ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Η ιδιωτικότητα στα μέσα κοινωνικής δικτύωσης»

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ: ΜΥΤΑΚΗ ΜΑΡΙΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΓΙΩΤΟΠΟΥΛΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

Πάτρα - 2017

Πρόλογος

Η ικανότητα της επικοινωνίας και της συμμετοχής έχει από τη μια πλευρά ως προϋπόθεση και ταυτόχρονα συνέπεια την πρόσβαση στις πηγές της πληροφόρησης, την ελευθερία της πληροφορίας. Από την άλλη πλευρά η ικανότητα αυτή περιορίζεται ή και αναιρείται, εάν δεν διασφαλίζεται η εμπιστευτικότητα των επικοινωνιών, το γνωστότερο σε όλους απόρρητο. Ο εμπιστευτικός χαρακτήρας που περιβάλλει μία επικοινωνία διευκολύνει την άσκηση και άλλων συνταγματικών ελευθεριών όπως π.χ. του ιδιωτικού βίου, της ελευθερίας της γνώμης ή ακόμη και της επαγγελματικής ελευθερίας. Η καταγραφή προσωπικών πληροφοριών και η καταγραφή ή παρακολούθηση των επικοινωνιών προσβάλλει την αξία του ανθρώπου και την ελευθερία του αλλά και δυσχεραίνει ουσιαστικά την απόλαυση και άλλων δικαιωμάτων καθώς και την άσκηση και άλλων συνταγματικά προστατευόμενων ελευθεριών. Το δικαίωμα του απορρήτου των επικοινωνιών είναι ένα ιδιαίτερα ευάλωτο. Προσβάλλεται πάντοτε εν κρυπτώ και παραβύστω, η προσβολή θίγει απεριόριστο αριθμό προσώπων, ο δε χαρακτήρας του ως μέσου ενάσκησης και άλλων δικαιωμάτων τα καθιστά και αυτά με τη σειρά τους ευάλωτα .
Η ιδιωτικότητα αποτελεί μια περισσότερο ευρεία έννοια. Οι εξελίξεις όμως στις νέες τεχνολογίες έχουν προσδώσει μεγαλύτερες διαστάσεις στην έννοια των προσωπικών δεδομένων και της προστασίας του.

Περίληψη

Η επικαιρότητα και η σημασία του θέματος της παρούσας εργασίας σχετίζεται άμεσα με τη δυναμική που παρουσιάζουν τα μέσα κοινωνικής δικτύωσης στη σύγχρονη πραγματικότητα, την αυξημένη ένταξη και ζήτηση των προσωπικών πληροφοριών στην καθημερινότητα και την ανάγκη προστασίας της ιδιωτικότητας ως βασική αξία της ανθρώπινης ζωής και δράσης. Μέσα από τη σχετική βιβλιογραφική ανασκόπηση προσδιορίστηκε η αλληλεπίδραση μέσων κοινωνικής δικτύωσης και ιδιωτικότητας του ατόμου, προσδιορίζοντας τους κινδύνους παραβίασής της και τους μηχανισμούς - πολιτικές προστασίας της.
Έχει θεσπιστεί σχετικό νομοθετικό πλαίσιο τόσο σε ευρωπαϊκό όσο και σε εγχώριο επίπεδο, απαιτείται όμως μια συνεχής διαδικασία δυναμικής προσαρμογής, με ζητούμενο τη συνεργασία του νομοθέτη με ανεξάρτητα τεχνικά κλιμάκια και επιτροπές, με τη δυσκολία της διαδικασίας να είναι αναμφισβήτητη. Ένας βασικός τρόπος προσέγγισης περιπτώσεων αυτού του είδους είναι το κατά πόσο συνδέεται ο ψηφιακός και ο πραγματικός εαυτός.
Υφίσταται πλήθος πεδίων κινδύνου που σχετίζονται με τα μέσα κοινωνικής δικτύωσης, απόρροια των τεχνολογικών παραμέτρων υλοποίησης της διαδικασίας (βάσεις δεδομένων, χρήση του ίδιου του Διαδικτύου και η δυνατότητα για την επανα-ταυτοποίηση ενός χρήστη, η ασύρματη δικτύωση και η εφαρμογή διάφορων μεθοδολογιών και «εργαλείων» που συμμετέχουν στη διαδικασία διαχείρισης και αποθήκευσης της προσωπικής πληροφορίας (όπως η εξόρυξη δεδομένων, η περιβάλλουσα νοημοσύνη και οι συγκλίνουσες τεχνολογίες) και τεχνολογικά «εργαλεία» όπως οι μηχανές αναζήτησης, τα λογισμικά ανάκτησης, οι υπηρεσίες σύννεφου και το κακόβουλο λογισμικό. Δεν πρέπει επίσης να παραβλεφθεί η σύγχρονη τάση των επιχειρήσεων για συλλογή διαδικτυακών δεδομένων που σχετίζονται με τις προτιμήσεις των καταναλωτών προκειμένου να εφαρμόσουν πολιτικές διαδικτυακού - ψηφιακού μάρκετινγκ.
Από τη σχετική επισκόπηση προέκυψε πλήθος περιπτώσεων παραβίασης της ιδιωτικότητας τόσο σε ευρύτερο επίπεδο ηλεκτρονικών επικοινωνιών όσο και σε στοχευμένο επίπεδο χρήσης μέσων κοινωνικής δικτύωσης. Στον αντίποδα, οι μηχανισμοί προστασίας μπορούν να εντοπιστούν τόσο σε επίπεδο εφαρμογής τεχνολογικών μεθόδων όσο και σε επίπεδο υιοθέτησης συγκεκριμένων πολιτικών - συμπεριφορών. Έτσι, θα πρέπει το σύστημα να έχει υιοθετήσει πολιτική ασφαλείας που θα διέπεται από το τρίπτυχο Ακεραιότητα – Διαθεσιμότητα – Εμπιστευτικότητα, ενώ η χρήση των κοινωνικών δικτύων θα πρέπει να γίνεται με βάση τη λογική προστασίας της ιδιωτικότητας τόσο από την πλευρά του διαχειριστή όσο και από αυτή του/της συμμετέχοντα/ουσας, ενώ καθοριστικός επίσης είναι ο ρόλος της συμπεριφοράς, η οποία θα πρέπει να έχει συγκεκριμένα χαρακτηριστικά. Οι τεχνολογικές εφαρμογές για την προστασία της ιδιωτικότητας στο διαδίκτυο διαχωρίζονται σε αυτές της ανωνυμίας ή ψευδωνυμίας και στις ονομαστικές. Ενδεικτικά αναφέρονται η ταυτοποίηση μέσω ραδιοσυχνοτήτων, οι βιομετρικές τεχνολογίες, το E-Token και οι «έξυπνες» κάρτες.
Σε κάθε περίπτωση, ζητούμενο είναι μια υπεύθυνη και δυναμική προσέγγιση του θέματος τόσο από τους επίσημους φορείς όσο και από τους διαχειριστές/χρήστες των μέσων κοινωνικής δικτύωσης.

Λέξεις – Κλειδιά: Ιδιωτικότητα, Προστασία, Μέσα Κοινωνικής Δικτύωσης

Abstract

The timeliness of the object of the present thesis is related on the potential of social media, the enhanced demand for personal data and the need for privacy protection as an essential value of daily human life and action. Through the relevant review the interaction between social media and personal privacy was defined, targeting in the dangers of infraction and the protection policies.
A relevant legislative framework has been set in European and domestic level. However, a continuous and dynamic adjustment is need, even if there is increased difficulty for the whole process. A correct approach of such cases is through the connection between the digital and the real person.
There are various danger fields which are connected to social media according to the privacy protection, result of several technological parameters (databases, wireless networking, potential of internet re-identification, technologies for information management like data mining, ambient intelligence and converging technologies and
several tools that can be used like search engines, recovery software cloud services and malware). Moreover, the synchronous business trending for digital marketing application should not be disregarded.
The relevant review indicates several cases of privacy violation for electronic communication generally and social media specifically. On the contrary, protection mechanisms are located in technological and policy – behavioral level. The safety policy that include integrity, availability and confidentiality must be applicated in every system. In technological level, applications are separated in nominal and anonymity categories (indicatively, radiofrequency identification, biometrics, E-Token and smart cards are reported).
In every case, the whole matter should be approached responsibly and dynamically from official operators, administrators, and users of social media.

Key-words: Privacy, Protection, Social Media

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Κατάλογος Εικόνων

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Στόχος και αντικείμενο της εργασίας

Το θέμα της παρούσας εργασίας είναι ιδιαίτερα επίκαιρο, μια ιδιότητα που προκύπτει από το γεγονός ότι χαρακτηρίζει και τις δύο συνιστώσες του. Η πρώτη από αυτές, η ιδιωτικότητα είναι συνυφασμένη με την ίδια την ανθρώπινη ύπαρξη και αποτελεί δικαίωμα του κάθε ανθρώπου σε συνεχή βάση, ως προαπαιτούμενο της αξιοπρέπειας και της αυτονομίας του. Η δεύτερη, αυτή των μέσων κοινωνικής δικτύωσης αποτελεί μια δυναμικά ενισχυόμενη πραγματικότητα που απαντάται σε κάθε έκφανση της σύγχρονης ανθρώπινης δραστηριότητας.

Στόχος της εργασίας είναι μέσα από τη σχετική βιβλιογραφική ανασκόπηση να προσδιοριστεί η αλληλεπίδραση μέσων κοινωνικής δικτύωσης και ιδιωτικότητας και να εντοπιστούν πεδία που ενέχουν κινδύνους και πολιτικές προστασίας τους.

Το αντικείμενο της εργασίας είναι να προσδιορίσει το μηχανισμό αυτής της αλληλεπίδρασης και να εξηγήσει κατά το δυνατό την εφαρμογή του, εντοπίζοντας τυχόν πεδία αδυναμιών και περιθώρια βελτίωσης.

Η δομή της εργασίας συνοψίζεται στις ακόλουθες ενότητες. Στο πρώτο κεφάλαιο, αυτό της εισαγωγής παρουσιάζεται ο σκοπός και το αντικείμενο της εργασίας ενώ παράλληλα επισημαίνεται η αναγκαιότητα ενασχόλησης με το συγκεκριμένο ζήτημα, παραθέτοντας στοιχεία για τις ανησυχίες που εκφράζουν οι χρήστες των μέσων κοινωνικής δικτύωσης αλλά και στατιστικά μεγέθη που καταδεικνύουν το βαθμό εισχώρησης των μέσων κοινωνικής δικτύωσης στην καθημερινότητα.

Στο δεύτερο κεφάλαιο παρουσιάζεται η έννοια της ιδιωτικότητας, ως προς τον ορισμό της, τη νομική της διάσταση αλλά και τη διάκρισή της με την έννοια των προσωπικών δεδομένων. Επιπρόσθετα γίνεται μια ιστορική αναδρομή της εξέλιξής της, έτσι ώστε να γίνει κατανοητή η διαχείριση των «απειλών» της και της αντιμετώπισής τους στο πέρασμα του χρόνου.

Στο τρίτο κεφάλαιο παρουσιάζονται τα μέσα κοινωνικής δικτύωσης, έτσι όπως αυτά υφίστανται στη σύγχρονη μορφή και έκτασή τους, ενώ στο τέταρτο κεφάλαιο αναλύεται η αλληλεπίδραση ιδιωτικότητας και μέσων κοινωνικής δικτύωσης εντοπίζοντας τα αντίστοιχα πεδία κινδύνου και τους δυνατούς μηχανισμούς παραβίασης καθώς επίσης και τους αντίστοιχους μηχανισμούς και πολιτικές προστασίας. Τέλος, στο πέμπτο κεφάλαιο, εξάγονται συγκεκριμένα συμπεράσματα για το συνολικό ζήτημα, ενώ επιπρόσθετα προσδιορίζονται σημεία που χρήζουν περαιτέρω έρευνας.

1.2 Αναγκαιότητα ενασχόλησης με το συγκεκριμένο ζήτημα

1.2.1 Εξάπλωση των μέσων κοινωνικής δικτύωσης

Η εξάπλωση του διαδικτύου και των μέσων κοινωνικής δικτύωσης πέρα από την επικρατούσα αίσθηση επιβεβαιώνονται και από αριθμούς, που στην προκειμένη περίπτωση «λένε την αλήθεια». Όσον αφορά στη χρήση του διαδικτύου, ενδεικτικό είναι ότι σε καθημερινή βάση (Κοσμετάτος, 2012):

- 864.000 ώρες βίντεο ανεβαίνουν στο YouTube,
- η πληροφορία που κυκλοφορεί στο διαδίκτυο αντιστοιχεί στην χωρητικότητα 168 εκατομμύριων DVD,
- αν τα μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονταν με τον παραδοσιακό τρόπο θα χρειάζονταν μόνο για τις ΗΠΑ 2 χρόνια για να επεξεργαστούν όλο αυτόν τον όγκο με τα γράμματα (τα οποία αντιστοιχούν σε 294 δισεκατομμύρια email).

Ειδικότερα όσον αφορά στην καταμέτρηση των χρηστών των διάφορων μέσων κοινωνικής δικτύωσης τα νούμερα είναι αντιπροσωπευτικά (Κόνσουλας, 2013). Σύμφωνα με την υπηρεσία Sidebar Monitor υφίστανται πάνω από 1.190.000.000 ενεργοί χρήστες στο Facebook (από τους οποίους οι Έλληνες είναι πάνω από 4.663.000 χρήστες, με τα αντίστοιχα μεγέθη για το Twitter να είναι 232.000.000 ενεργοί χρήστες παγκοσμίως και πάνω από 391.000 Έλληνες χρήστες. Σε επαγγελματικό επίπεδο, το επαγγελματικό Κοινωνικό Δίκτυο LinkedIn είχε ξεπεράσει τους 259.000.000 εγγεγραμμένους χρήστες παγκοσμίως, σύμφωνα με επίσημα στατιστικά στα τέλη του Οκτωβρίου του 2013, από τους οποίους οι Έλληνες ήταν λίγο πάνω από 698.000 χρήστες,.

1.2.2 Ανησυχία σχετικά με την «απειλή» της ιδιωτικότητας

Μπορεί η χρήση του διαδικτύου γενικότερα και των μέσων κοινωνικής δικτύωσης ειδικότερα να αποτελεί μια συνήθη και έντονη σύγχρονη πραγματικότητα, χωρίς όμως κάτι τέτοιο να σημαίνει ότι η συμμετοχή σε αυτήν γίνεται χωρίς ανησυχία και ενδοιασμούς. Έτσι, ακόμα και αν τα μέσα κοινωνικής δικτύωσης αποτελούν μια ισχυρή τάση – μόδα της εποχής, οι χρήστες του διαδικτύου και των μέσων εκφράζουν μια διάχυτη ανησυχία σχετικά με την απειλή της ιδιωτικότητάς του, στοιχείο που αποτελεί άλλωστε ένα βασικό εμπόδιο στην καθολική ανάπτυξη αυτών των εφαρμογών. Αυτή η διάχυτη ανησυχία αποτυπώνεται και σε στατιστικά στοιχεία σχετικών ερευνών, με χαρακτηριστικά στατιστικά στοιχεία όπως ότι το 81-87% των χρηστών του διαδικτύου ανησυχούν όσον αφορά στην ιδιωτικότητά τους, το 67-74% των χρηστών του διαδικτύου εκφράζουν ιδιαίτερη ανησυχία σχετικά με το κατά πόσο παραμένουν κρυφές – απόρρητες πληροφορίες που σχετίζονται με την ιδιωτική τους ζωή, το 41% των χρηστών κατά μέσο όρο εγκαταλείπουν ιστοχώρους που απαιτούν καταχώρηση

πληροφοριών, αντιδρώντας στην προσπάθεια εκμαίευσης πληροφοριών αυτού του είδους (Ζωρόθεος, 2007). Στα ίδια ερευνητικά πλαίσια, σύμφωνα με την ευρείας κλίμακας έρευνα EUROBAROMETER 359 (2011) που διεξήχθη σε 27 χώρες της Ε.Ε και σε δείγμα 26.500 συμμετεχόντων/ουσών ηλικίας 18-50 ετών, προέκυψε πως οι Ευρωπαίοι θεωρούν ως ανησυχητικές – επικίνδυνες συμπεριφορές από πλευράς έκθεσης ιδιωτικών πληροφοριών τη διαδικτυακή χρήση καρτών πληρωμής (54%), με αξιοσημείωτα μικρό το ποσοστό που θεωρεί πως διατηρεί τον πλήρη έλεγχο ως προς την προστασία των προσωπικών τους δεδομένων (26%) (Τσαγκανού, 2014).

Αυτή όμως η ανησυχία επιβεβαιώνεται και από επίσημες πηγές – φορείς που αναγνωρίζουν το πρόβλημα και κρούουν τον κώδωνα του κινδύνου. Ενδεικτικές είναι οι δηλώσεις της Προέδρου της Ομοσπονδιακής Επιτροπής Εμπορίου στα πλαίσια ομιλίας της στην έκθεση τεχνολογίας CES, που πραγματοποιήθηκε στο Las Vegas των ΗΠΑ, η οποία «προειδοποίησε για τις απειλές και τους κινδύνους, όσον αφορά την ιδιωτικότητα, που ενέχει η χρήση των διασυνδεδεμένων, "έξυπνων" gadgets και του Internet of Things (IoT)» (LIFO, 2015). Επίσης, χαρακτηριστικό είναι το γεγονός πως η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης έχει καθιερώσει, από το 2006, την 28η Ιανουαρίου ως Ευρωπαϊκή Ημέρα Προστασίας Προσωπικών Δεδομένων, στοχεύοντας στην ευαισθητοποίηση των πολιτών σε θέματα προστασίας προσωπικών δεδομένων.

Το ερώτημα που προκύπτει εύλογα είναι αν μια τέτοια ανησυχία είναι δικαιολογημένη. Λαμβάνοντας υπόψη την ετήσια έκθεση της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2016), το σύνολο των διεκπεραιωμένων υποθέσεων προσφυγών/καταγγελιών, ερωτημάτων και γνωστοποιήσεων αρχείων και επεξεργασιών ανήλθε σε 2.849 για το έτος 2015, με την Αρχή να εξετάζει 452 προσφυγές/καταγγελίες και 1.194 ερωτήματα υπευθύνων επεξεργασίας ή πολιτών σχετικά με τη νομιμότητα συγκεκριμένης επεξεργασίας ή τον τρόπο εφαρμογής της σχετικής νομοθεσίας.

Προκύπτει επομένως πως και ανησυχίες υφίστανται σε ευρεία βάση και πως αυτές οι ανησυχίες είναι δικαιολογημένες, τουλάχιστον υπό τη μορφή αναγκαίου ελέγχου, ακόμα δηλαδή και αν δεν υφίσταται παραβίαση ιδιωτικότητας, θα πρέπει να ελέγχονται τυχόν υποψίες – αμφιβολίες.

ΚΕΦΑΛΑΙΟ 2: Η ΕΝΝΟΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

2.1 Ορισμός και ανάλυση

Προκειμένου να κατανοηθούν οι διαστάσεις της προαναφερόμενης απειλής, θα πρέπει πρώτα να οριστεί η έννοια της ιδιωτικότητας. Έχουν κατά καιρούς δοθεί διάφοροι ορισμοί της έννοιας, καθένας από τους οποίους επικεντρώνεται σε μια συγκεκριμένη διάσταση της έννοιας. Χαρακτηριστικά αναφέρονται οι ακόλουθες προσεγγίσεις (παρατίθενται με χρονολογική σειρά):

- Σύμφωνα με την Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα (1948): «κανείς δεν πρέπει να υποβάλλεται σε περιορισμό ή παράνομη επέμβαση στην ιδιωτική του ζωή, την οικογένεια, το σπίτι ή την αλληλογραφία του, ούτε να υπόκειται σε παράνομες προσβολές της τιμής και της υπόληψης του. Επίσης, καθένας έχει το δικαίωμα της έννομης προστασίας από τέτοιου είδους παρεμβάσεις και επιθέσεις» (Σπυριδωνίδου, 2015).
- Σύμφωνα με τους Warren and Brandeis (1890) η ιδιωτικότητα ορίζεται ως «το δικαίωμα του να είσαι μόνος» (the right to be let alone), με ενδιαφέρον στοιχείο ότι οι συγγραφείς είχαν από τότε προβλέψει τη δυναμική ανάγκη για προστασία της στο πέρασμα του χρόνου.
- Σύμφωνα με τον Westin (1968) η ιδιωτικότητα αποτελεί το «δικαίωμα των ανθρώπων να επιλέγουν ελεύθερα και χωρίς περιορισμούς το βαθμό έκθεσης του εαυτού τους, τη στάση και τη συμπεριφορά τους απέναντι σε άλλους».
- Για τον Rachels (1975) η ιδιωτικότητα αφορά «την ικανότητα να ελέγχουμε ποιος έχει πρόσβαση σε εμάς» (Σπυριδωνίδου, 2015).

Λαμβάνοντας υπόψη το σύνολο αυτών των ορισμών στο πέρασμα του χρόνου, υφίσταται ένας «κοινός παρονομαστής», ο οποίος αφορά στην περιχαράκωση της πληροφορίας που σχετίζεται με την ιδιωτική ζωή του ατόμου, με τα όρια της διαδικασίας να τίθενται κάθε φορά από το ίδιο το άτομο.

Θα πρέπει να σημειωθεί πως όσον αφορά το αντικείμενο της παρούσας εργασίας, ενδιαφέρον παρουσιάζει η πληροφοριακή ιδιωτικότητα και η προστασία της, μια ανάγκη η οποία ενισχύθηκε από την εξέλιξη των νέων τεχνολογιών και τη συνεπαγόμενη διεύρυνση του προστατευτέου αγαθού αλλά και την αναγκαιότητα της κανονιστικής αντιμετώπισης των προσβολών της ιδιωτικότητας που σχετίζονται με τις διαδικασίες συλλογής, επεξεργασίας, διάχυσης, συσχετισμού των πληροφοριών που δημιούργησαν τα πληροφοριακά και επικοινωνιακά συστήματα και κυρίως τη δυνατότητα χρήσης, ανταλλαγής και συσχετισμού των δεδομένων που έχουν συλλεχθεί για πολλαπλούς και διαφορετικούς από τους αρχικούς σκοπούς. Αξιοσημείωτο είναι μάλιστα ότι μια τέτοια εξέλιξη είχε επισημανθεί σχετικά νωρίς (αρχές του’ 70), κατ’ αντιστοιχία με τους κινδύνους που συνεπαγόταν η εφαρμογή ενός νέου Panopticon (Bentham, 1995), με τη συγκεκριμένη ιδέα να αναφέρεται σε κλειστές επιτηρούμενες κοινότητες και την επιτήρηση να αποσκοπεί στην απόκτηση δύναμης επί της σκέψης των ανθρώπων, με προοπτική επί του συνόλου των ατόμων και των δραστηριοτήτων τους

(Μήτρου, 2016). Αντίστοιχη αναφορά με κοινά στοιχεία αυτά της συνεχούς παρακολούθησης από μία αόρατη και χωρίς φυσική υπόσταση εξουσία και την επιθυμία για άσκηση ελέγχου και επιρροή των αποφάσεων του υποκειμένου αποτελεί και η γνωστή έκφραση «Μεγάλος Αδελφός» η οποία χρησιμοποιείται ευρέως για να υποδηλώσει τέτοιου είδους πρακτικές.

2.1.1 Διάκριση Προσωπικών Δεδομένων και Ιδιωτικότητας

Συχνά παρατηρείται το φαινόμενο σύγχυσης ανάμεσα στις έννοιες της ιδιωτικότητας και των προσωπικών δεδομένων και στην ανάγκη και τον τρόπο υλοποίησης της προστασίας τους. Αυτή η σύγχυση μπορεί να ενταχθεί στο ευρύτερο πλαίσιο της εξέλιξης της ιδιωτικότητας τόσο ως όρου όσο και ως αξίας. Η εξέλιξη της τεχνολογίας σε συνδυασμό με την κοινωνική εξέλιξη που τη συνοδεύει ή προκύπτει από αυτή σε μια σχέση αλληλεπίδρασης έχει οδηγήσει στη σύγκλιση των δύο εννοιών (ιδιωτικότητα και προσωπικά δεδομένα), Η σύγκλιση αυτή είναι απόρροια όλων εκείνων των διαδικασιών που συνοδεύουν την προαναφερόμενη αλληλεπίδραση, όπως την παράλληλη εξέλιξη των τεχνολογιών πληροφορικής και επικοινωνιών, την αποκέντρωση της επεξεργασίας, τη διείσδυση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας και όλων εκείνων των τεχνολογικών δραστηριοτήτων που συνεπάγονται σημαντικές αλλαγές στο περιβάλλον χρήσης της προσωπικής πληροφορίας.

Μπορεί λοιπόν να θεωρηθεί πως η σύγκλιση των δύο εννοιών συνδέεται άμεσα με την τεχνολογική εξέλιξη και την ανάγκη προστασίας των προσωπικών δεδομένων που ενισχύεται σημαντικά από αυτή, ως αποτέλεσμα της αυξημένης ένταξης και ζήτησης των προσωπικών πληροφοριών στην καθημερινότητα (π.χ. ηλεκτρονικές συναλλαγές, δημιουργία προφίλ κτλ.)

Σύμφωνα με το άρθρο 2 του Ν. 2472/97 υφίστανται δύο είδη προσωπικών δεδομένων, τα δεδομένα προσωπικού χαρακτήρα και τα ευαίσθητα δεδομένα. Ως “δεδομένα προσωπικού χαρακτήρα”, νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων. Σημειώνεται ότι στη συγκεκριμένη κατηγορία δε λογίζονται τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Ως “ευαίσθητα δεδομένα”, νοούνται τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2017).

Η προστασία των προσωπικών δεδομένων έχει άμεση σχέση με την επεξεργασία τους και το κατά πόσο αυτή γίνεται σε νόμιμη βάση. Με τον όρο επεξεργασία νοείται «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή»

(Ν. 2472/97, Άρθρο 2). Έτσι λοιπόν, προκειμένου τα δεδομένα προσωπικού χαρακτήρα να τύχουν νόμιμης επεξεργασίας θα πρέπει:
α) Να συλλέγονται κατά τρόπο θεμιτό και νόμιμο για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.
β) Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας.
γ) Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.
δ) Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής, για την πραγματοποίηση των σκοπών της συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς επιστημονικούς ή στατιστικούς σκοπούς, εφ΄ όσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων (Ν. 2472/97, Άρθρο 4).

Προσεγγίζοντας λοιπόν ταυτόχρονα και συγκριτικά τις δύο έννοιες (ιδιωτικότητα και προσωπικά δεδομένα) προκύπτει πως παρά το ότι η ιδιωτικότητα αποτελεί μια περισσότερο ευρεία έννοια αφού αφορά στον ορισμό της ζωής του καθενός από τον ίδιο, οι εξελίξεις στις νέες τεχνολογίες έχουν προσδώσει μεγαλύτερες διαστάσεις στην έννοια των προσωπικών δεδομένων και της προστασίας τους, με την επιλογή του προαναφερόμενου ορισμού του ιδιωτικού βίου να επικεντρώνεται στα δεδομένα που περιγράφουν αυτόν τον βίο, στο βαθμό που μπορεί να γίνουν εκμεταλλεύσιμα για καθορισμό μια συμπεριφοράς. Έτσι, μπορούν να οδηγήσουν σε μια «ψευδαίσθηση επιλογής», προσβάλλοντας σε μια πρώτη φάση τα προσωπικά δεδομένα του ατόμου και σε μια δεύτερη (τόσο άμεσα όσο και έμμεσα, υπό την έννοια της μελλοντικής επίδρασης) την ιδιωτικότητά του.

2.2 Νομική διάσταση

Στη συγκεκριμένη ενότητα γίνεται μια συνοπτική καταγραφή των νομικών διατάξεων που διέπουν τη συνολική διαδικασία και της κύριας κατεύθυνσής τους. Σκοπός δεν είναι η εξαντλητική παράθεση νομικών κειμένων, αλλά η σκιαγράφηση του ευρύτερου νομικού πλαισίου και η αντίληψη του «πνεύματος του νόμου» που επικρατεί σχετικά με την προστασία της συγκεκριμένης έννοιας. Αναλυτικότερα:

- Άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου: το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας «οχυρώνεται» έναντι της δημόσιας αρχής, με τυχόν προσβολή του να συσχετίζεται με λόγους εθνικής ασφάλειας, δημόσιας ασφάλειας, οικονομικής ευημερίας της χώρας, αποτροπή εγκλήματος, προστασία της υγείας ή των ηθών και την προστασία των δικαιωμάτων και ελευθεριών των άλλων (Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου, 2010).
- Άρθρο 16 Της Συνθήκης για τη λειτουργία Της Ευρωπαϊκής Ένωσης: στα ίδια πλαίσια θεσπίζεται η προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2012).

- Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτόματη επεξεργασία προσωπικών δεδομένων: η σύμβαση επικεντρώνεται στην περίπτωση της αυτόματης; Επεξεργασίας δεδομένων, μια παράμετρος ιδιαίτερα σημαντική αν ληφθεί υπόψη πως πλήθος σχετικών αναζητήσεων.
- Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995: αποτελεί το πρώτο και σημαντικότερο νομοθετικό εργαλείο της Ένωσης για την προστασία της ιδιωτικότητας των πολιτών, με βασικό ζητούμενο την εναρμόνιση των επιμέρους εθνικών νομοθεσιών (Ακριβοπούλου, 2011). Σημαντικό στοιχείο που αφορά τη συγκεκριμένη οδηγία είναι ότι συμπεριλαμβάνονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα όπως εκείνα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την ερωτική ζωή και την υγεία (για την τελευταία μάλιστα τίθενται επιφυλάξεις που αφορούν την περίπτωση κατά την οποία η επεξεργασία είναι απαραίτητη για την υπεράσπιση των ζωτικών συμφερόντων του υπόψη προσώπου ή για παράδειγμα, σκοπούς προληπτικής ιατρικής και ιατρικής διάγνωσης).
- Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα: Μέσω της συγκεκριμένης οδηγίας αρχίζει πια να εντάσσεται δυναμικά το πλαίσιο των νέων ψηφιακών τεχνολογιών στη διαδικασία της ιδιωτικότητας. Ενδεικτικά, σύμφωνα με τη συγκεκριμένη οδηγία οι υπηρεσίες πληροφοριών καταλόγου, πρέπει να περιορίζονται στα απαραίτητα για την αναγνώριση της ταυτότητας συγκεκριμένου συνδρομητή, εκτός εάν ο συνδρομητής έχει δώσει τη ρητή συγκατάθεση του για τη δημοσίευση συμπληρωματικών δεδομένων προσωπικού χαρακτήρα, με το συνδρομητή να δικαιούται να ζητεί να μην συμπεριλαμβάνεται σε έντυπο ή ηλεκτρονικό κατάλογο, να δηλώνει ότι δεν επιτρέπει τη χρησιμοποίηση των προσωπικών του στοιχείων για απευθείας εμπορική προώθηση, να ζητά να παραλείπεται η διεύθυνση του εν μέρει και να μην επιτρέπει να υπάρχει αναφορά που να αποκαλύπτει το φύλο του, εφόσον τούτο είναι γλωσσικά εφικτό (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 1998).
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002: Αποτελεί μια βασική προσπάθεια εκσυγχρονισμού του νομοθετικού πλαισίου σύμφωνα με τις υφιστάμενες τεχνολογικές εξελίξεις, αντικαθιστώντας την προαναφερόμενη και εντάσσοντας τη χρήση του διαδικτύου στην ευρύτερη διαδικασία. Το χαρακτηριστικό της συγκεκριμένης οδηγίας είναι ότι συμπεριλαμβάνει ιδιαίτερες νέες μεθόδους «απειλής» της ιδιωτικότητας. Ενδεικτικά αναφέρονται τα γνωστά cookies, των οποίων η χρησιμοποίηση επιτρέπει η οδηγία, αποκλειστικά και μόνο για θεμιτούς σκοπούς και με την προϋπόθεση ότι αυτό γίνεται εν γνώσει του εκάστοτε χρήστη (λόγος για τον οποίο εμφανίζεται το γνωστό «παράθυρο» ενημέρωσης του επισκέπτη των ιστοσελίδων που χρησιμοποιούν τη συγκεκριμένη τεχνολογία). Το γενικό ζητούμενο της τεχνολογίας είναι να προστατεύεται ο χρήστης του διαδικτύου ανεξάρτητα από την τεχνολογία που εφαρμόζεται (Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2002).

- Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ(Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, 2006): Μέσω της συγκεκριμένης οδηγίας επιχειρήθηκε η διευθέτηση όλων εκείνων των ζητημάτων που αφορούν εκείνα τα δεδομένα που μπορούν να παρακρατηθούν από τους παρόχους υπηρεσιών επικοινωνίας και σχετίζονται με τη διερεύνηση, διαπίστωση και δίωξη των ποινικών αδικημάτων και την εν γένει αντιμετώπιση του ηλεκτρονικού εγκλήματος (με τα δεδομένα αυτά να αφορούν την πηγή, προορισμό, ημερομηνία, διάρκεια και τύπο της επικοινωνίας καθώς και τον προσδιορισμό του μέσου της επικοινωνίας ή την τοποθεσία της) (Ιγγλεζάκης, 2003).

Σε εγχώριο επίπεδο το αντίστοιχο νομικό πλαίσιο εντοπίζεται τόσο στο Σύνταγμα της Ελλάδος όσο και στο γενικότερο πνεύμα εναρμόνισης με τις οδηγίες της Ευρωπαϊκής Ένωσης.

Έτσι, όσον αφορά στο Σύνταγμα της Ελλάδος για την προστασία της ιδιωτικότητας υφίστανται:

- Το Άρθρο 9 &1 που θεμελιώνει το άσυλο της κατοικίας και σύμφωνα με το οποίο: «Η κατοικία του καθενός είναι άσυλο. Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη. Καμία έρευνα δεν γίνεται σε κατοικία, καρά μόνο όταν και όποτε ορίζει ο νόμος και πάντοτε με την παρουσία εκπροσώπων της δικαστικής εξουσίας».
- Το Άρθρο 9Α που θεμελιώνει την προστασία προσωπικών δεδομένων και σύμφωνα με το οποίο: «Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει».
- Το Άρθρο 19 που θεμελιώνει το απόρρητο επιστολών, ανταπόκρισης και επικοινωνίας: και σύμφωνα με το οποίο: «1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. Νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. 2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1. 3. Απαγορεύεται η χρήση αποδεικτικών μέσων που έχουν αποκτηθεί κατά παράβαση του άρθρου αυτού και των άρθρων 9 και 9Α.

Όσον αφορά στο γενικότερο πνεύμα εναρμόνισης με τις οδηγίες της Ευρωπαϊκής Ένωσης υφίστανται:

- Ο Νόμος 2472/1997 ο οποίος ενσωμάτωσε την Οδηγία 95/46/ΕΚ της Ευρωπαϊκής Ένωσης για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη

κυκλοφορία των δεδομένων αυτών. Σημειώνεται η διάκριση πως δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Ο νόμος 2472/1997 τροποποιήθηκε το 2000 και το 2001 και επιβάλλεται από την Αρχή Προστασίας Προσωπικών Δεδομένων. Συμπληρώνεται από:

  - το Νόμο 2774/1999 περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα καθώς και από
  - το Νόμο 3115/2003 ο οποίος προβλέπει τη σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών.
  - το Νόμο 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών), ο οποίος ενσωμάτωσε την Οδηγία 2002/58/ΕΚ, ενισχύοντας κατά πολύ τα δικαιώματα των χρηστών - συνδρομητών σε ζητήματα που σχετίζονται με το απόρρητο της επικοινωνίας και την προστασία της ιδιωτικότητάς τους.

- Ο Νόμος 3674/2008 μέσω του οποίου ενισχύθηκε το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας.
- Ο Νόμος 3783/2009 ο οποίος διέπει ζητήματα ταυτοποίησης των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας προπληρωμένου χρόνου ομιλίας, συνδρομητών με συμβόλαιο, ή άλλης μορφής κινητής τηλεπικοινωνίας, για λόγους εθνικής ασφάλειας και για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.
- Ο Νόμος 3917/2011 ο οποίος ενσωματώνει τις διατάξεις της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006, η οποία προβλέπει την εναρμόνιση των διατάξεων των κρατών μελών, ούτως ώστε να διατηρούνται για ορισμένο χρονικό διάστημα δεδομένα που παράγονται ή τυγχάνουν επεξεργασίας από τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων, με σκοπό τη διακρίβωση, διερεύνηση και δίωξη σοβαρών εγκλημάτων.

Είναι σημαντικό να δοθούν περαιτέρω λεπτομέρειες όσον αφορά στην ΑΔΑΕ, αφού αποτελεί εκείνον τον φορέα ο οποίος σε συνδυασμό με την Αρχή Προστασίας Προσωπικών Δεδομένων θα διαχειριστούν ή τουλάχιστον θα συμμετέχουν σε κάθε υπόθεση παραβίασης της ιδιωτικότητας η οποία θα ακολουθήσει την οδό της νομιμότητας. Ο ρόλος της αυτός έχει άμεση σχέση με τις αρμοδιότητές, σύμφωνα με τις οποίες:

α. Διενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας τακτικούς και έκτακτους ελέγχους, σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα της Εθνικής Υπηρεσίας Πληροφοριών, άλλων δημοσίων υπηρεσιών, οργανισμών, επιχειρήσεων του ευρύτερου δημόσιου τομέα, καθώς και ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία.

β. Λαμβάνει πληροφορίες σχετικές με την εκπλήρωση της αποστολής της, από τις ως άνω υπηρεσίες, οργανισμούς και λοιπά νομικά πρόσωπα και καλεί σε ακρόαση τους εκπροσώπους ή άλλα στελέχη τους.

γ. Προβαίνει σε κατάσχεση ψηφιακών πειστηρίων, μέσων παραβίασης του απορρήτου και σε καταστροφή στοιχείων που έχουν συλλεχθεί με παράνομη παραβίαση του απορρήτου των επικοινωνιών.
δ. Εξετάζει καταγγελίες ατόμων που θίγονται από τον τρόπο ή τη διαδικασία άρσης του απορρήτου.
ε. Συνεργάζεται με άλλες εθνικές αρχές και αρχές άλλων κρατών καθώς και με ευρωπαϊκούς και διεθνείς οργανισμούς που έχουν αντίστοιχο αντικείμενο.
στ. Εκδίδει κανονιστικές πράξεις που δημοσιεύονται στο ΦΕΚ, καθώς και συστάσεις και υποδείξεις σχετικά με θέματα της αρμοδιότητας της.
ζ. Συντάσσει ετήσια έκθεση πεπραγμένων στην οποία περιγράφεται το έργο της, διατυπώνονται παρατηρήσεις και προτείνονται νομοθετικές μεταβολές στο τομέα διασφάλισης του απορρήτου των επικοινωνιών. Στη συνέχεια, την υποβάλλει προς τον Πρόεδρο της Βουλής, τον Υπουργό Δικαιοσύνης καθώς και στους αρχηγούς των κομμάτων που εκπροσωπούνται στη Βουλή και στο Ευρωκοινοβούλιο (‘Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών’, 2016).

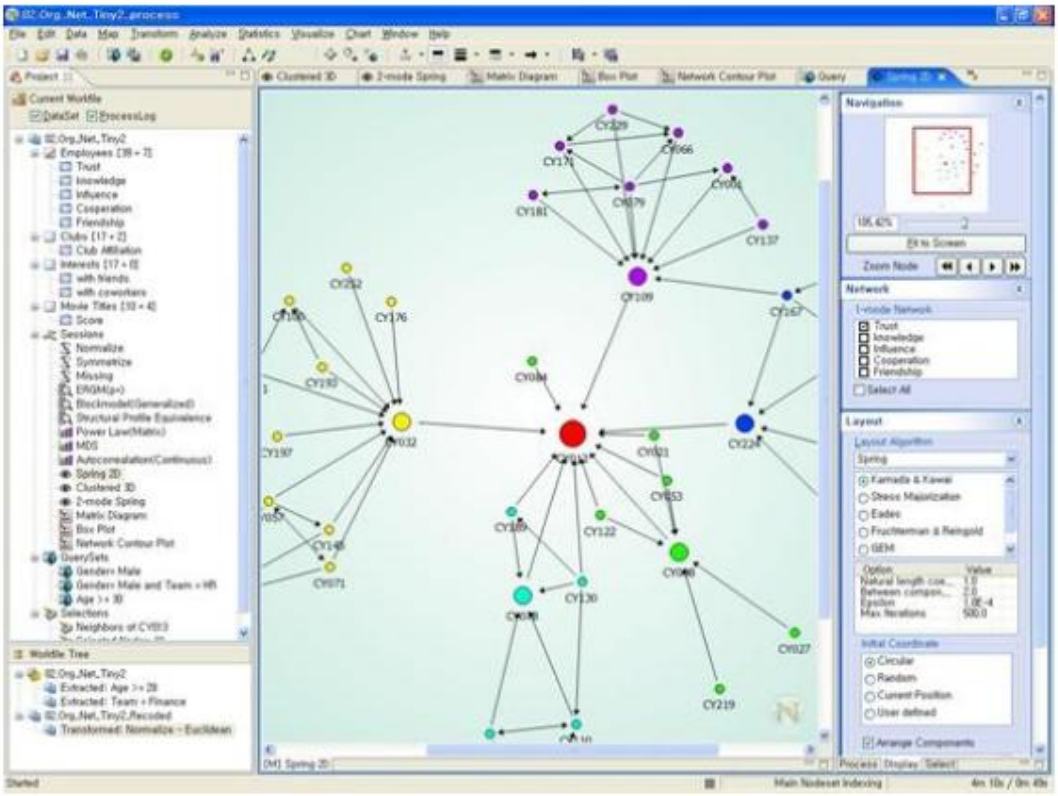
ΚΕΦΑΛΑΙΟ 3: ΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ ΩΣ ΜΕΡΟΣ ΤΗΣ ΚΑΘΗΜΕΡΙΝΟΤΗΤΑΣ

3.1 Η έννοια της κοινωνικής δικτύωσης

Σύμφωνα με τον ορισμό του (Milardo and National Council on Family Relations, 1988) το κοινωνικό δίκτυο «μια συλλογή από άτομα που γνωρίζουν και αλληλεπιδρούν με ένα συγκεκριμένο άτομο στόχο ή ζευγάρι», ενώ σύμφωνα με τους Brass, Butterfield and Skaggs (1998) πρόκειται για ένα σύνολο παραγόντων (άνθρωποι, οργανισμοί, κτλ) και μια σειρά από δεσμούς (φιλίες. χρηματικές συναλλαγές κ.τ.λ.) που αντιπροσωπεύουν κάποια σχέση -ή την απουσία αυτής- ανάμεσα στους παράγοντες.

Ορίζοντας την έννοια της κοινωνικής δικτύωσης θα μπορούσε να ειπωθεί πως πρόκειται για μια διαδικασία η οποία έχει ως στόχο να οδηγήσει σε μια συγκεκριμένη κοινωνική δομή, αποτελούμενη από κόμβους που συνδέονται μεταξύ τους με διάφορες γραμμές σύνδεσης – αλληλεπίδρασης, που αντιπροσωπεύουν με τη σειρά τους αξίες, οράματα, στόχους, ιδέες, οικονομικές συναλλαγές κτλ.

Για τη σημασία των κόμβων γίνεται επίσης αναφορά και από τον Pescosolido (2006), ο οποίος ορίζει ότι τα βασικά χαρακτηριστικά ενός κοινωνικού δικτύου είναι τα εξής: οι κόμβοι, οι δεσμοί, οι υποομάδες, το είδος των δεσμών, το κοινωνιόγραμμα. το μέγεθος, πυκνότητα, η δύναμη και η πολυπλοκότητα των δεσμών και το κοινωνιομετρικό αστέρι. Χαρακτηριστική είναι η απόδοση αυτών των κόμβων στην προσέγγιση ενός κοινωνικού δικτύου τόσο σε επίπεδο υλικού και αρχιτεκτονικής δομής όσο και ανάλυσης (όπως καταγράφεται παραστατικά από τη χρήση του λογισμικού NetMiner στην ακόλουθη εικόνα) στην οποία είναι εμφανής η αναπαράσταση και η διασύνδεση των σχετικών με το εκάστοτε δίκτυο κόμβων.



Εικόνα 1: Ανάλυση ενός κοινωνικού δικτύου με χρήση του λογισμικού NetMiner *(Ali Rohani and Siew Hock, 2009)*

Η σημασία της αλληλεπίδρασης αναδεικνύεται από τους Sundaram ***et al.*** (2012) σύμφωνα με τους οποίους η ανάλυση των κοινωνικών δικτύων βασίζεται στον προσδιορισμό των τρόπων με τους οποίους τα μέλη των δικτύων αλληλεπιδρούν και επικεντρώνεται στο βαθμό, το ύφος και το είδος αυτής της αλληλεπίδρασης.

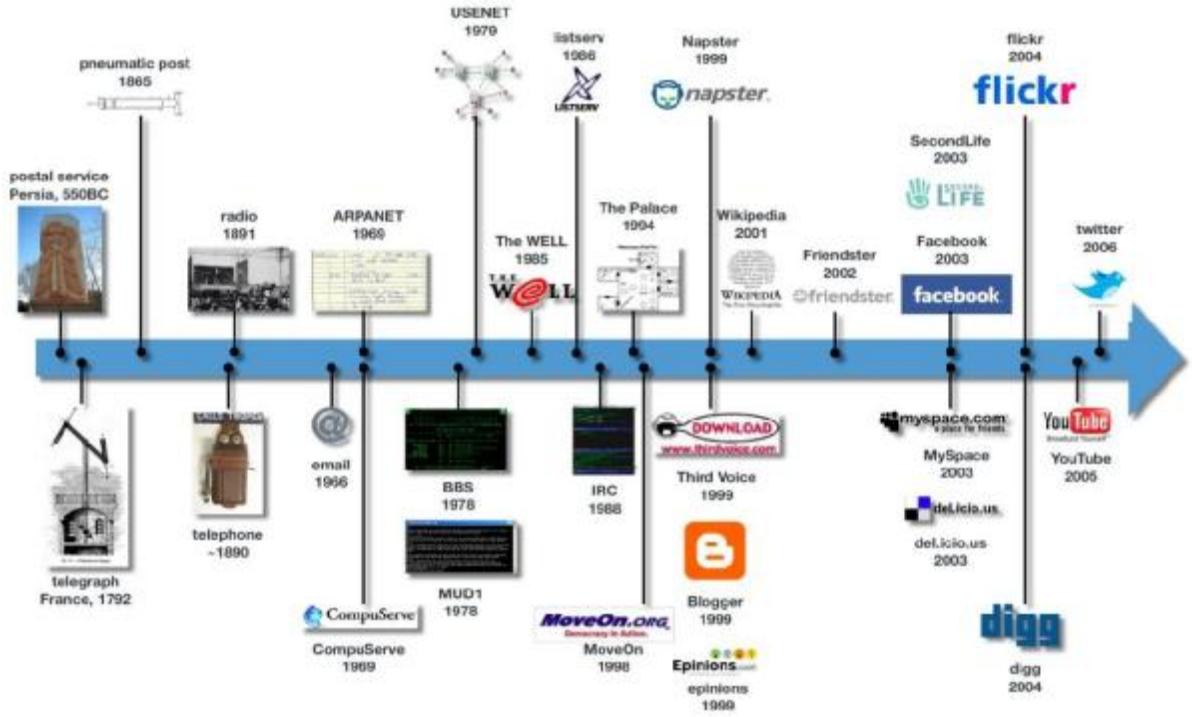
Επομένως, σύμφωνα με τους παραπάνω ορισμούς ακόμα και η οικογένεια αποτελεί ένα είδος κοινωνικού δικτύου, με τη διαφορά να έγκειται στην ισχύ των δεσμών που ενώνουν τους επιμέρους κόμβους του δικτύου, δηλαδή τα μέλη του. Στην περίπτωση του διαδικτύου, η διαδικασία οδηγεί στη δημιουργία on-line εικονικών κοινοτήτων φυσικών προσώπων, με τις συνδετικές γραμμές να σχετίζονται με ενδιαφέροντα, συμπεριφορές και δραστηριότητες, με το διαδίκτυο να αποτελεί ουσιαστικά τη βάση πάνω στην οποία μπορούν οι χρήστες να διαμοιραστούν περιεχόμενο που τους αφορά, σχηματίζοντας τις προαναφερόμενες κοινωνικές δομές (Πάσσας, 2009).

Τα κοινωνικά δίκτυα λοιπόν σήμερα παραδίνουν την σκυτάλη στα on line κοινωνικά δίκτυα, τα οποία σύμφωνα με τους (Boyd and Ellison, 2008) ορίζονται ως web-based υπηρεσίες που παρέχουν την δυνατότητα στα άτομα πρώτον να κατασκευάσουν ένα δημόσιο ή ημιδημόσιο προφίλ μέσα σε ένα οριοθετημένο σύστημα, δεύτερον να δημιουργήσουν μια λίστα με άλλους χρήστες με τους οποίους μοιράζονται μια σύνδεση και τρίτον να προβάλλουν και να διανείμουν την λίστα των συνδέσεων τους καθώς και αυτών που δημιουργήθηκαν από άλλους μέσα στο σύστημα. Τα ίδια χαρακτηριστικά (δηλαδή των ομάδων, του δικτύου και του διαμοιρασμού πληροφοριών) επισημαίνονται και από τους Kwon and Wen

(2010), σύμφωνα με τους οποίους τα online κοινωνικά δίκτυα είναι «δικτυακοί τόποι που επιτρέπουν την οικοδόμηση σχέσεων μεταξύ προσώπων σε απευθείας σύνδεση μέσω της συλλογής χρήσιμων πληροφοριών και του διαμοιρασμού αυτών με άλλους ανθρώπους. Επίσης, μπορούν να δημιουργήσουν ομάδες, οι οποίες επιτρέπουν την αλληλεπίδραση μεταξύ των χρηστών με παρόμοια ενδιαφέροντα» (Κουτσογιαννοπούλου, 2013).

Ο Zhang (2010) επισημαίνει ότι αυτή η μετάβαση στηρίζεται στην ενεργή συμμετοχή των χρηστών η οποία με τη σειρά της έχει άμεση σχέση με τα στοιχεία της διαδραστικότητας και της αλληλεπίδρασης στα μέσα επικοινωνίας τα οποία εισήλθαν με την έλευση του Web 2.0. Επομένως στοιχεία διαφοροποίησης σε σχέση με τις συμβατικές τεχνολογίες των μέσων ενημέρωσης έγκεινται αφενός στο κοινωνικό στοιχείο και αφετέρου στο βαθμό συμμετοχής του διαδικτύου. Την ίδια διαδικτυακή διάσταση των μέσω κοινωνικής δικτύωσης επισημαίνουν και οι Kaplan and Haenlein (2010) οι οποίοι ορίζουν τα μέσα κοινωνικής δικτύωσης σαν ένα σύνολο από διαδικτυακές εφαρμογές που βασίζονται στα ιδεολογικά και τεχνολογικά θεμέλια του Web 2.0 και επιτρέπουν την δημιουργία και την ανταλλαγή περιεχομένου που προέρχεται από τον ίδιο το χρήστη (User Generated Content). Αυτή τη μετάβαση του ίδιου του χρήστη σε εκδότη του περιεχομένου επισημαίνει και ο Evans (2008), αποδίδοντας στη συγκεκριμένη ιδιότητα την έννοια του εκδημοκρατισμού της πληροφορίας.

Η προαναφερόμενη μετάβαση στο πέρασμα του χρόνου αποδίδεται παραστατικά στην εικόνα που ακολουθεί

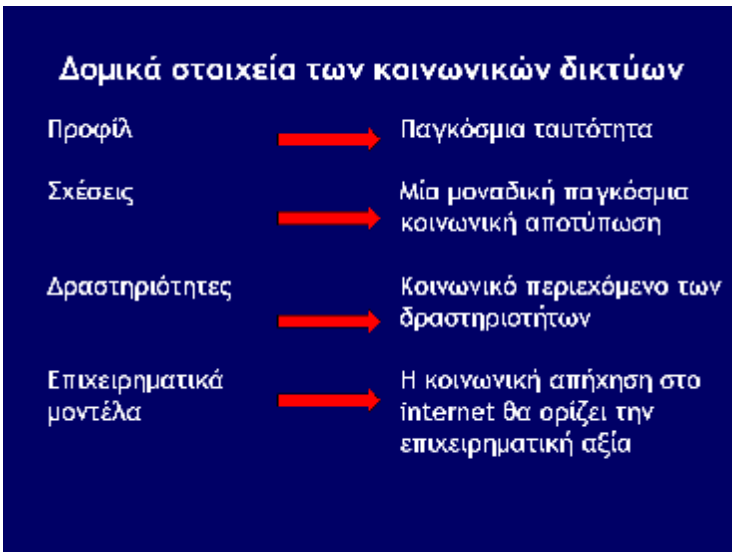


Εικόνα 2: Ενδεικτική χρονική εξέλιξη των μέσων κοινωνικής δικτύωσης (Κουτσογιαννοπούλου, 2013)

3.2 Η «επιτυχία» της διαδικασίας και η αποδοχή των μέσων κοινωνικής δικτύωσης

Η «επιτυχία» της διαδικασίας και η αποδοχή των μέσων κοινωνικής δικτύωσης προκύπτει από τη δυναμική των συγκεκριμένων μέσων στην καθημερινότητα. Αυτή η δυναμική έχει συσχετιστεί σε θεωρητικό πλαίσιο με το ότι αυθαίρετοι άνθρωποι σχετίζονται μεταξύ τους μέσω φίλων και μέσω φίλων των φίλων. Σε μια προσπάθεια εμπειρικής απόδειξης αυτού του θεωρητικού πλαισίου, ο Αμερικανός ψυχολόγος Miligram (1967) διεξήγαγε το πείραμα του «μικρού κόσμου», στο οποίο έστειλε επιστολές σε 60 εθελοντές στο Κάνσας και τους ζήτησε να τις διαβιβάσουν σε ένα συγκεκριμένο πρόσωπο στη Μασαχουσέτη μέσω φίλων και φίλων των φίλων τους. Οι επιστολές διαβιβάστηκαν μέσω μιας αλυσίδας 5 έως 7 ατόμων περίπου και έφθασαν στον παραλήπτη, επιβεβαιώνοντας έτσι πειραματικά τη δημιουργία ενός «μικρού κόσμου» από μικρό αριθμό προσωπικών γνωριμιών και οδηγώντας στο συμπέρασμα πως για τη σύνδεση δύο τυχαίων ατόμων χρειάζεται μια αλυσίδα έξι περίπου μεσαζόντων, λόγος για τον οποίο η συγκεκριμένη θεωρία ονομάστηκε «six degrees of separation» (Ali Rohani and Siew Hock, 2009).

Η ευρεία δηλαδή αποδοχή τους από το κοινό σχετίζεται άμεσα με τα δομικά χαρακτηριστικά των κοινωνικών δικτύων, όπως παρουσιάζονται στην εικόνα που ακολουθεί.



Εικόνα 3: Δομικά στοιχεία των κοινωνικών δικτύων (Πάσσας, 2009)

Σε αυτά τα δομικά στοιχεία συμπεριλαμβάνονται εγγενή πλεονεκτήματα του Διαδικτύου, όπως η απουσία γεωγραφικών και χρονικών περιορισμών αλλά και βασικά λειτουργικά χαρακτηριστικά των μέσων κοινωνικής δικτύωσης, όπως η συμμετοχή (Participation) (αφού από τη φύση τους ενθαρρύνουν τη συμμετοχή των χρηστών και τα σχόλια από τους ενδιαφερομένους), η διαφάνεια (Openness) (υπό την έννοια της δυνατότητας ανατροφοδότησης και της σπάνιας παρουσίας εμποδίων στην πρόσβαση και στην χρήση του περιεχομένου), η συνομιλία (Conversation) (υπό την έννοια της αμφίδρομης επικοινωνίας), η κοινότητα (Community) (χαρακτηριστικό το οποίο εξυπηρετεί την προαναφερόμενη ανάγκη

της κοινωνικότητας και της δημιουργίας κοινοτήτων, μια ανάγκη που λήφθηκε σοβαρά υπόψη κατά το σχεδιασμό των μέσων) και η συνεκτικότητα (Connectedness) (με τα δίκτυα να βασίζονται στη διασύνδεσή τους με άλλα μέσα, διευρύνοντας σημαντικά το εύρος κάθε μέσου).

Η χρήση και η ευρεία αποδοχή τους έχει συσχετιστεί με την έμφυτη τάση του ανθρώπου για επικοινωνία και την ανάγκη του για αλληλεπίδραση με τους ομοίους του. Ενδεικτικός της συγκεκριμένης διάστασης είναι ο ορισμός της κοινωνικής δικτύωσης από τους Gunawardena ***et al.*** (2009), σύμφωνα με τον οποίο η κοινωνική δικτύωση αποτελεί την πρακτική της επέκτασης της γνώσης μέσα από την δημιουργία συνδέσεων με άτομα με παρόμοια ενδιαφέροντα. Επομένως μέσα από τα on line κοινωνικά δίκτυα ο άνθρωπος αφενός εξυπηρετεί μια έντονη ανάγκη του και αφετέρου υλοποιεί αυτή την εξυπηρέτηση αξιοποιώντας την τεχνολογική εξέλιξη η οποία με τη σειρά της συμβαδίζει με τη δική του.

Στην εξυπηρέτηση ιδιαίτερων στοιχείων της ανθρώπινης φύσης αποδίδουν και άλλοι συγγραφείς την επιτυχία των μέσων κοινωνικής δικτύωσης, όπως της έμφυτης τάσης για σχολιασμό σε κοινωνικό επίπεδο και της ανάγκης για ψυχαγωγία (Flanagin, 2005), καθώς και της δημιουργίας κοινοτήτων εντός των οποίων οι άνθρωποι θα ανταλλάξουν ιδέες και θα αναπτυχθούν εξυπηρετώντας τις ανάγκες της κοινωνικής αναζήτησης και της κοινωνικής περιήγησης (Lampe, Ellison and Steinfield, 2006).

3.3 Μέσα κοινωνικής δικτύωσης

Στη συνέχεια γίνεται μια συνοπτική καταγραφή των μέσων κοινωνικής δικτύωσης έτσι ώστε να σκιαγραφηθεί μια συνοπτική εικόνα της υφιστάμενης κατάστασης και του βαθμού αποδοχής – συμμετοχής αυτή στη συνήθη καθημερινή δραστηριότητα (Κουτσογιαννοπούλου, 2013; Καραντινάκη, 2015).

Wikis

Πρόκειται για συνεργατικές ιστοσελίδες (οι οποίες πήραν την ονομασία τους από το γνωστότερο μέλος της ομάδας, τη γνωστή Wikipedia), με τον κάθε χρήστη να μπορεί στα πλαίσια συνεργασίας με τους υπόλοιπους να τροποποιεί το περιεχόμενό της. Σημαντικό στοιχείο είναι ότι υφίσταται σύστημα ασφαλείας – επαναφοράς στην πρότερη κατάσταση, έτσι ώστε να αποφεύγονται λανθασμένες, κακόβουλες ή αναποτελεσματικές συμμετοχές (Chao, 2007).

Ιστολόγια (blogs)

Από τον Richardson (2010) ορίζονται ως σύνολα από σκέψεις και συζητήσεις που σε πολλές περιπτώσεις, ανανεώνονται με μεγάλη συχνότητα και κάνουν τους αναγνώστες να αναμιγνύονται με ιδέες, ερωτήσεις και συνδέσμους, ζητώντας τους να σκεφτούν και να απαντήσουν σε διάφορα posts (άρθρα – καταχωρήσεις που αναρτώνται). Η τυπική δομή ενός blog (στην απλή μορφή του) περιλαμβάνει τον τίτλο, μια σύντομη περιγραφή και δύο λίστες πληροφοριών, αυτές των καταχωρήσεων και των αντίστοιχων υπερσυνδέσεων. Θα πρέπει να αναφερθεί πως το συγκεκριμένο μέσο κοινωνικής δικτύωσης έχει κατοχυρωθεί νομικά μέσω του Ν. 2121/93 τόσο ως προς το περιεχόμενό του όσο και ως προς την προστασία της

πνευματικής ιδιοκτησίας του περιεχομένου που το αφορά (γεγονός ιδιαίτερα σημαντικό αν αναλογιστεί κανείς την πληθώρα των σχετικών αναρτήσεων και τη διεκδίκηση της «πατρότητας» μιας ανάρτησης) (Deuze, 2003; Καραμπάσης, 2008; Wikipedia, 2017a)

Ιστοσελίδες Κοινωνικής Δικτύωσης

- Facebook: Πρόκειται για μια online κοινότητα κοινωνικής δικτύωσης η οποία έχει γνωρίσει εξαιρετική αποδοχή. Σε αυτή μπορεί ο κάθε χρήστης - μέλος της κοινότητας μπορεί να χρησιμοποιήσει ηλεκτρονικούς πίνακες ανακοινώσεων, άμεσα μηνύματα, ηλεκτρονικό ταχυδρομείο αλλά και υποβολή βίντεο και εικόνας προκειμένου να μοιραστεί με τα υπόλοιπα μέλη της κοινότητας τις πληροφορίες που επιθυμεί. Ιδρύθηκε το 2004, με την αρχική του μορφή να προορίζεται για τους φοιτητές στο Πανεπιστήμιο του Χάρβαρντ, ως μέσο κοινωνικής δικτύωσης.

Εικόνα 4: Ιστοσελίδα εισαγωγής στο μέσο κοινωνικής δικτύωσης Facebook

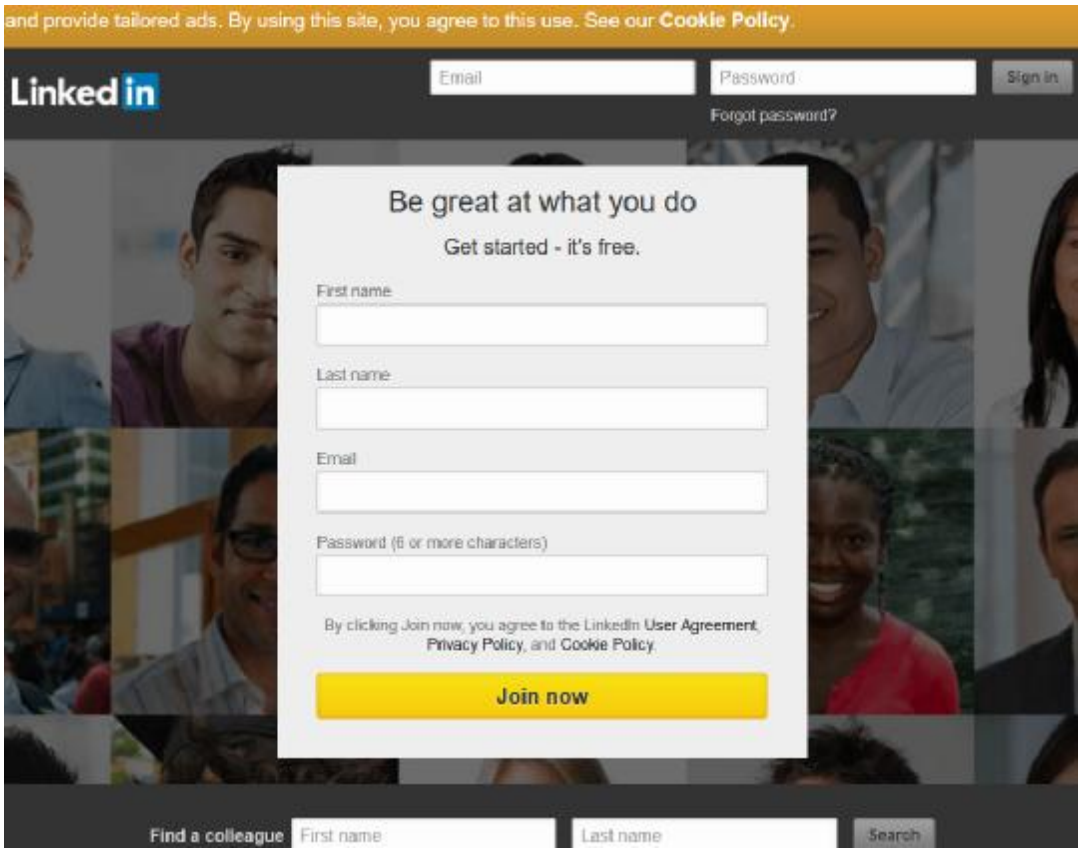
- Myspace: Το συγκεκριμένο site κοινωνικής δικτύωσης δημιουργήθηκε τον Ιούνιο του 2006 στις ΗΠΑ και η διαφοροποίησή του σε σχέση με το Facebook είναι ο προσανατολισμός του στη μουσική. Καινοτομία του αποτέλεσε η χρήση των «Moods» (ή Διαθέσεων), μικρών emoticons που χρησιμοποιούνται για να απεικονίσουν μια διάθεση του χρήστη (Κατεργιαννάκης, 2012)

Εικόνα 5: Ιστοσελίδα εισαγωγής στο μέσο κοινωνικής δικτύωσης **Myspace**

- Twitter: Εγκαινιάστηκε επίσημα τον Οκτώβριο του 2006 από την Obvious Corp. Αποτελεί τη δημοφιλέστερη microblogging εφαρμογή, όπου με τον όρο microblogging περιγράφεται μια τεχνολογία Web 2.0 που αφήνει τους χρήστες να δημοσιεύουν online σύντομες ενημερώσεις κειμένου (συνήθως λιγότερο από 140-200 χαρακτήρες).

Εικόνα 6: Ιστοσελίδα εισαγωγής στο μέσο κοινωνικής δικτύωσης **Twitter**

- LinkedIn: Πρόκειται για ακόμα ένα site κοινωνικής δικτύωσης, με τη βασική του ιδιότητα να έγκειται στο ότι αφορά στις επιχειρήσεις και στη στελέχωσή τους. Ξεκίνησε το Μάιο του 2003, με βασικό στόχο την εξεύρεση της επιθυμητής θέσης εργασίας, μέσω ανταλλαγής και διάθεσης όσον πληροφοριών σχετίζονται με τη συγκεκριμένη διαδικασία (βιογραφικό, συστάσεις κτλ.).



Εικόνα 7: Ιστοσελίδα εισαγωγής στο μέσο κοινωνικής δικτύωσης LinkedIn

Εφαρμογές Τηλεδιάσκεψης

Η δημοφιλέστερη εφαρμογή τηλεδιάσκεψης είναι το Skype η οποία χρησιμοποιεί τεχνολογία VoIP και επιτρέπει την πραγματοποίηση τηλεδιάσκεψης μεταξύ δύο ή περισσότερων ατόμων.

Forum

Πρόκειται ουσιαστικά για έναν on-line πίνακα ανακοινώσεων, στον οποίο μπορούν τα μέλη της διαδικτυακής αυτής κοινότητας να αναρτούν σχόλια, απόψεις, σημειώσεις, δημιουργώντας έναν τόπο ανταλλαγής ιδεών επί διάφορων θεμάτων

Κοινή χρήση βίντεο και εγγράφων

- YouTube: Δημιουργήθηκε το Φεβρουάριο του 2005 και τον Οκτώβριο του 2006, η εταιρεία αγοράστηκε από την Google. Στο συγκεκριμένο διαδικτυακό τόπο είναι δυνατή η ανάρτηση - μεταφόρτωση βίντεο, τα οποία στη συνέχεια παρακολουθούνται – κρίνονται και σχολιάζονται από τους χρήστες.
- Google Docs: Μέσω της συγκεκριμένης πλατφόρμας είναι δυνατή η ταυτόχρονη χρήση του συνόλου των προγραμμάτων μιας τυπικής σουίτας Office από πολλαπλούς χρήστες, επιτρέποντας τη συνεργασία σε πραγματικό ή μη χρόνο (Νεραντζίδου, 2011).

Εικονικά περιβάλλοντα

Πρόκειται για περιβάλλοντα που μιμούνται – προσομοιώνουν τον πραγματικό κόσμο, αναφερόμενα συχνά ως εικονικές κοινότητες, "virtual worlds". Σύμφωνα με τους Kaplan and Haenlein (2009) πρόκειται για υπολογιστικά προσομοιωμένα περιβάλλοντα που κατοικούνται από τρισδιάστατα avatars. Το γνωστότερο από αυτά τα περιβάλλοντα είναι το εικονικό περιβάλλον του Second Life, στο οποίο οι χρήστες φτιάχνουν ένα καινούργιο εαυτό και συμπεριφέρονται - δημιουργούν κοινωνικά δίκτυα με γνώμονα την ψηφιακή τους εικόνα, βιώνοντας ουσιαστικά μια παράλληλη πραγματικότητα.

3.3.1 Κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης

Έχουν γίνει κατά καιρούς διάφορες κατηγοριοποιήσεις των μέσων κοινωνικής δικτύωσης, χρησιμοποιώντας διαφορετικά κάθε φορά κριτήρια. Έτσι, η κατηγοριοποίηση του Zhang (2010) έχει λάβει υπόψη της το περιεχόμενο του μέσου, οδηγώντας στη διατύπωση των ακόλουθων κατηγοριών:

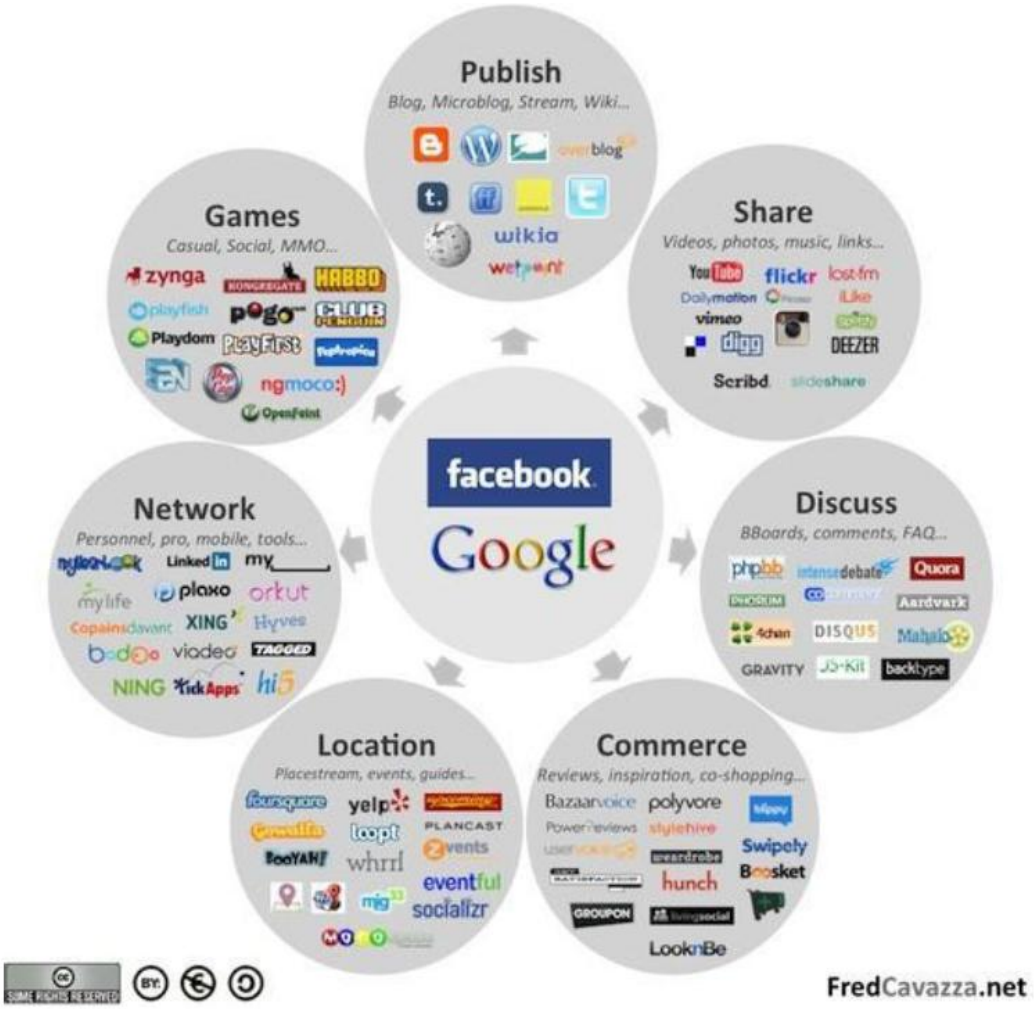
- Κοινωνικά δίκτυα ή σελίδες κοινωνικής δικτύωσης (social networks) (Facebook)
- Μέσα κοινωνικής σελιδοσήμανσης (social bookmarking) (Digg, delicious)
- Ιστοσελίδες συνεργατικής συγγραφής (collaborative authoring) (Wikipedia. Google Docs).
- Ιστοσελίδες ανταλλαγής πολυμέσων (multimedia sharing) (YouTube, Flickr)
- Ιστολόγια (blogs- micro blogging) (Blogger, Word Press, Twitter)
- Διαδικτυακές τηλεδιασκέψεις (Web conferencing) (WebEx, GoToMeeting, DimDim).

Ο Bard (2010) θέτει περισσότερα κριτήρια επί του περιεχομένου, όπως για παράδειγμα τη χρήση video και audio καθώς και τον τρόπο συμμετοχής (searching, publishing etc.), οδηγώντας τελικά σε 15 κατηγορίες μέσων κοινωνικής δικτύωσης όπως παρουσιάζονται στην ακόλουθη εικόνα

Εικόνα 8: Κατηγοριοποίηση social media κατά Bard (2010) (Κουτσογιαννοπούλου, 2013)

Τέλος, σε μια άλλη κατηγοριοποίηση (Cavazza, 2011) ως κριτήρια χρησιμοποιούνται ο βαθμός χρήσης (λόγος για τον οποίο το Facebook και η Google είναι τοποθετημένα στο κέντρο) και ο σκοπός χρήσης του δικτύου, διακρίνοντας τελικά τα social media σε 7 κατηγορίες:

- Δημοσιεύσεις (Publish): ιστολογία, wikis για παράδειγμα Twitter, Wikipedia.
- Διαμοιρασμός (Share): YouTube, Flickr. Digg.
- Συζήτηση (Discuss): forums, εργαλεία κοινωνικής αναζήτησης όπως τα 4Chan. Mahalo
- Εμπόριο (Commerce): περιλαμβάνονται λύσεις για reviews πελατών (BazaarVoice). κοινότητες συστάσεων (Polyvore) (με τη συγκεκριμένη κατηγορία να περιλαμβάνει και τη χρήση κουπονιών, με την γνωστή παλαιότερη Groupon)
- Τοποθεσία (Location):τοπικά κοινωνικά δίκτυα (Loopt). events sharing (Eventful, Patrasevents).
- Δίκτυο (Network): Hi5, My Life, Ning.
- Παιχνίδια (Games).



Εικόνα 9: Κατηγοριοποίηση social media κατά Cavazza (2011) (Cavazza, 2011)

ΚΕΦΑΛΑΙΟ 4: ΑΛΛΗΛΕΠΙΔΡΑΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΚΑΙ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

4.1 Πεδία κινδύνου και μηχανισμοί παραβίασης

4.1.1 Τεχνολογική Ανάπτυξη - Εξέλιξη

Η παραβίαση της ιδιωτικότητας η οποία εκφράζεται με έντονη ανησυχία από το κοινό το οποίο παρουσιάζει την ιδιότητα της αυξημένης συμμετοχής στα μέσα κοινωνικής δικτύωσης δεν αποτελεί απλά μια έκφραση της σχετικής αίσθησης αλλά πηγάζει άμεσα από την ύπαρξη διάφορων πεδίων κινδύνου, εντός των οποίων μπορεί να αναπτυχθεί μια δραστηριότητα που μπορεί να πλήξει την ιδιωτικότητα ενός ατόμου.

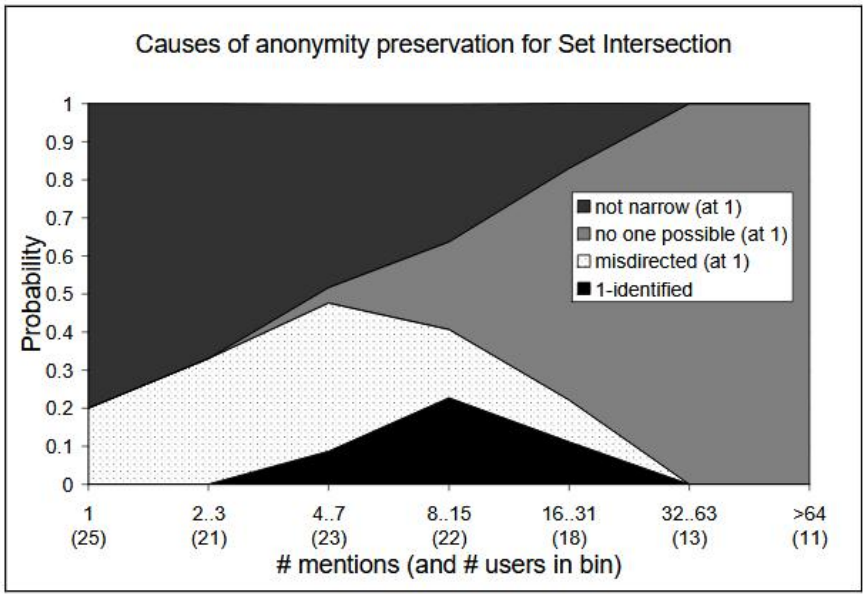
Το πρώτο και βασικό πεδίο κινδύνου όσον αφορά στη συγκεκριμένη δραστηριότητα αποτελεί το ίδιο το Διαδίκτυο και η σχετική τεχνολογική ανάπτυξη. Αυτή η τεχνολογική ανάπτυξη είχε ως συνέπεια την εμφάνιση απειλών που δεν υπήρχαν κατά την πρότερη αυτής της ανάπτυξης περίοδο.

Δύο χαρακτηριστικά επιμέρους πεδία αυτών των τεχνολογιών σύμφωνα με τους Johnson and Nissenbaum (1995), αποτελούν οι βάσεις δεδομένων και η επικοινωνία μεταξύ διαφορετικών μερών. Στην πρώτη περίπτωση η ιδιωτικότητα μπορεί να παραβιαστεί με την εκμαίευση – υποκλοπή ή μη σύμφωνη με το ίδιο το πρόσωπο χρήση προσωπικών πληροφοριών που αποθηκεύονται και ανταλλάσσονται μεταξύ των βάσεων δεδομένων. ενώ στη δεύτερη η ιδιωτικότητα μπορεί να παραβιαστεί μέσω μηχανισμών που αφορούν την ηλεκτρονική επιτήρηση, τα e-mail, την κρυπτογράφηση κ.α.

Βάσεις Δεδομένων

Η αναγκαιότητα και η ευρεία χρησιμότητα αυτών των βάσεων δεδομένων επισημαίνεται και από τους Frankowski et al. (2006), συσχετίζοντας τη λειτουργικότητα αυτών των βάσεων με την ανάγκη διάφορων οργανισμών να διατηρούν σχετικά αρχεία και δεδομένα. Οι βάσεις δεδομένων είναι απαραίτητες σε ερευνητικές ομάδες οι οποίες ενθαρρύνονται να κάνουν σύνολα δεδομένων για το κοινό, σε κοινοπραξίες για εμπορικούς σκοπούς, σε κρατικές υπηρεσίες προκειμένου να υφίστανται κάθε φορά επίσημα δεδομένα και καταγραφές για διαφορετικούς τομείς, σε επιχειρήσεις που μπορούν να αξιοποιήσουν τις σχετικές βάσεις δεδομένων είτε πρωτογενώς (για εφαρμογή δικής τους πολιτικής) είτε δευτερογενώς (πώληση των δεδομένων σε άλλες επιχειρήσεις).

Διερευνώντας στην προαναφερόμενη μελέτη (Frankowski et al., 2006) τη χρήση του Διαδικτύου ως πεδίο κινδύνου για την επανα-ταυτοποίηση ενός χρήστη που έχει δηλώσει προηγουμένως την προτίμησή του σε μια συγκεκριμένη ταινία (μέσω αναφοράς και βαθμολόγησης κατάταξης – rating) προέκυψε πως υφίσταται αυξημένη πιθανότητα επανα-ταυτοποίησης (γκρι και μαύρη περιοχή στο ακόλουθο διάγραμμα κατανομής πιθανοτήτων).



Σχήμα 1: Διάγραμμα κατανομής πιθανοτήτων επανα-ταυτοποίησης χρήστη Διαδικτύου έπειτα από δήλωση προτίμησης και βαθμολόγησης σε συγκεκριμένη ταινία ***(Frankowski et al., 2006)***

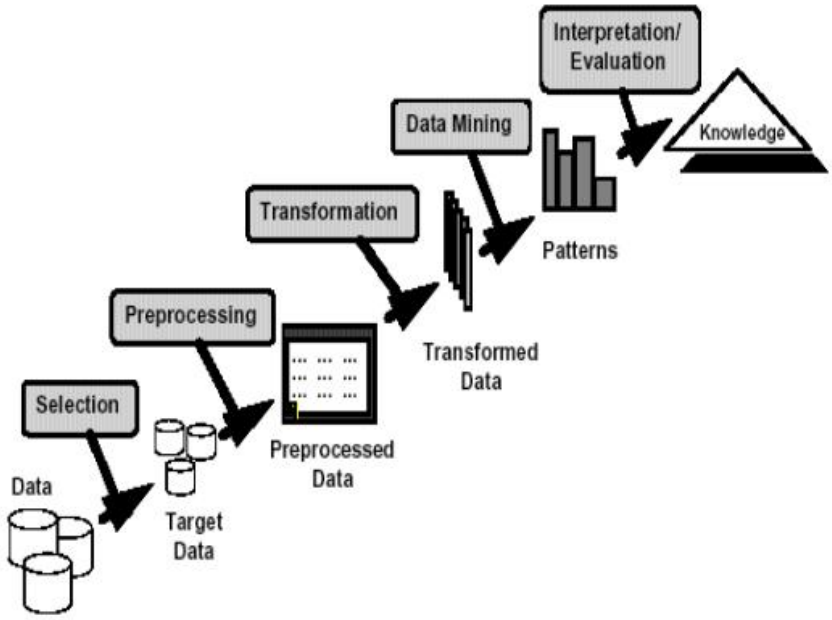
Αυτή η διαδικασία επανα-ταυτοποίησης του χρήστη και η ενδεχόμενη απειλή για την προστασία της ιδιωτικής ζωής έχει επισημανθεί εκτός της προαναφερόμενης σε πλήθος μελετών (Clarke, 1988; McCrohan, 1989; Thomas and Maurer, 1997; Culnan and Armstrong, 1999), με κοινή παράμετρο αυτών των μελετών το γεγονός της χρήσης τεχνολογιών ψηφιακών δικτύων και αποθήκευσης για την προώθηση των εκάστοτε στόχων τους.

Εντούτοις, στα πλαίσια αυξημένης εφαρμογής αυτής της πολιτικής επισημαίνεται από τους Culnan and Armstrong (1999) η ανάγκη εύρεσης ενός σημείου ισορροπίας ανάμεσα στην εφαρμογή πολιτικών αυτού του είδους και στην προστασία της ιδιωτικότητας των πελατών των επιχειρήσεων.

Εξόρυξη Δεδομένων

Η σημασία της τεχνολογικής ανάπτυξης αναδεικνύεται επίσης από τον Tavani (2005), υπό την έννοια του συνόλου των «εργαλείων» που συμμετέχουν στη διαδικασία διαχείρισης και αποθήκευσης της προσωπικής πληροφορίας. Χαρακτηριστικά, επισημαίνεται ο ρόλος της διαδικασίας της εξόρυξης δεδομένων (data mining) στη σύγχρονη επιχειρησιακή πραγματικότητα, κατά την οποία η πληροφορία βρίθει, χωρίς όμως αυτό να σημαίνει ότι είναι πάντα αξιοποιήσιμη. Ενδεικτικά αναφέρεται πως μία τυπική επιχειρησιακή βάση δεδομένων σήμερα περιέχει συχνά μεγάλο αριθμό εγγραφών (108-1012) δεδομένων πολλών διαστάσεων (10-104 μεταβλητές), με αποτέλεσμα να απαιτείται ένα «εργαλείο» αξιοποίησης αυτής της πληροφορίας (Τζιραλής, 2007).

Η εξόρυξη δεδομένων αποτελεί έναν όρο που χρησιμοποιείται για να περιγράψει το σύνολο της διαδικασίας εξόρυξης γνώσης από βάσεις δεδομένων (Knowledge Discovery in Databases), όπως παρουσιάζεται στο ακόλουθο σχήμα.



Σχήμα 2: Απεικόνιση της διαδικασίας εξόρυξης δεδομένων (Τζιραλής, 2007)

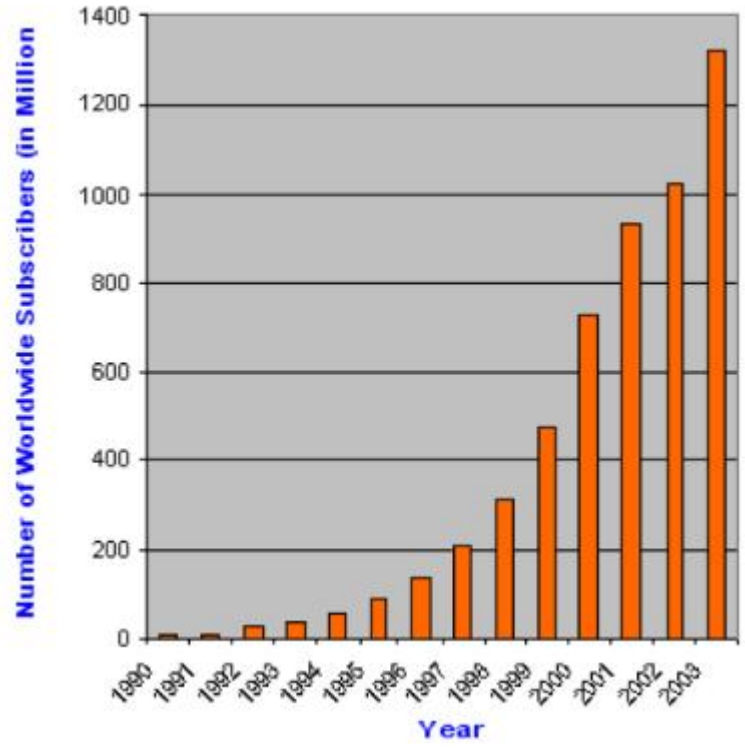
Στην εξαγόμενη γνώση συμπεριλαμβάνεται η κατανόηση μοτίβων και προτύπων, η εξαγωγή σχέσεων, οι προβλέψεις και η κατάτμηση της αγοράς σε επακριβώς καθορισμένες υποομάδες έτσι ώστε να είναι δυνατή η διαμόρφωση συγκεκριμένων ομάδων καταναλωτών.

Περιβάλλουσα νοημοσύνη και συγκλίνουσες τεχνολογίες

Ως άλλα μεθοδολογικά «εργαλεία» που μπορούν να λειτουργήσουν στη συγκεκριμένη κατεύθυνση αναφέρονται από τον Vedder (2011) η περιβάλλουσα νοημοσύνη (ambient intelligence) και οι συγκλίνουσες τεχνολογίες (converging technologies). Η περιβάλλουσα νοημοσύνη αναφέρεται στη σταδιακή ενσωμάτωση των τεχνικών μέσων και της τεχνολογίας στο περιβάλλον, βελτιώνοντας την επικοινωνία περιβάλλοντος και χρηστών και συμβαδίζοντας με εξελίξεις όπως η συνεχής μείωση του μεγέθους των υπολογιστών, των αισθητήρων και των ενεργοποιητών, η αύξηση της ικανότητας αποθήκευσης, μεταφοράς και επεξεργασίας των δεδομένων και η συνεχής βελτίωση της δικτύωσης και της ασύρματης επικοινωνίας. Οι συγκλίνουσες τεχνολογίες με τη σειρά τους αφορούν την διασταυρούμενη γονιμοποίηση μεταξύ των νανοτεχνολογιών. της βιοτεχνολογίας, των τεχνολογιών της πληροφορίας και της επικοινωνίας, καθώς και της γνωστικής επιστήμης οδηγώντας σε νέες δυνατότητες εξωτερικής παρέμβασης και επιρροής στη συμπεριφορά των ανθρώπων (Τσαγκανού, 2014). Η επιρροή στην προκειμένη περίπτωση σχετίζεται με συμπεριφορές που μπορούν να διαμορφωθούν από καταναλωτικής άποψης και από άποψης απουσίας ελέγχου των προσωπικών τους δεδομένων και της ιδιωτικότητάς τους.

Ασύρματη Δικτύωση

Μια τεχνολογική εξέλιξη με ιδιαίτερη σημασία όσον αφορά στην ενίσχυση της απειλής της ιδιωτικότητας αποτελεί η εξέλιξη της ασύρματης δικτύωσης, με τον όρο να αφορά οποιοδήποτε δίκτυο στο οποίο η επικοινωνία των χρηστών αλλά και των δομικών στοιχείων που το αποτελούν γίνεται πλήρως ή μερικώς χωρίς τη χρήση ενσύρματων μέσων, με πλήθος σχετικών τεχνολογιών (π.χ. δίκτυα IEEE 802.11, HIPERLAN/2, Bluetooth, IEEE 802.15, IEEE 802.16), δύο βασικές αρχιτεκτονικές (με σημεία πρόσβασης (infrastructure networks) και χωρίς σταθμούς βάσης (ad hoc networks)) και σημαντικά πλεονεκτήματα όπως το ότι παρουσιάζουν σημαντική ευελιξία, ότι δεν χρειάζονται καλώδια για την σύνδεση των τερματικών, ότι είναι δυνατή η κινητικότητα των χρηστών και ότι μπορούν να καλύπτουν ποικίλες ανάγκες δικτύωσης (Παπαπέτρου, 2017). Η ανάπτυξη της ασύρματης δικτύωσης και κατ' αντιστοιχία η προαναφερόμενη ενίσχυση της απειλής της ιδιωτικότητας είναι εμφανής στο ακόλουθο διάγραμμα, με την εξέλιξη να λαμβάνει χώρα με ραγδαίους ρυθμούς (με το παράδειγμα να αφορά μόνο τα κυψελοειδή συστήματα).



Σχήμα 3: Ανάπτυξη ασύρματης δικτύωσης (κυψελοειδή συστήματα) για την περίοδο 1990-2003 (Παπαπέτρου, 2017)

Η συγκεκριμένη μάλιστα ανάπτυξη, λαμβάνοντας υπόψη το γεγονός ότι καθιστά πλέον κατά πολύ ευκολότερες διαδικασίες όπως η συγχώνευση βάσεων δεδομένων, ενδυναμώνει εξ ορισμού την ανάπτυξη των κοινωνικών δικτύων, οδηγώντας σε υπερεπέκταση τις ηλεκτρονικές αλληλεπιδράσεις των διαδικτυακών ταυτοτήτων. Από τον Clarke (1988) επισημαίνεται μάλιστα πως οι ηλεκτρονικές διαμεσολαβήσεις της προσωπικής ταυτότητας μπορούν να γίνουν τόσο

εκτεταμένες που θα οδηγήσουν στην ανάδυση μιας «ψηφιακής προσωπικότητας» ως αναπόσπαστο μέρος της κατασκευής του κοινωνικού ατόμου.

Σε περισσότερο εξειδικευμένο επίπεδο όσον αφορά σε τεχνολογικά «εργαλεία» και μεθόδους που συμβάλλουν στην αύξηση της πιθανότητας προσβολής – παραβίασης της ιδιωτικότητας του ατόμου μέσα από τα κοινωνικά δίκτυα μπορούν να αναφερθούν τα εξής (Τσαγκανού, 2014):

Χρήση καρτών
Η χρήση καρτών για τις αγορές από καταστήματα λιανικής πώλησης, με τις πληροφορίες που λαμβάνονται από τις εταιρίες να αφορούν αγοραστικές συνήθειες καθώς και προσωπικές προτιμήσεις, να μπορούν να αξιοποιηθούν σε διαδικασίες στοχευμένου μάρκετινγκ.

Τα διαδικτυακά Cookies
Επιτρέπουν σε on line επιχειρήσεις και ιδιοκτήτες ιστοσελίδων να αποθηκεύουν και να ανακτούν πληροφορίες σχετικά με τους χρήστες που επισκέπτονται τις τοποθεσίες τους, με τις πληροφορίες αυτές να ανακτώνται και να «επιστρατεύονται» την επόμενη φορά που ο χρήστης θα αποκτήσει πρόσβαση στη συγκεκριμένη ή αντίστοιχη ιστοσελίδα (Τσαγκανού, 2014). Σε νομικό επίπεδο, η χρήση τους διέπεται από το άρθρο 4 παρ. 5 του ν. 3471/2006 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, ο οποίος ενσωματώνει την Οδηγία 2002/58/ΕΚ, μετά και την τροποποίηση του από το ν. 4070/2012, με τον οποίο ενσωματώθηκαν και οι τροποποιήσεις της Οδηγίας 2002/58/ΕΚ που πραγματοποιήθηκαν με την Οδηγία 2009/136/ΕΚ. Η συγκεκριμένη μάλιστα αναφορά έχει ως εξής: «η αποθήκευση πληροφοριών ή η απόκτηση πρόσβασης σε ήδη αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό συνδρομητή ή χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος συνδρομητής ή χρήστης έχει δώσει τη συγκατάθεση του μετά από σαφή και εκτενή ενημέρωση κατά την παρ. 1 του άρθρου 11 του ν. 2472/1997, όπως ισχύει. Η συγκατάθεση του συνδρομητή ή χρήστη μπορεί να δίδεται μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2016). Χαρακτηριστικό παράδειγμα αυτής της ενημέρωσης αποτελεί η εμφάνιση του σχετικού μηνύματος στην εικόνα της ιστοσελίδας εισαγωγής στο μέσο κοινωνικής δικτύωσης Twitter (αντίστοιχη προηγούμενη εικόνα).

Μηχανές αναζήτησης
Αποτελούν τη συχνότερα χρησιμοποιούμενη είσοδο στο διαδίκτυο αφού εξυπηρετούν την ανάγκη των χρηστών ως προς την εξεύρεση της αναζητούμενης κάθε φορά πληροφορίας. Αποτελούνται από μια ή περισσότερες βάσεις δεδομένων, το λογισμικό διαχείρισης αυτών των βάσεων και μια διεπαφή (interface) αλληλεπίδρασης με το χρήστη (Σεργκενλίδη, 2014). Ενδεικτικά στοιχεία της χρήσης των μηχανών αναζήτησης προς τη συγκεκριμένη κατεύθυνση είναι οι φόρμες που κατά καιρούς ζητείται από τους χρήστες να συμπληρωθούν με προσωπικά τους στοιχεία όταν επισκέπτονται μια ιστοσελίδα επιχείρησης ή οργανισμού, τα οποία στη συνέχεια και με αυτοματοποιημένο τρόπο μπορούν να χρησιμοποιηθούν.

Λογισμικά ανάκτησης

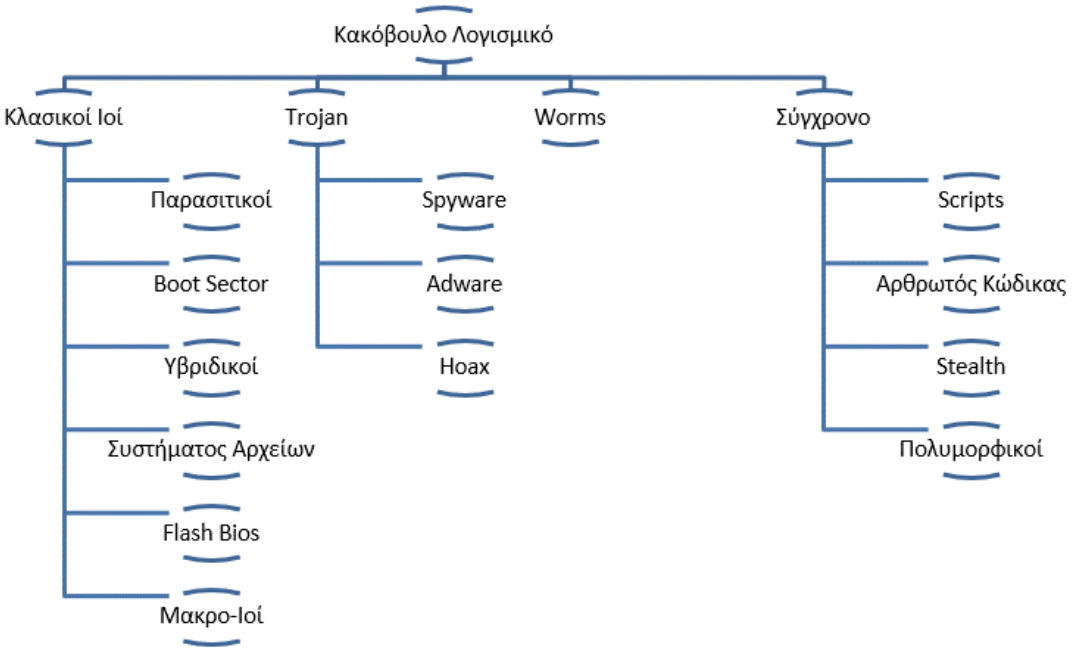
Λογισμικά που σχετίζονται με έγγραφα, αρχεία, μηνύματα ηλεκτρονικού ταχυδρομείου, ευαίσθητα προσωπικά δεδομένα και την ανάκτησή τους ακόμα και μετά τη διαγραφή τους. Το ζητούμενο στην προκειμένη περίπτωση είναι τέτοιου είδους διαδικασίες να γίνονται από εξουσιοδοτημένα άτομα έτσι ώστε να εξασφαλίζεται η προστασία της ιδιωτικότητας. Σε διαφορετική περίπτωση, είναι πιθανό να πραγματοποιηθούν κακόβουλες ή λανθασμένες ενέργειες και να παραβιαστεί η ιδιωτικότητα των χρηστών που σχετίζονται με τις αντίστοιχες βάσεις δεδομένων.

Υπηρεσίες σύννεφου

Οι συγκεκριμένες υπηρεσίες (οι οποίες είναι γνωστές με τον όρο Cloud Services), αφορούν σε υπηρεσίες με τις οποίες παρέχεται η δυνατότητα αποθήκευσης και διαχείρισης δεδομένων σε servers τρίτων κατασκευαστών, παρά τοπικά στον υπολογιστή (iCloud. Dropbox, Google Drive, OneDrive, κλπ.), με τα δεδομένα αυτά να περιλαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου, επαφές, φωτογραφίες, έγγραφα, μουσική και αρχεία διάφορων εφαρμογών τα οποία μπορούν να διαμοιράζονται μεταξύ διαφορετικών χρηστών. Βασικά πλεονεκτήματα των συγκεκριμένων υπηρεσιών είναι η ευκολία χρήσης, το μηδενικό ή πολύ μικρό κόστος, ο μεγάλος αποθηκευτικός χώρος που προσφέρουν και κυρίως η προσβασιμότητα χωρίς χρονικούς και γεωγραφικούς περιορισμούς. Ενδεικτική της ευρύτητας χρήσης τους είναι η ποικιλία των προσφερόμενων λύσεων από διάφορες εταιρίες τεχνολογίας, μεγάλου ή μικρότερου μεγέθους (Apple, Google, Microsoft, DropBox, SugarSync, Box κ.α.) (Ρήγας, 2014). Ζητήματα ασφαλείας όσον αφορά στις συγκεκριμένες παρεχόμενες υπηρεσίες έχουν τεθεί κατά καιρούς, με τα ζητήματα αυτά να εντοπίζονται σε διαφορετικά πεδία, όπως τα μέρη τα οποία έχουν πρόσβαση στα δεδομένα (με τον κίνδυνο να μεγιστοποιείται σε περιπτώσεις ανάθεσης υπηρεσιών σε τρίτους – outsourcing), ενδεχόμενες κυβερνοεπιθέσεις, απειλές εκ των έσω, κυβερνητικές υπηρεσίες, ελλιπή πρότυπα ασφάλειας αλλά και ελλιπή εξυπηρέτηση (π.χ αδυναμία απευθείας επικοινωνίας με κάποιο τεχνικό) (Tic Tac Laboratories, 2012).

Κακόβουλο Λογισμικό

Με το συγκεκριμένο όρο αποδίδεται μια ολόκληρη κατηγορία λογισμικού – ομάδας προγραμμάτων, τα οποία σύμφωνα με τον Cohen (1985) έχουν ως στόχο «να μολύνουν άλλα προγράμματα τροποποιώντας τον κώδικα τους ώστε να περιλαμβάνουν μια έκδοση του εαυτού τους». Υφίστανται διάφορα είδη τέτοιου λογισμικού καθώς και ποικιλία της στρατηγικής τους δράσης. Αποτελεί μια βασική παράμετρο της διαδικασίας ασφαλείας όσον αφορά στην προστασία της ιδιωτικότητας εντός των μέσων κοινωνικής δικτύωσης, αφού η διακίνησή του μέσω των συγκεκριμένων μέσων είναι ιδιαίτερα εύκολη. Μια συνοπτική εικόνα των υφιστάμενων ειδών είναι αυτή που ακολουθεί



Σχήμα 4: Διαφορετικά είδη κακόβουλου λογισμικού (Τσακνάκης, 2014)

Στη συνέχεια γίνεται μια συνοπτική παρουσίαση αυτών των ειδών (Ιόνιο Πανεπιστήμιο, 2007; Βλάχος, 2011; Τσακνάκης, 2014):

- Παρασιτικοί Ιοί: Δρουν μέσω του μηχανισμού της προσάρτησης (στην αρχή ή στο τέλος άλλων προγραμμάτων), παρουσιάζοντας σήμερα μειωμένη αποτελεσματικότητα.
- Ιοί boot sector: Δρουν στον τομέα εκκίνησης του υπολογιστή (όπως η περιοχή MBR (Master Boot Record) σε περιπτώσεις που υφίστανται κατατμημένες περιοχές του δίσκου (partitions), με το σύγχρονο δυναμικό τους να είναι περιορισμένο εξαιτίας περιορισμένης χρήσης εξωτερικών μέσων εκκίνησης.
- Υβριδικοί Ιοί: Αποτελούν το συνδυασμό των προαναφερόμενων ειδών, με αποτέλεσμα να παρουσιάζουν αυξημένη αποτελεσματικότητα. Γνωστός ιός του συγκεκριμένου είδους αποτελεί ο ιός Melissa (1999) ο οποίος σε πρώτη φάση μόλυνε το word template του χρήστη και σε δεύτερη αυτοπολλαπλασιαζόταν με την αυτοαποστολή του στις πρώτες 50 διευθύνσεις του βιβλίου διευθύνσεων του χρήστη.
- Ιοί Συστήματος Αρχείων: Δρουν μέσω του πίνακα FAT του συστήματος, με αποτέλεσμα να παρουσιάζει αυξημένο μολυσματικό δυναμικό.
- Ιοί Flash Bios: Στοχεύοντας στο πρόγραμμα BIOS της μητρικής μπορούν να προσβάλλουν τη μνήμη ROM της μητρικής, με αποτέλεσμα σε πολλές περιπτώσεις να απαιτείται αντικατάσταση τμήματος hardware (π.χ. ο ιός Chernobyl (1999) η δράση του οποίου οδηγούσε στην αναγκαία αντικατάσταση του chip της μητρικής πλακέτας του υπολογιστή - motherboard).
- Μακρο-Ιοί: Το πεδίο δράσης τους αποτελούν αρχεία που περιέχουν μακροεντολές (macros). Λαμβάνοντας υπόψη την ευρεία χρήση των μακροεντολών, σε καθημερινές εφαρμογές (όπως π.χ. η σουίτα Office),

γίνεται αντιληπτό πως οι συγκεκριμένοι ιοί απαιτούν ιδιαίτερη προσοχή ως προς τη διαχείριση - αντιμετώπισή τους.

- Worms: Το βασικό χαρακτηριστικό του συγκεκριμένου είδους είναι η αυτονομία του, με αποτέλεσμα να μην απαιτείται φορέας - ξενιστής για να «φιλοξενήσει» παρασιτική δράση. Περιλαμβάνουν ενσωματωμένο κώδικα και πολλαπλασιάζονται με τη χρήση του δικτύου, με βασική στρατηγική δράσης τη δέσμευση μνήμης μεγαλύτερου μεγέθους από αυτό που πραγματικά απαιτεί η εκάστοτε μεταβλητή εισόδου, επιτρέποντας έτσι τον πολλαπλασιασμό και την αντιγραφή σε γειτονικές θέσεις (χαρακτηριστικά παραδείγματα αποτελούν ο ιός Blaster, η επίθεση του οποίου έπληξε ταυτόχρονα μεγάλο αριθμό υπολογιστών της Microsoft (330.000 υπολογιστές, 11/08/2003), με την αντιμετώπισή του να απαιτεί την αλλαγή των διευθύνσεων των διακομιστών της εταιρείας και ο ιός I love you (Μάιος 2000)). Η αντιμετώπιση της συγκεκριμένης κατηγορίας ιών είναι δυναμική και απαιτεί την τακτική ενημέρωση των λογισμικών ασφαλείας των υπολογιστών των χρηστών.
- Δούρειοι Ίπποι (Trojan Horses): Αποτελούν το συχνότερα χρησιμοποιούμενο είδος ιών, με την ονομασία του να μαρτυρά τον τρόπο δράσης του. Ο τρόπος αυτός συνίσταται στην είσοδο του ιού μέσω της κάλυψής του με τη μορφή ενός χρήσιμου προγράμματος.
- Spyware: Αποτελεί μια ιδιαίτερα επικίνδυνη μορφή ιών αφού μπορεί να οδηγήσει στην υποκλοπή κρίσιμων προσωπικών δεδομένων (π.χ. κωδικοί χρήσης και συναλλαγών). Χαρακτηριστικό παράδειγμα αποτελούν οι συχνά παλαιότερα χρησιμοποιούμενοι dialers που ευθύνονταν για υπέρογκες χρεώσεις κλήσεων.
- Adware (advertising-supported software): Συνδυάζεται συχνά με το προαναφερόμενο είδος με απώτερο σκοπό τη δημιουργία μιας mailing list από τα υποκλεπτόμενα κάθε φορά στοιχεία, με βάση μηχανισμούς όπως η αλλαγή της αρχικής σελίδας του browser (browser hijacking), η λανθασμένη αναδρομολόγηση (web spoofing) κ.α.
- Hoax: Αποτελεί έναν ιό που βασίζεται σε «ψευδείς» προειδοποιήσεις που προτρέπουν το χρήστη να κάνει ενέργειες που δήθεν απαιτούνται για την προστασία του συστήματός του (χαρακτηριστικό παράδειγμα αποτελεί ο ιός της αστυνομίας που προέτρεπε τους χρήστες να καταβάλουν συγκεκριμένο ποσό ως πρόστιμο σε συγκεκριμένο λογαριασμό για να «ξεκλειδώσει» ο υπολογιστής τους).
- Γλώσσες Συγγραφής σεναρίων (scripting languages): Ο μηχανισμός δράσης του στηρίζεται στην εκτέλεση κινητού κώδικα (από τη μεριά του client) όπως Javascript, Java Applets και ActiveX.
- Αρθρωτός Κώδικας: Στην προκειμένη περίπτωση η προσάρτηση μπορεί να γίνει όχι μόνο στην αρχή ή στο τέλος αλλά και στο μέσο ενός προγράμματος κάλυψης, αφού το συνολικό πρόγραμμα αποτελείται από ανεξάρτητα τμήματα (components) κώδικα τα οποία θα πρέπει να συνενωθούν για την τελική λειτουργία του ενιαίου προγράμματος (π.χ. dynamic link libraries, plug - in).
- Ιοί Stealth: Η ανάπτυξη τους έγινε προκειμένου να ξεπεραστεί η δράση των λογισμικών antivirus σε ενδεχόμενους ελέγχους ελέγχου ακεραιότητας ενός προγράμματος, με τον ιό να επιστρέφει μη ανιχνεύσιμη από το antivirus έκδοση του εκάστοτε αρχείου, με σύνηθες πεδίο δράσης τον πυρήνα Kernel.

- Πολυμορφικοί Ιοί: Πρόκειται για ιούς οι οποίοι βασίζονται στη λήψη διαφορετικών μορφών μέσω τεχνικών συμπίεσης, κρυπτογράφησης ή εισαγωγής «θορύβου», προκειμένου να «ξεγελάσει» το εκάστοτε antivirus (χαρακτηριστικό παράδειγμα της κατηγορίας αποτελούν οι ρουτίνες μετάλλαξης - Mutation Engines).

Όπως γίνεται αντιληπτό από την παραπάνω επισκόπηση, υφίσταται πλήθος μορφής ιών αλλά και στρατηγικών δράσης τους, παρουσιάζοντας έτσι αυξημένο δυναμικό και δυνατότητα χρήσης τους από επίδοξους παραβάτες της ιδιωτικότητας εντός των μέσων κοινωνικής δικτύωσης.

4.1.2 Σύγχρονες επιχειρησιακές τάσεις

Δεν πρέπει να παραβλεφθεί η σύγχρονη τάση των επιχειρήσεων για συλλογή διαδικτυακών δεδομένων που σχετίζονται με τις προτιμήσεις των καταναλωτών προκειμένου να εφαρμόσουν πολιτικές διαδικτυακού - ψηφιακού μάρκετινγκ. Τέτοιου είδους πολιτικές έχουν ως βασική προϋπόθεση για την αποδοτική εφαρμογή τους, τη χρήση πληροφοριών που σχετίζονται κατά το δυνατό αμεσότερα με τον εκάστοτε καταναλωτή (με συνεπαγόμενο τον αυξημένο κίνδυνο παραβίασης της ιδιωτικότητας). Υφίσταται πλήθος πολιτικών οι οποίες μπορούν να ενταχθούν στη συγκεκριμένη κατηγορία, δείγμα της ισχύος αυτής της τάσης και επομένως της αξίας του πληροφοριακού περιεχομένου που μπορεί να σχετίζεται με την ιδιωτικότητα του υποψήφιου καταναλωτή. Έτσι, στη συγκεκριμένη κατηγορία πολιτικών μπορούν να ενταχθούν (Σεργκενλίδη, 2014):

- το Content Ad, διαφήμιση που εμφανίζεται κεντρικά στην ιστοσελίδα, προσαρμοσμένη με συνάφεια στο περιεχόμενο της ιστοσελίδας προκειμένου να επιτευχθούν μεγαλύτερα ποσοστά ανταπόκρισης (Βλάχος και Δρόσος, 2004),
- το IP Targeting, το οποίο παρέχει τη δυνατότητα αναγνώρισης της προέλευσης του χρήστη βάσει της διεύθυνσης IP αξιοποιώντας τις δυνατότητες του Domain Name System (DNS), βασίζοντας έτσι τη στόχευση σε γεωγραφικά κριτήρια,
- το email marketing, το οποίο βασίζεται σε αποστολή μηνύματος σε μεγάλη βάση δεδομένων με δυνατότητες υψηλής στόχευσης (με συνηθέστερο στοιχείο που χρησιμοποιείται στη συγκεκριμένη διαδικασία να είναι το γνωστό newsletter (Perlman, 2009)),
- οι διαδικασίες βελτιστοποίησης των μηχανών αναζήτησης (Search engine optimization - SEO), με το συγκεκριμένο όρο να περιγράφει το σύνολο των τεχνικών που χρησιμοποιούνται για να ενισχύσουν την κατάταξη ενός ιστότοπου στα αποτελέσματα μιας αναζήτησης, με βασικά αναγκαία στοιχεία την κατανόηση των προσδοκιών και τη χρήση των σωστών keywords,
- το Διαδικτυακό μάρκετινγκ, ευρέως γνωστό ως SEM (Search Engine Marketing), το οποίο μπορεί να βελτιώσει την ορατότητα της ιστοσελίδας μιας επιχείρησης στις μηχανές αναζήτησης ώστε να αυξηθεί η επισκεψιμότητα της, με γνωστότερες μεθόδους εφαρμογής το PPC (pay-per-click) (σύμφωνα με την οποία όταν ένας χρήστης κάνει «κλικ» στη διαφήμιση ο διαφημιζόμενος θα πρέπει να καταβάλει τα συμφωνημένα

έξοδα διαφήμισης) και το CPM (cost per mile) όπου ο διαφημιζόμενος χρεώνεται ένα συμφωνημένο ποσό ανά χίλιες εμφανίσεις της διαφήμισης του,

- τα online streaming video τα οποία απευθύνονται κυρίως σε νεανικό κοινό (Vukasovič, 2013),
- ο γενικότερος προσανατολισμός προς την πολιτική του "content marketing", η οποία βασίζεται στο γεγονός ότι οι πολίτες σήμερα έχουν ανάγκη να ενημερωθούν ουσιαστικά και σε βάθος, λαμβάνοντας χρήσιμες και αντικειμενικές πληροφορίες απαλλαγμένοι από προσκολλήσεις σε συγκεκριμένα brand names,
- το Native Advertising το οποίο αποτελεί βασικό τομέα του Content Marketing και εστιάζει στην οικοδόμηση σχέσεων και εμπιστοσύνης με υποψήφιους πελάτες. Παραδείγματα της συγκεκριμένης πολιτικής είναι ένα προωθημένο tweet στο Twitter, ένα άρθρο που προτείνεται στο Facebook κάποια σελίδα που βρίσκεται ανάμεσα σε άρθρα στο Flipboard, μια διαφήμιση στο Google κ.α. (Κερασιώτης, 2014).

Μπορεί επομένως να παρατηρηθεί πως υφίσταται πλήθος πολιτικών που μπορούν να αξιοποιήσουν την προσωπική πληροφορία στα πλαίσια μιας επιχειρησιακής δραστηριότητας, καθιστώντας έτσι την παραβίαση της ιδιωτικότητας μια «ελκυστική» δράση για πολλούς και διαφορετικούς λόγους.

4.2 Περιπτώσεις παραβίασης της ιδιωτικότητας

Το μέγεθος του φαινομένου και η παραβίαση της ιδιωτικότητας αποτελεί ένα φαινόμενο η συχνότητα και η ένταση του οποίου επιβεβαιώνεται όχι μόνο από σχετικά στατιστικά στοιχεία αλλά και από αντίστοιχα περιστατικά. Στην παρούσα ενότητα γίνεται μια σύντομη ενδεικτική και ασφαλώς όχι εξαντλητική παρουσίαση περιστατικών αυτού του είδους, προκειμένου να σχηματιστεί μια ευρύτερη και σαφή εικόνα για την ύπαρξη και την ένταση του φαινομένου.

Απόφαση 1/2015 Αρχής Προστασίας Προσωπικών Δεδομένων
Σε διενέργεια σχετικού ελέγχου της Δίωξης Ηλεκτρονικού Εγκλήματος με τη συνδρομή της Αρχής σε εταιρεία που δραστηριοποιείται στον τομέα της εμπορίας δεδομένων προσωπικού χαρακτήρα, διαπιστώθηκε ότι κατείχε μεγάλο όγκο δεδομένων συνδρομητών παρόχου υπηρεσιών ηλεκτρονικής επικοινωνίας. Τα δεδομένα αφορούσαν την περίοδο 2008-2010 και πάνω από 8.000.000 συνδρομητές, περιλαμβάνοντας μεν στοιχεία που είναι ανακοινώσιμα σε καταλόγους (είναι δηλαδή δυνατή η εύρεσή τους από δημόσια προσβάσιμη πηγή) αλλά και στοιχεία μη ανακοινώσιμα σε καταλόγους (όπως π.χ. ο ΑΦΜ). Αξιοσημείωτο είναι το γεγονός ότι σε πάνω από 350.000 περιπτώσεις ο συνδρομητής είχε ρητά ζητήσει από τον πάροχο να μην περιλαμβάνονται τα στοιχεία του σε καταλόγους καθώς και ότι υφίσταται διασταύρωση με άλλα δεδομένα (διαφορετικής προέλευσης) προκειμένου να σχηματιστεί μια περισσότερο ολοκληρωμένη και «αξιοποιήσιμη» βάση δεδομένων. Λαμβάνοντας υπόψη ότι θα έπρεπε από τον πάροχο να έχουν εφαρμοστεί μέτρα ασφάλειας που

θα απέτρεπαν τη μαζική εξαγωγή δεδομένων από τις βάσεις δεδομένων των συστημάτων του, αποφασίστηκε ότι έλαβε χώρα παραβίαση των προσωπικών δεδομένων των συνδρομητών και επιδικάστηκε στον πάροχο πρόστιμο ύψους 60.000 ευρώ.

Απόφαση 86/2015 Αρχής Προστασίας Προσωπικών Δεδομένων
Μετά από σχετική καταγγελία εξετάστηκε η νομιμότητα της διαδικασίας ηχογράφησης των εισερχόμενων κλήσεων στο τμήμα εξυπηρέτησης πελατών, της ακρόασης αυτών, σε πραγματικό χρόνο, από τους προϊσταμένους του τμήματος και της εξ αποστάσεως πρόσβασης στα συστήματα της εταιρίας από συνεργαζόμενες τρίτες εταιρείες. Όσον αφορά στη καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης, αποδόθηκε ιδιαίτερη σημασία στην ύπαρξη ηχογραφημένης ειδοποίησης πριν από την έναρξη της τηλεφωνικής συνδιάλεξης που πρόκειται να καταγραφεί, οδηγώντας στο συμπέρασμα πως η παραπάνω διαδικασία αποτελεί νόμιμη επαγγελματική πρακτική. Επίσης, τα δεδομένα που προέκυψαν χρησιμοποιήθηκαν από την εταιρία για στατιστικούς και μόνο λόγους. Όσον αφορά στην ενέργεια των προϊσταμένων του τμήματος (ακρόαση σε πραγματικό χρόνο), δεν θεωρήθηκε παράνομη πρακτική αφού εντάχθηκε στη σχέση μεταξύ συνδρομητή και εταιρίας και στη μη μεταβολή της (ούτε όσον αφορά στους πελάτες της εταιρίας ούτε όσον αφορά στους εργαζόμενους της εταιρίας και σε ενδεχόμενη διαδικασία επιτήρησής τους). Εντούτοις, ως προς τη δεύτερη περίπτωση έγινε σύσταση για σαφέστερη ενημέρωση των εργαζομένων σχετικά με τη συγκεκριμένη επιτήρηση. Τέλος, όσον αφορά στην τρίτη παράμετρο της υπόθεσης, την εξ αποστάσεως επεξεργασία δεδομένων από συνεργαζόμενες τρίτες εταιρίες, δεν προέκυψε παραβίαση, αρκεί να τηρούνται τα προβλεπόμενα στο άρθρο 10 του ν. 2472/1997 για το απόρρητο και την ασφάλεια.

Αποφάσεις 26, 38 και 72/2015 Αρχής Προστασίας Προσωπικών Δεδομένων
Οι συγκεκριμένες αποφάσεις αφορούσαν υποθέσεις καταγγελιών σχετικά με αζήτητα μηνύματα ηλεκτρονικού ταχυδρομείου (spam) για το σκοπό της προώθησης προϊόντων και υπηρεσιών από τρίτους. Στις εξεταζόμενες περιπτώσεις καταγράφηκε παράνομη συλλογή και περαιτέρω επεξεργασία προσωπικών δεδομένων κατά παράβαση του άρθρου 4 ν. 2472/1997 και του άρθρου 11 παρ. 1 του ν. 3471/2006. Αναλυτικότερα, οι εν λόγω εταιρίες διατηρούσαν λίστες με διευθύνσεις ηλεκτρονικού ταχυδρομείου οι οποίες χρησιμοποιήθηκαν για την αποστολή διαφημιστικών μηνυμάτων, ενώ ήρθαν στην κατοχή τους με διάφορους τρόπους (π.χ. χρήση λογισμικού συλλογής διευθύνσεων ηλεκτρονικού ταχυδρομείου). Ενδεικτικά για να γίνει αντιληπτό το μέγεθος ενδεικτικής περίπτωσης, το μεγαλύτερο από αντίστοιχα αρχεία αριθμούσε 174.787 διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Περίπτωση τηλεφωνικής όχλησης για προωθητικούς σκοπούς
Σε σχετική υπόθεση χρησιμοποιήθηκε παραβατικά τηλεφωνικός αριθμός συνδρομητή ο οποίος είχε αναρτηθεί από το υποκείμενο των δεδομένων (συνδρομητής) σε γνωστό διαδικτυακό τόπο πώλησης αυτοκινήτων για την προώθηση προϊόντων και υπηρεσιών. Από την Αρχή Προστασίας Προσωπικών Δεδομένων έγινε σχετική σύσταση (έπειτα από την αντίστοιχη καταγγελία και τη

σχετική διερεύνηση της υπόθεσης) λαμβάνοντας υπόψη ότι η συλλογή και χρήση προσωπικών δεδομένων για το σκοπό της απευθείας προώθησης επιτρέπεται μόνο με τη συγκατάθεση του υποκειμένου των δεδομένων, ή χωρίς αυτή όταν τα δεδομένα συλλέγονται από δημόσιους – επαγγελματικούς καταλόγους, όταν έχουν δημοσιοποιηθεί από το ίδιο το υποκείμενο ή όταν βασίζονται σε αντίστοιχη πελατειακή σχέση – επαφή.
Εντούτοις, σε ανάλογη υπόθεση θα πρέπει να σημειωθεί πως παραβιάσεις παρατηρήθηκαν και σε περιπτώσεις επαγγελματικών καταλόγων, με εξέταση σχετικών καταγγελιών να διαπιστώνει πως γνωστή εταιρία του συγκεκριμένου αντικειμένου προέβη σε παραβατικές συμπεριφορές όπως λανθασμένη εμφάνιση προσωπικών δεδομένων και κοινοποίηση των δεδομένων παρά τις προβεβλημένες αντιρρήσεις του υποκειμένου (υπ' αριθμ. 2/2015 απόφαση Αρχής Προστασίας Προσωπικών Δεδομένων).

Περιστατικό διαρροής δεδομένων πιστωτικών καρτών
Ένα σημαντικό περιστατικό παραβίασης προσωπικών δεδομένων αποτελεί σχετικό καταγραφόμενο περιστατικό διαρροής δεδομένων πιστωτικών καρτών από ηλεκτρονικό σύστημα κρατήσεων ξενοδοχείου, το οποίο κοινοποιήθηκε από τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια των Δικτύων και Πληροφοριών (ENISA) στην Αρχή Προστασίας Προσωπικών Δεδομένων. Η συγκεκριμένη διαρροή αποδόθηκε στη λήψη μειωμένων μέτρων ασφαλείας του ηλεκτρονικού συστήματος του ξενοδοχείου και στην έλλειψη ισχυρών μηχανισμών αυθεντικοποίησης των χρηστών του συστήματος, αφού ήταν δυνατή η εξαγωγή αυτών των δεδομένων μέσω απομακρυσμένης σύνδεσης χρήστη ο οποίος γνώριζε τον κωδικό πρόσβασης εξουσιοδοτημένου χρήστη (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2016).

Ευρεία και λανθασμένη χρήση των cookies
Σε σχετική έρευνα που πραγματοποιήθηκε από την Ευρωπαϊκή Επιτροπή (478 ιστοσελίδες σε 8 κράτη μέλη της Ευρωπαϊκής Ένωσης) με σκοπό να διερευνηθεί το κατά πόσο είναι συνηθισμένη πρακτική η χρήση cookies τα κυριότερα ευρήματα μπορούν να συνοψιστούν στα εξής χαρακτηριστικά σημεία (Van Eecke and De Bruyn, 2015):

- 16.555 (σε πρώτο ή δεύτερο επίπεδο) cookies ήταν συνολικά εγκατεστημένα σε 478 ιστοσελίδες, οδηγώντας σε ένα μέσο όρο παρουσίας 34.6 cookies ανά ιστοσελίδα
- πάνω από το 70% των cookies προέρχονταν από τρίτους (third party cookies), επρόκειτο δηλαδή για cookies που είχαν εγκατασταθεί από διαφορετική διαδικτυακή διεύθυνση (domain) από την επισκεπτόμενη
- πάνω από το 86% των cookies ήταν μόνιμου χαρακτήρα, επρόκειτο δηλαδή για αρχεία που παραμένουν στον τοπικό υπολογιστή του χρήστη για μεγάλο χρονικό διάστημα, αντί να διαγράφονται με το κλείσιμο της εκάστοτε ιστοσελίδας. Η μέση διάρκεια παραμονής για τα πρώτου επιπέδου ήταν 14,34 έτη ενώ για τα δεύτερου επιπέδου (εγκατεστημένα από τρίτους) ήταν 1,77 έτη.
- Μόνο 7 ιστοσελίδες δεν είχαν εγκατεστημένα cookies.

- Το συχνότερο μέσο προειδοποίησης του χρήστη για την ύπαρξη των cookies ήταν η χρήση ενός cookie banner (59%) ή ένας σύνδεσμος στην κεφαλίδα ή στο υποσέλιδο της ιστοσελίδας.
- Το 26% των ιστοσελίδων δεν περιείχε κάποια προειδοποίηση σχετικά με τα εγκατεστημένα cookies (με την πλειονότητα αυτών των ιστοσελίδων να προέρχονται από την Τσεχία)
- Από το υπόλοιπο ποσοστό των ιστοσελίδων (που ενημέρωναν για τη χρήση cookies), το 43% δεν παρείχε επαρκή πληροφόρηση για το είδος και το σκοπό χρήσης των cookies
- Μόνο το 16% των ιστοσελίδων έδιναν στο χρήστη τη δυνατότητα λεπτομερούς ελέγχου των cookies που ήταν εγκατεστημένα στην ιστοσελίδα, με το 84% αυτών να απαιτεί επαναρύθμιση του browser για την άσκηση του συγκεκριμένου ελέγχου.

Από τους τρεις τομείς δραστηριότητας που αφορούσαν οι ιστοσελίδες (μέσα μαζικής ενημέρωσης, ηλεκτρονικό εμπόριο και δημόσιος τομέας) στην περίπτωση των μέσων μαζικής ενημέρωσης εμφανίστηκαν τα περισσότερα cookies, με το δημόσιο τομέα να εμφανίζει τα λιγότερα).

Όπως μπορεί να παρατηρηθεί από τον ακόλουθο πίνακα, η κατάσταση στην Ελλάδα κινείται στα μεσαία επίπεδα και στους τρεις τομείς.

Country	e-commerce	Media	Public	Mean
CZ	19.8	44.2	9.6	**25.9**
DK	20.8	75.3	11.7	**40.0**
ES	29.2	59.2	5.7	**37.0**
FR	30.6	73.3	38.8	**n/a**
GR	16.3	15.8	3.0	**14.3**
NL	25.9	42.2	5.5	**35.4**
SI	8.1	5.3	1.5	**5.5**
UK	37.5	83.1	6.9	**44.2**
Mean	**23.5**	**49.8**	**10.3**	**28.9**

Πίνακας 1: Μέσος αριθμός αρχείων cookies που εγκαθίστανται από ιστοσελίδες ανά τομέα δραστηριότητας και χώρα σύμφωνα με τα αποτελέσματα του προγράμματος Automated Cookies Sweep (European Commission, 2015)

Παραβίαση της ιδιωτικότητας από το Google Street View

Στη γνωστή εταιρία επιβλήθηκε πρόστιμο από την Ομοσπονδιακή Επιτροπή Επικοινωνιών (Federal Communications Commission, FCC) σε συνεργασία με την εισαγγελία των ΗΠΑ, με βάση το γεγονός ότι το 2010 τα ειδικά οχήματα του Street View παράλληλα με τη φυσιολογική τους δραστηριότητα (λεπτομερή χαρτογράφηση περιοχών με σκοπό την τρισδιάστατη απεικόνισή τους) υπέκλεπταν παράλληλα και μεγάλο όγκο προσωπικών δεδομένων.

Τα δεδομένα αυτά είχαν περισυλλεγεί από οικιακά ασύρματα δίκτυα, καθώς τα οχήματα του Street View προέβαιναν σε «αναγνωρίσεις/χαρτογραφήσεις» περιοχών στο διάστημα 2008-2010 και περιλάμβαναν e-mail, ιατρικά και οικονομικά αρχεία και κωδικούς, από εκατομμύρια μη κρυπτογραφημένα ασύρματα δίκτυα. Η συγκεκριμένη παραβατική δραστηριότητα (υποκλοπή δεδομένων) από πλευράς της εταιρίας αποδόθηκε στο ότι στο λογισμικό του Street View είχε συμπεριληφθεί κατά λάθος τμήμα κώδικα που ήταν «υπεύθυνο» για τη συγκεκριμένη δράση. Ασφαλώς η λειτουργία του συγκεκριμένου κώδικα θα έπρεπε να έχει διακοπεί αμέσως όταν έγινε αντιληπτή, γεγονός το οποίο οδήγησε την επιτροπή στη συγκεκριμένη απόφαση.
Από την ίδια εταιρία έχουν σημειωθεί και άλλες παραβάσεις ιδιωτικότητας (π.χ «παράκαμψη» των ρυθμίσεων ιδιωτικότητας (privacy settings) στο browser Safari το 2012, παραδοχή της περί χρήσης «παραπλανητικών τακτικών» στο πλαίσιο της προώθησης του κοινωνικού δικτύου Buzz και παρατεταμένη περίοδος επιτήρησης σχετικά με τη συγκεκριμένη δράση, ανάλογες αποφάσεις στη Γερμανία και στην Ελβετία σε ευρωπαϊκό επίπεδο κ.α.). Στην προκειμένη περίπτωση θα πρέπει να σημειωθεί η προτεινόμενη πολιτική αντιμετώπισης, η οποία περιλάμβανε την οργάνωση εκπαιδευτικών προγραμμάτων σε θέματα ιδιωτικότητας και διαχείρισης προσωπικών δεδομένων, αναδεικνύοντας έτσι τη σημασία της εκπαίδευσης όσον αφορά στην αντιμετώπιση του συγκεκριμένου προβλήματος (Ναυτεμπορική, 2013; Σπυριδωνίδου, 2015).

Το δικαίωμα στη λήθη

Μια υπόθεση – ορόσημο όσον αφορά στην αναγνώριση του δικαιώματος στη λήθη (the right to be forgotten) κάθε φυσικού προσώπου να ζητήσει από μια διαδικτυακή μηχανή αναζήτησης να αφαιρέσει τις συνδέσεις σε πληροφορίες που το αφορούν, λαμβανομένων υπόψη παραγόντων, όπως η φύση των πληροφοριών ως προσωπικών δεδομένων, η παλαιότητα της πληροφορίας, το συμφέρον του κοινού για πρόσβαση σε αυτήν και ο ρόλος του ατόμου-φορέα των δεδομένων στη δημόσια ζωή. Η υπόθεση αυτή (C-131/12 Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González) που εξετάστηκε από το Δικαστήριο της Ευρωπαϊκής Ένωσης, αφορούσε την εμφάνιση ανακοίνωσης για πλειστηριασμό ακινήτων κατόπιν κατάσχεσης που επιβλήθηκε λόγω κοινωνικοασφαλιστικών οφειλών (1988), όταν λάμβανε χώρα αναζήτηση του συγκεκριμένου ονόματος στη σχετική μηχανή της Google, ακόμα και 11 χρόνια μετά. Ο θιγόμενος θεώρησε πως η εμφάνιση της συγκεκριμένης παραπομπής αποτελούσε δυσφήμηση για το πρόσωπό του, αφού η υπόθεση είχε από μέρους του διευθετηθεί, ζητώντας τόσο από την Ισπανική όσο και από την Αμερικάνικη Google να αποσύρουν το όνομά του από τις δυσφημιστικές καταχωρήσεις, με την υπόθεση να εκκρεμεί. Εντούτοις, η συγκεκριμένη υπόθεση αποτέλεσε την αφετηρία για πλήθος σχετικών καταγγελιών, χωρίς αυτό να σημαίνει πως μπορεί να αποτελέσει εφαλτήριο για τη θέσπιση γενικού «δικαιώματος στη λήθη», αφού κάθε τέτοιου είδους υπόθεση θα πρέπει να προσεγγίζεται χωριστά (Νομικά Νέα, 2017).

Παραβίαση ασφαλείας σε υπηρεσίες «σύννεφου»

Βασικό πλήγμα για την ασφάλεια που διέπει τις υπηρεσίες σύννεφου αποτέλεσε η μεγάλη διαρροή φωτογραφιών και βίντεο διασημοτήτων η οποία έλαβε χώρα τον

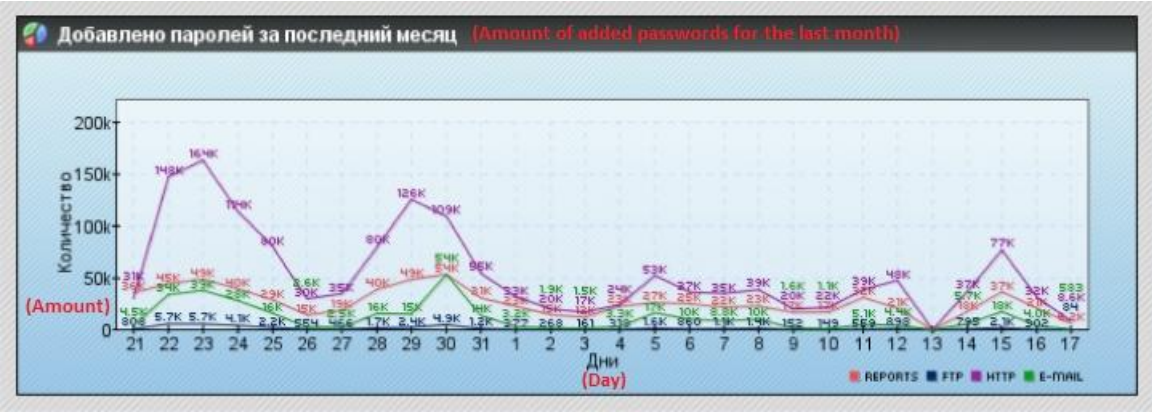
Αύγουστο του 2014 μετά τη δράση του 29χρονου Έντουαρτ Μάτζερτσικ (Edward Majerczyk) από το Ιλινόις των ΗΠΑ στο iCloud της Apple ή/και στο Gmail διασήμων. Ο συγκεκριμένος, από το Σεπτέμβριο 2013 έως τον Αύγουστο 2014 υπέκλεψε φωτογραφίες εκατοντάδων διασημοτήτων του Χόλιγουντ, αφού κατόρθωσε να τους ξεγελάσει για να συγκεντρώσει τα στοιχεία εισόδου τους στο λογαριασμό τους, παραβιάζοντας έτσι κατάφορα την ιδιωτικότητά τους, με αξιοσημείωτο το γεγονός ότι κατά την παραδοχή της ενοχής του δήλωσε ότι το πραγματοποίησε για λόγους «προσωπικής ευχαρίστησης». Η αποτελεσματικότητα του δράστη αποδόθηκε από τον CEO της Apple, Tim Cook, σε συνέντευξη που έδωσε στη "Wall Street Journal", είτε στο ότι ο χάκερ κατάφερε να απαντήσει σωστά στις ερωτήσεις ασφαλείας των θυμάτων με αποτέλεσμα να ανακτήσει τους κωδικούς από τα Apple Ids είτε να μαντέψει τους κωδικούς κάνοντας χρήση τεχνικών ηλεκτρονικού ψαρέματος (phising). Αντίστοιχα φαινόμενα είχαν επαναληφθεί και παλαιότερα (π.χ. λήψη γυμνών φωτογραφιών από το τηλέφωνο γνωστής ηθοποιού) (Σπυριδωνίδου, 2015; Tech in.gr, 2016)

Περιστατικό παραβίασης λογαριασμών χρηστών των κοινωνικών δικτύων

Εστιάζοντας στο αντικείμενο της παρούσας εργασίας, η δράση παραβίασης της ιδιωτικότητας δεν θα μπορούσε να λείπει από την περίπτωση των κοινωνικών δικτύων. Ενδεικτική και ιδιαίτερα χαρακτηριστική εξαιτίας της μαζικότητας και του μεγέθους του φαινομένου είναι η περίπτωση παραβίασης δύο εκατομμύριων λογαριασμών χρηστών το Νοέμβριο του 2013, με τους λογαριασμούς να προέρχονται από διάφορους ιστότοπους (Facebook, Google, Yahoo, Linked In σε σύνολο 93.000 ιστοσελίδων). Αναλυτικότερα η παραβίαση όσον αφορά στα μέσα κοινωνικής δικτύωσης αφορούσε τα ακόλουθα μεγέθη, με το server μέσω του οποίου έγινε η επίθεση να εντοπίζεται στην Ολλανδία (Pagliery, 2013):

- 318.000 λογαριασμούς Facebook
- 70.000 λογαριασμούς Gmail, Google+ και YouTube
- 60.000 λογαριασμούς Yahoo
- 22.000 λογαριασμούς Twitter
- 9.000 λογαριασμούς Odnoklassniki (ένα ευρείας χρήσης Ρωσικό κοινωνικό δίκτυο)
- 8.000 λογαριασμούς ADP (Automatic Data Processing – μια Αμερικανική εταιρεία επενδύσεων και υπηρεσιών μισθοδοσίας)
- 8.000 λογαριασμούς Linkedln

Η πραγματοποίηση της παραβίασης αποδόθηκε στη χρήση κακόβουλου λογισμικού τύπου δουρείου ίππου, το οποίο εγκαταστάθηκε στους υπολογιστές των χρηστών και επέτρεπε την υποκλοπή ονομάτων και κωδικών χρηστών για πάνω από ένα μήνα (Pagliery, 2013). Ενδεικτικά η υποκλοπή κωδικών σε ημερήσια βάση για τη συγκεκριμένη περίοδο παρουσιάζεται στο ακόλουθο διάγραμμα.

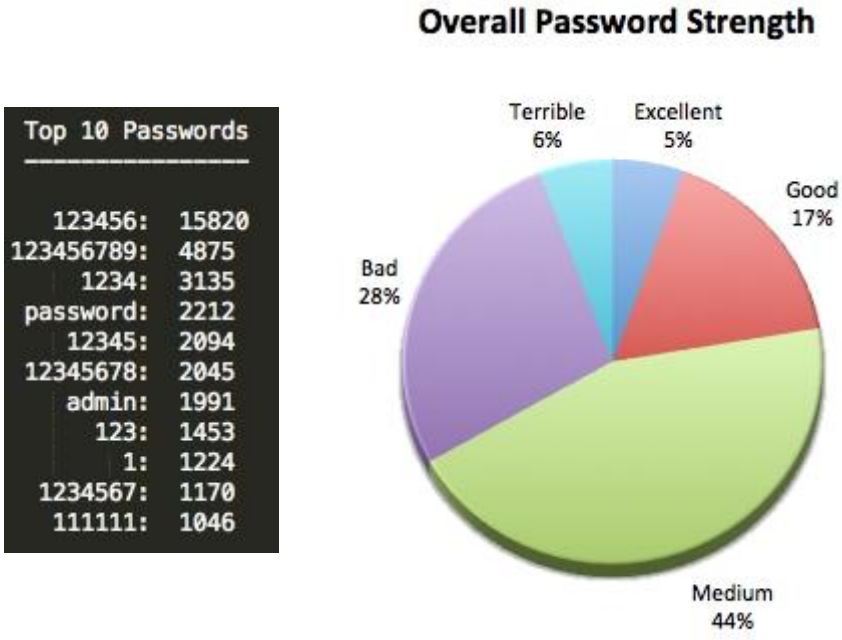


Σχήμα 5: Ημερήσια μεταβολή υποκλοπής κωδικών με τη χρήση κακόβουλου λογισμικού κατά την παραβίαση ιδιωτικότητας σε κοινωνικά δίκτυα το Νοέμβριο του 2013 (Chechik, 2013)

Αναλυτικότερα, όσον αφορά στο είδος των δεδομένων τα οποία παραβιάστηκαν, αυτά περιλάμβαναν (Chechik, 2013; Σπυριδωνίδου, 2015):

- 1.580.000 κωδικούς ιστοσελίδων 320.000 κωδικούς ηλεκτρονικού ταχυδρομείου
- 41.000 κωδικούς FTP για μεταφορά αρχείων (File Transfer Protocol)
- 3.000 κωδικούς για απομακρυσμένη βοήθεια υπολογιστών
- 3.000 κωδικούς προστασίας.

Ιδιαίτερα ενδιαφέρον όσον αφορά στην προσέγγιση του φαινομένου υπό το πρίσμα της αντιμετώπισής του είναι το αποτέλεσμα της ανάλυσης των κωδικών προστασίας που είχαν χρησιμοποιηθεί από τους χρήστες, με την επιλογή τους να παρουσιάζει φανερή αδυναμία (αφού όπως παρουσιάζεται στην ακόλουθη εικόνα αφενός οι επιλογές ήταν ιδιαίτερα συνήθεις και προβλέψιμες και αφετέρου μόνο το 22% των κωδικών παρουσιάστηκαν ισχυροί).



Εικόνα 10: Επιλογή κωδικών προστασίας από τους χρήστες κοινωνικών δικτύων σε περιστατικό παραβίασής τους (Chechik, 2013)

Ασφαλώς η λίστα παραβατικών περιπτώσεων όπως οι προαναφερόμενες μπορεί να συνεχιστεί κατά πολύ. Ωστόσο, η προσέγγιση επικεντρώθηκε σε περιπτώσεις ηλεκτρονικής επικοινωνίας, με τη διαδικασία να έχει άμεση σχέση με τη χρήση των μέσων κοινωνικής δικτύωσης, η οποία αποτελεί και αντικείμενο της παρούσας εργασίας.

4.3 Μηχανισμοί προστασίας

Στην παρούσα ενότητα γίνεται μια συνοπτική αναφορά στους μηχανισμούς προστασίας της ιδιωτικότητας (επικεντρώνοντας τη συγκεκριμένη προσέγγιση στο πλαίσιο των μέσων κοινωνικής δικτύωσης). Αυτοί οι μηχανισμοί προστασίας μπορούν να εντοπιστούν τόσο σε επίπεδο εφαρμογής τεχνολογικών μεθόδων όσο και σε επίπεδο υιοθέτησης συγκεκριμένων πολιτικών - συμπεριφορών. Εντούτοις, ένα φυσιολογικό ερώτημα που εγείρεται όσον αφορά στη συγκεκριμένη προσέγγιση είναι το αν και το κατά πόσο είναι εφικτή μια τέτοια προστασία.

Αρχικά θα πρέπει να εντοπιστεί η εξ ορισμού δυσκολία που προκύπτει από την τεχνολογική εξέλιξη και τη φύση της, αφού πρόκειται για μια εξέλιξη «μη αναστρέψιμη, ταχύτατη και ταυτόχρονα μη προδιαγνώσιμη τουλάχιστον σε ένα σχετικό βάθος χρόνου» (Μήτρου, 2016). Αυτή μάλιστα η εξέλιξη έχει ιδιαίτερη σημασία αν ληφθεί υπόψη πως δεν είναι δυνατή η ικανότητα της ανάλογης ρύθμισης του συστήματος, τόσο χρονικά όσο και ποιοτικά. Έτσι, ο νομοθέτης τείνει να παρεμβαίνει σημειακά και κατά περίπτωση, επιχειρώντας να γενικεύσει κατάλληλα εκ των υστέρων, πόσο μάλλον όταν η τεχνολογία και η εφαρμογή της

θα πρέπει να γίνεται κάθε φορά πλήρως κατανοητή. Για παράδειγμα η ένταξη της στατικής διεύθυνσης IP (Internet Protocol) στο σύνολο των προσωπικών δεδομένων αντίθετα με αυτή της δυναμικής, προϋποθέτει ιδιαίτερη ενασχόληση και κατανόηση του αντικειμένου και της ευρύτερης διαδικασίας δικτύωσης.

Παραστατικά αυτή η δυσκολία αποδίδεται από τη Μήτρου (2016) ως μια προσπάθεια «να επιχειρεί κανείς να αλλάξει λάστιχα σε ένα αυτοκίνητο εν κινήσει».

Επίσης είναι λογικό να υφίσταται σύγχυση εξαιτίας της πολύπλοκης διασύνδεσης ψηφιακού και πραγματικού κόσμου (ειδικά όσον αφορά σε εικονικά περιβάλλοντα). Ένας βασικός τρόπος προσέγγισης περιπτώσεων αυτού του είδους είναι το κατά πόσο συνδέεται ο ψηφιακός και ο πραγματικός εαυτός, Ανάλογη είναι και η προσέγγιση που διέπει και την περίπτωση των μέσων κοινωνικής δικτύωσης με το εκάστοτε προφίλ να αποτελεί και τον ψηφιακό εαυτό. Ζητούμενο αποτελεί να προστατευτούν εκείνα τα σημεία που μπορούν να «μαρτυρήσουν» τη διασύνδεση ψηφιακής και πραγματικής υπόστασης.

Ενθαρρυντικό είναι το γεγονός της έμπρακτης υποστήριξης της Ευρωπαϊκής Κοινότητας έναντι των Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies, PETs), με ζητούμενο το επίπεδο υιοθέτησης αυτών των τεχνολογιών να γίνει σε θεσμική και όχι σε συμπληρωματική βάση.

Επισημαίνεται επίσης η σημασία της αρχικής λήψης μέτρων, στο στάδιο του σχεδιασμού ανάλογων εφαρμογών (privacy by design) καθώς και στην ενσωμάτωση στοιχείων με τρόπο φιλικό προς το χρήστη (privacy-fiendly default settings)

Βασικό πρόβλημα της διαδικασίας αποτελεί η έλλειψη προτυποποίησης των μηχανισμών προστασίας της ιδιωτικότητας, με την ανάγκη ύπαρξης προτύπων ή τουλάχιστον κοινής γραμμής αντιμετώπισης να επισημαίνεται και στην Παγκόσμια Διάσκεψη των Επιτρόπων και Αρχών Προστασίας Προσωπικών Δεδομένων (2008) στην οποία αναφέρθηκε η ανάγκη «να εκπονηθεί μία κοινή πρόταση για τη θέσπιση διεθνών προδιαγραφών για την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων» (Μήτρου, 2016). Πέρα από το επίπεδο φορέων η συγκεκριμένη ανάγκη έχει γίνει κατανοητή και από τους μεγάλους παρόχους σχετικών υπηρεσιών (π.χ. πάροχοι μηχανών αναζήτησης) οι οποίοι προτείνουν την καθιέρωση κοινών προδιαγραφών. Εντούτοις, η δημιουργία, καθιέρωση και θέσπιση ενός παγκόσμιας εμβέλειας ρυθμιστικού εργαλείου δυσχεραίνει κατά πολύ αφενός για τεχνολογικούς λόγους (προβλήματα συμβατότητας διαφορετικών τεχνολογιών) και αφετέρου εξαιτίας λειτουργίας της ίδιας της αγοράς (με τη λήψη και διατήρηση της εκάστοτε δεσπόζουσας θέσης να είναι το λογικό και αναμενόμενο ζητούμενο), πόσο μάλλον αν γίνει κατανοητό πως δεν μπορεί να υπάρξει συναίνεση σε ένα τόσο ευρύ επίπεδο. Σημαντικός επίσης είναι και ο ρόλος που μπορεί να διαδραματίσει στην προκειμένη περίπτωση το κράτος, τουλάχιστον όσον αφορά στη διάθεση και στη συνεργασία δημόσιων και ιδιωτικών φορέων.

4.3.1 Πολιτικές προστασίας

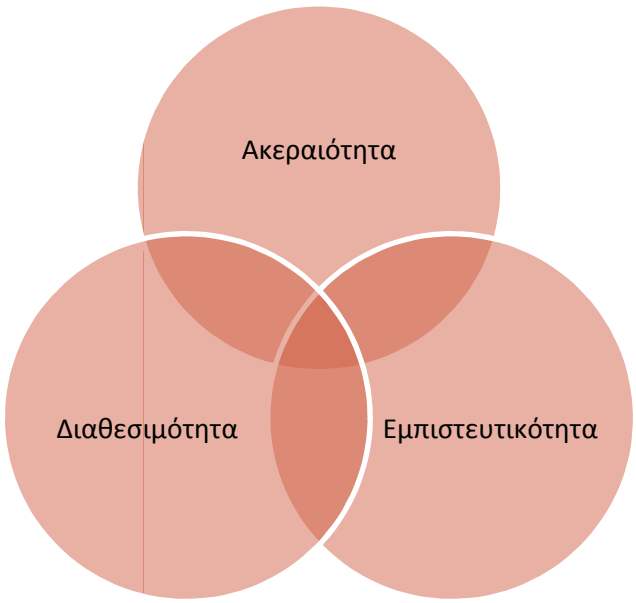
Πολιτική ασφαλείας

Προκειμένου να εξασφαλιστεί κατά το δυνατό η προστασία της ιδιωτικότητας σε επίπεδο συστήματος θα πρέπει το σύστημα αυτό να διέπεται από

την αντίστοιχη πολιτική ασφαλείας. Η τήρηση συγκεκριμένων αρχών που συγκροτούν τη συγκεκριμένη πολιτική καθιστά ισχυρό τον έλεγχο της πρόσβασης στο σύστημα. Οι αρχές αυτές είναι (Lee, 1999; Σπυριδωνίδου, 2015):

- Ακεραιότητα (Integrity): Αναφέρεται στη διατήρηση της κατάστασης (αρχικής ή μεταγενέστερης) των δεδομένων ενός πληροφοριακού συστήματος χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και στην αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.
- Διαθεσιμότητα (Availability): Αποτελεί την περισσότερο διασυνδεδεμένη με τη χρήση των δεδομένων αρχή, αφού αναφέρεται στην ανά πάσα στιγμή διάθεση των δεδομένων και ετοιμότητα του δικτύου, σύμφωνα με τις επιθυμίες των χρηστών του.
- Εμπιστευτικότητα (Confidentiality): Συνεπάγεται την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένα άτομα. Αναφέρεται συχνά και ως αρχή απορρήτου.

Ζητούμενο είναι να πληρείται το σύνολο των προαναφερόμενων αρχών, οι οποίες αλληλοσυμπληρώνονται (όπως παρουσιάζεται στο ακόλουθο σχήμα) και καθιστούν από κοινού ένα υπολογιστικό σύστημα ασφαλές, επαρκές και αποδοτικό. Η μεμονωμένη διατάραξη της ισορροπίας μπορεί να προκαλέσει αστάθεια στο σύνολο του συστήματος. Ενδεικτικό είναι το γεγονός ότι πολλές κακόβουλες επιθέσεις στοχεύουν στη διατάραξη ενός εκ των τριών αρχών (π.χ. η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα).



Σχήμα 6: Βασικές αρχές πολιτικής ασφαλείας ενός υπολογιστικού συστήματος

Επιπρόσθετα το σύστημα θα πρέπει να διατηρεί ελεγχόμενες σε επιθυμητή μορφή - επίπεδο συγκεκριμένες παραμέτρους που έχουν να κάνουν με τη συνολική λειτουργία του όσον αφορά στην ασφάλεια των δεδομένων που καλείται κάθε

φορά να διαχειριστεί. Οι παράμετροι αυτές σύμφωνα με τις κατευθυντήριες γραμμές του ΟΟΣΑ (2002) είναι (Τσαγκανού, 2014):

- Ευαισθητοποίηση: Αφορά στο πως πρέπει οι ίδιοι οι συμμετέχοντες να αντιμετωπίζουν το δυναμικό ενδεχόμενο της παραβίασης των δεδομένων του συστήματος και κατ' επέκταση της προσβολής της ιδιωτικότητάς τους. Θα πρέπει δηλαδή να γίνεται κατανοητό ότι το σύστημα αντιμετωπίζει σε δυναμικό επίπεδο τέτοιου είδους απειλές και επομένως η υιοθέτηση αντίστοιχων αποτελεσματικών πρακτικών ασφαλείας είναι μια απαραίτητη διαδικασία.
- Ευθύνη: Καθένας από τους συμμετέχοντες σε μια διαδικασία διαχείρισης υπολογιστικού συστήματος και των δεδομένων του είναι υπεύθυνος για τις ενέργειές του και για το κατά πόσο αυτές θέτουν σε κίνδυνο τη λειτουργία του συστήματος στο σύνολό του (π.χ. διανομή της πληροφορίας και έλεγχος εισόδου στο σύστημα)
- Ανταπόκριση: Αφορά στην ετοιμότητα των χρηστών του συστήματος σχετικά με τον εντοπισμό – ανίχνευση τυχόν δυσλειτουργιών και τρωτών σημείων και τη γρήγορη προσαρμογή και εφαρμογή διαδικασιών που θα επιτρέπουν την αποδοτική προστασία των δεδομένων του συστήματος.
- Ηθική: Η συγκεκριμένη παράμετρος σχετίζεται γενικότερα με την ηθική συμπεριφορά των χρηστών του συστήματος σχετικά με το σεβασμό των δικαιωμάτων των υπόλοιπων χρηστών και τη συνεχή προσπάθεια ανάπτυξης βέλτιστων πρακτικών.
- Δημοκρατία: Αποτελεί την κοινωνική προέκταση της προαναφερόμενης παραμέτρου της ηθικής υπό την έννοια της υιοθέτησης όλων εκείνων των αξιών που συνιστούν ένα δημοκρατικό σύστημα (ελευθερία σκέψης, ανταλλαγής πληροφοριών, διαφάνεια και σεβασμός εμπιστευτικότητας πληροφοριών και προσωπικών δεδομένων).
- Αξιολόγηση του κίνδυνου: Θα πρέπει να υφίσταται μελέτη εκτίμησης κινδύνου των πληροφοριών - δεδομένων του συστήματος η οποία θα επαναθεωρείται σε τακτά χρονικά διαστήματα ή όποτε προκύπτει λόγω ιδιαίτερων συνθηκών μια τέτοια ανάγκη. Η μελέτη θα περιλαμβάνει όλους εκείνους τους παράγοντες που εμπλέκονται στη διαδικασία κινδύνου και ιδιαίτερα τον εντοπισμό των πηγών κινδύνου καθώς και τα προτεινόμενα μέτρα αντιμετώπισης – περιορισμού τους.
- Ασφάλεια κατά το σχεδιασμό και την εφαρμογή: Λαμβάνοντας υπόψη πως δεν απαιτούνται τα ίδια πρωτόκολλα και εφαρμογές για το σύνολο των πληροφοριών και δεδομένων του συστήματος, η συγκεκριμένη παράμετρος σχετίζεται με τη βέλτιστη αντιστοιχία εφαρμοζόμενων πρακτικών και μεθοδολογιών και είδους των δεδομένων, έτσι ώστε να υφίσταται αναλογία εφαρμογής ασφαλείας και αξίας πληροφοριακού περιεχομένου.
- Διαρκής έλεγχος και Επανεκτίμηση: Το ζήτημα της ασφάλειας θα πρέπει να επανεξετάζεται τακτικά έτσι ώστε να γίνονται κάθε φορά οι απαραίτητες τροποποιήσεις, διορθώσεις και προσαρμογές.

Πολιτικές ιδιωτικότητας

Λαμβάνοντας υπόψη πως οι τεχνολογικές εξελίξεις υφίστανται σε δυναμική πορεία, με έναν αέναο ανταγωνισμό μεταξύ μηχανισμών παραβίασης και

προστασίας της ιδιωτικότητας, είναι σημαντικό να γίνει αντιληπτό από το σύνολο των χρηστών των κοινωνικών δικτύων και του Διαδικτύου γενικότερα πως το ζήτημα μπορεί να αντιμετωπιστεί σε επίπεδο υιοθέτησης συγκεκριμένων συμπεριφορών – πολιτικών. Θα πρέπει δηλαδή σε πρώτη φάση, η δραστηριότητα εντός των κοινωνικών δικτύων να γίνεται και να διέπεται με βάση τη λογική προστασίας της ιδιωτικότητας τόσο από την πλευρά του διαχειριστή όσο και από αυτή του/της συμμετέχοντα/ουσας.

Έτσι, θα πρέπει να αποφεύγεται να ζητείται από τους ιστότοπους οι χρήστες να παρέχουν κάθε είδους ιδιωτική πληροφορία, η πηγή από την οποία προέρχονται τα ιδιωτικά δεδομένα να είναι κρυμμένη – κρυπτογραφημένη και οι διαχειριστές να εφαρμόζουν πολιτικές ιδιωτικότητας (Privacy Policies) (Cranor, 1999).

Το ζήτημα των πολιτικών ιδιωτικότητας είναι ιδιαίτερα σημαντικό. Συνήθως αναγράφονται από τους ιστότοπους στην αρχική τους σελίδα και δηλώνουν ουσιαστικά τον τρόπο με τον οποίο προτίθεται ο συγκεκριμένος ιστότοπος να διαχειριστεί τα δεδομένα του εκάστοτε επισκέπτη – χρήστη, αποτελώντας ουσιαστικά ένα είδος συμβολαίου που συμφωνείται και υπογράφεται μεταξύ των επισκεπτών της ιστοσελίδας και της εταιρίας. Εντούτοις, αν και εκ πρώτης όψεως η συγκεκριμένη πολιτική φαντάζει ως η ενδεδειγμένη και η αποδοτικότερη για την επίτευξη της προστασίας της ιδιωτικότητας σε κάθε είδους διαδικτυακή δράση, παρουσιάζει συγκεκριμένα μα σημαντικά κενά, απόρροια των μειονεκτημάτων της. Στα μειονεκτήματα αυτά συμπεριλαμβάνονται (Pollach, 2007):

- το γεγονός ότι το διαβαστεί από το χρήστη και να γίνει κατανοητή η συνολική πολιτική από το χρήστη είναι μια χρονοβόρα και κοπιαστική διαδικασία, πόσο μάλλον όταν υφίστανται σημεία στα οποία ο χρήστης διαφωνεί ή χρειάζεται διευκρινίσεις (αφού θα πρέπει να επικοινωνήσει και να διαπραγματευτεί με το διαχειριστή),
- το γεγονός ότι η εκάστοτε πολιτική ιδιωτικότητας μιας διαδικτυακής κοινότητας - επιχείρησης μπορεί να αλλάξει ανά πάσα στιγμή, με αυτή τη νέα αλλαγή να μη γίνει εγκαίρως γνωστή και επομένως αποδεκτή από τον εκάστοτε χρήστη,
- το γεγονός ότι δεν υφίσταται κάποιος φυσικός ή τεχνικός (ηλεκτρονικός) μηχανισμός που να μπορεί να επιβλέπει, να ελέγχει και το κυριότερο να προλαμβάνει τη μη τήρηση των όσων αναφέρονται στην πολιτική ιδιωτικότητας της επιχείρησης. Σε μια τέτοια περίπτωση (μη συμμόρφωσης – τήρησης των όρων από τη μεριά της κοινότητας ή της επιχείρησης), η διαδικασία θα πρέπει να εκκινηθεί από τον ίδιο το χρήστη (Ζωρόθεος, 2007).

Συμπεριφορά χρηστών

Όπως προκύπτει από την αναφορά στις παραπάνω πολιτικές, η προστασία των προσωπικών δεδομένων πέρα από τα απαραίτητα τεχνολογικά «εργαλεία» και την εφαρμογή τους αποτελεί σε σημαντικό βαθμό ζήτημα συμπεριφοράς των χρηστών των μέσων κοινωνικής δικτύωσης. Η συμπεριφορά λοιπόν αυτή θα πρέπει να διέπεται από συγκεκριμένα χαρακτηριστικά, καθ’ όλη τη διάρκεια συμμετοχής σε αυτά τα μέσα, αλλά και στην ευρύτερη διαδικτυακή παρουσία των χρηστών. Τέτοια συμπεριφορικά χαρακτηριστικά είναι:

- Η συνεχής προσπάθεια για τη διατήρηση του ελέγχου των προσωπικών δεδομένων.
- Το να τίθεται υπό σκέψη κάθε αίτημα λήψης – χρήσης των προσωπικών δεδομένων (π.χ. γιατί είναι απαραίτητη αυτή η χρήση, ποιος είναι αυτός που τα ζητά, κατά πόσο έμπιστος είναι αυτός που τα ζητά ή που πρόκειται να τα χρησιμοποιήσει, ποιο είναι το ενδεχόμενο τα προσωπικά δεδομένα να δοθούν στη συνέχεια σε άλλα πρόσωπα – φορείς).
- Το να μη δίνεται απάντηση σε αιτήματα αποκάλυψης προσωπικών δεδομένων, πόσο μάλλον όταν δεν υπάρχει απόλυτη σιγουριά για τον αποστολέα του αιτήματος (π.χ. e-mails και μηνύματα στο κινητό, στο Facebook ή σε άλλο μέσο κοινωνικής δικτύωσης).
- Το να αποδίδεται ιδιαίτερη προσοχή στα λεγόμενα «ψιλά γράμματα» γιατί πρόκειται για ένα πεδίο το οποίο προτιμάται συχνά από τις εταιρίες, προκειμένου να «κρύψουν» τυχόν διαφημιστικούς σκοπούς και παραβατική χρήση προσωπικών δεδομένων.
- Το να αποδίδεται ιδιαίτερη προσοχή στην εκάστοτε πολιτική ιδιωτικότητας, η οποία μπορεί να διαφέρει ανάμεσα σε διαφορετικές ιστοσελίδες. Η κατανόηση της συγκεκριμένης πολιτικής μπορεί να δώσει χρήσιμες πληροφορίες για το πως αντιμετωπίζει η εκάστοτε ιστοσελίδα τα προσωπικά δεδομένα του χρήστη (π.χ. αν εγκαθιστά αρχεία cookies, αν προωθεί τις πληροφορίες σε διαφημιστικές εταιρείες ή άλλα τρίτα μέρη κ.α.)
- Το να συμβαδίζει η συμμετοχή σε ένα μέσο ή η χρήση μιας ιστοσελίδας με το αίσθημα ασφάλειας που αποπνέει στον κάθε χρήστη. Σε διαφορετική περίπτωση (έλλειψη αισθήματος ασφάλειας) είναι προτιμότερο η χρήση μιας εναλλακτικής λύσης.
- Η χρήση ισχυρών συνθηματικών ασφαλείας (passwords) διαφορετικών ανά μέσο – ιστοσελίδα, αυξημένης πολυπλοκότητας και αλφαριθμητικής σύνθεσης (χρήση γραμμάτων, αριθμών και συμβόλων). Άλλωστε, είναι ενδεικτικό όπως προαναφέρθηκε ότι το ζήτημα της επιλογής κωδικών ασφαλείας αποτελεί ένα ιδιαίτερο «αδύναμο» πεδίο της διαδικασίας, με τις επιλογές των κωδικών ασφαλείας του παραδείγματος να μην είναι οι ενδεδειγμένες για ένα μεγάλο ποσοστό χρηστών (της τάξης του 78% για το σύνολο του παραδείγματος παραβίασης της ιδιωτικότητας των χρηστών μέσων κοινωνικής δικτύωσης).
- Το να αποδίδεται ιδιαίτερη προσοχή στη χρήση «κοινόχρηστων» (shared) υπολογιστών ή στη διαχείριση κοινόχρηστων αρχείων αφού γίνεται έτσι εύκολη η ανίχνευση του «ποιος χρησιμοποιεί τι και πότε».
- Η αποσύνδεση από ιστοσελίδες, για την είσοδο στις οποίες απαιτείται η χρήση συνθηματικών ασφαλείας έπειτα από την ολοκλήρωση της εκάστοτε «επίσκεψης» (ένα χαρακτηριστικό σφάλμα που κάνουν πολλοί χρήστες όταν χρησιμοποιούν τις ιστοσελίδες μέσων κοινωνικής δικτύωσης, με το απλό «κλείσιμο» του φυλλομετρητή (browser) να θεωρείται ως μια ασφαλή «αποχώρηση» από το συγκεκριμένο ιστότοπο).
- Διατήρηση του εκάστοτε τερματικού με το οποίο συνδέεται ο χρήστης σε υψηλά επίπεδα ασφάλειας από πλευράς «εφοδιασμού» του με τα κατάλληλα «εργαλεία» όπως τείχος προστασίας (firewall) και προγράμματα antivirus και malware για την προστασία από κακόβουλα αρχεία - λογισμικό, τα οποία όμως θα πρέπει να είναι ενημερώνονται τακτικά.

- Επικοινωνία και αξιοποίηση των σχετικών φορέων και οργάνων όπως η Αρχή Προστασίας Προσωπικών Δεδομένων σε κάθε υπόνοια – υποψία κατά την οποία θεωρεί κανείς ότι θίγονται τα προσωπικά του δεδομένα, πόσο μάλλον όταν πρόκειται για μια βέβαιη κατάσταση (π.χ. αντίληψη ότι κάποιος «ανεβάζει» προσωπικές φωτογραφίες στο διαδίκτυο).

4.3.2 Τεχνολογικές εφαρμογές προστασίας

Σύμφωνα με τους Smith and Shao (2007) οι τεχνολογικές εφαρμογές που έχουν χρησιμοποιηθεί κατά καιρούς για την προστασία της ιδιωτικότητας στο διαδίκτυο διαχωρίζονται σε δύο βασικές κατηγορίες, στις τεχνολογίες ανωνυμίας ή ψευδωνυμίας και στις ονομαστικές τεχνολογίες. Στην πρώτη περίπτωση ζητούμενο αυτών των εφαρμογών είναι η απόκρυψη της πραγματικής ταυτότητας του χρήστη μέσω μηχανισμών που αποτρέπει τη σύνδεση οποιασδήποτε ιδιωτικής πληροφορίας που διακινείται στο διαδίκτυο με την πραγματική υπόσταση ενός ατόμου. Στη δεύτερη περίπτωση ζητούμενο είναι η παροχή βοήθειας στους χρήστες του διαδικτύου και κατ' επέκταση των κοινωνικών δικτύων όσον αφορά στην προστασία των ιδιωτικών τους πληροφοριών. Η βοήθεια αυτή συμπεριλαμβάνει τρόπους αξιολόγησης για εκείνους τους ιστότοπους στους οποίους μπορεί να αποδοθεί εμπιστοσύνη αλλά και ιδιωτικές πληροφορίες οι οποίες δεν είναι αναγκαίες προκειμένου να ολοκληρωθούν συγκεκριμένες συναλλαγές, επαφές και αλληλεπιδράσεις.

Στους πίνακες που ακολουθούν καταγράφονται οι βασικότερες τεχνολογίες κάθε κατηγορίας ως προς τη χρησιμοποιούμενη αρχιτεκτονική δομή αλλά και τα πεδία εφαρμογής της καθεμιάς. Κοινό χαρακτηριστικό όλων αυτών των τεχνολογιών είναι ότι δεν σχεδιάστηκαν με βάση τη το πως θα γίνουν διαχειρίσιμες από τον εκάστοτε πελάτη – χρήση των υπηρεσιών του διαδικτύου ή ενός κοινωνικού δικτύου αλλά με αντικειμενοστραφή προσανατολισμό, δηλαδή με άξονα την προστασία των δεδομένων. Βασικές παράμετροι αυτών των τεχνολογιών αποτελούν το πρωτόκολλο P3P (platform for privacy preferences) που επιτρέπει στο χρήστη να εκφράσει την προτίμηση του για συγκεκριμένες πολιτικές ιδιωτικότητας, και οι ασπίδες ιδιωτικότητας (privacy shields), η ύπαρξη των οποίων συνεπάγεται ότι ο αντίστοιχος ιστότοπος που διαθέτει τη συγκεκριμένη τεχνολογία ενεργεί σοβαρά και υπεύθυνα ως προς την προστασία των ιδιωτικών δεδομένων των χρηστών του (Ζωρόθεος, 2007).

Technology	Architecture			Usable	Application areas		
	T3P	3P	De		E-mail	Web	Other
Anonymous techniques							
Anonymous e-mail	X			X	X		
"Anonymizer"	X			X		X	
"Crowds"			X	X		X	
Simple Chaum mix	X			X	X		
Network of Chaum mixes			X	X	X		
"Onion Routing"			X	X		X	X
Credential systems (CS)							
Chaum's CS	X			X		X	
Damgaård's CS		X				X	
Chen's CS	X			X		X	
Lysyanskaya et al.'s CS	X					X	
Camenisch et al.'s CS	X			X		X	
"Idemix"	X			X		X	
Database privacy							
Query restriction	X			X			
Data perturbation	X			X			
Output perturbation	X			X			

Key: T3P = Trusted third party
3P = Third party
De = Decentralized

Πίνακας 2:Τεχνολογίες ανωνυμίας ή ψευδωνυμίας (Ζωρόθεος, 2007)

Technology	Privacy philosophy		T3P	Applicable to e-commerce
	Helper	Enforcement		
TRUSTe	X		X	X
PS	X			X
P3P	X		X	X
E-P3P		X	X	X
ESM's		X		X
ROBM's		X	X	
SS's		X		X

Key: T3P = Trusted third party

Πίνακας 3: Ονομαστικές τεχνολογίες (Ζωρόθεος, 2007)

Όπως μπορεί να παρατηρηθεί από τους παραπάνω πίνακες υφίσταται ποικιλία εφαρμογών, με καθεμία από αυτές να περιλαμβάνει σε χαμηλότερα επίπεδα πλήθος άλλων εφαρμογών και τεχνολογιών, τόσο μεμονωμένα όσο και συνδυαστικά.

Ενδεικτικά, αναφέρονται οι τυφλές υπογραφές Chaum. που εισήχθησαν από τον David Chaum το 1982 και αποτελούν μέρος του αντίστοιχου credential system του παραπάνω πίνακα. Μέσω της τυφλής υπογραφής δίνεται η δυνατότητα στον υπογράφοντα να ταυτοποιήσει ένα έγγραφο χωρίς να έχει κάποια πληροφορία για αυτό, εξασφαλίζοντας έτσι την αδυναμία πλαστογράφησης αλλά και την ιδιότητα της τυφλότητα (blindness), της αδυναμίας δηλαδή του υπογράφοντα να αντλήσει κάποια πληροφόρηση από το έγγραφο που υπογράφει.

Προκειμένου να γίνει αντιληπτό το πως λειτουργεί το συγκεκριμένο «εργαλείο» σε πραγματικές συνθήκες, ας υποτεθεί ένα σενάριο ηλεκτρονικής ψηφοφορίας (e-voting) βασισμένο στις τυφλές υπογραφές Chaum. Στο συγκεκριμένο σενάριο (το οποίο είναι ιδιαίτερα συχνό στα κοινωνικά δίκτυα αφού μέσω αυτού μπορεί να εκφραστεί η προτίμηση σε ένα συγκεκριμένο αντικείμενο) υφίστανται τρία διαφορετικά μέρη, ο διαχειριστής, οι ψηφοφόροι και ο μετρητής. Αρχικά ο διαχειριστής ελέγχει ότι ο εκάστοτε ψηφοφόρος έχει το δικαίωμα της ψήφου. Τότε, χρησιμοποιώντας κάποιον παράγοντα τύφλωσης, ο ψηφοφόρος «τυφλώνει» την ψήφο του και ζητά από το διαχειριστή να παράξει μια υπογραφή για την συγκεκριμένη ψήφο, η υποβολή της οποίας γίνεται με την αφαίρεση της τύφλωσης. Ο έλεγχος του ότι πρόκειται για μια έγκυρη ψήφο γίνεται μέσω ενός κλειδιού επαλήθευσης από το διαχειριστή και το αποτέλεσμα του ελέγχου καθορίζει αν η ψήφος αποσταλεί στον μετρητή. Ο μετρητής με τη σειρά του χρησιμοποιεί το κλειδί του διαχειριστή για να ελέγξει την εγκυρότητα του ζευγαριού ψήφου-υπογραφής και στη συνέχεια το προσθέτει στη λίστα του (αν προκύψει εγκυρότητα). Έτσι, τα αποτελέσματα προκύπτουν τελικά χωρίς ο διαχειριστής να γνωρίζει το ποιος ψήφισε τι, εξασφαλίζοντας έτσι την ανωνυμία (Κιαγιάς, 2008).

Μια άλλη βασική τεχνολογία αποτελεί αυτή του mix-server ή mixer, ο οποίος αποτελεί ένα δίκτυο που ανακατεύει μια ομάδα μηνυμάτων και τις περνά στον παραλήπτη σε μια αναδιαταγμένη σειρά, με βασικό στόχο την εξασφάλιση της ιδιωτικότητας του αποστολέα. Έτσι, δεν είναι δυνατό να διακριθεί το ποιος έστειλε το κάθε μήνυμα και επομένως να προκύψουν οι σχέσεις αποστολέα-παραλήπτη χρησιμοποιώντας σε συνδυασμό το κατάλληλο κάθε φορά σύστημα κρυπτογράφησης. Για να γίνει αντιληπτή η χρησιμότητα ενός τέτοιου συστήματος, στο προαναφερόμενο σενάριο ηλεκτρονικής ψηφοφορίας η υιοθέτησή – εφαρμογή του θα εξασφάλιζε ότι ούτε ο μετρητής θα γνώριζε το ποιος ψήφισε τι (Κιαγιάς, 2008).

Ταυτοποίηση μέσω ραδιοσυχνοτήτων

Η συγκεκριμένη διαδικασία περιλαμβάνει τις γνωστές RFID (Radio Frequency Identification) ετικέτες. Το βασικό τους χαρακτηριστικό είναι ότι επιτρέπουν σε κάθε αντικείμενο να έχει το δικό του μοναδικό αναγνωριστικό. Αποτελούν ουσιαστικά εξέλιξη των ευρύτατα χρησιμοποιούμενων barcodes μέσω των οποίων αντιστοιχίζεται ένας αριθμός ταυτότητας σε έναν τύπο προϊόντος. Σημαντικά τους πλεονεκτήματα αποτελούν το ότι μπορούν να διαβαστούν εξ αποστάσεως, (επιτρέποντας έτσι την ταυτοποίηση – αναγνώριση σε πραγματικό χρόνο) και το ότι μπορούν να αποθηκεύουν μεγάλο όγκο δεδομένων. Η λειτουργία τους βασίζεται στη ασύρματη επικοινωνία (μέσω ραδιοκυμάτων) ετικετών και

κέντρων ελέγχου με τη χρήση ενδιάμεσου λογισμικού. Ωστόσο, η απρόσκοπτη και ασφαλής (από την πλευρά των προσωπικών δεδομένων) λειτουργία αυτών των συστημάτων προϋποθέτει την εφαρμογή των προαναφερόμενων πολιτικών στο σύνολο των επιμέρους μονάδων του συστήματος, ιδιαίτερα λαμβάνοντας υπόψη σχετικές αμφισβητήσεις (Brito, 2004; Wikipedia, 2016)

Βιομετρικές τεχνολογίες

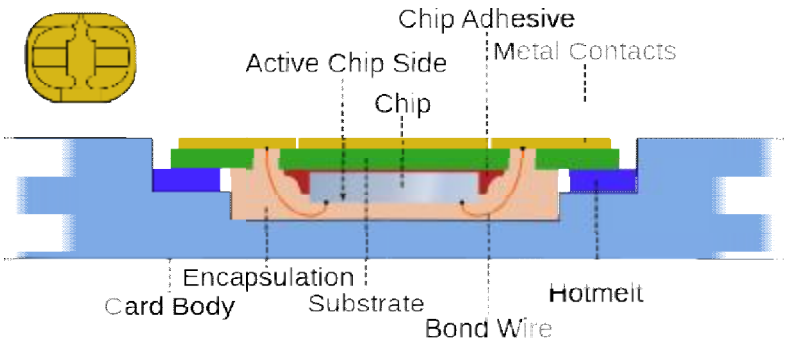
Αποτελούν ένα σύνολο τεχνολογιών οι οποίες βασίζονται στη μέτρηση συγκεκριμένων βιολογικών χαρακτηριστικών (δακτυλικά αποτυπώματα, ίριδα ματιού, γεωμετρία παλάμης και δαχτύλων, αναγνώριση προσώπου και φωνής, σχήμα αυτιών, αμφιβληστροειδής χιτώνας, μυρωδιά, θερμότητα προσώπου, φλέβα χεριού. DNA. αποτύπωμα παλάμης), καθώς και χαρακτηριστικών συμπεριφοράς (τρόπος βαδίσματος, υπογραφή, φωνή. τρόπος πληκτρολόγησης) που προέρχονται από το ανθρώπινο σώμα, με βάση το γεγονός ότι τα συγκεκριμένα χαρακτηριστικά μπορούν να συνδεθούν μοναδικά με ένα άτομο και επομένως να συνδράμουν αποτελεσματικά στην ταυτοποίησή του. Ωστόσο η εφαρμογή της συγκεκριμένης τεχνολογίας θα πρέπει να γίνεται ιδιαίτερα προσεκτικά, λαμβάνοντας υπόψη το είδος των δεδομένων που μετρούνται αλλά και εκείνων που προστατεύονται (π.χ. ποια βιομετρικά στοιχεία θα πρέπει να μετρηθούν για την πραγματοποίηση μιας συναλλαγής και πως η δημιουργηθείσα βάση δεδομένων θα προστατευθεί από κακόβουλες ή λανθασμένες ενέργειες διαχείρισής της)

E-Token

Στη συγκεκριμένη τεχνολογία χρησιμοποιείται μια συσκευή που μπορεί να χρησιμοποιηθεί αποτελεσματικά για τον έλεγχο και επομένως την προστασία ενός ατόμου, με την πρόσβαση στο σύστημα να απαιτεί τόσο την κατοχή της συσκευής όσο και τη γνώση του αντίστοιχου κωδικού. Σε φυσική μορφή μπορεί να είναι μια κάρτα ή ένα USB stick, ενώ διαπιστευτήρια ταυτότητας μπορούν να χρησιμοποιηθούν κωδικοί πρόσβασης, ψηφιακές υπογραφές, πιστοποιητικά και ιδιωτικά κλειδιά (Dartmouth, 2017).

Έξυπνες κάρτες

Πρόκειται για κάρτες (smart cards) που μπορούν να χρησιμοποιηθούν για διάφορες δραστηριότητες, ως πιστωτικές κάρτες ή κάρτες σε ATM. ως κάρτες καυσίμων, για κινητά τηλέφωνα ως κάρτες SIM, ως κάρτες άδειας για συνδρομητική τηλεόραση, ως κάρτες για τα μέσα μαζικής μεταφοράς, ως ηλεκτρονικά πορτοφόλια και μπορούν μέσω κρυπτογραφικών πρωτοκόλλων να συμβάλουν αποτελεσματικά στην αναγνώριση, πιστοποίηση, αποθήκευση και επεξεργασία των δεδομένων μιας εφαρμογής, παρέχοντας αυξημένη ασφάλεια στο χρήστη. Εντούτοις, είναι ευάλωτες όσον αφορά στη φυσική τους φθορά - καταστροφή αλλά και σε ενδεχόμενες επιθέσεις κακόβουλου λογισμικού (Rankl and Effing, 1997; Wikipedia, 2017b).



Εικόνα 11: Η δομή μιας έξυπνης κάρτας **(Wikipedia, 2017b)**

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

Μέσα από τα on line κοινωνικά δίκτυα ο άνθρωπος αφενός εξυπηρετεί μια έντονη ανάγκη του και αφετέρου υλοποιεί αυτή την εξυπηρέτηση αξιοποιώντας την τεχνολογική εξέλιξη η οποία με τη σειρά της συμβαδίζει με τη δική του. Άλλα στοιχεία της ανθρώπινης φύσης που εξυπηρετούνται είναι η έμφυτη τάση για σχολιασμό σε κοινωνικό επίπεδο, η ανάγκη για ψυχαγωγία και δημιουργία κοινοτήτων εντός των οποίων οι άνθρωποι θα ανταλλάξουν ιδέες και θα αναπτυχθούν εξυπηρετώντας κατ΄ επέκταση τις ανάγκες της κοινωνικής αναζήτησης και της κοινωνικής περιήγησης.

Η επικαιρότητα και η σημασία του θέματος της παρούσας εργασίας σχετίζεται άμεσα με τη δυναμική που παρουσιάζουν τα μέσα κοινωνικής δικτύωσης στη σύγχρονη πραγματικότητα, την ταχύτητα των τεχνολογικών εξελίξεων στο συγκεκριμένο τομέα, αλλά και τον ορισμό της έννοιας της ιδιωτικότητας ως το «δικαίωμα του να επιλέγει κανείς ελεύθερα το βαθμό έκθεσης του εαυτού του, τη στάση και τη συμπεριφορά του». Σε αυτά θα πρέπει να προστεθεί και η αξία της ίδιας της πληροφορίας, όχι μόνο ως μέσο άσκησης ελέγχου αλλά και ως στοιχείο που μπορεί να δημιουργήσει αξία και κέρδος για τα μέρη που θα την εκμεταλλευτούν.

Ζητούμενο αποτελεί μέσα από τη σχετική βιβλιογραφική ανασκόπηση να προσδιοριστεί η αλληλεπίδραση μέσων κοινωνικής δικτύωσης και ιδιωτικότητας του ατόμου, με απώτερο σκοπό τον προσδιορισμό κινδύνων παραβίασής της και μηχανισμών - πολιτικών προστασίας της.

Η εξάπλωση του διαδικτύου και των μέσων κοινωνικής δικτύωσης επιβεβαιώνονται από πλήθος στατιστικών στοιχείων. Αξιοσημείωτο είναι το γεγονός της διάχυτης ανησυχίας που επικρατεί για την ιδιωτικότητα των χρηστών παρά την αυξημένη συμμετοχή τους, μια διαπίστωση που μοιάζει εκ πρώτης όψης αντιφατική. Εντούτοις, καταδεικνύει την ανάγκη εκπαίδευσης των χρηστών σε συνεχή βάση, έτσι ώστε να διαμορφωθεί τελικά μια συγκεκριμένη συμπεριφορά – κουλτούρα ως προς τη συμμετοχή στα μέσα κοινωνικής δικτύωσης με παράλληλη απόδοση σεβασμού στην ιδιωτικότητα των χρηστών.

Ιδιωτικότητα και προσωπικά δεδομένα ως έννοιες συγκλίνουν, με τη σύγκλιση αυτή να προκύπτει από την αυξημένη ένταξη και ζήτηση των προσωπικών πληροφοριών στην καθημερινότητα (π.χ. ηλεκτρονικές συναλλαγές, δημιουργία προφίλ κτλ.)

Σε επίπεδο Ευρωπαϊκής Κοινότητας και σχετικών διατάξεων - οδηγιών (και αντίστοιχα εγχώριας εναρμόνισης) παρατηρείται ένα σαφές και ισχυρό νομοθετικό πλαίσιο, το οποίο παρουσιάζει επίσης τάση προσαρμογής στα νέα δεδομένα (π.χ διατάξεις που αφορούν τα cookies, τους παρόχους ηλεκτρονικής επικοινωνίας κ.α.). Εντούτοις, δεν μπορεί να παραβλεφθεί ο δυναμικός χαρακτήρας της διαδικασίας ανάπτυξης και εφαρμογής της τεχνολογίας και κατ' επέκταση των μέσων κοινωνικής δικτύωσης. Αυτό έχει ως αποτέλεσμα να απαιτείται μια συνεχής διαδικασία δυναμικής προσαρμογής. Μια πρόταση προς τη συγκεκριμένη κατεύθυνση θα ήταν η συνεργασία του νομοθέτη με ανεξάρτητα τεχνικά κλιμάκια και επιτροπές, καθώς επίσης και η ανάδειξη του ρόλου των επιμελητηρίων (έτσι θα είναι δυνατές αλλαγές - προσαρμογές του τύπου ένταξη της στατικής διεύθυνσης IP (Internet Protocol) στο σύνολο των προσωπικών δεδομένων αντίθετα με αυτή της δυναμικής). Φορείς όπως η Αρχή Διασφάλισης

του Απορρήτου των Επικοινωνιών και η Αρχή Προστασίας Προσωπικών Δεδομένων μπορούν να διαδραματίσουν καθοριστικό ρόλο ως προς τη συγκεκριμένη κατεύθυνση. Άλλωστε η πρόταση νομοθετικών μεταβολών αποτελεί μέρος του έργου που καλούνται εξ ορισμού να παράξουν.

Η δυσκολία της διαδικασίας είναι αναμφισβήτητη (σαν να προσπαθεί κανείς να αλλάξει λάστιχα σε ένα αυτοκίνητο εν κινήσει,, όπως χαρακτηριστικά αναφέρεται (Μήτρου, 2016)). Ένας βασικός τρόπος προσέγγισης περιπτώσεων αυτού του είδους είναι το κατά πόσο συνδέεται ο ψηφιακός και ο πραγματικός εαυτός, Ανάλογη είναι και η προσέγγιση που διέπει και την περίπτωση των μέσων κοινωνικής δικτύωσης με το εκάστοτε προφίλ να αποτελεί και τον ψηφιακό εαυτό. Ζητούμενο αποτελεί να προστατευτούν εκείνα τα σημεία που μπορούν να «μαρτυρήσουν» τη διασύνδεση ψηφιακής και πραγματικής υπόστασης. Επισημαίνεται επίσης η σημασία της αρχικής λήψης μέτρων, στο στάδιο του σχεδιασμού ανάλογων εφαρμογών (privacy by design) καθώς και στην ενσωμάτωση στοιχείων με τρόπο φιλικό προς το χρήστη (privacy-fiendly default settings)

Βασικό πρόβλημα της διαδικασίας αποτελεί η έλλειψη προτυποποίησης των μηχανισμών προστασίας της ιδιωτικότητας, με την ανάγκη ύπαρξης προτύπων ή τουλάχιστον κοινής γραμμής αντιμετώπισης να αποτελεί βασικό επίσης ζητούμενο. Εντούτοις, η δημιουργία, καθιέρωση και θέσπιση ενός παγκόσμιας εμβέλειας ρυθμιστικού εργαλείου δυσχεραίνει κατά πολύ αφενός για τεχνολογικούς λόγους (προβλήματα συμβατότητας διαφορετικών τεχνολογιών) και αφετέρου εξαιτίας λειτουργίας της ίδιας της αγοράς (με τη λήψη και διατήρηση της εκάστοτε δεσπόζουσας θέσης να είναι το λογικό και αναμενόμενο ζητούμενο).

Η κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης μπορεί να γίνει λαμβάνοντας υπόψη διάφορα κριτήρια, όπως το περιεχόμενο του μέσου, τη χρήση video και audio, τον τρόπο συμμετοχής, το βαθμό αλλά και το σκοπό χρήσης του δικτύου.

Υφίσταται πλήθος πεδίων κινδύνου που σχετίζονται με τα μέσα κοινωνικής δικτύωσης, απόρροια των τεχνολογικών παραμέτρων υλοποίησης της διαδικασίας. Σε αυτά τα πεδία συμπεριλαμβάνονται παράμετροι όπως οι βάσεις δεδομένων οι οποίες παρουσιάζουν ευρεία χρησιμότητα, η χρήση του ίδιου του Διαδικτύου και η δυνατότητα για την επανα-ταυτοποίηση ενός χρήστη σε πολλές και διαφορετικές δραστηριότητές τους, η ασύρματη δικτύωση, η εφαρμογή διάφορων μεθοδολογιών και «εργαλείων» που συμμετέχουν στη διαδικασία διαχείρισης και αποθήκευσης της προσωπικής πληροφορίας (όπως η εξόρυξη δεδομένων (data mining), η περιβάλλουσα νοημοσύνη (ambient intelligence) και οι συγκλίνουσες τεχνολογίες (converging technologies) – νανοτεχνολογίες, βιοτεχνολογίες, τεχνολογίες της πληροφορίας και της επικοινωνίας, καθώς και της γνωστικής επιστήμης)

Σε περισσότερο εξειδικευμένο επίπεδο όσον αφορά σε τεχνολογικά «εργαλεία» και μεθόδους που συμβάλλουν στην αύξηση της πιθανότητας προσβολής – παραβίασης της ιδιωτικότητας του ατόμου μέσα από τα κοινωνικά δίκτυα μπορούν να αναφερθούν οι μηχανές αναζήτησης, τα λογισμικά ανάκτησης, οι υπηρεσίες σύννεφου και το κακόβουλο λογισμικό. Ειδικότερα όσον αφορά στην τελευταία κατηγορία, όπως προέκυψε από τη σχετική επισκόπηση, υφίσταται πλήθος μορφής ιών αλλά και στρατηγικών δράσης τους, παρουσιάζοντας έτσι αυξημένο δυναμικό και δυνατότητα χρήσης τους από επίδοξους παραβάτες της ιδιωτικότητας εντός των μέσων κοινωνικής δικτύωσης. Δεν πρέπει επίσης να παραβλεφθεί η σύγχρονη τάση των επιχειρήσεων για συλλογή διαδικτυακών δεδομένων που σχετίζονται με τις προτιμήσεις των καταναλωτών προκειμένου να

εφαρμόσουν πολιτικές διαδικτυακού - ψηφιακού μάρκετινγκ (Content Ad, IP Targeting, email marketing, Search engine optimization, Search Engine Marketing, online streaming video, content marketing, Native Advertising etc.).

Από τη σχετική επισκόπηση προέκυψε πλήθος περιπτώσεων παραβίασης της ιδιωτικότητας τόσο σε ευρύτερο επίπεδο ηλεκτρονικών επικοινωνιών όσο και σε στοχευμένο επίπεδο χρήσης μέσων κοινωνικής δικτύωσης. Στον αντίποδα, οι μηχανισμοί προστασίας μπορούν να εντοπιστούν τόσο σε επίπεδο εφαρμογής τεχνολογικών μεθόδων όσο και σε επίπεδο υιοθέτησης συγκεκριμένων πολιτικών - συμπεριφορών.

Σε επίπεδο υιοθέτησης συγκεκριμένων πολιτικών - συμπεριφορών, θα πρέπει το σύστημα να έχει υιοθετήσει πολιτική ασφαλείας που θα διέπεται από το τρίπτυχο Ακεραιότητα – Διαθεσιμότητα - Εμπιστευτικότητα αλλά και συγκεκριμένες παραμέτρους. Επίσης θα πρέπει η δραστηριότητα εντός των κοινωνικών δικτύων να γίνεται και να διέπεται με βάση τη λογική προστασίας της ιδιωτικότητας τόσο από την πλευρά του διαχειριστή όσο και από αυτή του/της συμμετέχοντα/ουσας (με περιορισμό των μειονεκτημάτων που παρουσιάζει η μέχρι σήμερα εφαρμογή τους). Καθοριστικός επίσης είναι ο ρόλος της συμπεριφοράς, η οποία θα πρέπει να έχει συγκεκριμένα χαρακτηριστικά, καθ' όλη τη διάρκεια συμμετοχής σε αυτά τα μέσα, αλλά και στην ευρύτερη διαδικτυακή παρουσία των χρηστών.

Οι τεχνολογικές εφαρμογές που έχουν χρησιμοποιηθεί κατά καιρούς για την προστασία της ιδιωτικότητας στο διαδίκτυο διαχωρίζονται σε δύο βασικές κατηγορίες, στις τεχνολογίες ανωνυμίας ή ψευδωνυμίας και στις ονομαστικές τεχνολογίες. Υφίσταται ποικιλία εφαρμογών, με καθεμία από αυτές να περιλαμβάνει σε χαμηλότερα επίπεδα πλήθος άλλων εφαρμογών και τεχνολογιών, τόσο μεμονωμένα όσο και συνδυαστικά. Ενδεικτικά αναφέρονται η ταυτοποίηση μέσω ραδιοσυχνοτήτων, οι βιομετρικές τεχνολογίες, το E-Token και οι «έξυπνες» κάρτες.

Σε κάθε περίπτωση, λαμβάνοντας υπόψη πως η ψηφιακή προσωπικότητα θα αποτελεί στο εγγύς μέλλον αναπόσπαστο μέρος της κατασκευής του κοινωνικού ατόμου, το ζήτημα της προστασίας της ιδιωτικότητας θα πρέπει να προσεγγίζεται δυναμικά και υπεύθυνα τόσο από τους επίσημους φορείς όσο και από τους διαχειριστές/χρήστες των μέσων κοινωνικής δικτύωσης.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Ακριβοπούλου, Μ. (2011) 'Η προστασία της ιδιωτικότητας στην ΕΕ: Μια ανάλυση του νομοθετικού πλαισίου και της νομολογίας του ΔΕΚ', *Τριμηνιαία Επιθεώρηση Ελληνικής και Ευρωπαϊκής Συνταγματικής Θεωρίας και Πράξης*.

2. 'Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών' (2016). Available at: http://www.adae.gr/ (Accessed: 30 May 2017).

3. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (2016) *Ετήσια Έκθεση 2015*.

4. *Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα* (2017). Available at: http://www.dpa.gr/ (Accessed: 30 May 2017).

5. Βλάχος, Β. (2011) 'Ασφάλεια του Διαδικτύου και Ηλεκτρονική Δημοκρατία', in *Συνέδριο των Πανεπιστημίων Μακεδονίας και Ανατολικού Λονδίνου για την ασφάλεια του Διαδικτύου και την ηλεκτρονική δημοκρατία*. Θεσσαλονίκη.

6. Βλάχος, Π. and Δρόσος, Δ. (2004) *Νέες τεχνολογίες και διαφήμιση*. Αθήνα.

7. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (1998) *Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα*. Available at: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31997L0066&from=EL.

8. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (2002) 'Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002'. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:el:PDF.

9. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (2006) *Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006 , για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίω*. Available at: http://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A32006L0024.

10. Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης (2012) *Ενοποιημένη Απόδοση της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης*.

Available at: http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:12012E/TXT&from=EL.

11. Ευρωπαϊκή Σύμβαση Δικαιωμάτων Ανθρώπου (2010) *Άρθρο 8 – Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής | ΕΥΡΩΠΑΪΚΗ ΣΥΜΒΑΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΑΝΘΡΩΠΟΥ*. Available at: https://hrconvention.wordpress.com/2010/07/03/άρθρο-8-δικαίωμα-σεβασμού-της-ιδιωτική/ (Accessed: 29 May 2017).

12. Ζωρόθεος, Α. (2007) *Ιδιωτικότητα και Διαδίκτυο*. Οικονομικό Πανεπιστήμιο Αθηνών.

13. Ιγγλεζάκης, Ι. (2003) *Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου*. Σάκκουλα.

14. Ιόνιο Πανεπιστήμιο (2007) 'Επιστημονικές Σημειώσεις Ασφάλειας'. Τμήμα Πληροφορικής. Available at: http://195.130.124.90/~emagos//security/Simeioseis-Asfaleia Part B.pdf.

15. Καραμπάσης, Ζ. (2008) *Το blogging στην Ελλάδα: Προφίλ, κίνητρα και πρακτικές των ελληνόφωνων bloggers*. Πάντειο Πανεπιστήμιο.

16. Καραντινάκη, Α. (2015) *Σύγχρονες μορφές επικοινωνίας και η επιρροή τους στις ανθρώπινες σχέσεις*. ΑΤΕΙ Ιονίων Νήσων.

17. Κατεργιαννάκης, Ν. (2012) *Μοντέλα Μάρκετινγκ στα Κοινωνικά Δίκτυα [Μια μελέτη για την Ελλάδα]*. Πανεπιστήμιο Μακεδονίας.

18. Κερασιώτης, Π. (2014) *Τι είναι το Native Advertising και γιατί σε ενδιαφέρει?* Available at: http://www.smokypixel.gr/2014/06/ti-einai-to-native-advertising-kai-giati-se-endiaferei/.

19. Κιαγιάς, Α. (2008) 'Κρυπτογραφία: Αρχές και πρωτόκολλα', in *Fall - Διάλεξη 10*.

20. Κόνσουλας, Θ. (2013) *Ελληνικά -και μη- στατιστικά των Social Media για το 2013*. Available at: http://www.socialmedialife.gr/104344/social-media-stats-2013/.

21. Κοσμετάτος, Σ. (2012) 'Το ίντερνετ σε αριθμούς: τι συμβαίνει κάθε μέρα'. Available at: http://www.newsonly.gr/article.asp?catid=36388&subid=2&pubid=128976962.

22. Κουτσογιαννοπούλου, Ν. (2013) *Τα νέα μέσα ηλεκτρονικής κοινωνικής δικτύωσης (Social Media) και η σχέση τους με την καταναλωτική συμπεριφορά*. Πανεπιστήμιο Πατρών.

23. Μήτρου, Λ. (2016) 'Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνίες - Η νομική διάσταση', in. Available at: https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjN7NLc_unRAhXIWxQKHUWEBIkQFggkMAE&url=http%

3A%2F%2Fwww.icsd.aegean.gr%2Fwebsite_files%2Fproptyxiako%2F658467167.doc&usg=AFQjCNEpy4t4yTf9Vc7Pip3v8bIYH68YyQ&bvm=bv.145822982,d.d2s&cad.

24. Ναυτεμπορική (2013) *Google: Επτά εκατ. δολ. για παραβίαση ιδιωτικότητας από το Street View*. Available at: http://www.naftemporiki.gr/story/626217/google-epta-ekat-dol-gia-parabiasi- (Accessed: 2 July 2017).

25. Νεραντζίδου, Μ. (2011) *Χρήση κοινωνικών μέσων δικτύωσης στην εκπαίδευση Μια έρευνα σε φοιτητές και καθηγητές του ΑΤΕΙ Θεσσαλονίκης*. ΑΤΕΙ Θεσσαλονίκης.

26. Νομικά Νέα (2017) 'Το "δικαίωμα στη λήθη" και οι μηχανές αναζήτησης'. Available at: http://nomika-nea.gr/το-δικαίωμα-στη-λήθη-και-οι-μηχανές-αν/.

27. Παπαπέτρου, Ε. (2017) 'Ασύρματα Δίκτυα'. Πανεπιστήμιο Ιωαννίνων. Available at: http://www.cse.uoi.gr/~epap/MYE006/downloads/lect1.pdf.

28. Πάσσας, Ι. Α. (2009) 'Κοινωνικά δίκτυα στο Internet. Η νέα πρόκληση στην επικοινωνία για τη νέα γενιά'.

29. Ρήγας, Δ. (2014) *Cloud Services ('Υπηρεσίες Σύννεφου'), Κέντρο Πληροφορικής και Τεχνολογίας*. Available at: http://dide.lef.sch.gr/plinetl/109 (Accessed: 4 July 2017).

30. Σεργκενλίδη, Α. (2014) *Αποτελεσματικότητα του Digital Advertising στις σύγχρονες Ελληνικές επιχειρήσεις*. Πανεπιστήμιο του Derby και Μεσογειακό Κολλέγιο (MC).

31. Σπυριδωνίδου, Κ. (2015) *Ασφάλεια και Προστασία της Ιδιωτικότητας στο Διαδίκτυο*. Εθνικό Μετσόβιο Πολυτεχνείο.

32. Τζιραλής, Γ. (2007) 'Εισαγωγή στο Data Mining Από τα δεδομένα στη γνώση'. ΕΜΠ ΜΜ ΒΔΕΕ. Available at: http://gtziralis.com/wp-content/uploads/mis_introtodatamining.pdf.

33. Τσαγκανού, Μ. (2014) *Η κοινωνική παράμετρος στην προστασία της ιδιωτικότητας του ατόμου - χρήστη Νέων Τεχνολογιών*. Πανεπιστήμιο Πατρών.

34. Τσακνάκης, Δ. (2014) *Ανάλυση - Αξιολόγηση Λογισμικού Antivirus και Τεχνικές Αποφυγής του*. Πανεπιστήμιο Πειραιά. Available at: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/6439/MTE1134.pdf?sequence=1&isAllowed=y.

35. Ali Rohani, V. and Siew Hock, O. (2009) 'On Social Network Web Sites: Definition, Features, Architectures and Analysis Tools', *Journal of Computer Engineering*, 1, pp. 3–11. Available at: http://jacr.iausari.ac.ir/article_2392_e8aa31fb1ae5cc322a7686de2fe54d61.pdf (Accessed: 30 May 2017).

36. Bentham, J. (1995) ‘The Panopticon Writings’, in *The Panopticon Writings*, pp. 29–95. doi: 10.1007/s00287-006-0116-6.

37. Boyd, D. M. and Ellison, N. B. (2008) ‘Social Network Sites: Definition, History, and Scholarship’, *Journal of Computer-Mediated Communication*, 13, pp. 210–230. doi: 10.1111/j.1083-6101.2007.00393.x.

38. Brass, D. J., Butterfield, K. D. and Skaggs, B. C. (1998) ‘Relationships and unethical behavior: A social network perspective’, *Academy of Management Review*, pp. 14–31. doi: 10.2307/259097.

39. Brito, J. (2004) ‘Relax Don’t Do It: Why RFID Privacy Concerns are Exaggerated and Legislation is Premature’, *UCLA Journal of Law and Technology*, 5.

40. Cavazza, F. (2011) *Social Media Landscape 2011 | FredCavazza.net*. Available at: https://fredcavazza.net/2010/12/14/social-media-landscape-2011/ (Accessed: 30 May 2017).

41. Chao, J. (2007) ‘Student project collaboration using wikis’, in *Software Engineering Education Conference, Proceedings*, pp. 255–261. doi: 10.1109/CSEET.2007.49.

42. Chechik, D. (2013) *Look What I Found: Moar Pony!*, *Trustwave*. Available at: https://www.trustwave.com/Resources/SpiderLabs-Blog/Look-What-I-Found---Moar-Pony!/ (Accessed: 4 July 2017).

43. Clarke, R. (1988) ‘Information technology and dataveillance’, *Communications of the ACM*, 31(5), pp. 498–512. doi: 10.1145/42411.42413.

44. Cranor, L. F. (1999) ‘Internet privacy’, *Communications of the ACM*, 42(2), pp. 28–38. doi: 10.1145/293411.293440.

45. Culnan, M. J. and Armstrong, P. K. (1999) ‘Information Privacy Concerns, Fairness, and Impersonal Trust: An Empirical Investigation’, *Organization Science*, 10(1), pp. 104–115.

46. Dartmouth (2017) *Software and Computers | Information Technology Services*. Available at: http://tech.dartmouth.edu/its/services-support/help-yourself/knowledge-base/software-and-computers (Accessed: 5 July 2017).

47. Deuze, M. (2003) ‘The web and its journalisms: considering the consequences of different types of newsmedia online’, *New Media & Society*. Available at: https://scholarworks.iu.edu/dspace/bitstream/handle/2022/6602/DeuzeNMS2003.pdf?sequence=1&isAllowed=y (Accessed: 13 May 2017).

48. Van Eecke, P. and De Bruyn, J. (2015) *EUROPE: European cookie sweep results published: average of 34.6 cookies per website. Privacy Matters*. Available at: http://blogs.dlapiper.com/privacymatters/europe-european-cookie-sweep-results-published-average-of-34-6-cookies-per-website/

(Accessed: 3 July 2017).

49. European Commission (2015) *ARTICLE 29 DATA PROTECTION WORKING PARTY COOKIE SWEEP COMBINED ANALYSIS – REPORT*. Available at: http://ec.europa.eu/justice/data-protection/index_en.htm (Accessed: 3 July 2017).

50. Evans, D. (2008) *Social media marketing : an hour a day*. Wiley.

51. Flanagin, A. J. (2005) 'IM Online: Instant Messaging Use Among College Students', *Communication Research Reports*, 22(3), pp. 175–187. doi: 10.1080/00036810500206966.

52. Frankowski, D., Cosley, D., Sen, S., Terveen, L. and Riedl, J. (2006) 'You Are What You Say: Privacy Risks of Public Mentions'. Available at: http://www.cs.cornell.edu/~danco/research/papers/privacy-sigir2006.pdf (Accessed: 16 June 2017).

53. Gunawardena, C., Hermans, M. B., Sanchez, D., Richmond, C., Bohley, M. and Tuttle, R. (2009) 'A theoretical framework for building online communities of practice with social networking tools', *Educational Media International*, 46(1), pp. 3–16. doi: 10.1080/09523980802588626.

54. Johnson, D. G. and Nissenbaum, H. (1995) *Computers, Ethics and Social Values*. Edited by Pearson. Available at: https://www.pearson.com/us/higher-education/program/Johnson-Computers-Ethics-and-Social-Values/PGM148861.html.

55. Kaplan, A. M. and Haenlein, M. (2009) 'The fairyland of Second Life: Virtual social worlds and how to use them', *Business Horizons*, 52(6), pp. 563–572. doi: 10.1016/j.bushor.2009.07.002.

56. Kaplan, A. M. and Haenlein, M. (2010) 'Users of the world, unite! The challenges and opportunities of Social Media', *Business Horizons*, 53(1), pp. 59–68. doi: 10.1016/j.bushor.2009.09.003.

57. Kwon, O. and Wen, Y. (2010) 'An empirical study of the factors affecting social network service use', *Computers in Human Behavior*, 26(2), pp. 254–263. doi: 10.1016/j.chb.2009.04.011.

58. Lampe, C., Ellison, N. and Steinfield, C. (2006) 'A Face(book) in the Crowd: Social Searching vs. Social Browsing', in *Proceedings of the 2006 20th Anniversary Conference on Computer-Supported Cooperative Work CSCW '06*, pp. 167–170. doi: 10.1145/1180875.1180901.

59. Lee, E. S. (1999) *Essays about computer security*. University of Cambridge. Available at: http://www.cl.cam.ac.uk/~mgk25/lee-essays.pdf (Accessed: 4 July 2017).

60. LIFO (2015) *Απειλή για την ιδιωτικότητα τα 'έξυπνα' gadgets*. Available at: http://www.candianews.gr/2015/01/07/apili-gia-tin-idiotikotita-ta-exipna-gadgets/.

61. McCrohan, K. F. (1989) ‘Information Technology, Privacy, and the Public Good’, *Journal of Public Policy & Marketing*, 8(1), pp. 265–278. doi: 10.2307/30000325.

62. Milardo, R. M. and National Council on Family Relations. (1988) *Families and social networks*. Sage Publications. Available at: https://books.google.gr/books/about/Families_and_social_networks.html?id=qEtHAAAAMAAJ&redir_esc=y (Accessed: 30 May 2017).

63. Pagliery, J. (2013) *2 million Facebook, Gmail and Twitter passwords stolen in massive hack, CNN Tech*. Available at: http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/ (Accessed: 4 July 2017).

64. Perlman, C. (2009) *eBoot camp : proven Internet marketing techniques to grow your business*. John Wiley & Sons.

65. Pescosolido, B. A. (2006) ‘Of Pride and Prejudice: The Role of Sociology and Social Networks in Integrating the Health Sciences’, *Journal of Health and Social Behavior*. SAGE PublicationsSage CA: Los Angeles, CA, 47(3), pp. 189–208. doi: 10.1177/002214650604700301.

66. Pollach, I. (2007) ‘What’s wrong with online privacy policies?’, *Communications of the ACM*, 50(9), pp. 103–108. doi: 10.1145/1284621.1284627.

67. Rankl, W. (Wolfgang) and Effing, W. (Wolfgang) (1997) *Smart card handbook*. Wiley.

68. Richardson, W. (2010) *Blogs, wikis, podcasts, and other powerful Web tools for classrooms*. Corwin.

69. Smith, R. and Shao, J. (2007) ‘Privacy and e-commerce: a consumer-centric perspective’, *Electronic Commerce Research*. Kluwer Academic Publishers-Plenum Publishers, 7(2), pp. 89–116. doi: 10.1007/s10660-007-9002-9.

70. Sundaram, H., Lin, Y.-R., De Choudhury, M. and Kelliher, A. (2012) ‘Understanding Community Dynamics in Online Social Networks: A multidisciplinary review’, *IEEE Signal Processing Magazine*, 29(2), pp. 33–40. doi: 10.1109/MSP.2011.943583.

71. Tavani, H. T. (2005) ‘Search Engines, Personal Information and the Problem of Privacy in Public’, *IRIE International Review of Information Ethics*, 3(6). Available at: http://www.i-r-i-e.net/inhalt/003/003_tavani.pdf (Accessed: 16 June 2017).

72. Tech in.gr (2016) *Παραδέχτηκε την ενοχή του ο χάκερ του CelebGate*. Available at: http://tech.in.gr/news/article/?aid=1500104351 (Accessed: 4 July 2017).

73. Thomas, R. E. and Maurer, V. G. (1997) ‘Database Marketing Practice:

Protecting Consumer Privacy', *Journal of Public Policy & Marketing*, 16(1), pp. 147–155. doi: 10.1503/cmaj.101556.

74. Tic Tac Laboratories (2012) *6 κίνδυνοι για τα δεδομένα μας στο σύννεφο | Ανάκτηση Δεδομένων - Data Recovery*. Available at: https://tictac.gr/6-kindunoi-gia-ta-dedomena-mas-sto-sunnefo (Accessed: 4 July 2017).

75. Vedder, A. (2011) 'Chapter 2 Privacy 3.0', in *Innovating Government, Information Technology and Law Series 20*, pp. 17–29. doi: 10.1007/978-90-6704-731-9.

76. Vukasovič, T. (2013) 'Journal of Media and Communication Studies Building successful brand by using social networking media', 5(6), pp. 56–63. doi: 10.5897/JMCS2013.

77. Warren, S. D. and Brandeis, L. D. (1890) 'The Right to Privacy', *Harvard Law Review*, IV(5). Available at: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (Accessed: 25 May 2017).

78. Westin, A. F. (1968) 'Privacy And Freedom', 166. Available at: http://scholarlycommons.law.wlu.edu/wlulr (Accessed: 29 May 2017).

79. Wikipedia (2016) *RFID*. Available at: https://el.wikipedia.org/wiki/RFID (Accessed: 5 July 2017).

80. Wikipedia (2017a) *Μέσα κοινωνικής δικτύωσης - Βικιπαίδεια*. Available at: https://el.wikipedia.org/wiki/Μέσα_κοινωνικής_δικτύωσης (Accessed: 30 May 2017).

81. Wikipedia (2017b) *Smart card*. Available at: https://en.wikipedia.org/wiki/Smart_card.

82. Zhang, J. (2010) *Social Media and Distance Education*. Available at: https://www.scribd.com/document/160525480/Social-Media-and-Distance-Education-De-Oracle (Accessed: 30 May 2017).