχει επίσης, μεγάλο μερίδιο ευθύνης. Θα πρέπει να είναι επιφυλακτικός στις σχέσεις που αναπτύσσει με άλλους χρήστες, πόσο περισσότερο ειδικά μ' αυτούς που δεν γνωρίζει. 	<ul style="list-style-type: none"> • Οργανωτικός
	<ul style="list-style-type: none"> • Τα κοινωνικά δίκτυα δίνουν την δυνατότητα στον χρήστη σύμφωνα με την τρέχουσα πολιτική ιδιωτικότητας της κάθε σελίδας, να ρυθμίζει και να ορίζει ποίοι θα έχουν πρόσβαση στις πληροφορίες. 	<ul style="list-style-type: none"> • Οργανωτικός • Διαδικαστικός

Πίνακας 1: Διαμοιρασμός προσωπικών δεδομένων

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Social Networking Phishing	<ul style="list-style-type: none"> • Λήψη add-ons για ασφαλέστερη περιήγηση στο διαδίκτυο και τον εντοπισμό phishing script στις ιστοσελίδες. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Χρήση antivirus με safe browsing advisor. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Χρήση προγραμμάτων κατασκοπείας (Anti-spyware), χρήση anti-virus και εφαρμογών είναι οι καλύτερες άμυνες ενάντια στους ιούς, malware και σε άλλες ηλεκτρονικές απειλές. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Ανανέωση (Update) των φυλλομετρητών (web browsers). 	<ul style="list-style-type: none"> • Τεχνικός • Οργανωτικός
	<ul style="list-style-type: none"> • Αποφυγή εισαγωγής προσωπικών στοιχείων σε pop-up παράθυρα, όπως επίσης και να αγνοούνται μηνύματα όπου ζητείται να γίνει "κλικ" σε έναν σύνδεσμο. 	<ul style="list-style-type: none"> • Οργανωτικός
	<ul style="list-style-type: none"> • Προσοχή στο URL των ιστοσελίδων. Κακόβουλες σελίδες μπορεί να χρησιμοποιούν μια παραλλαγή στην ορθογραφία ή ένα διαφορετικό τομέα (π.χ., .com έναντι .net) στο URL. 	<ul style="list-style-type: none"> • Οργανωτικός

Πίνακας 2: Social Networking Phishing

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Social Networking Spam	<ul style="list-style-type: none"> • Το spam ρυθμίζεται από το αρ. 11 του ν. 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/EK για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. 	<ul style="list-style-type: none"> • Νομικός
	<ul style="list-style-type: none"> • Χρήση antivirus με safe browsing advisor. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Χρήση προγραμμάτων κατασκοπείας (Anti-spyware), χρήση anti-virus και εφαρμογών είναι οι καλύτερες άμυνες ενάντια στους ιούς, malware και σε άλλες ηλεκτρονικές απειλές. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Προσοχή στο URL των ιστοσελίδων. Κακόβουλες σελίδες μπορεί να χρησιμοποιούν μια παραλλαγή στην ορθογραφία ή ένα διαφορετικό τομέα (π.χ., .com έναντι .net) στο URL. 	<ul style="list-style-type: none"> • Οργανωτικός

Πίνακας 3: Social Networking Spam

Απειλή	Αντίμετρα	Τύπος Αντιμέτρων
Cyberbullying (Ηλεκτρονικός εκφοβισμός)	<ul style="list-style-type: none"> • Σε περίπτωση ηλεκτρονικού εκφοβισμού οι χρήστες καλό θα είναι να απενεργοποιούν και να δημιουργούν νέο λογαριασμό, με νέο ηλεκτρονικό ταχυδρομείο. Καθώς επίσης και να ενημερώνουν τις αρμόδιες αρχές. Με αποδεικτικά στοιχεία της δράσης όπως ημερομηνίες και ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου κ.α. 	<ul style="list-style-type: none"> • Οργανωτικός • Νομικός
	<ul style="list-style-type: none"> • Οι χρήστες καλό θα είναι να διατηρούν τις προσωπικές πληροφορίες ιδιωτικές (διευθύνσεις, φωτογραφίες, διευθύνσεις ηλεκτρονικού ταχυδρομείου, σταθερά ή κινητά τηλέφωνα, ονόματα σχολείων, τοπός διαμονής, πληροφορίες για την οικογένεια και τους φίλους κωδικούς πρόσβασης κ.α). Με τον τρόπο αυτό, οι κακόβουλοι χρήστες δεν έχουν πρόσβαση στις πληροφορίες αυτές, άρα δεν είναι και σε θέση να κάνουν κατάχρηση. 	<ul style="list-style-type: none"> • Οργανωτικός
	<ul style="list-style-type: none"> • Χρήση του netiquette (Network Etiquette), δηλαδή κανόνες σωστής συμπεριφορά στο διαδίκτυο. Θα πρέπει μέσα από το οικογενειακό και το σχολικό περιβάλλον να ενημερωθούν οι έφηβοι χρήστες σχετικά με την υπεύθυνη συμπεριφορά. Να τους ενημερώσουν επίσης, ότι ένα μήνυμα που αποστέλλεται ή ένα σχόλιο που δημοσιεύεται σε κάποιο κοινωνικό δίκτυο είναι δύσκολο να μπορέσουν να το πάρουν πίσω. 	<ul style="list-style-type: none"> • Οργανωτικός
	<ul style="list-style-type: none"> • Σύμφωνα με την νομοθεσία το cyber bullying, εντάσσεται στις εγκληματικές πράξεις που μπορεί να βλάψουν τα παιδιά, είτε βλάπτοντας την σωματική, είτε την ψυχική τους υγεία. Αν και δεν υπάρχει συγκεκριμένο ποινικό αδίκημα που ονομάζεται ηλεκτρονική παρενόχληση, οι δραστηριότητες μπορεί να είναι ποινικά αδικήματα βάσει του Ν. 3727/2008. 	<ul style="list-style-type: none"> • Νομικός

Πίνακας 4: Cyberbullying (Ηλεκτρονικός εκφοβισμός)

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Παραβίαση προσωπικών δεδομένων	<ul style="list-style-type: none"> • Πριν από την αποστολή ή καταχώρηση ευαίσθητων πληροφοριών οι χρήστες θα πρέπει να ελέγχουν την ασφάλεια της ιστοσελίδας. 	<ul style="list-style-type: none"> • Οργανωτικός
	<ul style="list-style-type: none"> • Ο χρήστης μπορεί να ασφαλίσει τους λογαριασμούς του. Αν ζητήσει προστασία πέρα από τους κωδικούς πρόσβασης. Πολλοί πάροχοι προσφέρουν τώρα πρόσθετους τρόπους, για να μπορούν να ελέγχουν πριν ασκήσουν τις δραστηριότητές τους σε εκείνη την περιοχή. 	<ul style="list-style-type: none"> • Οργανωτικός • Διαδικαστικός
	<ul style="list-style-type: none"> • Αδύναμα συνθηματικά, ελλιπή μέτρα προστασίας (firewalls, antivirus κ.τ.λ.) καθιστούν το χρήστη ευάλωτο σε κακόβουλο λογισμικό (keyloggers , Trojans, sniffers), σε αυτοματοποιημένες επιθέσεις (dictionary , brute force attacks κ.α.), αλλά και σε άλλες μορφές επιθέσης όπως session hijacking, phishing, social engineering κ.α. 	<ul style="list-style-type: none"> • Τεχνικός • Οργανωτικός

Πίνακας 5: Παραβίαση προσωπικών δεδομένων

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Grooming (προσέλκυση παιδιών για γενετήσιους λόγους)	<ul style="list-style-type: none"> • Οι γονείς πρέπει να κατανοήσουν όρους, όπως POS (parents over shoulder) “γονείς πάνω από τον ώμο” και LMIRL (let’s meet in real life) “ας ανταποκριθούμε στην πραγματική ζωή”. Θα πρέπει να μάθουν να αναγνωρίζουν τα πρώτα προειδοποιητικά σημάδια. Παράδειγμα αποτελεί έρευνα, που έδειξε ότι το λιγότερο από το 30% των γονέων θα μπορούσε να αποκωδικοποιήσει την στενογραφία που χρησιμοποιούν τα παιδιά και οι έφηβοι σε chat rooms και στα κοινωνικά δίκτυα. 	<ul style="list-style-type: none"> • Οργανωτικό ς
	<ul style="list-style-type: none"> • Χρήση συστημάτων φιλτραρίσματος και εργαλείων γονικού ελέγχου. Προγράμματα που μπορούν να εγκατασταθούν στον υπολογιστή του χρήστη και να καταγράψουν λεπτομερώς τις κινήσεις ενός χρήστη στο Διαδίκτυο. Μπορούν επίσης, να μπλοκάρουν ύποπτους ιστοχώρους, να επιτρέπουν την πρόσβαση συγκεκριμένες ώρες και ημέρες, ακόμα και να απενεργοποιήσουν τελείως τον υπολογιστή. 	<ul style="list-style-type: none"> • Τεχνικός
	<ul style="list-style-type: none"> • Η προσβολή της γενετήσιας αξιοπρέπειας ποινικοποιείται. Παρά το γεγονός ότι δεν υπάρχει ο όρος «grooming» στον ελληνικό ποινικό κώδικα, παρ’ όλα αυτά η πράξη αυτή τιμωρείται βάσει του άρθρου 348B Π.Κ., όπως αυτό προστέθηκε με τον νόμο 3727/2008. Κύριο στοιχείο της αντικειμενικής υπόστασης του 348 Π.Κ. είναι ο ενήλικας μέσω της τεχνολογίας πληροφόρησης και επικοινωνίας να αποσκοπεί στην αποπλάνηση του παιδιού (339 Π.Κ.) και στο φυσικό κόσμο. 	<ul style="list-style-type: none"> • Νομικός

Πίνακας 6: *Grooming (προσέλκυση παιδιών για γενετήσιους λόγους)*

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Οικονομικές απάτες	<ul style="list-style-type: none"> Οι χρήστες δεν θα πρέπει να αποκαλύπτουν προσωπικά ή οικονομικά στοιχεία σε μηνύματα στα κοινωνικά δίκτυα ή στο ηλεκτρονικό ταχυδρομίο. 	<ul style="list-style-type: none"> Οργανωτικός
	<ul style="list-style-type: none"> Σκεφτείτε πριν ενεργήσετε. Οι χρήστες θα πρέπει να είναι επιφυλακτικοί με τις επικοινωνίες που τον “εκλιπαρούν” να δράσει άμεσα, γιατί σχεδόν πάντα προσφέρεται κάτι που ακούγεται «πολύ καλό για να είναι αληθινό» ή ζητά προσωπικές πληροφορίες. 	<ul style="list-style-type: none"> Οργανωτικός
	<ul style="list-style-type: none"> Εγκατάσταση φίλτρων (πακέτα λογισμικού) με τα οποία μπορεί να αποκλειστεί η προσπέλαση σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο 	<ul style="list-style-type: none"> Τεχνικός

Πίνακας 7: Οικονομικές απάτες

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Κλοπή κωδικών	<ul style="list-style-type: none"> Ασφαλίστε τους λογαριασμούς σας. Πολλές ιστοσελίδες δημιουργούν κωδικούς πρόσβασης μεγάλους και ισχυρούς. Ο συνδυασμός κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων για να δημιουργηθεί ένας πιο ασφαλής κωδικός πρόσβασης. 	<ul style="list-style-type: none"> Οργανωτικός
	<ul style="list-style-type: none"> Ξεχωριστοί, μοναδικοί κωδικοί πρόσβασης για κάθε λογαριασμό. 	<ul style="list-style-type: none"> Οργανωτικός
	<ul style="list-style-type: none"> Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης εξέδωσε το 1992, κανονιστική ρύθμιση σύμφωνα με την οποία είναι <u>υποχρέωση</u> κάθε εταιρίας και οργανισμού η <u>διαμόρφωση πολιτικής ασφάλειας</u> με σκοπό την προστασία των πληροφοριών που βρίσκονται υπό την κατοχή της. 	<ul style="list-style-type: none"> Νομικός

Πίνακας 8: Κλοπή κωδικών

Απειλή	Αντίμετρα	Τύπος αντιμέτρων
Πλαστοπροσωπία	<ul style="list-style-type: none"> • Το Twitter το 2008 και στην συνέχεια το GooglePlus δημιούργησαν ένα μηχανισμό επαλήθευσης. Είναι ένα «σήμα γνησιότητας» για να αντιμετωπίζονται τα ψεύτικα προφίλ. Στην αρχή ξεκίνησε δοκιμαστικά, αλλά όταν έγιναν προσπάθειες για μαζικότερη επέκταση σε όλους τους χρήστες δημιουργήθηκαν προβλήματα. Η χρήση του «σήματος» έχει παραμείνει για ένα μικρό αριθμό χρηστών, κυρίως επωνύμων. Το 2013 και το Facebook χρησιμοποίησε το σήμα για διασημότητες, δημοσιογράφους, κυβερνητικούς αξιωματούχους και για δημοφιλείς μάρκες και επιχειρήσεις. 	<ul style="list-style-type: none"> • Διαδικαστικός

Πίνακας 9: Πλαστοπροσωπία

Στους πίνακες καταγράφονται οι συχνότεροι κίνδυνοι που εμφανίζονται στα κοινωνικά δίκτυα. Γίνεται σαφές, ότι ο χρήστης είναι ευάλωτος και γίνεται στόχος επιθέσεων που σκοπό έχουν τον περιορισμό της ιδιωτικότητάς του, την οικονομική εκμετάλλευσή του, την αποπλάνησή του κ.α. Για την σωστή αντιμετώπιση των περισσότερων απειλών βασικό ρόλο παίζει η ενημέρωση και η γνώση που θα πρέπει να έχει ένας χρήστης. Όπως φαίνεται και στους παραπάνω πίνακες, συχνότερος τύπος αντιμέτρων είναι ο Οργανωτικός. Αυτός ο τύπος αφορά θέματα σχετικά με τις γνώσεις και την απαραίτητη επιμόρφωση που απαιτείται να έχει ένας χρήστης για την ομαλή και χωρίς κίνδυνο πλοήγηση του στο διαδίκτυο, ειδικότερα τους χρήστες που συμμετέχουν σε κάποια Σελίδα Κοινωνικής Δικτύωσης. Μην παραλείψουμε να αναφέρουμε, ότι σημαντικό ρόλο παίζουν επίσης και οι τεχνικές γνώσεις που έχει ο κάθε χρήστης σε σχέση με τους Η/Υ. Βέβαια και οι τεχνικές γνώσεις, έχουν να κάνουν με την εκπαίδευση που έχει λάβει ο κάθε χρήστης, έτσι ώστε να είναι σε θέση να χρησιμοποιεί τα κατάλληλα μέσα και προγράμματα.



ΕΝΟΤΗΤΑ 5^Η

Νομοθεσίες και Πολιτικές Προστασίας

5.1 Ορισμοί

Οι ιστοσελίδες κοινωνικής δικτύωσης συλλέγουν και επεξεργάζονται προσωπικά δεδομένα. *Προσωπικά δεδομένα* είναι οι πληροφορίες που αναφέρονται και περιγράφουν ένα άτομο, όπως τα στοιχεία αναγνώρισης, τα φυσικά χαρακτηριστικά, η εκπαίδευση, η εργασία, τα ενδιαφέροντα και οι συνήθειες. Το άτομο στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων. Τα *κοινωνικά δίκτυα* ορίζονται στο άρθρο 1, παράγραφος 2, της κοινοτικής Οδηγίας 98/34/ΕΚ ως υπηρεσίες της κοινωνίας της πληροφορίας. Οι υπηρεσίες αυτές θα πρέπει να σέβονται τα δικαιώματα των χρηστών και να λειτουργούν σύμφωνα, με τις ευρωπαϊκές και εθνικές νομοθεσίες για την ιδιωτική ζωή και την προστασία των προσωπικών δεδομένων.

Η *ιδιωτικότητα* αποτελείται και έχει εμπλουτιστεί με δικαιώματα, “όπως το δικαίωμα σε ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο (ή άσυλο της κατοικίας), η ελαχιστοποίηση των παρεμβάσεων, η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς.”¹¹

Η συλλογή και επεξεργασία προσωπικών δεδομένων επέφερε θετικά αποτελέσματα στην ανάπτυξη κάποιων επιστημών, η ανεξέλεγκτη όμως και χωρίς όρια χρήση αυτών, μπορεί να προκαλέσει τα αντίθετα αποτελέσματα και να κρύψει πολλούς κινδύνους. Η χρήση προσωπικών δεδομένων, κυρίως στο διαδίκτυο δομείται συνήθως από μια κενή περιεχομένου διαδικασία συγκατάθεσης. Πρόκειται για το φαινόμενο “just click submit”, στο οποίο οι χρήστες σπάνια θα διαβάσουν ένα “privacy statement” πριν πατήσουν το πλήκτρο για την είσοδο στη ιστοσελίδα.^[4] Έτσι ο χρήστης χωρίς να ελέγχει, αποδέχεται όρους που αφορούν τα προσωπικά δεδομένα με αποτέλεσμα να εξουσιοδοτεί και να μεταβιβάζει πληροφορίες που έπειτα, να μην μπορεί να ελέγξει την χρήση και μεταβίβαση τους. Διαμορφώνεται λοιπόν, ένα δίκαιο προστασίας δεδομένων που αποτελείται από ένα σύνολο όρων, κανόνων, προϋποθέσεων, απαγορεύσεων σε σχέση με την συλλογή, κατοχή και επεξεργασία προσωπικών δεδομένων, καθώς επίσης και τα νομικά και θεσμικά πλαίσια, τις εγγυήσεις και τους περιορισμούς των δικαιωμάτων προστασίας των προσωπικών δεδομένων.

¹¹ Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου, Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας

Απόρρητη, θεωρείται μια πληροφορία που βρίσκεται σε κατάσταση περιορισμένης προσβασιμότητας και αποκλείει σε τρίτους την γνώση, την χρήση και την αξιοποίηση τους. Εξαιρείται, η περίπτωση που εμπίπτει κάποιος νομικός λόγος για την άρση του απορρήτου.

Διαμορφώθηκε ένα κανονιστικό πλαίσιο, με το οποίο σύμφωνα με το άρθρο 16 της Οδηγίας 95/46/EK για την προστασία των προσωπικών δεδομένων, ορίζει μια ρύθμιση για το απόρρητο σύμφωνα με την οποία, όποιος επεξεργάζεται δεδομένα το πράττει μόνο κατ' εντολή του υπεύθυνου επεξεργασίας. Ως υπεύθυνος επεξεργασίας, νοείται εκείνους που καθορίζει τους στόχους και τον τρόπο επεξεργασίας των προσωπικών δεδομένων. Είτε φυσικό, είτε νομικό πρόσωπο, δημοσίου ή ιδιωτικού δικαίου. Στην Ελλάδα σύμφωνα με το άρθρο 10, παράγραφος 1 του ν. 2472/97 προσδιορίζεται επίσης, ότι συνολικά η επεξεργασία προσωπικών δεδομένων θεωρείται απόρρητη.

5.2 Κανονιστικές προσεγγίσεις

Η συνεχής τεχνολογική εξέλιξη, η συνεχής αύξηση του αριθμού και ανάπτυξη των ΙΚΔ κατέστησε αναγκαία, την λήψη μέτρων για την αντιμετώπιση των κινδύνων και την διασφάλιση της προστασίας του ατόμου. Βέβαια η αντιμετώπιση αυτή δεν είναι ίδια σε όλες τις έννομες τάξεις, καθώς εκτός της Ευρώπης, λίγες μόνο χώρες έχουν εισάγει δεσμευτικούς κανόνες στην προστασία προσωπικών δεδομένων.

5.2.1 Ευρωπαϊκή νομοθεσία

Στην Ευρώπη καταγράφονται οι πρώτες κανονιστικές ρυθμίσεις για την προστασία των προσωπικών δεδομένων, τόσο σε εθνικό όσο και σε υπερεθνικό επίπεδο. Σύμφωνα με την **Σύμβαση της Ρώμης**, η οποία υπογράφηκε στις 4 Νοεμβρίου το 1950, στο άρθρο 8 διατυπώθηκε η ανάγκη για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Συγκεκριμένα, θεσπίστηκε το δικαίωμα κάθε προσώπου να γίνεται σεβαστή η οικογενειακή και ιδιωτική του ζωή, καθώς επίσης και η κατοικία και η αλληλογραφία του. Μέτρο απαραίτητο και αναγκαίο, για την εθνική και δημόσια ασφάλεια μιας χώρας, την οικονομική ευημερία, την προάσπιση της τάξης ή για την προστασία των δικαιωμάτων και των ελευθεριών τρίτων προσώπων. Στην κοινοτική Οδηγία **95/46/EK** θεσπίστηκαν βασικές αρχές επεξεργασίας των προσωπικών δεδομένων. Η Οδηγία αυτή υπερασπίστηκε, την προστασία των φυσικών προσώπων από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελεύθερη κυκλοφορία των δεδομένων αυτών, εισάγωντας ειδικές υπεχρεώσεις σχετικά με την ασφάλεια των προσωπικών δεδομένων. Αξιοσημείωτο είναι επίσης, ότι καταχωρήθηκαν τα δικαιώματα των προσώπων (ενημέρωση, πρόσβαση, αντίταξη). Η Οδηγία 95/46/EK θεσπίστηκε στις 24 Οκτωβρίου 1995 και αποτέλεσε κείμενο αναφοράς σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα. Η Οδηγία αυτή, εφαρμόζεται στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας με αυτοματοποιημένες διαδικασίες καθώς και στη μη

αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

Στην συνέχεια συμπληρώθηκε από την Οδηγία **97/66/ΕΚ**, στην οποία θεσπίστηκε η προστασία του ατόμου έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον επικοινωνιακό τομέα. Αργότερα όμως αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ για να προασπίσει θέματα, όπως είναι η φύση των διαδικτυακών διευθύνσεων (IP addresses) και η συνεπακόλουθη νομική αντιμετώπισή τους. Οι κανονιστικές ρυθμίσεις που θεσπίστηκαν από την Ευρωπαϊκή Ένωση και αφορούσαν το κομμάτι των προσωπικών δεδομένων χαρακτηρίστηκαν από έλλειψη συνοχής και ολιστικής αντίληψης. Γι' αυτό το 2004 θεσπίστηκε το «**Πρόγραμμα της Χάγης για την ενδυνάμωση της ελευθερίας, της ασφάλειας και της δικαιοσύνης στην ΕΕ**». Στο πρόγραμμα αυτό εντάσσεται το πλαίσιο ώστε, να επιτρέπεται η ανταλλαγή δεδομένων στις χώρες της Ευρώπης μέσα σε ένα πεδίο αστυνομικής και δικαστικής συνεργασίας.

Το Μάρτιο του 2008, η Διεθνής Ομάδα για την Προστασία των Προσωπικών Δεδομένων στις Τηλεπικοινωνίες (IWGDPT) εξέδωσε ένα έγγραφο συστάσεων για τις υπηρεσίες κοινωνικής δικτύωσης, στο οποίο συμμετείχε ενεργώς και η ελληνική Αρχή. Στις 12 Ιουνίου του 2009 εγκρίθηκε η ομάδα εργασίας του άρθρου 29, η οποία είχε συσταθεί με την Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24^{ης} Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

5.2.2 Ελληνική νομοθεσία

Η Ελλάδα είναι από τις πρώτες χώρες της Ευρωπαϊκής Ένωσης, που μετέφερε την κοινοτική Οδηγία για την προστασία των προσωπικών δεδομένων και την εναρμόνισε στο εσωτερικό της δίκαιο. Στο άρθρο 9 Α' του νόμου 2472/97 (ΦΕΚ Α' 50/10.04.19970) του Συντάγματος, συγκροτείται το συνταγματικό δικαίωμα προστασίας προσωπικών δεδομένων, για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Έπειτα συμπεριλήφθηκε και η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, από τροποποιήσεις που έγιναν στο νόμο και σύμφωνα, με το νόμο 3471/06 (ΦΕΚ Α' 133/28.06.2006). Στο νέο άρθρο 9 Α' του Συντάγματος το 2001, κρίθηκε αναγκαίο να οριστεί ότι, καθένας έχει δικαίωμα προστασίας, από τη συλλογή, την επεξεργασία και τη χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ορίζει ο νόμος». Η διασφάλιση της προστασίας ανατίθεται σε μια ανεξάρτητη αρχή, η οποία συγκροτείται και λειτουργεί, σύμφωνα με τους νόμους. Στον νόμο 2472/97, θεωρείται ότι τα δεδομένα, τα οποία υπόκεινται σε επεξεργασία, πρέπει να είναι προσωπικού χαρακτήρα. Στο άρθρο 2 Α', α' και γ', ως δεδομένα προσωπικού χαρακτήρα, θεωρείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Ως υποκείμενο των δεδομένων, θεωρείται, «το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων

συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική». ¹²

Η Οδηγία 97/66/EK στόχευε στην διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής, όπως επίσης και στην ελεύθερη κυκλοφορία των δεδομένων αυτών, καθώς και στην ανάπτυξη των τηλεπικοινωνιών.

5.2.3 Διεθνής νομοθεσία

Η απόφαση της 2450/19.12.1968 που αφορούσε τους κινδύνους των τεχνολογικών εξελίξεων ως προς τα ανθρώπινα δικαιώματα ήταν από τα πρώτα κείμενα της Γενικής Συνέλευσης των Ηνωμένων Εθνών. Έπειτα ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), εξέδωσε τις λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων». ¹³

Όμως το πλαίσιο γενικών αρχών στερούνταν δεσμετικού χαρακτήρα, για τον λόγο αυτό συγκέντρωσε την συναίνεση χωρών που στερούνταν συνολικής νομοθεσίας για την προστασία προσωπικών δεδομένων, όπως η ΗΠΑ. Η συνεχής εξέλιξη και η αυξανόμενη διασυνοριακή ροή προσωπικών δεδομένων, οδήγησαν στην υιοθέτηση ορισμένων κανόνων και διαδικασιών για την ευχερή και νόμιμη ροή των δεδομένων αυτών.

Σε αντίθεση, η Ευρώπη με την Οδηγία 95/46/EK , άρθρο 25, απαιτεί σε ικανοποιητικά επίπεδα την προστασία των προσωπικών δεδομένων, για την διαβίβαση των δεδομένων σε μια Τρίτη χώρα και δημιουργεί ένα αίσθημα ασφάλειας στους χρήστες. Επίσης, παρουσιάζεται αύξηση των εθνικών νόμων, αλλά και η ανάπτυξη περιφερειακών πρωτοβουλιών, όπως αυτή στις χώρες του APEC (Asia-Pacific Economic Cooperation) για τη χρήση και διασυνοριακή ροή προσωπικών πληροφοριών ή το έτος 2007, την ιβηρο-νοτιοαμερικανική πρωτοβουλία εκπόνησης κατευθυντήριων αρχών προστασίας προσωπικών δεδομένων.

¹² Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ν. 2472/1997 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού με ενσωματωμένες τροποποιήσεις.

¹³ Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου, Κωνσταντίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκρίτζαλης, Σωκράτης Κάτσικας

5.3 Πολιτικές Προστασίας Προσωπικών Δεδομένων

5.3.1 Η Πολιτική της Ευρώπης

Οι ιστοσελίδες Κοινωνικής Δικτύωσης αποτελούν πλέον την πιο διαδεδομένη μορφή επικοινωνίας. Παρέχουν στους χρήστες την δυνατότητα να μοιράζονται και να δημοσιοποιούν διάφορες πληροφορίες για τον εαυτό τους και την προσωπικότητά τους. Αυτό καθιστά δύσκολη την απόκρυψη, τη μη συλλογή και τη μη επεξεργασία προσωπικών στοιχείων και δεδομένων. Στις 04/11/2010 πάρθηκαν αποφάσεις από την ΕΕ έτσι ώστε, να μπορούν οι καταναλωτές να ελέγχουν καλύτερα πώς συλλέγονται και χρησιμοποιούνται τα προσωπικά τους στοιχεία. Αυτή η νέα στρατηγική για την προστασία των προσωπικών δεδομένων, είχε σκοπό να διασφαλίσει ότι όλοι οι χρήστες θα γνωρίζουν πώς χρησιμοποιούνται τα στοιχεία που εμπιστεύονται σε εταιρείες, δημόσιες αρχές και ιστοσελίδες κοινωνικής δικτύωσης. Επίσης, σκοπό είχε να διαμορφώσει μια κοινή προσέγγιση σε όλη την ΕΕ, αφού οι μέχρι τότε κανόνες και νόμοι δεν εφαρμοζόταν με τον ίδιο τρόπο από όλες τις χώρες, καθώς δεν ήταν σαφές κάθε φορά ποιος νόμος ισχύει και σε ποια περίπτωση. Εισήγαγε και την έννοια του "δικαιώματος διαγραφής από τη μνήμη", δηλαδή του δικαιώματος καθενός να ζητά την πλήρη διαγραφή των δεδομένων του αμέσως μετά την εξυπηρέτηση του αρχικού σκοπού αποστολής τους.¹⁴

Η Ευρωπαϊκή Επιτροπή, στις 25/01/2012 στις Βρυξέλλες είχε προτείνει τη σφαιρική μεταρρύθμιση των κανόνων του 1995 περί προστασίας δεδομένων της ΕΕ, με στόχο την ενίσχυση των επιγραμμικών δικαιωμάτων στην ιδιωτικότητα και την ενδυνάμωση της ψηφιακής οικονομίας της Ευρώπης.

Η Επιτροπή είχε προτείνει να επικαιροποιηθούν και να εκσυγχρονιστούν οι αρχές οι οποίες διατυπώνονταν στην οδηγία περί προστασίας δεδομένων του 1995, έτσι ώστε να κατοχυρώνονταν μελλοντικώς τα δικαιώματα στην ιδιωτικότητα. Συγκεκριμένα, η αντιπρόεδρος της επιτροπής για θέματα δικαιοσύνης στην ΕΕ, είχε δηλώσει ότι: «Πριν από 17 έτη, το ποσοστό των Ευρωπαίων που χρησιμοποιούσαν το διαδίκτυο δεν ξεπερνούσε το 1%. Σήμερα, τεράστιοι όγκοι προσωπικών δεδομένων διαβιβάζονται και ανταλλάσσονται από χώρα σε χώρα και από τη μία ήπειρο στην άλλη μέσα σε κλάσματα δευτερολέπτου. Η προστασία των προσωπικών δεδομένων αποτελεί θεμελιώδες δικαίωμα όλων των Ευρωπαίων, πλην όμως οι πολίτες δεν είναι πάντα βέβαιοι για το αν ασκούν πλήρη έλεγχο επί των προσωπικών τους δεδομένων. Οι προτάσεις μου θα συμβάλουν στην οικοδόμηση εμπιστοσύνης στις επιγραμμικές υπηρεσίες, καθώς οι πολίτες θα είναι καλύτερα ενημερωμένοι σχετικά με τα δικαιώματά τους και θα ασκούν μεγαλύτερο έλεγχο επί των πληροφοριών που τους αφορούν».

¹⁴ Ευρωπαϊκή Επιτροπή, Μέτρα προστασίας της ιδιωτικής ζωής στην ψηφιακή εποχή, http://ec.europa.eu/news/justice/101105_el.htm

Οι χρήστες του διαδικτύου έχουν αυξηθεί με ταχύτατους ρυθμούς τα τελευταία χρόνια. Ειδικότερα οι χρήστες που έχουν εγγραφεί στα κοινωνικά δίκτυα και πλέον αποτελούν αναπόσπαστο κομμάτι στην προσωπική τους ζωή. Η χρήση των κοινωνικών δικτύων μειώνει την ιδιωτικότητα στο διαδίκτυο και ιδιαίτερα όταν η χρήση τους συνεπάγεται από έλλειψη ενημέρωσης και γνώσης εγκυμονεί πολλούς κινδύνους. Οι χρήστες θα πρέπει να ενημερώνονται και να ακολουθούν μια σειρά από μέτρα τα οποία θα τους προστατεύουν. Στις αρχές Νοεμβρίου του 2011 ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) της Ε.Ε δημοσίευσε μια έκθεση σχετικά με την κυβερνο-παρενόχληση και την αθέμιτη προσέγγιση των παιδιών μέσω του διαδικτύου καθώς και 18 συστάσεις για προστασία από τους βασικούς κινδύνους. Προτείνει για την ασφαλή χρήση των σελίδων κοινωνικών δικτύων, βασικές συστάσεις όπως:

- *Ενίσχυση των αρχών επιβολής του νόμου των Κρατών Μελών: οι πρόσθετες γνώσεις και οι πόροι είναι σημαντικοί. Αυτή η επιπλέον ενίσχυση χρειάζεται για τη σωστή κάλυψη των κανονιστικών θεμάτων, της συλλογής στατιστικών στοιχείων για περιπτώσεις κατάχρησης, και της παρακολούθησης των παραβιάσεων της ιδιωτικής ζωής.*
- *Η κοινωνία των πολιτών και οι κοινωνικοί εταίροι χρειάζονται πηγές γνώσης σχετικά με τη χρήση του διαδικτύου και τις ηλεκτρονικές υπηρεσίες. Επιπλέον, θα πρέπει να πραγματοποιηθούν στα κοινωνικά δίκτυα χορηγούμενες ηλεκτρονικές εκστρατείες για την πρόληψη της κυβερνο-παρενόχλησης/αθέμιτης προσέγγισης.*
- *Συμβουλές για ασφαλή και με σωστό έλεγχο χρήση των σελίδων κοινωνικής δικτύωσης.*
- *Οι γονείς/κηδεμόνες/εκπαιδευτές χρειάζονται καλύτερες τεχνολογικές δεξιότητες για να καλύψουν το κενό γνώσεων μεταξύ των ενήλικων και των εφήβων.*

5.3.2 Πολιτική για την προστασία των παιδιών και μέτρα στην εκπαίδευση

Το διαδίκτυο παίζει σημαντικό ρόλο και την ζωή των παιδιών και έχει γίνει μέρος της καθημερινότητάς τους. Όλα τα παιδιά πλέον ασχολούνται με το διαδίκτυο, κυρίως στον χώρο της εκπαίδευσης και με την ένταξή τους στα κοινωνικά δίκτυα από πολύ μικρή ηλικία. Θα πρέπει οι νέοι να ενημερωθούν για τους κινδύνους που εγκυμονεί το διαδίκτυο και το κατά πόσο μπορεί να τους βλάψει η κακή και λανθασμένη χρήση του. Ο Ευρωπαϊκός Οργανισμός (ENISA) τόνισε κάποια μέτρα για τους ανήλικους που χρησιμοποιούν το διαδίκτυο όπως:

- *Τη χρήση εξειδικευμένων ρυθμίσεων ασφαλείας εφήβων, και την προσαρμογή των υφιστάμενων στις ανάγκες των εφήβων*
- *Την εκτίμηση των επιπτώσεων στην προστασία των προσωπικών δεδομένων για τις εφαρμογές που επεξεργάζονται τα στοιχεία των εφήβων*
- *Την ανάπτυξη μηχανισμών που θα επιτρέπουν την απενεργοποίηση όλων των ενεργών (ηλεκτρονικών) τμημάτων*

- *Μηχανισμούς ελέγχου πρόσβασης βάσει ηλικίας*

Σε προηγούμενη ενότητα αναφέραμε αναλυτικότερα τους κινδύνους που μπορεί να αντιμετωπίσουν οι χρήστες στα κοινωνικά δίκτυα. Ο ENISA σε έκθεσή του αναφέρει τους σημαντικότερους κινδύνους για τους εφήβους, σε σύνολο 13 εντοπισμένων. Οι κυριότεροι με βάση την έκθεση αυτή είναι η σοβαρή απώλεια της σωματικής ή της ψυχικής υγείας, η ανεπανόρθωτη έκθεση σημαντικών προσωπικών πληροφοριών στο διαδίκτυο, η διάκριση με βάση τη συμπεριφορά του ατόμου στο διαδίκτυο και κακή χρήση των προσωπικών δεδομένων.

Θα πρέπει να μάθουν να ελέγχουν την αξιοπιστία των πληροφοριών που βρίσκουν στο διαδίκτυο. Να ενημερώνονται από έγκυρες και έγκριτες πηγές, από επίσημες και επώνυμες σελίδες με στοιχεία για την προέλευση τους, γιατί μπορεί οι λανθασμένες πληροφορίες να δημιουργήσουν εσφαλμένες εντυπώσεις, κακή ενημέρωση και μπορεί ακόμα να είναι και επικίνδυνες. Να δίνεται ιδιαίτερη προσοχή στις σελίδες που ζητείται εγγραφή και προσωπικά στοιχεία του χρήστη. Τα κοινωνικά δίκτυα λειτουργούν και κρύβουν κινδύνους, όπως συμβαίνει και στην κοινωνία που ζούμε. Δεν αποτελούν μόνο χώρο ευχάριστης απασχόλησης και επικοινωνίας με «φίλους», αλλά ελλοχεύουν πολλούς κινδύνους και εξυπηρετούν χιλιάδες σκοπούς. Είναι από τις σελίδες στο διαδίκτυο που έχουν ως απαραίτητο πεδίο την εισαγωγή προσωπικών στοιχείων, άρα αυτόματα χάνεται και η έννοια της ιδιωτικότητας σε έναν μεγάλο βαθμό. Γι' αυτό οι χρήστες θα πρέπει να μάθουν να διαχειρίζονται, να ελέγχουν και να ρυθμίζουν τις πληροφορίες που παρέχουν. Οι πληροφορίες και τα σχόλια που κοινοποιούνται θα πρέπει να εξετάζονται και να είναι πολύ προσεκτικοί οι χρήστες πριν τα αναρτήσουν, γιατί είναι εύκολη η πρόσβαση από άτομα που ίσως δεν θα ήθελαν να τις δουν και να υπάρχουν δυσάρεστες συνέπειες. Θα πρέπει επίσης να δίνεται ιδιαίτερη προσοχή στους κωδικούς πρόσβασης των χρηστών.

ΕΝΟΤΗΤΑ 6^Η

6.1 Συμπεράσματα

Τα κοινωνικά δίκτυα αποτελούν μέρος των ανθρώπων παγκοσμίως και συνέχεια κερδίζουν έδαφος. Όλο και περισσότεροι χρήστες δημιουργούν λογαριασμούς και πειραματίζονται πάνω στις νέες τεχνολογίες. Τα οφέλη είναι πολλά, αλλά δεν πάυουν να υπάρχουν και πολλές επιπτώσεις από την χρήση τους.

6.1.1 Θετικές επιδράσεις

Ένα από τα βασικότερα πλεονεκτήματα των κοινωνικών δικτύων είναι ότι μειώνουν τις αποστάσεις. Πολλοί χρήστες καταφεύγουν για να κατεφέρουν να επικοινωνήσουν με «φίλους», να εκφράσουν τα συναισθήματα, τις αποψεις τους, τις σκέψεις τους κ.α. Παρέχονται πληροφορίες, ειδήσεις, γεγονότα έτσι χρήστες ενημερώνονται αυτόματα με το τι συμβαίνει και μπορούν να ανταλλάσουν απόψεις πάνω σε πολλά θέματα. Όπως δείχνουν τα γεγονότα και τα στατιστικά, τα κοινωνικά δίκτυα έχουν αντέξει στον χρόνο, έχουν εξελιχθεί και έχουν εδραιωθεί στην καθημερινή ζωή των ανθρώπων, αυτό παρατηρείται και από την ολοένα αυξανόμενη χρήση των smartphones.

Με τον όρο smartphones (έξυπνα τηλέφωνα), εννοούμε τα κινητά τηλέφωνα που έχουν ενσωματωμένο λειτουργικό σύστημα με εξελιγμένη υπολογιστική ικανότητα και συνδεσιμότητα σε σχέση με τα παλιά απλά κινητά τηλέφωνα. Τέτοια λειτουργικά συστήματα (OS) είναι το Android της Google, το iOS της Apple, διάφορες ενσωματωμένες διανομές Linux, όπως το Maemo και το MeeGo κ.α. Με την χρήση των smartphones αυξάνεται η επιθυμία και η ανάγκη των χρηστών να ενταχθούν στα κοινωνικά δίκτυα, όπως επίσης να αναπτύξουν και να ενισχύσουν την επικοινωνία διαδικτυακά. Οι εταιρίες θα πρέπει να ελέγξουν τις ελλείψεις και τα κενά που υπάρχουν στα κοινωνικά δίκτυα, να αξιοποιήσουν την δύναμη που έχουν και να σχεδιάσουν μια αρχιτεκτονική που θα μειώσει τους κινδύνους και θα βελτιώσει την ασφάλεια των χρηστών και θα παρέχει προστασία στα προσωπικά τους δεδομένα.

Οι σελίδες κοινωνικής δικτύωσης παρέχουν πολλά οφέλη στην επικοινωνία των χρηστών, στην επιστήμη, στην κοινωνία, ενώνει τους ανθρώπους με τις πληροφορίες και ανοίγει νέους δρόμους στην αγορά, πάντα μέσα σε ένα ασφαλές και περιορισμένο πλαίσιο.

6.1.2 Αρνητικές επιδράσεις

Βέβαια στον αντίποδα υπάρχουν και αρκετά αρνητικά σημεία στα κοινωνικά δίκτυα για τα οποία δεν θα πρέπει να εθελουφούμε. Όλες οι σελίδες κοινωνικής δικτύωσης παρουσιάζουν μεγάλα κενά και σημαντικές ελλείψεις στον τρόπο που αντιμετωπίζουν τα προσωπικά δεδομένα. Έναν από τους μεγαλύτερους φόβους αποτελεί, το κατά πόσο τα κοινωνικά δίκτυα προστατεύουν τις πληροφορίες και τα προσωπικά δεδομένα των χρηστών. Ερωτήματα όπως, αν παραβιάζεται η προσωπική ζωή των χρηστών, αν οι πληροφορίες που συλλέγονται ελέγχονται από κάποιον και αν προτατεύονται σε περίπτωση που αποθηκευτούν τέτοια δεδομένα απασχολούν τους χρήστες και την κοινωνία, ακόμα και αν έχουν κατοχυρωθεί νομοθετικά δικαιωμάτα που τους προστατεύουν παρατηρούνται ακόμα σημαντικές ελλείψεις.

Επίσης, έντονη ανησυχία αποτελεί το γεγονός ότι έχουν χαθεί τελείως τα όρια της ιδιωτικής ζωής των ανθρώπων, οι χρήστες ανα πάσα στιγμή κοινοποιούν φωτογραφίες και δεδομένα με την τοποθεσία τους (check-in). Πλέον, μέσω των smartphones οι χρήστες δηλώνουν την ακριβή τοποθεσία που βρίσκονται με την βοήθεια GPS, με ποίους βρίσκονται, καθώς επίσης μπορούν να κοινοποιήσουν και φωτογραφικό υλικό ή βίντεο, δίνοντας το στίγμα τους.

Επιπλέον, θα πρέπει να ερευνηθεί το κατά πόσο οι χρήστες είναι ενημερωμένοι με τις ενέργειες και τα εργαλεία που χρησιμοποιούν μέσα από τα κοινωνικά δίκτυα ή αν απλά αποδέχονται τους όρους χρήσης και χρησιμοποιούν εφαρμογές, χωρίς να έχουν κάποια κριτική σκέψη. Εάν συνειδητοποιούν τις συνέπειες και τους κινδύνους που μπορεί να προκληθούν με την δημοσιοποίηση κάποιων πληροφοριών. Παράλληλα, ανησυχητικό είναι το γεγονός ότι οι εταιρίες εκμεταλλεύονται τα δεδομένα και τις πληροφορίες αυτές των χρηστών για εμπορικούς σκοπούς. Παρέχουν τα δεδομένα αυτά σε διαφημιστικές εταιρίες, δημιουργώντας το καταναλωτικό προφίλ κάθε χρήστη. Με τον τρόπο αυτό, ελέγχουν και υποβαθμίζουν την αντίληψη και την ιδιωτική ζωή των χρηστών, μετατρέποντάς τους σε απλούς καταναλωτές.

6.2 Επίλογος

Αδιαμφισβήτητα, η εποχή της πληροφορίας και της κοινωνικοποίησης έχει αρχίσει να αλλάζει ριζικά. Τα κοινωνικά δίκτυα έχουν καταστεί απαραίτητα εργαλεία στην σημερινή κοινωνία, έχουν γίνει κομμάτι της καθημερινότητάς των ανθρώπων παγκοσμίως, έχοντας την τάση συνεχώς να εξελίσσονται και να αναπτύσσονται. Η τεχνολογική αυτή ανάπτυξη, έχει μικρύνει τις αποστάσεις και έχει φέρει σε επαφή πολλούς ανθρώπους που ίσως να μην είχαν ποτέ την ευκαιρία να συναντηθούν. Όμως, αυτή η τεχνολογική άνθιση θα πρέπει να συμβαδίζει με την προστασία και την ασφάλεια των χρηστών. Θα πρέπει να γίνει σωστή αξιολόγηση των κινδύνων και των απειλών, έτσι ώστε να αξιοποιηθούν οι θετικές πτυχές της εξέλιξης αυτής.

Το μεγαλύτερο πρόβλημα που αντιμετωπίζουν οι χρήστες που συμμετέχουν στις ΙΚΔ αφορά την ασφάλεια των προσωπικών τους δεδομένων και την απώλεια της ιδιωτικότητάς τους. Για τον λόγο αυτό οι εταιρίες και τα κράτη θα πρέπει να ενημερώνουν τους χρήστες για την σωστή και ασφαλή περιήγηση τους στα κοινωνικά δίκτυα και στο διαδίκτυο γενικότερα. Το δικαίωμα στην προσωπική ζωή αποτελεί αναφαίρετο δικαίωμα του καθενός σε όλες τις υγιείς κοινωνίες, αυτό ισχύει και στο διαδίκτυο. Για την σωστή και ασφαλή χρήση θα πρέπει να υπάρχουν οι απαραίτητες ρυθμίσεις, αλλά απαραίτητη προϋπόθεση αποτελεί επίσης, η διάθεση των χρηστών για μια ασφαλή «ζωή» στο Διαδίκτυο.

Βιβλιογραφία

- Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών, Εκδόσεις Παπασωτηρίου, Κωνστανίνος Λαμπρινουδάκης, Λίλιαν Μήτρου, Στέφανος Γκριτζαλης, Σωκράτης Κάτσικας
- Ευαίσθητα Προσωπικά Δεδομένα, Εκδόσεις Σάκκουλα, Ιωάννης Ιγγλεζάκης
- Enisa (European Network and Information Security Agency), Cyber-Bulling and online Grooming: helping to protect against the risks
- Ερευνητική εργασία, Κοινωνικά Δίκτυα: ο ρόλος τους στις κοινωνικές και οικονομικές σχέσεις, Υπεύθυνοι καθηγητές: Γεωργίου Γεώργιος, Πορίκης Νικόλαος
- Αξιολόγηση Ιστοσελίδων Κοινωνικής Δικτύωσης, Μεταπτυχιακός Φοιτητής: Τσάκαλος Ευάγγελος, Επιβλέπουσα Καθηγήτρια: Βλαχοπούλου Μάρω
- Social Network Sites: Definiton, History and Scholarship, Danah m. Boyd, Nicole B. Ellison : <http://www.danah.org/papers/JCMCIntro.pdf>
- Διδακτορική Διατριβή, Προς το Web 3.0, Τζανέτος Πομονής: http://nemertes.lis.upatras.gr/jspui/bitstream/10889/4196/1/pomonis_PhD.pdf
- Static Brain, Social Networking Statistics: <http://www.statisticbrain.com/social-networking-statistics/>
- World Map of Social Networks: <http://vincos.it/world-map-of-social-networks/>
- Statista, The Statistics Portal:
 - <http://www.statista.com/topics/751/facebook/>
 - <http://www.statista.com/topics/737/twitter/>
 - <http://www.statista.com/chart/1553/fastest-growing-apps-worldwide/>
 - <http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>
 - <http://www.statista.com/chart/1549/social-traffic-sources/>
 - <http://www.statista.com/chart/1539/brand-reach-on-social-networks/>

- <http://www.statista.com/chart/1522/twitters-user-growth/>
- <http://www.statista.com/chart/1520/number-of-monthly-active-twitter-users/>
- Safeline.gr, Νομοθεσία – Νομικό Πλαίσιο:
<http://www.safeline.gr/nomothesia/nomiko-plaisio>
- Monitor Sidebar: <http://monitor.sidebar.gr/>
- Wikipedia, Facebook Statistics:
http://en.wikipedia.org/wiki/Facebook_statistics
- Ηλεκτρονικός εκφοβισμός:
http://gre.tabby.eu/uploads/1/6/8/6/16865702/booklet_cyp.pdf
- Enisa in Greek – European Union Agency for Network and Information Security: <https://www.enisa.europa.eu/media/enisa-in-greek>
- Κοινωνικά Δίκτυα (Web 2.0) και Εκπαίδευση: <http://bepip-pakeep.cti.gr/mahara/artefact/file/download.php?file=18337&view=2912>
- Τεχνολογίες web 2.0, Εθνικό Πληροφοριακό Σύστημα Έρευνας & Τεχνολογίας (ΕΠΣΕΤ):
<http://www.epset.gr/el/content/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B5%CF%82-web-20>
- Ευρωπαϊκό Κοινοβούλιο:
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pa/1010/1010738/1010738el.pdf
- Ασφάλεια στο Διαδίκτυο: <http://www.pi.ac.cy/InternetSafety/index.htm>
- Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων, Ισχύουσα Κοινοτική Νομοθεσία:
http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/Telecoms/Linkage/el_397L0033.html
- Ευρωπαϊκή Επιτροπή, Προστασία δεδομένων προσωπικού χαρακτήρα:
http://ec.europa.eu/justice/data-protection/index_el.htm
- EUROPA, Δελτίο Τύπου: http://europa.eu/rapid/press-release_IP-12-46_el.htm
- Αρχή Προστασίας Δεδομένων προσωπικού Χαρακτήρα:

- http://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL#1
 - http://www.dpa.gr/portal/page?_pageid=33,32920&_dad=portal&_schema=PORTAL
 - http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL
 - http://www.dpa.gr/portal/page?_pageid=33,15065&_dad=portal&_schema=PORTAL
- Mail Online, Science & Tech: <http://www.dailymail.co.uk/sciencetech/article-2340893/Britons-second-prolific-Facebook-Twitter-users-EUROPE-fifth-aged-65.html>
 - Wikipedia, Phishing : <http://en.wikipedia.org/wiki/Phishing>
 - E-Lawyer: <http://elawyer.blogspot.gr/2012/09/facebook.html>
 - Ελληνική Αστυνομία, Υπουργείο Δημόσιας Τάξης & Προστασίας του Πολίτη: http://www.astynomia.gr/index.php?option=ozo_content&lang=%27.%27&perform=view&id=20338&Itemid=965&lang=
 - CNN, Twitter unveils new profile page design: <http://edition.cnn.com/2014/04/08/tech/social-media/twitter-profile/>
 - BBC, Twitter Ban: <http://www.bbc.com/news/world-europe-26681236>
 - Theguardian, Turkey blocks use of Twitter: <http://www.theguardian.com/world/2014/mar/21/turkey-blocks-twitter-prime-minister>
 - MotherJones, MAP: Here are the Countries that block Facebook, Twitter & YouTube: <http://www.motherjones.com/politics/2014/03/turkey-facebook-youtube-twitter-blocked>
 - Twitter:
 - <https://twitter.com/privacy>
 - <https://twitter.com/tos>

➤ Facebook:

- <https://www.facebook.com/help/places>
- <https://www.facebook.com/notes/facebook/who-what-when-and-nowhere/418175202130>
- <https://www.facebook.com/about/privacy/>