ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΑΜΕΤΑΠΤΥΧΙΑΚΟ - ΔΙΑΤΜΗΜΑΤΙΚΟ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ Δ.Π.Μ.Σ.

“ΜΑΘΗΜΑΤΙΚΗ ΠΡΟΤΥΠΟΠΟΙΗΣΗ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ”

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΚΩΝΣΤΑΝΤΙΝΑΣ ΣΠΥΡΙΔΩΝΙΔΟΥ

ΠΤΥΧΙΟΥΧΟΣ ΣΧΟΛΗΣ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΕΜΠ

Επιβλέπων Καθηγητής:

Στεφανέας Πέτρος

ΑΘΗΝΑ, Μάρτιος 2015

ΕΥΧΑΡΙΣΤΙΕΣ

Θεωρώ υποχρέωσή μου να ευχαριστήσω τον επιβλέποντα καθηγητή του Εθνικού Μετσόβιου Πολυτεχνείου, κ. Στεφανέα Πέτρο για τις εποικοδομητικές παρατηρήσεις του, που συνέβαλαν τα μέγιστα ώστε να μπορέσω να ολοκληρώσω τη συγγραφή της εργασίας μου μέσα σε κλίμα απόλυτης συνεννόησης, καθώς επίσης και τα μέλη της επιτροπής κ. Θεολόγου και κ. Κολέτσο, αμφότεροι καθηγητές του Εθνικού Μετσόβιου Πολυτεχνείου.

Τέλος, ευχαριστώ όλους όσοι με στήριξαν στην προσπάθεια αυτή.

Abstract

The Web has spurred an information revolution even, reaching sectors left untouched by the personal computing boom of the 80's. It made information ubiquity a reality for sizeable segments of the world population, transcending all socioeconomic levels. The ease of information access, coupled with the availability of personal data, also made it easier and more tempting for interested parties (individuals, businesses, and governments) to intrude on people's privacy in unprecedented ways levels.

Internet privacy involves the right of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Internet privacy is a subset of computer privacy. Although we recognize that many and different levels of privacy violations exist, the present study is analyzing the internet privacy from user's perspectives focusing on its preservation or loss.

Internet users' privacy can be violated in different ways and with different intentions. Unauthorized information transfer, weak security, data magnets (cookies, software downloads etc.), and indirect forms of information collection are some of them.

However, internet users on their vast majority tend to neglect or overlook the privacy settings and over-share data that can be easily either stolen or used in many ways against them as there are parties who would use these data in their favor. This is easily perceptible through social media where users share their whole life believing that it is protected.

As far as the programmers and the managers of the information systems, they must take into account the appropriate privacy enhancing technologies in order to provide privacy and protection to the internet user, considering that the legislative measures are not sufficient.

Keywords:

Internet privacy, data anonymization, privacy attacks, malicious software, privacy enhancing technologies

ΕΙΣΑΓΩΓΗ

Από τα πρώτα χρόνια της πορείας των επικοινωνιών και της επιστημονικής ανάπτυξης στον τομέα της πληροφορικής, ένα από τα πιο αξιοσημείωτα θέματα που εξακολουθεί να υφίσταται είναι η διαχείριση των προσωπικών δεδομένων και η προστασία της ιδιωτικότητας του χρήστη. Η ανάπτυξη των τεχνολογιών κατέστησε αντιληπτή τη μετατροπή της κοινωνίας σε κοινωνία της πληροφορίας μέσω του διαδικτύου. Σύμφωνα με ειδικούς, το διαδίκτυο τείνει να μετατραπεί από ένα μέρος όπου καταφεύγει ο χρήστης για να αναζητήσει κάποια πληροφορία, σε ένα μέρος όπου απλά θα βρίσκεται.

Η επίδραση του διαδικτύου αναφορικά με την προστασία του χρήστη και των προσωπικών του δεδομένων δεν μπορεί να γίνει ακόμα αντιληπτή. Οι κανονισμοί και οι νομοθετικές ρυθμίσεις θέτουν κάποια όρια τα οποία δεν επαρκούν. Θα πρέπει να χρησιμοποιηθούν και οι κατάλληλες τεχνικές ενίσχυσης της ιδιωτικότητας στο διαδίκτυο ανάλογα πάντα με τα τεχνολογικά ζητήματα που προκύπτουν και τις απαιτήσεις του χρήστη και των εταιρειών.

Σήμερα, ολοένα και μεγαλύτερος αριθμός χρηστών χρησιμοποιεί τις διαδικτυακές εφαρμογές και τις νέες τεχνολογίες για τις συναλλαγές του με φορείς και επιχειρήσεις, για την αγορά προϊόντων και υπηρεσιών αλλά και για την ενημέρωσή του. Αυτό όμως που δε γνωρίζουν είναι κατά πόσο τα προσωπικά δεδομένα που αποκαλύπτουν τίθενται υπό εκμετάλλευση και κατά συνέπεια παύουν πλέον να είναι προστατευμένοι. Ωστόσο, το παράδοξο που παρατηρείται είναι πως ιδίως σε εφαρμογές κοινωνικής δικτύωσης, τα άτομα εξακολουθούν να αποκαλύπτουν σε μεγάλο βαθμό προσωπικά τους δεδομένα, αν και ανησυχούν για την παραβίαση της ιδιωτικότητάς τους.

Στη παρούσα διπλωματική εργασία μελετάται η ιδιαίτερη αυτή έννοια της ιδιωτικότητας του χρήστη αναφορικά με το διαδίκτυο.

Πιο συγκεκριμένα στο πρώτο κεφάλαιο αποσαφηνίζεται ο όρος της ιδιωτικότητας, της ασφάλειας και της προστασίας των προσωπικών δεδομένων όπως αυτά νοούνται στη σημερινή ψηφιακή εποχή.

Στο δεύτερο κεφάλαιο επιχειρείται μια παρουσίαση της ισχύουσας νομοθεσίας για ζητήματα ιδιωτικότητας κυρίως σε ευρωπαϊκό αλλά και σε παγκόσμιο επίπεδο.

Στο τρίτο κεφάλαιο, αναλύονται οι λόγοι παραβίασης της ιδιωτικότητας και του απορρήτου των τεχνολογιών διαδικτύου καθώς και οι πηγές της συγκεκριμένης παραβίασης.

Στο τέταρτο κεφάλαιο παρουσιάζονται χαρακτηριστικές μελέτες περίπτωσης παραβίασης της ιδιωτικότητας που έκαναν αίσθηση στον τεχνολογικό κόσμο του 21ου αιώνα.

Στο πέμπτο κεφάλαιο πραγματοποιείται ανάλυση του κακόβουλου λογισμικού που εφαρμόζεται για να πραγματοποιηθούν επιθέσεις στο διαδίκτυο με σκοπό την αλίευση προσωπικών δεδομένων του χρήστη και την παράνομη δραστηριότητά τους.

Εν συνεχεία, το έκτο κεφάλαιο αναφέρεται στους κινδύνους από το διαμοιρασμό αρχείων στο διαδίκτυο είτε μέσω συστημάτων ομότιμης δικτύωσης (peer-to-peer) είτε μέσω υπολογιστικού νέφους (cloud computing).

Στο έβδομο κεφάλαιο ερευνώνται τα μέσα κοινωνικής δικτύωσης αλλά και τα θέματα ασφάλειας και ιδιωτικότητας που εγείρει η δημοσίευση προσωπικών στοιχείων από τους χρήστες.

Στο όγδοο κεφάλαιο, μελετώνται οι βασικότερες τεχνικές διασφάλισης της ιδιωτικότητας των δεδομένων και της ανωνυμίας των χρηστών από τα πληροφοριακά συστήματα. Οι υπεύθυνοι των εν λόγω συστημάτων θα πρέπει να αποτρέπουν την παραβίαση της ιδιωτικότητας και να την συμπεριλαμβάνουν ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπο-ανάπτυξη σύστημα.

Τέλος, στο ένατο κεφάλαιο μελετάται ο κλάδος της ιδιωτικότητας και της ανωνυμοποίησης των δεδομένων ο οποίος στοχεύει στο μετασχηματισμό των αρχικών δεδομένων ούτως ώστε να μειωθεί η συσχέτισή τους και να περιοριστεί η απώλειά της πληροφορίας. Η ανωνυμοποίηση των δεδομένων αποτελεί έναν σημαντικό κλάδο της Επιστήμης των Υπολογιστών καθώς η πλειονότητα της ανθρώπινης δραστηριότητας καταγράφεται ούτως ώστε να ερευνηθεί και η προστασία των δεδομένων αυτών συνιστά βασική αρχή της.

Πίνακας Περιεχομένων

Κατάλογος Σχημάτων

ΚΕΦΑΛΑΙΟ 1
ΙΔΙΩΤΙΚΟΤΗΤΑ, ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ, ΕΜΠΙΣΤΟΣΥΝΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

1.1 Η Έννοια της Ιδιωτικότητας

Defining privacy

Η ιδιωτικότητα ως έννοια από μόνη της είναι ιδιαίτερα ενδιαφέρουσα και μυστηριώδης, ίσως επειδή σχεδόν κανένας δεν συμφωνεί στο τι πραγματικά είναι. Ωστόσο, το δικαίωμα στην ιδιωτικότητα είναι εκείνο που ενέπνευσε πλήθος συζητήσεων και αντιπαραθέσεων σε πολλά επιστημονικά πεδία όπως νομικό, φιλοσοφικό, κοινωνικό, πολιτικό και πιο πρόσφατα τεχνολογικό πεδίο.

Νοούμενη ως προστασία έναντι της έξωθεν επιτήρησης και της ετερόνομης ρύθμισης της ανθρώπινης ύπαρξης και ζωής, η ιδιωτικότητα ανάγεται στις απαρχές της καταγεγραμμένης ανθρώπινης ιστορίας και διατρέχει την εξέλιξή της. Μάλιστα ορισμένοι συγγραφείς, όπως ο John Curtis Raines [1], εντοπίζουν την πρώτη «εκδήλωση ιδιωτικότητας» ήδη στη «Γένεση», όταν ο Θεός αντιστάθηκε στη δύναμη να προσηλώσει το βλέμμα του στους γυμνούς πρωτόπλαστους, ενώ στην κλασική ελληνική σκέψη η διάκριση μεταξύ ιδιωτικού και δημόσιου χώρου και βίου συνιστούσε μία αυταπόδεικτη και αξιωματική παραδοχή.

Οι ορισμοί ποικίλλουν ανάλογα με το περιεχόμενο, την κουλτούρα και το περιβάλλον. Σε άρθρο του 1890, οι Samuel Warren και Louis Brandeis [2] ορίζουν την ιδιωτικότητα ως «το δικαίωμα του να είσαι μόνος» (the right to be let alone) και τονίζεται η αναγκαιότητα να κατοχυρωθεί συνταγματικά η έννοια της ιδιωτικότητας. Επίσης στο ίδιο άρθρο αναφέρεται πως η σημασία του θέματος της ιδιωτικότητας συνεχώς θα μεγαλώνει καθώς η αξία της είναι πολύ μεγαλύτερη από ότι στο παρελθόν. Μετά από μακροχρόνιες κοινωνικές συζητήσεις το 1965, για πρώτη φορά θεσπίζεται το συνταγματικό δικαίωμα στην ιδιωτικότητα από το ανώτατο δικαστήριο των Η.Π.Α. και έτσι κατοχυρώνεται και συνταγματικά [3]. Χαρακτηριστικά αναφέρουμε τη δήλωση το Lyndon B. Johnson, προέδρου των Η.Π.Α. (1963-1969), πως «κάθε άνθρωπος θα πρέπει να γνωρίζει ότι οι συνομιλίες του, οι συναναστροφές του και η προσωπική του ζωή είναι ιδιωτικά».

Το 1967 ο Alan Westlin ορίζει την ιδιωτικότητα ως 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» [4] .

Ο κανονιστικός όρος της έννοιας έχει ήδη τις ρίζες του ακόμα πιο πίσω, στον J.S. Mill (1806-1873), ο οποίος συνηγορεί υπέρ της προστασίας της ατομικής ελευθερίας έναντι σε εισβολές από κυβερνήσεις, κοινωνικούς φορείς και άλλους πολίτες [5].

Μια από τις πιο πρόσφατες αναφορές στην ιδιωτικότητα είναι της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα (1948), όπου στο άρθρο 17 αναφέρει πως «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 υπόληψής του. Επίσης, καθένας έχει το δικαίωμα της έννομης προστασίας από τέτοιου είδους παρεμβάσεις και επιθέσεις».

Ο Rachels το 1975 κάνει λόγο για «την ικανότητα να ελέγχουμε ποιος έχει πρόσβαση σε εμάς» και ο Benn το 1988 θέτει το σεβασμό στην προσωπική ζωή ως συνώνυμο του σεβασμού στην αυτονομία και την αξιοπρέπεια του ατόμου.

Οι κοινωνιολόγοι ορίζουν την έννοια της ιδιωτικότητας ως το δικαίωμα κάποιου να ελέγχει τη συλλογή και τη χρήση των πληροφοριών σχετικά με τον εαυτό του [6].

Εκατό και πλέον χρόνια μετά από το δικαίωμα του ατόμου σε μια ανενόχλητη ιδιωτική ζωή των αμερικανών δικαστών Warren και Brandeis, και υπό τη καταλυτική επίδραση της τεχνολογικής επανάστασης, ήδη η κλασική αντίληψη της ιδιωτικότητας έχει σημαντικά εμπλουτιστεί με επιμέρους δικαιώματα, όπως το δικαίωμα στην ιδιωτική ζωή, ο περιορισμός της προσβασιμότητας, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο, η ελαχιστοποίηση των παρεμβάσεων, η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και το δικαίωμα στην απόλαυση της μοναξιάς, της – υπό στενή εννοία- ιδιωτικότητας, της ανωνυμίας και της απόσυρσης.

Γενικά, η ατομική ιδιωτικότητα αποτελεί ένα κοινωνικό και πολιτισμικό ζήτημα. Ωστόσο , με την πανταχού παρουσία των υπολογιστών και την εμφάνιση του διαδικτύου, η ιδιωτικότητα εξελίχθηκε σε ψηφιακό πρόβλημα. Πιο συγκεκριμένα, η επανάσταση του διαδικτύου άλλαξε άρδην τον τρόπο που αντιλαμβανόμαστε την ιδιωτικότητα οδηγώντας στον όρο internet privacy ήτοι ασφάλεια του διαδικτύου.

Ο συγκεκριμένος όρος αναφέρεται στο δικαίωμα των χρηστών του διαδικτύου να αποκρύπτουν προσωπικές πληροφορίες και να απολαμβάνουν ένα βαθμό ελέγχου στα δεδομένα που μοιράζονται με άλλους χρήστες του διαδικτύου.

1.2 Η Ιδιωτικότητα στη ψηφιακή εποχή

Με τη πάροδο του χρόνου, η τεχνολογική δυνατότητα διείσδυσης στη ζωή και την επικοινωνία, στην προσωπικότητα και στις συνήθειες του χρήστη ανέδειξε και την ποιοτική διάσταση των κινδύνων που συνδέονται με την Κοινωνία της Πληροφορίας, καθώς ήδη η ποσοτική αύξηση συνεπέφερε την αύξηση της έντασης του βαθμού προσβολής των δικαιωμάτων. Ήδη, στις αρχές του '70 τα φιλοσοφικά, πολιτικά και νομικά ζητήματα που υπογράμμιζαν το δικαίωμα στην –πληροφοριακή πλέον- ιδιωτικότητα, βρέθηκαν στο επίκεντρο μιας συζήτησης που διέβλεπε στη τεχνολογία της πληροφορικής τους κινδύνους οι οποίοι δεν περιορίζονταν σε κλειστές επιτηρούμενες κοινότητες αλλά αφορούσαν προοπτικά το σύνολο των ατόμων και των δραστηριοτήτων τους.

Στη σημερινή εποχή της πληροφορίας, ο όγκος των δεδομένων που καθημερινά διακινείται μέσω του διαδικτύου είναι απλά ασύμμετρος. Σύμφωνα με τον Moor (1997) [7] επειδή είναι σχεδόν αδύνατον να ελεγχθεί το σύνολο των πληροφοριών ενός ατόμου, στη σημερινή εποχή, θα πρέπει να δημιουργηθούν ζώνες ιδιωτικότητας (zones of privacy), οι οποίες θα επιτρέπουν στα άτομα να ελέγχουν τα επίπεδα προσβασιμότητας στην ιδιωτική τους πληροφορία ανάλογα με τη συγκεκριμένη κατάσταση που βρίσκονται κάθε φορά. Επομένως η ιδιωτικότητα μπορεί να εκληφθεί ως μια σύνθεση της δυνατότητας ελέγχου της προσωπικής πληροφορίας και της περιορισμένης πρόσβασης σε αυτήν από άλλους.

Σύμφωνα με έρευνα της EMC Corporation τον Ιούνιο του 2014 [8] η οποία είχε στόχο να καταγράψει τις απόψεις καταναλωτών υπηρεσιών διαδικτύου από πολλές χώρες, σε σχέση με την προστασία της ιδιωτικότητάς τους, οι χρήστες θέλουν τα πλεονεκτήματα που προσφέρει η τεχνολογία χωρίς να υποχωρούν σε θέματα που άπτονται της προστασίας της ιδιωτικής τους ζωής. Μέσω της έρευνας, στην οποία συμμετείχαν 15.000 καταναλωτές από 15 χώρες, αποκαλύπτεται ότι οι απόψεις των χρηστών του διαδικτύου σχετικά με την ιδιωτικότητα, διαφέρουν πολύ από χώρα σε χώρα και ανάλογα με το είδος της online δραστηριότητας.

Η πολύχρονη συζήτηση, σε σχέση με το πόσο ορατές θα πρέπει να είναι στις κυβερνητικές υπηρεσίες και τις επιχειρήσεις οι δραστηριότητες, η επικοινωνία και, γενικά, η συμπεριφορά μεμονωμένων ατόμων, συνεχίζεται και στη ψηφιακή εποχή. Το EMC αναζητά τις απόψεις των χρηστών αναφορικά με το δικαίωμα της ιδιωτικότητας στο ψηφιακό κόσμο και μετρά τη διάθεσή

τους να παραβλέψουν τα πλεονεκτήματα και την άνεση που προσφέρει το διαδίκτυο, προκειμένου να διασφαλίσουν την προστασία των προσωπικών τους δεδομένων.

Η επεξεργασία των στοιχείων της έρευνας ανέδειξε τρία παράδοξα:

- ***Το παράδοξο του "Τα θέλουμε όλα" – "We Want it All":*** Οι χρήστες δηλώνουν ότι θέλουν όλες τις ανέσεις και τα πλεονεκτήματα που τους προσφέρει η ψηφιακή τεχνολογία, παρόλα αυτά απαντούν ότι δεν είναι πρόθυμοι να τα ανταλλάξουν με την ιδιωτική τους ζωή.
- ***Το παράδοξο του "Μην κάνεις τίποτα" – "Take No Action":*** Παρόλο που ο κίνδυνος να παραβιαστεί η ιδιωτικότητά τους επηρεάζει άμεσα πολλούς χρήστες, οι περισσότεροι δηλώνουν ότι δεν παίρνουν κάποιο ιδιαίτερο μέτρο προστασίας – αντίθετα μεταθέτουν το βάρος αυτό σε όσους διαχειρίζονται προσωπικά δεδομένα, όπως οι επιχειρήσεις ή οι κρατικές υπηρεσίες.
- ***Το παράδοξο του "Κοινωνικού Διαμοιρασμού" - "Social Sharing" :*** Οι χρήστες των κοινωνικών μέσων δηλώνουν ότι αναγνωρίζουν την αξία της ιδιωτικότητας, παρόλα αυτά μοιράζουν ελεύθερα έναν τεράστιο όγκο προσωπικών δεδομένων – παρά την έλλειψη εμπιστοσύνης στους θεσμούς που θα πρέπει να προστατεύουν τέτοιες πληροφορίες.

Το EMC επιβεβαιώνει πως οι χρήστες του διαδικτύου συμπεριφέρονται διαφορετικά ανάλογα με το είδος των online δραστηριοτήτων τους, οι οποίες, με βάση τη φύση τους και τη συμπεριφορά του χρήστη αναφορικά με την προστασία της ιδιωτικότητας, χωρίζονται σε:

- ***Social me*:** Επικοινωνία μέσω κοινωνικών δικτύων, email, μηνύματα κειμένου/ sms και άλλες τηλεπικοινωνιακές πλατφόρμες.
- ***Financial me*:** Επικοινωνία με τράπεζες και άλλους χρηματοπιστωτικούς οργανισμούς.
- ***Citizen me*:** Επικοινωνία με κρατικές υπηρεσίες.
- ***Medical me*:** Επικοινωνία με γιατρούς, νοσοκομεία και ασφαλιστικές υπηρεσίες.
- ***Employee me*:** Επικοινωνία με συστήματα και ιστοσελίδες που σχετίζονται με αγορά εργασίας.
- ***Consumer me*:** Επικοινωνία με online καταστήματα.

Οι απόψεις περί ιδιωτικότητας διαφέρουν σημαντικά από κατηγορία σε κατηγορία. Για παράδειγμα, στην περίπτωση της επικοινωνίας με κρατικές υπηρεσίες (Citizen Me) οι συμμετέχοντες δείχνουν εξαιρετικά πρόθυμοι να δεχτούν την παραβίαση της ιδιωτικότητας για χάρη της προστασίας ή της εύκολης online πρόσβασης στα κρατικά επιδόματα. Την ίδια στιγμή, το "κοινωνικό τους Εγώ" (Social Me) δηλώνει ότι είναι λιγότερο πρόθυμο να

θυσιάσει την προστασία των ιδιωτικών δεδομένων για χάρη ακόμη καλύτερης κοινωνικής δικτύωσης.

Αξιοσημείωτο είναι το γεγονός πως, παρόλο που περισσότεροι από τους μισούς συμμετέχοντες στην έρευνα δήλωσαν ότι έχουν πέσει θύματα παραβίασης προσωπικών δεδομένων (υφαρπαγή προσωπικού κωδικού email, υφαρπαγή κωδικών εισόδου στα κοινωνικά δίκτυα κ.τ.λ.), πολλοί είναι εκείνοι που δεν παίρνουν κανένα μέτρο προστασίας, ούτε καν τα βασικά. Πιο συγκεκριμένα:

- Το 62% δεν αλλάζει τακτικά τα passwords που χρησιμοποιεί.
- 4 στους 10 δεν κάνουν τις κατάλληλες ρυθμίσεις privacy στα κοινωνικά δίκτυα.
- Το 39% δεν χρησιμοποιεί password στο κινητό ή την ταμπλέτα.

Σύμφωνα με τους ερωτηθέντες, ο μεγαλύτερος κίνδυνος για το μέλλον της ιδιωτικότητας προέρχεται από τις επιχειρήσεις που χρησιμοποιούν, πωλούν ή ανταλλάσσουν προσωπικά δεδομένα έναντι χρηματικού κέρδους (51%) και από την έλλειψη ενδιαφέροντος από την πλευρά του κράτους (31%). Αντίστοιχα, «η έλλειψη προσωπικής επίβλεψης και προσοχής από κανονικούς ανθρώπους σαν κι εμένα» αξιολογήθηκε σε πολύ χαμηλή θέση (11%).

Αναφορικά με την έκρηξη των μέσων κοινωνικής δικτύωσης παρατηρείται πως:

- Οι ερωτηθέντες εκτιμούν ότι μέσα στα επόμενα πέντε χρόνια δεν θα είναι σε θέση να προστατεύσουν την ιδιωτικότητά τους εντός των μέσων κοινωνικής δικτύωσης.
- Λίγοι καταναλωτές πιστεύουν ότι υπάρχουν τόσο η δεοντολογία όσο και οι δεξιότητες που απαιτούνται για την προστασία της ιδιωτικότητας στα μέσα κοινωνικής δικτύωσης.
- Μόλις το 51% ισχυρίζεται ότι εμπιστεύεται την ικανότητα των παρόχων (υπηρεσιών κοινωνικής δικτύωσης) να προστατεύσουν τα προσωπικά δεδομένα, ενώ μόνο το 39% δηλώνει ότι εμπιστεύεται τη δεοντολογία των οργανισμών αυτών.
- Η πλειοψηφία των καταναλωτών (84%) δηλώνει ότι δεν τους αρέσει να ξέρει κανείς κάτι για αυτούς ή τις συνήθειές τους, εκτός αν επιλέξουν οι ίδιοι να αποκαλύψουν τέτοιες πληροφορίες.
- Ερωτηθέντες ηλικίας άνω των 65 ετών δηλώνουν πολύ πιο ανήσυχοι σε σχέση με την προστασία της ιδιωτικότητας, και δείχνουν τη λιγότερη προθυμία να αποκαλύψουν τις διαδικτυακές τους συνήθειες.

1.3 Η Προστασία της Ιδιωτικότητας τώρα και στο μέλλον

Τα στοιχεία της έρευνας EMC επιβεβαιώνουν πως χρόνο με το χρόνο η εμπιστοσύνη του κόσμου σε σχέση με το επίπεδο προστασίας της ιδιωτικότητάς του μειώνεται. Σε σύγκριση με ένα χρόνο πριν, το 59% των ερωτηθέντων από όλες τις χώρες αισθάνεται ότι τώρα η ιδιωτικότητά του προστατεύεται λιγότερο. Η Βραζιλία και οι Η.Π.Α. εμφανίζουν το υψηλότερο ποσοστό ερωτηθέντων που αισθάνονται ότι η ιδιωτικότητά τους έχει περιοριστεί (71% και 70% αντίστοιχα). Η Γαλλία είναι η μόνη χώρα στην οποία η πλειοψηφία (56%) διαφωνεί με τη δήλωση ότι φέτος η ιδιωτικότητά τους έχει περιοριστεί σε σχέση με την περσινή χρονιά. Σημαντικό επίσης είναι και το ποσοστό του 81% των συμμετεχόντων που εκτιμά ότι η προστασία της ιδιωτικότητας θα υποχωρήσει μέσα στα επόμενα πέντε χρόνια.

Στις 25 Νοεμβρίου 2014 το θέμα της προστασίας της ιδιωτικότητας στο διαδίκτυο συζητήθηκε εκτενώς στη συνεδρίαση του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) και έκτοτε περιγράφεται ως ανθρώπινο δικαίωμα [9].

Μάλιστα, ο Οργανισμός Ηνωμένων Εθνών με ψήφισμά του, κάλεσε όλες τις χώρες- μέλη του να προστατέψουν το δικαίωμα της ιδιωτικής ζωής των πολιτών τους στον τομέα των ψηφιακών επικοινωνιών αλλά και να τους προσφέρουν λύσεις, αν νιώσουν ότι η ιδιωτική τους ζωή παραβιάζεται. Μέτρο, το οποίο έγινε αποδεκτό από την πλειοψηφία της Επιτροπής Ανθρωπίνων Δικαιωμάτων της Γενικής Συνέλευσης.

Το ψήφισμα ωστόσο, υποστηρίχθηκε από 65 χώρες-μέλη αλλά όχι από τις Ηνωμένες Πολιτείες, την Αυστραλία, τη Βρετανία, τον Καναδά και τη Νέα Ζηλανδία, χώρες οι οποίες αποτελούν μια συμμαχία αντικατασκοπείας, γνωστή και ως FIVE EYES.

Το ψήφισμα αυτό προτρέπει για πρώτη φορά στην ιστορία τις κυβερνήσεις να «παρέχουν στα άτομα, των οποίων το δικαίωμα στην ιδιωτική ζωή έχει παραβιαστεί παράνομα ή αυθαίρετα, την πρόσβαση σε αποτελεσματικά ένδικα μέσα». Μάλιστα, το κείμενο του ψηφίσματος για πρώτη φορά περιλαμβάνει ρητά μια αναφορά που δεν περιορίζεται μόνο στο περιεχόμενο κάθε επικοινωνίας μέσω διαδικτύου αλλά επεκτείνει το όριο του τι ορίζεται ως «ηλεκτρονικά προσωπικά δεδομένα» και στη συλλογή των metadata, τα οποία περιλαμβάνουν την ημερομηνία και την ώρα που στάλθηκε ένα email ή τη διάρκεια τηλεφωνημάτων.

Σύμφωνα με τον Niels Ole Finnemann, καθηγητή και διευθυντή του NetLab της Δανίας, οι χρήστες διακρίνονται σε δύο κατηγορίες, αυτούς που προτιμούν την ευκολία και αυτούς που προτιμούν την ιδιωτικότητα («The citizens will divide between those who prefer convenience and those who prefer privacy»). Αρκετοί επιστήμονες και

ερευνητές υποστηρίζουν πως μέχρι το 2025 οι πληροφορίες που σήμερα θεωρούμε ιδιωτικές, θα είναι ακόμα πιο διάχυτες και πιο ρευστές [10].

Για τις απειλές και τους κινδύνους της ρευστότητας των πληροφοριών και της εν γένει παραβίασης της ιδιωτικότητας, προειδοποίησε η Πρόεδρος της Ομοσπονδιακής Επιτροπής Εμπορίου των Η.Π.Α. κυρίως σε ό, τι αφορά τα έξυπνα gadgets και το Internet of Things (IoT) [11]. Ένα μέλλον γεμάτο με συσκευές που είναι μόνιμα συνδεδεμένες στο διαδίκτυο, συλλέγουν κάθε πιθανό προσωπικό δεδομένο και μπορούν να σκιαγραφήσουν μια «βαθιά προσωπική» εικόνα για τον τρόπο ζωής του χρήστη τους. Κάθε κίνηση του χρήστη σε smartphones και tablets μετατρέπεται σε ένα σημείο δεδομένων όπου εύκολα μπορεί να συλλεχθεί, να χρησιμοποιηθεί και να διαμοιραστεί. Το σημαντικό είναι πως ο χρήστης συμφωνεί σε αυτή τη διαδικασία διαμοιρασμού κάθε φορά που συμφωνεί με την πολιτική προστασίας οποιασδήποτε διαδικτυακής υπηρεσίας. Σύμφωνα με το δικηγόρο Chris Calabrese της Αμερικανικής Ένωσης Πολιτικών Ελευθεριών, οι χρήστες πιστεύουν λανθασμένα πως η πολιτική προστασίας σημαίνει πως χαίρουν προστασίας , ενώ στην ουσία η πολιτική αυτή είναι ο τρόπος να περιγράψουν τα δικαιώματα τα οποία δεν έχουν.

1.4 Η προστασία των προσωπικών δεδομένων

Με την εξέλιξη της τεχνολογίας και της κοινωνίας, η ιδιωτικότητα ως όρος και αξία εξελίσσεται και μεταλλάσσεται λαμβάνοντας τη μορφή πλέον του σεβασμού των δεδομένων προσωπικού χαρακτήρα. Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η αποκέντρωση της επεξεργασίας, η διείσδυση της επεξεργασίας και της δικτύωσης στο σύνολο σχεδόν της ανθρώπινης δραστηριότητας αλλάζουν ριζικά το περιβάλλον χρήσης της προσωπικής πληροφορίας, αλλά και τα ζητήματα που εγείρονται σε σχέση με την προστασία της.

Σε αντίθεση με την ιδιωτικότητα υπό στενή εννοία, η προστασία προσωπικών δεδομένων εγείρεται ως αίτημα αναπόσπαστα συνδεδεμένο με την τεχνολογική εξέλιξη.

Η ανάπτυξη των νέων τεχνολογιών και οι νέες μορφές διαφήμισης και ηλεκτρονικών συναλλαγών, οδήγησαν στην αυξημένη ζήτηση προσωπικών πληροφοριών από τον ιδιωτικό και δημόσιο τομέα. Οι προσωπικές αυτές πληροφορίες που αναφέρονται σε κάθε είδους δραστηριότητα, προσωπική είτε επαγγελματική του ατόμου, ονομάζονται προσωπικά δεδομένα.

Σύμφωνα με την κοινοτική οδηγία 95/46/ΕΚ και το νόμο 2472/97, τα προσωπικά δεδομένα διακρίνονται σε απλά και ευαίσθητα. Ευαίσθητα θεωρούνται τα δεδομένα εκείνα που αφορούν τη φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστική οργάνωση, την υγεία, την κοινωνική πρόνοια και την ερωτική ζωή, τα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και τη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων [12]. Το δικαίωμα της προστασίας των προσωπικών δεδομένων έγκειται στην πλήρη και διαφανή επίγνωση του καθενός για το ποιος και τι γνωρίζει για αυτόν.

Γίνεται σαφές επομένως, πως η έννοια των προσωπικών δεδομένων και της προστασίας τους λαμβάνει μεγαλύτερες διαστάσεις από την έννοια της ιδιωτικότητας και συνδέεται άμεσα με τις εξελίξεις στις νέες τεχνολογίες.

1.5 Εμπιστοσύνη και Ασφάλεια

Η εμπιστοσύνη είναι μια σύνθετη και πολυδιάστατη μεταβλητή πράγμα το οποίο τη καθιστά εξαιρετικά δύσκολη στο να καθοριστεί. Αποτελεί αναπόσπαστο μέρος της ιδιωτικής ζωής τόσο στη συμβατική της μορφή, την ανταλλαγή των υποσχέσεων που θα πρέπει τα άτομα να εμπιστεύονται, όσο και στη θεσμική της μορφή, την εμπιστοσύνη δηλαδή που απαιτεί η αποκάλυψη ιδιωτικών πληροφοριών σε αφηρημένες οντότητες (εταιρείες, κυβέρνηση).

Με τη χρήση των νέων τεχνολογιών, όπου τα προσωπικά δεδομένα ανταλλάσσονται, μεταφέρονται και αποθηκεύονται με αυξανόμενη ταχύτητα και σε διαφορετικά περιβάλλοντα, η εμπιστοσύνη των καταναλωτών σε προϊόντα και υπηρεσίες ζωτικής σημασίας συνιστά πολύ σημαντική παράμετρο για τη συνέχιση και την εξέλιξη της σχέσης τους με κάθε οργανισμό και επιχείρηση. Πολλοί χρήστες ενδέχεται να αισθάνονται ευχαριστημένοι ή δυσαρεστημένοι με το σύστημα , την επιχείρηση ή την κυβέρνηση, ωστόσο είναι αναπόφευκτο πολλές φορές να δείξουν εμπιστοσύνη και να μη μείνουν αποξενωμένοι, αφού η εμπιστοσύνη είναι βασική προϋπόθεση για τη συνεργασία.

Εντούτοις, η συνεργασία αυτή επιφέρει και θέματα ασφάλειας αναφορικά με τις πληροφορίες, το υλικό και το λογισμικό. Μέσα από την

επιλογή και εφαρμογή των κατάλληλων εγγυήσεων, η ασφάλεια βοηθά στην αποστολή του οργανισμού με την προστασία των φυσικών και οικονομικών πόρων του, τη φήμη, τη νομική θέση, τους εργαζόμενους, τους πελάτες και άλλα υλικά και άυλα περιουσιακά στοιχεία.

Ο στόχος ενός αξιόπιστου συστήματος του υπολογιστή είναι να ελέγχει την πρόσβαση των χρηστών σε δεδομένα. Αυτός ο έλεγχος διέπεται από ένα σύνολο γενικών σκοπών και στόχων που ονομάζεται ***πολιτική ασφάλειας***. Στηρίζεται δε, σε τρεις βασικές ιδέες οι οποίες είναι απαραίτητες για την ορθή λειτουργία ενός συστήματος, και είναι οι εξής [13] :

- ***Ακεραιότητα (Integrity)***: Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.
- ***Διαθεσιμότητα (Availability):*** Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση. Για παράδειγμα: το φαινόμενο Slashdot, κατά το οποίο ένας σύνδεσμος προς μια ιστοσελίδα φιλοξενούμενη σε διακομιστή με σύνδεση χαμηλής χωρητικότητας δημοσιεύεται σε δημοφιλή ιστότοπο, με συνέπεια εκατοντάδες χιλιάδες αναγνώστες να υπερφορτώσουν τη σύνδεση της αναφερομένης ιστοσελίδας. Το φαινόμενο αυτό προκαλεί το ίδιο αποτέλεσμα.

- ***Εμπιστευτικότητα (Confidentiality):*** Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Σχήμα 1: Βασικές Αρχές Ασφάλειας

ΚΕΦΑΛΑΙΟ 2
ΝΟΜΟΘΕΣΙΑ

2.1 Άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου

Αν ο 20ος αιώνας ήταν ο αιώνας της έκρηξης των τεχνολογιών πληροφορικής, ο 21ος αιώνας θα είναι σίγουρα ο αιώνας της αποκορύφωσής τους. Μέσα, δε, στο περιβάλλον αυτό το άτομο είναι εκτεθειμένο όσο ποτέ άλλοτε σε διαφόρων ειδών προσβολές της ιδιωτικότητάς του. Στον ευρωπαϊκό χώρο, και κατ' επέκταση και στον ελληνικό, ύψιστη δικλείδα ασφαλείας για την προστασία της ιδιωτικότητας του ατόμου αποτελεί το άρθρο 8 της Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) καθώς όλες σχεδόν οι έννομες σχέσεις και δραστηριότητες του πραγματικού κόσμου μεταφέρονται πλέον εξ ολοκλήρου ή παράλληλα στον ψηφιακό.

Σύμφωνα με το εν λόγω άρθρο «Κάθε πρόσωπο έχει δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας του και της αλληλογραφίας του. Επίσης, κατά την ενάσκηση αυτού του δικαιώματος δεν επιτρέπεται παρέμβαση δημόσιας αρχής, παρά μόνον εφόσον είναι σύμφωνη με το νόμο και είναι αναγκαία σε μια δημοκρατική κοινωνία για λόγους εθνικής ασφάλειας, δημόσιας ασφάλειας ή οικονομικής ευημερίας της χώρας, για την αποτροπή των εκτροπών ή του εγκλήματος, για την προστασία της υγείας ή των ηθών, ή για την προστασία των δικαιωμάτων και ελευθεριών των άλλων» [14].

Ωστόσο, η ιδιωτικότητα αποτελεί μια έννοια με εξαιρετικά δύσκολο εννοιολογικό προσδιορισμό. Από την αντίληψη της ιδιωτικότητας του 19ου αιώνα ως το δικαίωμα του ατόμου σε μια ανενόχλητη ιδιωτική ζωή (the right to be alone), έχουμε φτάσει σε μια σειρά δικαιωμάτων που την έχουν εμπλουτίσει, όπως το δικαίωμα στην ιδιωτική ζωή με τη στενή έννοια, ο αποκλειστικός έλεγχος της πρόσβασης στον ιδιωτικό χώρο, η προσδοκία της εχεμύθειας, το δικαίωμα στο απόρρητο και στην ανωνυμία κ.ά. Χαρακτηριστικό, δε, είναι το γεγονός ότι η έννοια της ιδιωτικότητας προσεγγίζεται σε κάθε νομικό κείμενο με διαφορετικό τρόπο, έστω και παραπλήσιο, χωρίς την ύπαρξη ενός κοινά αποδεκτού ορισμού, κάτι που καταδεικνύει αφενός την ευρύτητά της και αφετέρου τη μη «στατικότητα» μιας έννοιας, η οποία επηρεάζεται από τις συνεχόμενες τεχνολογικές, κυρίως, εξελίξεις [15].

Επισημαίνεται, επίσης, πως η έννοια της ιδιωτικότητας είναι διάφορη από εκείνη των δεδομένων προσωπικού χαρακτήρα. Το ίδιο το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) προσεγγίζει την προστασία των δεδομένων προσωπικού χαρακτήρα ως μια πτυχή της κανονιστικής προστασίας και του περιεχομένου της ιδιωτικότητας [16].

Το άρθρο 8 της ΕΣΔΑ δύναται να τύχει εφαρμογής σε κάθε δραστηριότητα που λαμβάνει χώρα στο σύγχρονο ψηφιακό περιβάλλον και απειλεί το δικαίωμα στην προστασία της ιδιωτικότητας. Μέχρι σήμερα το Ευρωπαϊκό Δικαστήριο Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) έχει ασχοληθεί σχεδόν με κάθε τομέα του σύγχρονου ψηφιακού περιβάλλοντος.

Χαρακτηριστικό παράδειγμα αποτελεί η υπόθεση Copland τον Απρίλιο του 2007, κατά την οποία, το ΕΔΔΑ έκρινε ένοχο το δημόσιο Κολλέγιο στο οποίο εργαζόταν η προσφεύγουσα, για παραβίαση της ιδιωτικής ζωής και της αλληλογραφίας, καθώς παρακολουθούσε τα τηλεφωνήματα, το ηλεκτρονικό ταχυδρομείο και τις επισκέψεις της σε διάφορες ιστοσελίδες.

2.2 Ευρωπαϊκή νομοθεσία για την προστασία της Ιδιωτικότητας

Το άρθρο 8 της ΕΣΔΑ αποτελεί, όπως προαναφέρθηκε, τη βασική νομική διάταξη για την προστασία της ιδιωτικότητας στον ευρωπαϊκό χώρο, και τον βασικό άξονα γύρω από τον οποίο περιστρέφεται η ευρωπαϊκή νομοθεσία. Το εν λόγω άρθρο σε συνδυασμό με τα άρθρα 7 και 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης αποτελούν τους θεμέλιους λίθους για την προστασία της ιδιωτικότητας. Πιο συγκεκριμένα, το άρθρο 7 αναφέρει ότι: «Κάθε πρόσωπο έχει το δικαίωμα στο σεβασμό της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και των επικοινωνιών του», ενώ στο άρθρο 8 αναφέρονται τα εξής: «1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. 2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερόμενου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεχθέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους. 3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής».

Παρακάτω παρατίθενται νομοθετικά κείμενα αναφορικά με την προστασία της ιδιωτικότητας του ατόμου.

2.2.1 Άρθρο 16 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης

1. Κάθε πρόσωπο έχει δικαίωμα προστασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

2. Το Ευρωπαϊκό Κοινοβούλιο και το Ευρωπαϊκό Συμβούλιο, αποφασίζοντας σύμφωνα με τη συνήθη νομοθετική διαδικασία, θεσπίζουν τους κανόνες σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης, καθώς και από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της Ένωσης, και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών. Η τήρηση των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητων αρχών [17].

2.2.2 Σύμβαση 108 του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοποιημένη επεξεργασία προσωπικών δεδομένων

Σκοπός της συγκεκριμένης σύμβασης είναι να εξασφαλίσει για κάθε άτομο, ανεξάρτητα από την ιθαγένεια ή κατοικία του, το σεβασμό των δικαιωμάτων του και των θεμελιωδών ελευθεριών του, και ιδίως το δικαίωμα στην ιδιωτική ζωή, όσον αφορά την αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν».

2.2.3 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995

Στο επίκεντρο του νομοθετικού πλαισίου της Ευρωπαϊκής Ένωσης τίθεται η οδηγία 95/46/ΕΚ η οποία συνιστά ακόμα και σήμερα το πρώτο, σημαντικότερο νομοθετικό εργαλείο της Ένωσης για την προστασία της ιδιωτικότητας των πολιτών. Στόχος της συγκεκριμένης οδηγίας είναι η εξασφάλιση στα κράτη μέλη της προστασίας των θεμελιωδών ελευθεριών και δικαιωμάτων και ιδίως της ιδιωτικής ζωής. Στοχεύει επίσης στην εναρμόνιση των επιμέρους εθνικών νομοθεσιών για την προστασία προσωπικών δεδομένων, διασφαλίζοντας ταυτόχρονα την ελεύθερη κυκλοφορία τους.

Βασικά σημεία της οδηγίας είναι από την μία πλευρά η έννοια της αυτοματοποιημένης επεξεργασίας των προσωπικών δεδομένων, η οποία αποτελεί και το πεδίο εφαρμογής της και συνίσταται στη συλλογή, αποθήκευση, μεταβολή, χρήση, αποκάλυψη, ταυτοποίηση, αναπαραγωγή τους κλπ, και από την άλλη η έννοια των προσωπικών δεδομένων ως επώνυμων δεδομένων, τα οποία μπορούν να συνδεθούν σε ένα αναγνωρίσιμο υποκείμενο, φυσικό πρόσωπο [18].

Στόχος της οδηγίας είναι η προστασία των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, μέσω του καθορισμού κατευθυντήριων αρχών που προσδιορίζουν τη νομιμότητα της επεξεργασίας αυτής. Οι αρχές αυτές αφορούν:

- Την ποιότητα των δεδομένων: τα δεδομένα προσωπικού χαρακτήρα πρέπει συγκεκριμένα να αποτελούν αντικείμενο θεμιτής και ρητής επεξεργασίας και να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς. Θα πρέπει εξάλλου να είναι ακριβή και, αν χρειάζεται, ενημερωμένα.
- Τη νόμιμη επεξεργασία των δεδομένων: η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν μπορεί να γίνεται παρά αν το υπόψη άτομο κατά τρόπο αναμφισβήτητο δώσει τη συναίνεσή του ή αν η επεξεργασία είναι απαραίτητη:
  - για την εκτέλεση σύμβασης της οποίας το υπόψη πρόσωπο αποτελεί συμβαλλόμενο μέρος,
  - για την τήρηση νομικής υποχρέωσης στην οποία υπόκειται ο υπεύθυνος της επεξεργασίας,
  - για τη διαφύλαξη ζωτικού συμφέροντος του υπόψη προσώπου,
  - για την εκτέλεση αποστολής δημόσιου συμφέροντος,
  - για την υλοποίηση του θεμιτού συμφέροντος που επιδιώκεται από τον υπεύθυνο της επεξεργασίας.
- Τις ειδικές κατηγορίες επεξεργασίας: θα πρέπει να απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τις δημόσιες απόψεις, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις, τη συνδικαλιστική τοποθέτηση, καθώς και την επεξεργασία δεδομένων σχετικά με την υγεία και την ερωτική ζωή. Η διάταξη αυτή συνοδεύεται από 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.
- Την ενημέρωση των ενδιαφερόμενων προσώπων σχετικά με την επεξεργασία δεδομένων: ορισμένες πληροφορίες (ταυτότητα του υπεύθυνου της επεξεργασίας, σκοπιμότητες της επεξεργασίας, παραλήπτες των δεδομένων κλπ.) θα πρέπει να παρέχονται από τον υπεύθυνο της επεξεργασίας στο πρόσωπο για το οποίο συλλέγει δεδομένα που το αφορούν.
- Το δικαίωμα πρόσβασης των προσώπων αυτών στα δεδομένα: κάθε σχετικό πρόσωπο θα πρέπει να έχει το δικαίωμα να εξασφαλίσει από τον υπεύθυνο της επεξεργασίας:
  - τη διαβεβαίωση ότι τα δεδομένα που το αφορούν γίνονται ή δεν γίνονται αντικείμενο επεξεργασίας και την κοινοποίηση των δεδομένων που αποτελούν το αντικείμενο επεξεργασίας,
  - τη διόρθωση, τη διαγραφή ή την απαγόρευση της πρόσβασης στα δεδομένα των οποίων η επεξεργασία δεν είναι σύμφωνη προς την παρούσα επεξεργασία - ιδίως σε ό,τι αφορά τον ατελή ή ανακριβή χαρακτήρα των δεδομένων - καθώς και την

κοινοποίηση των τροποποιήσεων αυτών προς τρίτους προς τους οποίους τα δεδομένα αυτά έχουν διαβιβασθεί.

- Τις εξαιρέσεις και τους περιορισμούς: αρχές σχετικά με την ποιότητα των δεδομένων, την πληροφόρηση του υπόψη προσώπου, το δικαίωμα πρόσβασης και τη δημοσιότητα των επεξεργασιών μπορούν να έχουν περιορισμένη εμβέλεια ώστε να διαφυλαχθεί, μεταξύ άλλων, η κρατική ασφάλεια, η άμυνα, η δημόσια ασφάλεια, η επιδίωξη ποινικών παραβάσεων, ένα οικονομικό ή δημοσιονομικό σημαντικό συμφέρον ενός κράτους μέλους ή της ΕΕ ή η προστασία του εν λόγω προσώπου.
- Το δικαίωμα αντίταξης στην επεξεργασία δεδομένων: το υπόψη πρόσωπο θα πρέπει να έχει το δικαίωμα να αντιταχθεί, για θεμιτούς λόγους, στην επεξεργασία δεδομένων που το αφορούν. Θα πρέπει επίσης να δύναται να αντιταχθεί, εφόσον το ζητήσει και δωρεάν, στην επεξεργασία δεδομένων που προβλέπεται για σκοπούς διερεύνησης. Θα πρέπει επιπλέον να ενημερώνεται πριν από τη διαβίβαση των δεδομένων σε τρίτους για σκοπούς έρευνας και θα πρέπει να του παρέχεται το δικαίωμα αντίταξής του στη διαβίβαση αυτή.
- Την εμπιστευτικότητα και την ασφάλεια της επεξεργασίας: κάθε πρόσωπο που ενεργεί υπό την εξουσία του υπευθύνου της επεξεργασίας ή εκείνη υπεργολάβου, καθώς και ο ίδιος ο υπεργολάβος, που έχει πρόσβαση σε προσωπικά δεδομένα, δεν δύναται να τα επεξεργαστεί παρά κατόπιν εντολής του υπευθύνου επεξεργασίας. Εξάλλου, ο υπεύθυνος της επεξεργασίας θα πρέπει να εφαρμόζει τα ενδεδειγμένα μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα έναντι τυχαίας ή παράνομης καταστροφής, τυχαίας απώλειας, αλλοίωσης, διάδοσης ή πρόσβασης χωρίς άδεια.
- Την κοινοποίηση των αποτελεσμάτων της επεξεργασίας σε ελεγκτική αρχή: ο υπεύθυνος επεξεργασίας οφείλει να απευθύνει κοινοποίηση στην αρμόδια ελεγκτική αρχή πριν από την εκτέλεση μιας επεξεργασίας. Προηγούμενες εξετάσεις ως προς τους ενδεχόμενους κινδύνους έναντι των δικαιωμάτων και ελευθεριών των υπόψη προσώπων θα πρέπει να γίνονται από την ελεγκτική αρχή μέχρι τη λήψη της κοινοποίησης. Η δημοσιότητα των αποτελεσμάτων της επεξεργασίας θα πρέπει να διασφαλίζεται και οι ελεγκτικές αρχές οφείλουν να τηρούν μητρώο των κοινοποιημένων αποτελεσμάτων επεξεργασίας [19].

2.2.4 Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002

Ένα νομοθετικό εργαλείο τρίτης γενιάς συνιστά η e-Privacy Οδηγία, 2002/58/ΕΚ η οποία υιοθετήθηκε στις 12 Ιουλίου 2002 και καλείται να ανταποκριθεί στις σύγχρονες προκλήσεις που θέτουν οι εξελιγμένες, ψηφιακές τεχνολογίες. Η συγκεκριμένη οδηγία αντικαθιστά την Οδηγία 97/66/ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας στον τομέα των τηλεπικοινωνιών, προκειμένου να εισάγει ένα νέο εκσυγχρονισμένο

ρυθμιστικό πλαίσιο το οποίο να περιλαμβάνει και τη χρήση του διαδικτύου. Εκτός των άλλων, λαμβάνει υπόψη της όλες τις σύγχρονες δυνατότητες που παρέχει το διαδίκτυο για την παραβίαση της ιδιωτικότητας του ατόμου, όπως τα cookies, worms, spyware.

Κύριος στόχος της οδηγίας είναι να προστατεύεται ο χρήστης του διαδικτύου ανεξάρτητα από την τεχνολογία που εφαρμόζεται [20].

Ειδική ρύθμιση υπάρχει και για τα cookies, των οποίων τη χρησιμοποίηση επιτρέπει η οδηγία, αποκλειστικά και μόνο για θεμιτούς σκοπούς και με την προϋπόθεση ότι αυτό γίνεται εν γνώσει του εκάστοτε χρήστη.

2.2.5 Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006

Δούρειο ίππο στην προστασία των προσωπικών δεδομένων στο πλαίσιο της Ευρωπαϊκής Ένωσης συνιστά η Οδηγία 2006/24/ΕΚ αναφορικά με την παρακράτηση προσωπικών δεδομένων από τους παρόχους υπηρεσιών επικοινωνίας. Τα προσωπικά δεδομένα δεν αφορούν το περιεχόμενο των επικοινωνιών αλλά μόνο traffic και location data. Αυτό σημαίνει πως τα δεδομένα που μπορούν να παρακρατηθούν αφορούν την πηγή, προορισμό, ημερομηνία, διάρκεια και τύπο της επικοινωνίας καθώς και τον προσδιορισμό του μέσου της επικοινωνίας ή την τοποθεσία της. Λόγω της σημασίας που έχουν αυτά τα δεδομένα για τη διερεύνηση, διαπίστωση και δίωξη των ποινικών αδικημάτων, θεωρήθηκε σκόπιμο να διασφαλιστεί η διατήρηση για ορισμένο χρονικό διάστημα των δεδομένων αυτών. Πρόκειται για τη λεγόμενη φύλαξη ορισμένων κατηγοριών δεδομένων (Data Retention), από τους παρόχους υπηρεσιών διαδικτύου, η οποία κρίνεται ιδιαίτερα χρήσιμη στο πλαίσιο της σύγχρονης πολιτικής στο τομέα του ηλεκτρονικού εγκλήματος [21].

Τέλος, σημαντικές για την προστασία της ιδιωτικότητας στον ευρωπαϊκό χώρο είναι και μια σειρά Συστάσεων της Ευρωπαϊκής Επιτροπής, όπως η R(99) 5 για την προστασία της ιδιωτικότητας στο διαδίκτυο, η R(89) 9 για τον προσδιορισμό των ηλεκτρονικών εγκλημάτων και η R(95) 13 για τα ζητήματα της ποινικής διαδικασίας στην πληροφορική και ηλεκτρονική τεχνολογία [22].

Επιπρόσθετα, η Ευρωπαϊκή Επιτροπή έχει ήδη επεξεργαστεί ένα νέο νομοθετικό πλαίσιο για την ισχύουσα νομοθεσία 95/46/ΕΚ υποστηρίζοντας πως θεσπίστηκε σε μία εποχή όπου η χρήση του διαδικτύου δεν ήταν διαδεδομένη στην πλειοψηφία των πολιτών. Αντίθετα, σήμερα 250 εκατομμύρια πολιτών της Ένωσης χρησιμοποιούν το διαδίκτυο καθημερινά, καθιστώντας έτσι, σε

συνδυασμό με τις τεχνολογικές εξελίξεις που τρέχουν με ταχύτερο ρυθμό από το δίκαιο, επιτακτική την ανάγκη αναθεώρησης της ισχύουσας ευρωπαϊκής νομοθεσίας [23].

2.3 Ελληνική νομοθεσία για την προστασία της Ιδιωτικότητας

Η Ελλάδα ούσα μέλος της Ευρωπαϊκής Ένωσης, ενστερνίζεται την ευρωπαϊκή νομοθεσία και βρίσκεται συνεχώς σε επιφυλακή των τεχνολογικών εξελίξεων αλλά και των προβλημάτων που απορρέουν από αυτήν.

2.3.1 Σύνταγμα της Ελλάδος

Η προστασία της ιδιωτικότητας στο θεμελιώδη νόμο του κράτους προβλέπεται στα εξής άρθρα:

- ***Άρθρο 9 παρ. 1 (Άσυλο της κατοικίας):*** «Η κατοικία του καθενός είναι άσυλο. Η ιδιωτική και οικογενειακή ζωή του ατόμου είναι απαραβίαστη. Καμία έρευνα δεν γίνεται σε κατοικία, παρά μόνο όταν και όποτε ορίζει ο νόμος και πάντοτε με την παρουσία εκπροσώπων της δικαστικής εξουσίας».
- ***Άρθρο 9^{A} (Προστασία προσωπικών δεδομένων):*** «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».
- ***Άρθρο 19 (Απόρρητο επιστολών, ανταπόκρισης και επικοινωνίας):*** «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 9^{A}».

2.3.2 Νόμος 2472/1997

Ο νόμος 2472/1997 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. Υιοθετεί τον ευρύ ορισμό της έννοιας των δεδομένων προσωπικού χαρακτήρα, της έννοιας της επεξεργασίας τους και της έννοιας του αρχείου δεδομένων προσωπικού χαρακτήρα, ώστε να καταλαμβάνεται κάθε είδους επεξεργασία δημόσια ή μη, αυτοματοποιημένη ή μη. Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων και ως «ευαίσθητα δεδομένα», 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 ανωτέρα, ενώσεις προσώπων.

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. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από τον νόμο. Η ΑΔΑΕ έχει τις εξής αρμοδιότητες:

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 αρμοδιότητάς 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 [24].

Τέλος, οι ρυθμίσεις του νόμου 2472/97 συμπληρώθηκαν από το Νόμο 3471/06 (Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών). Ο νόμος αυτός κατοχύρωσε σημαντικά δικαιώματα των συνδρομητών και χρηστών τηλεπικοινωνιακών υπηρεσιών. Ενσωματώνοντας την Οδηγία 2002/58/ΕΚ, αποσκοπεί στην εισαγωγή ειδικών ρυθμίσεων που αφορούν τόσο το απόρρητο της επικοινωνίας και την προστασία της ιδιωτικότητας των χρηστών από πρακτικές όπως π.χ. η εγκατάσταση κατασκοπευτικού λογισμικού (spyware) όσο και την οργάνωση της προστασίας των δεδομένων των συνδρομητών και χρηστών έναντι των παρόχων.

2.3.3 Νόμος 3674/2008

Ο συγκεκριμένος νόμος ενισχύει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας.

2.3.4 Νόμος 3783/2009

Σκοπός του συγκεκριμένου νόμου είναι η ταυτοποίηση 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.

2.3.5 Νόμος 3917/2011

Με το συγκεκριμένο νόμο ενσωματώνονται στην εθνική έννομη τάξη οι διατάξεις της Οδηγίας 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006, η οποία προβλέπει στην 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.

Με το άρθρο 3 του ίδιου νόμου εισάγεται εξαίρεση στην, κατ' αρχήν, απαγόρευση διατήρησης δεδομένων, που απορρέει από τις διατάξεις του νόμου 3471/2006, και εξειδικεύονται οι προϋποθέσεις υπό τις οποίες θεμελιώνεται η υποχρέωση των παρόχων για τη διατήρηση των δεδομένων. Η υποχρέωση διατήρησης αφορά αποκλειστικά σε δεδομένα κίνησης και θέσης φυσικών και νομικών προσώπων και στα συναφή δεδομένα που απαιτούνται για την αναγνώριση του συνδρομητή ή του εγγεγραμμένου χρήστη και δεν εφαρμόζεται στο περιεχόμενο των ηλεκτρονικών επικοινωνιών.

2.4 Προστασία της Ιδιωτικότητας σε άλλες χώρες

2.4.1 Το διεθνές κανονιστικό περιβάλλον

Ως προς την αντίδραση της διεθνούς κοινότητας στους κινδύνους των νέων τεχνολογιών πληροφορικής για τα ανθρώπινα δικαιώματα, η απόφαση 2450/19.12.1968 της γενικής συνέλευσης των Ηνωμένων Εθνών κατατάσσεται στα πρώτα σχετικά κείμενα. Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) υπήρξε ο δεύτερος διεθνής οργανισμός που δημοσίευσε τις λεγόμενες «Κατευθυντήριες Αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές προσωπικών δεδομένων» (1980). Αυτό το αρχικό πλαίσιο γενικών αρχών στερείται δεσμευτικού χαρακτήρα και παρά- ή ακριβώς για - τον λόγο αυτόν συγκέντρωσε για μεγάλο διάστημα τη συναίνεση πολλών χωρών και κυρίως εκείνων που στερούνταν συνολικής νομοθεσίας για την προστασία των προσωπικών δεδομένων.

Ωστόσο, η διαρκής και ραγδαία αυξανόμενη διασυνοριακή ροή μεγάλου όγκου προσωπικών δεδομένων δημιουργεί πιέσεις αναφορικά με την υιοθέτηση κανόνων και διαδικασιών. Η Οδηγία 95/46/ΕΚ απαιτεί την ύπαρξη «ικανοποιητικού επιπέδου προστασίας» των προσωπικών δεδομένων για να

είναι σύννομη η διαβίβαση δεδομένων σε μια τρίτη χώρα. Διαπιστώνεται επίσης και μια αύξηση περιφερειακών πρωτοβουλιών ανά τον κόσμο.

2.4.2 Ηνωμένες Πολιτείες Αμερικής

Το αμερικανικό σύνταγμα δεν περιέχει ειδική διάταξη για την προστασία της ιδιωτικής ζωής. Ωστόσο, το Αμερικανικό Ανώτατο Δικαστήριο έχει καταλήξει στην ερμηνεία ότι η Διακήρυξη των Δικαιωμάτων (Bill of Rights) δημιουργεί τις προϋποθέσεις προστασίας της ιδιωτικής ζωής. Η ιδιωτικότητα δεν αναφέρεται ρητά στη Διακήρυξη των Δικαιωμάτων του Αμερικανικού Συντάγματος, αλλά στην Πρώτη και Τέταρτη Τροποποίηση. Στην Πρώτη εξασφαλίζεται η ελευθερία της θρησκείας, του λόγου, του τύπου και του συνέρχεσθαι, ενώ στην Τέταρτη αναφέρεται ότι το δικαίωμα του ατόμου να αισθάνεται ασφαλές στην προσωπική του ζωή και στο σπίτι του, καθώς και η προστασία του έναντι αναίτιων ερευνών και κατασχέσεων, θα πρέπει να εξασφαλίζεται.

Η προστασία της ιδιωτικής ζωής ρυθμίζεται από την Πράξη για την Ιδιωτικότητα (Privacy Act) του 1974 [25]. Η πράξη αυτή ψηφίστηκε από το Κογκρέσο με σκοπό να περιορίσει τα δεδομένα των κυβερνητικών αρχείων λόγω της αποκάλυψης ότι το Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau of Investigation, FBI) διατηρούσε κρυφά βάση δεδομένων για αντιπάλους στον πόλεμο του Βιετνάμ.

Η συνήθης πρακτική στις ΗΠΑ είναι να αντιμετωπίζονται οι παραβιάσεις όταν εμφανίζονται, σε αντίθεση με την Ευρώπη, όπου η νομοθεσία επιδιώκει την πρόληψη της παραβίασης.

2.4.3 Κίνα

Το άρθρο 38 του Συντάγματος της Λαϊκής Δημοκρατίας της Κίνας αναγνωρίζει το δικαίωμα στην αξιοπρέπεια στους κατοίκους της και το άρθρο 40 ορίζει τους περιορισμούς αυτού του δικαιώματος. Η προστασία κρατικών μυστικών και η έρευνα για κακουργήματα δίνει το δικαίωμα στις κυβερνητικές υπηρεσίες να υποκλέψουν συνομιλίες, αν αυτό κριθεί απαραίτητο.

Το 2000 κατατέθηκε η διάταξη σχετικά με τις υπηρεσίες διαδικτύου σύμφωνα με την οποία απαιτείται από όλους τους παρόχους η καταγραφή των

περιεχομένων των chat rooms, forums και ιστοσελίδων. Τα περιεχόμενα αυτά καθώς και οι πληροφορίες για το άτομο που ανήρτησε ένα μήνυμα θα πρέπει να φυλάσσονται το λιγότερο για 60 ημέρες.

Επιπροσθέτως, υπάρχουν περίπου 60 κανονισμοί σχετικά με το διαδίκτυο, οι οποίοι ακολουθούν τον κανόνα ότι κάτι πρέπει να είναι ανοιχτό αλλά πολύ καλά φυλασσόμενο. Αυτό σημαίνει πως οι συσκευές επικοινωνίας καταγράφονται για να προστατευτεί η οικονομία και η ασφάλεια του κράτους.

2.4.4 Μεγάλη Βρετανία

Το Γραφείο Επιτρόπου Πληροφοριών είναι η ανεξάρτητη αρχή που ρυθμίζει τα δικαιώματα και την ιδιωτικότητα των πολιτών. Αναφορικά με τα προσωπικά δεδομένα που διακινούνται στο διαδίκτυο, η βρετανική αρχή εξέδωσε έναν οδηγό σχετικά με το πώς γίνεται η συλλογή και η επεξεργασία προσωπικών δεδομένων στο διαδίκτυο [26].

Η Βρετανική ομάδα προστασίας της ιδιωτικής ζωής (Privacy International) δραστηριοποιείται ήδη από το 1990 στην προστασία της ιδιωτικότητας σε όλο τον κόσμο. Ανάμεσα στις πολλές επεμβάσεις της είναι και η καταγγελία κατά της ιστοσελίδας eBay, την οποία κατηγόρησε για κακή χρήση των προσωπικών δεδομένων των χρηστών της, καθώς είναι δύσκολη η διαγραφή λογαριασμών από τους χρήστες. Για τον ίδιο λόγο κατήγγειλε και την βρετανική Amazon.

ΚΕΦΑΛΑΙΟ 3
Η ΠΑΡΑΒΙΑΣΗ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΙΣ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

3.1 Λόγοι παραβίασης της Ιδιωτικότητας και του Απορρήτου των Τεχνολογιών Διαδικτύου

Η ραγδαία αύξηση των χρηστών του διαδικτύου, είχε ως αποτέλεσμα να αποδειχθεί πηγή πολύτιμων πληροφοριών για τους κυβερνοεγκληματίες. Χαρακτηριστικό παράδειγμα, μια από τις μεγαλύτερες κλοπές δεδομένων στην ιστορία του διαδικτύου και της πληροφορικής, είναι η παραβίαση του Playstation Network της Sony που πραγματοποιήθηκε τον Απρίλιο του 2011 με αποτέλεσμα τη διαρροή στοιχείων 100 εκατομμυρίων χρηστών παγκοσμίως [27].

Στα στοιχεία που η Sony εκτιμά πως εκλάπησαν συμπεριλαμβάνονται ονόματα, διευθύνσεις, χώρες προέλευσης, email, ημερομηνίες γέννησης, κωδικοί πρόσβασης σε Playstation Network και Qriocity και Handle/ PSN online ID's.

Άλλο ένα αντίστοιχο περιστατικό, τον Απρίλιο του 2011 ήταν η μαζική κλοπή δεδομένων από τις βάσεις δεδομένων της αμερικανικής εταιρείας online marketing, Epsilon (δεκάδες εκατομμύρια ονόματα και διευθύνσεις email - η εταιρεία εξυπηρετεί 2.500 εταιρείες σε όλο τον κόσμο), κατά την οποία αποκτήθηκαν στοιχεία μεγάλων αμερικανικών τραπεζών, ξενοδοχείων και καταστημάτων, τα οποία θεωρείται πως σύντομα θα αρχίσουν να χρησιμοποιούνται σε κυβερνοεγκληματικές δραστηριότητες. Επίσης, ανάλογης έκτασης περιστατικό είχε απασχολήσει και το 2006 τη Citibank, με μαζική κλοπή αριθμών PIN.

Οι επιθέσεις αυτές απέναντι στους χρήστες του διαδικτύου εκμεταλλεύονται τις αδυναμίες του συστήματος του χρήστη, οι οποίες μπορεί να είναι σχεδιαστικές, λειτουργικές αλλά και ανθρώπινες προκειμένου να αντλήσουν τις προσδοκώμενες πληροφορίες. Τα αποτελέσματα των ενεργειών αυτών έχουν αναδείξει την ασφάλεια των πληροφοριών και την προστασία της ιδιωτικότητας στο διαδίκτυο σε θέματα εξαιρετικής σημασίας καθώς αφορούν τομείς όπως η παραδοσιακή πληροφοριακή ασφάλεια, η αρχιτεκτονική των υπολογιστών, ο σχεδιασμός των συστημάτων, η μηχανική λογισμικού, η τεχνολογία διαδικτύου, τα μαθηματικά, οι νόμοι.

Οι λόγοι των επιθέσεων αυτών ποικίλλουν. Πιο συγκεκριμένα η παραβίαση της ιδιωτικότητας και του απορρήτου της επικοινωνίας των χρηστών οφείλεται σε:

3.1.1 Αλλοίωση δεδομένων (Data Distortion)

Σύμφωνα με τις Ευρωπαϊκές Οδηγίες, τα δεδομένα ενός ατόμου πρέπει να είναι ακριβή και ενημερωμένα, όσο αυτό είναι εφικτό, ενώ παράλληλα πρέπει να παρέχεται στα άτομα το δικαίωμα να επεμβαίνουν στα στοιχεία αυτά και να τα διορθώνουν ή ακόμα και να τα μπλοκάρουν σε περίπτωση που αυτά δεν ανταποκρίνονται στην πραγματικότητα. Και αυτό διότι, η αλλοίωση δεδομένων μπορεί να οδηγήσει σε στιγματισμό και να επιφέρει σημαντικό πλήγμα στη φήμη ενός ανθρώπου και η φήμη είναι το μέσο με το οποίο αλληλεπιδρούμε με τους άλλους σε μια κοινωνία [28].

3.1.2 Συλλογή Δεδομένων (Data Aggregation)

Η συλλογή του όγκου των πληροφοριών από διαφορετικές πηγές και η εξαγωγή συμπερασμάτων για ένα πρόσωπο, αποτελεί μια από τις μεγαλύτερες προκλήσεις για την ιδιωτικότητα. Η ομαδοποίηση δεδομένων αναφέρεται στην τάση για συσσώρευση, διατήρηση και χρήση πληροφοριών (όπως η ηλικία, το επάγγελμα) και για διάφορους λόγους, όπως η αρχειοθέτηση και η ανάλυση. Ωστόσο, από τη συσχέτιση αυτή των δεδομένων ενδέχεται να προκύψουν στοιχεία για τα άτομα που δεν ήταν γνωστά. Οι χρήστες δίνουν σε διάφορους ιστότοπους μερικά από τα στοιχεία τους και πιστεύουν πως έτσι προστατεύονται. Όταν όμως τα στοιχεία αυτά συγχωνευτούν από κοινού, τότε προκύπτουν πολύ περισσότερες πληροφορίες για τη ζωή του χωρίς να το γνωρίζει. Σύμφωνα με τη βιβλιογραφία αναφορικά με την ιδιωτικότητα, υπάρχουν τρεις τύποι, πιθανώς επικαλυπτόμενων συνόλων, προσωπικών χαρακτηριστικών:

- ***Εντοπισμός χαρακτηριστικών*:** ιδιότητες, όπως ο αριθμός κοινωνικής ασφάλισης, που προσδιορίζουν ένα άτομο κατά μοναδικό τρόπο.

- ***Οιονεί προσδιοριστικά χαρακτηριστικά***: ένας συνδυασμός ιδιοτήτων που μπορούν να προσδιορίσουν ένα άτομο μοναδικά, όπως ο αριθμός ταυτότητας και ο αριθμός φορολογικού μητρώου.

- ***Ευαίσθητα χαρακτηριστικά:*** ιδιότητες που οι χρήστες μπορεί να ήθελαν να κρατήσουν κρυφά από το κοινό, όπως είναι οι πολιτικές πεποιθήσεις, και οι ερωτικές προτιμήσεις.

Η αποκάλυψη χαρακτηριστικών παρατηρείται όταν ένας αντίπαλος είναι σε θέση να προσδιορίσει την αξία ενός ευαίσθητου χαρακτηριστικού του χρήστη, το οποίο ο τελευταίος θα ήθελε να παραμείνει ιδιωτικό. Αυτό το χαρακτηριστικό μπορεί να είναι ένα γνώρισμα του ίδιου του κόμβου, οι σύνδεσμοί του ή οι συσχετίσεις του.

3.1.3 Αποκλεισμός των χρηστών από τη δυνατότητα πρόσβασης στα προσωπικά τους δεδομένα (Exclusion)

Το πρόβλημα του αποκλεισμού δημιουργείται όταν στους χρήστες δεν παρέχεται η δυνατότητα πρόσβασης, διόρθωσης και ελέγχου των προσωπικών τους δεδομένων, με αποτέλεσμα οι χρήστες να αισθάνονται ανασφαλείς και ανενημέρωτοι αναφορικά με τη χρήση των δεδομένων τους.

3.1.4 Χρήση των προσωπικών δεδομένων των χρηστών για σκοπούς άλλους για τους οποίους συλλέχθηκαν (Secondary Use)

Η δευτερογενής χρήση είναι μια μορφή όπου στοιχεία που έχουν συλλεχθεί για ένα σκοπό, τελικά χρησιμοποιούνται για κάποιο άλλο χωρίς τη συγκατάθεση του εμπλεκόμενου ατόμου. Ήδη από το 1980, χρονιά που ο ΟΟΣΑ εξέδωσε τις κατευθυντήριες αρχές που διέπουν την προστασία της ιδιωτικότητας και τις διασυνοριακές ροές των προσωπικών δεδομένων, γίνεται αναφορά στη αρχή του προσδιορισμένου σκοπού (Purpose specification principle), σύμφωνα με την οποία θα πρέπει να προσδιορίζονται επακριβώς οι σκοποί για τους οποίους συλλέγονται τα προσωπικά δεδομένα και η χρήση

τους να συνάδει με τους σκοπούς αυτούς, ενώ κάθε αλλαγή στους σκοπούς θα πρέπει να αναφέρεται. Ο λόγος για τον οποίο υπάρχει τόσο μεγάλο ενδιαφέρον για τη μη εξουσιοδοτημένη χρήση των δεδομένων από τρίτους, είναι γιατί δημιουργεί αισθήματα φόβου στο χρήστη για τη μελλοντική τους χρήση καθώς δεν μπορεί να γνωρίζει τις επιπτώσεις που θα έχει στη ζωή του.

3.1.5 Παραβίαση απορρήτου (Breach of confidentiality)

Η παραβίαση απορρήτου παραβιάζει την εμπιστοσύνη σε μια συγκεκριμένη σχέση. Είναι η αναίρεση μιας υπόσχεσης που έχει δοθεί για τη διατήρηση των προσωπικών πληροφοριών ενός ατόμου εμπιστευτικά. Η βασική διαφορά μεταξύ της αποκάλυψης πληροφοριών και της παραβίασης του απορρήτου έγκειται στο γεγονός πως η πιο σημαντική πτυχή της δεύτερης είναι η διατάραξη της σχέσης εμπιστοσύνης που έχει αναπτυχθεί και το αίσθημα προδοσίας που αισθάνεται το άτομο.

3.1.6 Αποκάλυψη κοινωνικών συνδέσεων

Η αποκάλυψη κοινωνικών συνδέσεων συμβαίνει όταν ένας αντίπαλος είναι σε θέση να μάθει την ύπαρξη μιας ευαίσθητης συσχέτισης μεταξύ δύο χρηστών, μια σχέση που οι χρήστες θα ήθελαν να παραμείνει κρυφή από το κοινό.

Παραδείγματα ευαίσθητων σχέσεων μπορούν να βρεθούν σε κοινωνικά δίκτυα, σε δεδομένα επικοινωνίας, σε δεδομένα ασθενών και άλλα. Σε κοινωνικό δίκτυο δεδομένων, βάσει των σχέσεων φιλίας ενός ατόμου και των προτιμήσεων των φίλων του, μπορεί να είναι δυνατό να εξαχθούν συμπεράσματα για τις προσωπικές προτιμήσεις του εν λόγω προσώπου. Σε ένα τηλεπικοινωνιακό δίκτυο, η κλήση ενός άγνωστου ατόμου σε ένα γνωστό οργανισμό, μπορεί να θέσει σε κίνδυνο την ταυτότητα του αγνώστου, μέσω της άντλησης πληροφοριών. Σε κληρονομικά στοιχεία νοσούντων, γνωρίζοντας τις οικογενειακές σχέσεις μεταξύ των ατόμων που έχουν διαγνωστεί με κληρονομικές ασθένειες και αυτών που δεν έχουν, μπορεί να προκύψουν

συμπεράσματα για την πιθανότητα των υγιών ατόμων να νοσήσουν από τις προαναφερθείσες ασθένειες.

3.1.7 Αποκάλυψη συνδέσμων συσχέτισης

Ένας άλλος τύπος της παραβίασης της ιδιωτικότητας είναι η αποκάλυψη των συνδέσμων συσχέτισης αναφορικά με το εάν ένα άτομο ανήκει σε μια συγκεκριμένη ομάδα. Ακόμη κι αν δυο χρήστες συνδέονται με την ίδια ομάδα, μπορεί επίσης να είναι ευαίσθητο δεδομένο. Μερικές φορές, η αποκάλυψη συσχετίσεων μπορεί να οδηγήσει σε αποκάλυψη χαρακτηριστικών, κοινωνικών συνδέσεων ή ταυτότητας. Συνεπώς, η απόκρυψη των συσχετίσεων είναι ένας βασικός τρόπος διατήρησης της ιδιωτικότητας των ατόμων.

Ένας τύπος αποκάλυψης μπορεί να οδηγήσει σε ένα άλλο είδος. Για παράδειγμα, μια επίθεση από-ταυτοποίησης όπου η αποκάλυψη του συνδέσμου συσχέτισης μπορεί να οδηγήσει στην αποκάλυψη της ταυτότητας ενός υποθετικά ανώνυμου χρήστη του διαδικτύου, είναι η εξής: Ένας αντίπαλος ξεκινάει την επίθεση μέσω μιας ιστοσελίδας κοινωνικής δικτύωσης και συλλέγει πληροφορίες σχετικά με τη κοινωνική ομάδα στην οποία είναι μέλος. Υποτίθεται ότι είναι γνωστές οι ταυτότητες των χρηστών κοινωνικών δικτύων. Σύμφωνα με τα δεδομένα που συλλέγονται, κάθε χρήστης που συμμετέχει σε μία τουλάχιστον ομάδα έχει μια υπογραφή ομάδας, η οποία είναι το σύνολο των ομάδων που ανήκει. Στη συνέχεια, ο αντίπαλος εφαρμόζει μια επίθεση κλοπής ιστορικού, η οποία συλλέγει το ιστορικό περιήγησης του διαδικτυακού χρήστη - στόχου. Με την εύρεση των υπογραφών των ομάδων των χρηστών κοινωνικής δικτύωσης και την αντιστοίχιση του ιστορικού περιήγησης του χρήστη, ο αντίπαλος είναι σε θέση να βρει ένα υποσύνολο των πιθανών χρηστών του δικτύου που μπορεί να ανήκει ο διαδικτυακός χρήστης. Στο τελευταίο στάδιο της επίθεσης, ο αντίπαλος ψάχνει για αντιστοίχηση μεταξύ του αναγνωριστικού (id) των δυνητικών χρηστών και του ιστορικού περιήγησης του ατόμου-στόχου, η οποία μπορεί να οδηγήσει στην απο-ταυτοποίηση του χρήστη του διαδικτύου.

Ένα άλλο παράδειγμα της αποκάλυψης συνδέσμου συσχέτισης που οδηγεί στην αποκάλυψη ταυτότητας είναι η αναζήτηση δεδομένων. Στην περίπτωση που οι χρήστες που θέτουν ερωτήματα σε μια μηχανή αναζήτησης είναι άτομα σε ένα κοινωνικό δίκτυο, και τα ερωτήματα αναζήτησης μπορεί να

αφορούν τις ομάδες συσχέτισης, στη συνέχεια, μπορούν να αποκαλυφθούν οι δεσμοί μεταξύ των χρηστών με αποτέλεσμα τα ερωτήματα να είναι ικανά να βοηθήσουν έναν αντίπαλο στον εντοπισμό ανθρώπων στο δίκτυο. Οι χρήστες αλληλεπιδρούν με τις μηχανές αναζήτησης με τρόπο που τους επιτρέπει να αποκαλύπτουν πολλές προσωπικές πληροφορίες στο κείμενο των ερωτημάτων τους. Υπήρξε ένα σκάνδαλο το 2006, όταν η AOL, υπηρεσία παροχής διαδικτύου, κυκλοφόρησε ένα "ανώνυμο" δείγμα πάνω από μισό εκατομμύριο χρηστών και τις απορίες που είχαν θέσει στη μηχανή αναζήτησης της AOL. Η παρουσίαση των στοιχείων ήταν καλοπροαίρετη και είχε στόχο την ενίσχυση της έρευνας με πραγματικά στοιχεία. Κάθε χρήστης καθορίζεται από ένα μοναδικό αναγνωριστικό, και κάθε ερώτημα περιείχε πληροφορίες σχετικά με το αναγνωριστικό χρήστη, το ερώτημα αναζήτησης, την ιστοσελίδα που έχει επισκεφθεί ο χρήστης, την κατάταξη της εν λόγω ιστοσελίδας, τα αποτελέσματα αναζήτησης και τη χρονική σήμανση του ερωτήματος.

Η αποκάλυψη των συνδέσμων συσχέτισης μπορεί επίσης να οδηγήσει γνωστοποίηση χαρακτηριστικών, όπως παρουσιάζεται σε μια επίθεση ενοχής προς σύνδεση (guilty-by-association attack). Αυτή η επίθεση υποθέτει ότι υπάρχουν ομάδες χρηστών των οποίων οι ευαίσθητες τιμές των γνωρισμάτων είναι οι ίδιες, ανακτώντας έτσι την ευαίσθητη τιμή ενός χρήστη και τη συσχέτιση ενός άλλου χρήστη στην ομάδα βοηθώντας στην ανάκτηση ευαίσθητης τιμής του δεύτερου χρήστη. Η επίθεση αυτή έχει χρησιμοποιηθεί σε bit-torrent δίκτυο ανταλλαγής αρχείων για την ανακάλυψη των συνηθειών λήψης αρχείων. Κοινότητες που εντοπίστηκαν βάσει των κοινωνικών συνδέσμων και παρακολουθούσαν μόνο ένα χρήστη ήταν αρκετό για να βγάλουν συμπεράσματα για τα ενδιαφέροντα των άλλων ατόμων της κοινότητας. Στη συγκεκριμένη περίπτωση, το ευαίσθητο χαρακτηριστικό είναι ότι οι χρήστες θα ήθελαν να κρατήσουν ιδιωτικό το εάν παραβιάζουν πνευματικά δικαιώματα. Αυτή η επίθεση έχει επίσης εφαρμοστεί για τον προσδιορισμό δόλιων κλήσεων σε ένα τηλεφωνικό δίκτυο.

3.2 Πηγές παραβίασης της Ιδιωτικότητας και της Ασφάλειας

Η ασφάλεια του διαδικτύου είναι ένα πολύπλοκο ζήτημα που περιλαμβάνει πολλές όψεις της παραδοσιακής πληροφοριακής ασφάλειας, της αρχιτεκτονικής των υπολογιστών, του σχεδιασμού συστημάτων, της μηχανικής λογισμικού, της τεχνολογίας του διαδικτύου, των μαθηματικών αλλά και της

νομοθεσίας. Παρακάτω εστιάζουμε σε επιθέσεις κατά τις οποίες η έννοια της ιδιωτικότητας και της ασφάλειας του χρήστη τίθεται εν αμφιβόλω.

3.2.1 Συλλογή προσωπικών δεδομένων μέσω της online εγγραφής

Η online εγγραφή συνεπάγεται πως ο χρήστης παρέχει προσωπικές πληροφορίες, όπως το όνομά του, το επώνυμο, τη διεύθυνση, το τηλέφωνο και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του. Επιπρόσθετα, κατά τη διαδικασία εγγραφής, είναι πολύ πιθανό να αποκαλύψει και άλλες ευαίσθητες πληροφορίες όπως τον αριθμό της πιστωτικής του κάρτας ή και αριθμούς λογαριασμούς σε περίπτωση που επιθυμεί να πραγματοποιήσει ηλεκτρονικές αγορές [29].

3.2.2 Εντοπισμός του χρήστη μέσω των πρωτοκόλλων IP

Το IP είναι ένα πρωτόκολλο στρώματος δικτύου το οποίο παρέχει μια χωρίς σύνδεση υπηρεσία μεταφοράς δεδομένων. Η υπηρεσία αυτή πολλές φορές αναφέρεται και ως μη αξιόπιστη εφόσον το δίκτυο δεν εγγυάται τη σωστή παράδοση των δεδομένων και δεν ενημερώνει τα τερματικά συστήματα για τυχόν απώλειες πακέτων που οφείλονται σε πιθανά λάθη ή σε συμφόρηση στο δίκτυο [30].

Κάθε φορά επομένως, που ο χρήστης συνδέεται σε μια ιστοσελίδα αποκαλύπτεται η διεύθυνση IP του υπολογιστή του, η οποία αποκαλύπτει με τη σειρά της στο διαχειριστή του δικτύου πολλά πράγματα όσον αφορά την online δραστηριότητά του.

3.2.3 Software downloads

Το κατέβασμα λογισμικού από το διαδίκτυο συνήθως απαιτεί ένα μοναδικό αναγνωριστικό για κάθε χρήστη το οποίο το παρέχει η συγκεκριμένη

εταιρεία. Σε κάποιες περιπτώσεις, οι εταιρείες αυτές χρησιμοποιούν αυτό το αναγνωριστικό για να παρακολουθούν την online δραστηριότητα του χρήστη. Χαρακτηριστικό παράδειγμα η Realetworks όπου το 1999 κατηγορήθηκε πως παρακολουθούσε τα μουσικά cd και τα αρχεία mp3 τα οποία έπαιζαν οι χρήστες που κατέβαζαν το RealPlayer λογισμικό της.

Οι παραπάνω πηγές παραβίασης αποτελούν εσωτερικές απειλές, δηλαδή, «νόμιμοι» χρήστες του συστήματος προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε πόρους του συστήματος. Πιο συγκεκριμένα,

- Χρήστες της εταιρείας/ διαχειριστή δικτύου/ οργανισμού που παρακάμπτουν τις διαδικασίες ελέγχου για την πρόσβαση σε διαβαθμισμένα δεδομένα/ πληροφορίες.
- Χρήστες που αποκτούν πρόσβαση σε λογαριασμούς χρηστών με περισσότερα δικαιώματα σε σχέση με τα δικαιώματα που ήδη έχουν.

Ωστόσο, η ασφάλεια και η ιδιωτικότητα του χρήστη απειλούνται και από εξωτερικούς εισβολείς με κυριότερο εξ αυτών, το κακόβουλο λογισμικό.

ΚΕΦΑΛΑΙΟ 4
ΧΑΡΑΚΤΗΡΙΣΤΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΠΑΡΑΒΙΑΣΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

4.1 Google Street View

Το Street View ξεκίνησε από την ομάδα μηχανικών της Google στις Η.Π.Α. το 2007, ως πειραματικό έργο συλλέγοντας τις πρώτες εικόνες από δημόσιους δρόμους. Έκτοτε, έχει επεκταθεί με πανοραμικές εικόνες 360 μοιρών και περιλαμβάνει τοποθεσίες και στις επτά ηπείρους [31]. Ουσιαστικά η υπηρεσία αυτή προσθέτει τρισδιάστατη προοπτική στους χάρτες της Google, καθώς επιτρέπει στο χρήστη να πλοηγηθεί ψηφιακά στο περιβάλλον μιας πόλης. Ωστόσο, για την προστασία του απορρήτου, της ανωνυμίας και της ιδιωτικότητας των ατόμων κατά τη συλλογή των εικόνων αυτών, ελήφθησαν μια σειρά από μέτρα, όπως θόλωμα των προσώπων και των πινακίδων κυκλοφορίας.

Η προστασία της εν λόγω ιδιωτικότητας κλονίστηκε όταν το 2010 αποκαλύφθηκε πως τα ειδικά οχήματα του Street View, τα οποία χαρτογραφούσαν λεπτομερώς τις περιοχές στις οποίες κινούνταν, υπέκλεπταν παράλληλα και μεγάλο όγκο προσωπικών δεδομένων, στα οποία περιλαμβάνονταν e-mail, ιατρικά και οικονομικά αρχεία και κωδικοί, από εκατομμύρια μη κρυπτογραφημένα ασύρματα δίκτυα. Η εταιρεία απέδωσε ευθύνες σε έναν μεμονωμένο μηχανικό λογισμικού, ωστόσο η θέση της Ομοσπονδιακής Επιτροπής Επικοινωνιών (Federal Communications Commission, FCC) ήταν πως ο συγκεκριμένος μηχανικός συνεργαζόταν με άλλα άτομα και είχε προσπαθήσει να ενημερώσει σχετικά τους ανωτέρους του· κατά την Επιτροπή, ήταν περισσότερο θέμα ελλιπούς επίβλεψης παρά κακόβουλης σκέψης από πλευράς του, με αποτέλεσμα την επιβολή προστίμου 25.000 δολαρίων στην εταιρεία για παρεμπόδιση των ερευνών.

Τρία χρόνια μετά, ο γενικός εισαγγελέας της Νέας Υόρκης ανακοίνωσε το συμβιβασμό μεταξύ της Google και 38 πολιτειών των Η.Π.Α. στην καταβολή του χρηματικού ποσού των επτά εκατομμυρίων δολαρίων για τη συγκεκριμένη συλλογή προσωπικών δεδομένων από την εταιρεία, χωρίς να έχει δοθεί σχετική άδεια [32].

Παράλληλα, η εταιρεία δεσμεύτηκε να ξεκινήσει ένα πρόγραμμα εκπαίδευσης εργαζομένων πάνω σε θέματα ιδιωτικότητας και διαχείρισης προσωπικών δεδομένων, το οποίο θα διαρκέσει τουλάχιστον δέκα χρόνια. Επίσης, πρέπει να ξεκινήσει διαφημιστική εκστρατεία για την ενημέρωση των καταναλωτών πάνω στην προστασία των προσωπικών τους δεδομένων.

Η θέση της Google είναι πως η υποκλοπή δεδομένων έλαβε χώρα εξαιτίας ενός κώδικα που είχε συμπεριληφθεί κατά λάθος στο λογισμικό του Street View. Αν και το εν λόγω πρόστιμο είναι το μεγαλύτερο που έχει επιβληθεί σε τέτοια υπόθεση, το ποσό παραμένει μικρό για μία εταιρεία του μεγέθους της Google. Ωστόσο, είναι πολλοί αυτοί (κυρίως μέλη οργανώσεων για θέματα ιδιωτικότητας και επικριτές της εταιρείας) οι οποίοι χαρακτηρίζουν τον εν λόγω συμβιβασμό ως «κομβικό» σημείο, καθώς αλλάζει τα δεδομένα σχετικά με μία επιχείρηση που έχει εξελιχθεί σε «κίνδυνο» για την ιδιωτικότητα των καταναλωτών.

Το καλοκαίρι του 2012, η αμερικανική Ομοσπονδιακή Επιτροπή Εμπορίου (Federal Trade Commission, FTC) επέβαλε πρόστιμο 22,5 εκατομμυρίων δολαρίων στην Google για «παράκαμψη» των ρυθμίσεων ιδιωτικότητας (privacy settings) στο browser Safari. Επίσης, το 2011, η εταιρεία συμφώνησε να επιτηρείται για διάστημα 20 ετών από την Επιτροπή μετά την παραδοχή της περί χρήσης «παραπλανητικών τακτικών» στο πλαίσιο της προώθησης του κοινωνικού δικτύου Buzz.

Στα πλαίσια του νέου συμβιβασμού, η εταιρεία όφειλε να στήσει μέσα σε έξι μήνες ένα πρόγραμμα προστασίας ιδιωτικότητας, οργανώνοντας παράλληλα, μία φορά το χρόνο, μία «εβδομάδα ιδιωτικότητας» για τους εργαζομένους της, ανεβάζοντας στο YouTube βίντεο με οδηγίες σχετικά με την κρυπτογράφηση δεδομένων σε ασύρματα δίκτυα και δημοσιεύοντας σχετικές διαφημίσεις σε εφημερίδες των εν λόγω 38 πολιτειών των ΗΠΑ.

Σε ευρωπαϊκό έδαφος, αρκετές χώρες έχουν επιβάλει πρόστιμα στη Google για την παραβίαση των προσωπικών δεδομένων των πολιτών τους από την συγκεκριμένη υπηρεσία, ανάμεσά τους η Γερμανία και η Ελβετία.

Παρόλα αυτά, είναι γεγονός πως η εξέλιξη της τεχνολογίας εγείρει θέματα ιδιωτικότητας και θέματα που άπτονται στο κατά πόσο ο χρήστης είναι πρόθυμος να θυσιάσει την προστασία της ιδιωτικότητάς του με αντάλλαγμα τα οφέλη της τεχνολογίας [33].

4.2 The right to be forgotten

Στις 13 Μαΐου 2014 το Δικαστήριο της Ευρωπαϊκής Ένωσης (ΔΕΕ) με απόφασή του κατοχύρωσε το «δικαίωμα στη λήθη» ανθρώπων που θέλουν να ελέγξουν τα αποτελέσματα των αναζητήσεων που τους αφορούν [34]. Το δικαστήριο αποφάνθηκε ότι η μηχανή αναζήτησης Google οφείλει σε κάποιες περιπτώσεις να συμμορφώνεται με τα αιτήματα για απομάκρυνση συνδέσμων

που οι ενδιαφερόμενοι θεωρούν ανεπιθύμητους. Διακήρυξε δηλαδή ότι κάθε φυσικό πρόσωπο έχει το δικαίωμα 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 επεξεργασία των προσωπικών δεδομένων από μηχανές αναζήτησης δεν θεωρείται, άλλωστε, ότι εξυπηρετεί «δημοσιογραφικούς σκοπούς» και ως εκ τούτου δεν εμπίπτει στη σχετική εξαίρεση της Οδηγίας 95/46/ΕΚ. Για τη διάγνωση αν συντρέχει προσβολή του εν λόγω δικαιώματος, το Δικαστήριο έκρινε ότι απαιτείται να γίνεται στάθμιση αφ' ενός των εμπορικών συμφερόντων της εταιρείας της μηχανής αναζήτησης και του δικαιώματος έκφρασης και πληροφόρησης των χρηστών του διαδικτύου, και αφ' ετέρου, των δικαιωμάτων για την προστασία των προσωπικών δεδομένων, την ιδιωτική ζωή και την προσωπική ελευθερία του ατόμου. Σύμφωνα με την απόφαση, η στάθμιση πρέπει να γίνεται βάσει των πραγματικών περιστατικών της συγκεκριμένης υπόθεσης, από την ίδια την εταιρεία της μηχανής αναζήτησης και όχι από τα δικαστήρια ή από ανεξάρτητη αρχή, η οποία θα εξετάζει αν οι κρίσιμες πληροφορίες είναι ανεπαρκείς, ανακριβείς, απαρχαιωμένες ή μη απαραίτητες.

Επιπρόσθετα, το Δικαστήριο αποφάσισε ότι η προστασία της προσωπικότητας προηγείται της ελευθερίας της πληροφορίας, σε μια απόφαση της οποία οι συνέπειες δεν έχουν γίνει ακόμα πλήρως κατανοητές.

Η υπόθεση παραπέμφθηκε στο Ευρωπαϊκό Δικαστήριο από την ισπανική Δικαιοσύνη, στην οποία είχε προσφύγει ένας πολίτης ονόματι Μάριο Κοστέχα. Ο Κοστέχα διαπίστωσε ότι, γράφοντας το όνομά του στη μηχανή αναζήτησης της Google, στα αποτελέσματα εμφανιζόταν καταχώριση σε εφημερίδα του 1998 σχετική με ακίνητό του, που επρόκειτο να εκπλειστηριαστεί λόγω χρεών προς ασφαλιστικά ταμεία. Τα bots της Google, που σαρώνουν διαρκώς το διαδίκτυο για νέες πληροφορίες, είχαν εντοπίσει την καταχώριση όταν ψηφιοποιήθηκε το αρχείο της εφημερίδας. Ο Κοστέχα ζήτησε από την Google να απομακρύνει το σύνδεσμο, υποστηρίζοντας πως το χρέος έχει προ πολλού πληρωθεί και ότι η ανάρτηση τον δυσφημίζει.

Τη δημοσίευση της απόφασης ακολούθησαν δεκάδες χιλιάδες αιτήσεις για διαγραφή δεδομένων από όλη την Ευρώπη. Η μαζική αυτή αντίδραση προκάλεσε έντονη αμηχανία σε σχέση με τους μηχανισμούς εξέτασης των εν λόγω αιτημάτων, δεδομένου μεταξύ άλλων, ότι η παραπάνω απόφαση ανέθεσε την εν λόγω αρμοδιότητα στον ίδιο το φορέα επεξεργασίας

προσωπικών δεδομένων. Ευλόγως εγείρονται ζητήματα σχετικά με τους κανόνες που θα καθιερωθούν για τη διαδικασία υποβολής των αιτήσεων και την έγκριση της διαγραφής των δεδομένων, με το πρωτόκολλο απομάκρυνσης των συνδέσμων, με το κόστος της διαδικασίας και τον επιμερισμό του, με τη δυνατότητα ελέγχου των αποφάσεων των αρμόδιων φορέων, και άλλα.

Εξάλλου, η παραδοχή από το ΔΕΕ ότι μια διαδικτυακή μηχανή αναζήτησης μπορεί να συνίσταται ως υπεύθυνος επεξεργασίας προσωπικών δεδομένων προκαλεί αντιδράσεις, διότι ερμηνεύει υπερβολικά ευρέως την εν λόγω έννοια, επιτρέποντας να υπαχθούν σε αυτή όλα τα μέσα κοινωνικής δικτύωσης, οι εταιρίες cloud computing, οι υπεύθυνοι για τη λειτουργία διαδικτυακών μέσων μαζικής ενημέρωσης ανεξαιρέτως, ακόμα και απλοί bloggers, αποδίδοντας έτσι ευθύνη για την επεξεργασία προσωπικών δεδομένων σε πρόσωπα που θεωρούνται «ενδιάμεσοι» ως προς τις υπηρεσίες της πληροφορίας.

Αναφορικά με τη συγκεκριμένη περίπτωση, το Δικαστήριο κλήθηκε να αποφανθεί και για ακόμα ένα ζήτημα, το κατά πόσον η Ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα και την προστασία της ιδιωτικότητας εφαρμόζεται και σε παρόχους υπηρεσιών εγκατεστημένων εκτός ΕΕ, όπως η Google, η οποία εδρεύει στις Ηνωμένες Πολιτείες Αμερικής. Χρησιμοποιώντας ως κριτήριο τις διαφημιστικές υπηρεσίες της Google, οι οποίες διαφέρουν από χώρα σε χώρα, με το σκεπτικό ότι η εταιρεία υπάγεται στο δίκαιο της χώρας από την οποία εισπράττει διαφημιστικά έσοδα, αλλά και το γεγονός ότι η θυγατρική Google Spain προέβαινε η ίδια σε επεξεργασία δεδομένων προσωπικού χαρακτήρα που τα διέθετε στη συνέχεια προς αναζήτηση σε κατοίκους κράτους-μέλους της ΕΕ, έκρινε πως τόσο η θυγατρική εταιρία, όσο και η μητρική εταιρία, όπου και βρίσκεται ο φυσικός server, υπόκεινται στην Ευρωπαϊκή νομοθεσία για τα προσωπικά δεδομένα.

Πάρα ταύτα, κάθε ιστορία διαδικτυακής διαπόμπευσης ή διαδικτυακής αποκάλυψης είναι εντελώς ξεχωριστή και ως τέτοια θα έπρεπε να εξετάζεται. Το ερώτημα είναι αν οι πάροχοι θα μπορέσουν να ικανοποιήσουν τα αιτήματα λήθης σε αυτό το σύμπαν των τρισεκατομμυρίων αναρτήσεων από δισεκατομμύρια χρήστες. Ακόμη και αν η Google το ήθελε, η εξαφάνιση πληροφοριών μοιάζει ανέφικτη. Το ίδιο ισχύει και για τους λοιπούς παρόχους.

Μολονότι η εξέλιξη αυτή έγινε δεκτή με ενθουσιασμό από μεγάλο μέρος του πληθυσμού, που είδαν σε αυτή μια νίκη του κινήματος υπέρ της προστασίας των προσωπικών δεδομένων στο διαδίκτυο, έχουν εκφραστεί αμφιβολίες για το κατά πόσο αυτού του είδους η παρέμβαση θα έχει θεμιτά αποτελέσματα. Ειδικοί στα ψηφιακά δικαιώματα προειδοποίησαν ότι η απόφαση αυτή μπορεί να οδηγήσει σε λογοκρισία στο διαδίκτυο καθώς ανοίγει

την πόρτα σε όσους είναι δυσαρεστημένοι με τα αποτελέσματα της αναζήτησης για να απομακρύνουν ή να αλλάζουν τις πληροφορίες που τους αφορούν. Επίσης υπάρχει κίνδυνος αλλοίωσης του παρελθόντος σε τέτοιο βαθμό ώστε να υπάρξει κίνδυνος διαγραφής της ιστορίας.

4.3 Παραβίαση ασφαλείας στο iCloud

Τον Ιούνιο του 2011, η Apple, μια από τις μεγαλύτερες πολυεθνικές εταιρείες τεχνολογίας, ανακοίνωσε μια σειρά υπηρεσιών στο λεγόμενο «σύννεφο», υπό την επωνυμία iCloud. Ουσιαστικά πρόκειται για υπηρεσίες αυτόματου συγχρονισμού όχι μόνο μηνυμάτων ηλεκτρονικών ταχυδρομείου, επαφών, φωτογραφιών, εγγράφων ή μουσικής αλλά και αγορασμένων εφαρμογών και όλων των δεδομένων των χρηστών σε όλες τις συσκευές που φέρουν τα λειτουργικά συστήματα της Apple.

Η συζήτηση περί ασφάλειας στις υπηρεσίες cloud, τις οποίες χρησιμοποιούν όλο και περισσότεροι χρήστες του διαδικτύου για σκοπούς αποθήκευσης (Dropbox, Google Drive, OneDrive, κλπ) βρέθηκε στο επίκεντρο λόγω της μεγάλης διαρροής φωτογραφιών και βίντεο διασημοτήτων [35].

Τον Αύγουστο του 2014, ανώνυμος χάκερ παραβίασε την ιδιωτική ζωή πολλών διασημοτήτων του Hollywood, δίνοντας στη δημοσιότητα ορισμένες πολύ προκλητικές φωτογραφίες τους. Το ουσιαστικό της υπόθεσης δεν είναι η κυκλοφορία διασήμων γυναικών σε προσωπικές τους στιγμές στο διαδίκτυο, αλλά η παραβίαση των ευαίσθητων δεδομένων ενός μεγάλου αριθμού θυμάτων μέσω του iCloud της Apple, το οποίο αποδείχθηκε όχι και τόσο ασφαλές.

Σημειώνεται ότι οι φωτογραφίες – κάποιες εκ των οποίων φέρονται να είναι αληθινές, και κάποιες άλλες όχι- δημοσιεύθηκαν αρχικά στο 4Chan και στη συνέχεια ακολούθησε εξάπλωσή τους στο διαδίκτυο, μέσω εργαλείων κοινωνικής δικτύωσης (Twitter, Reddit κ.ά.), αναρτήσεων σε ιστοσελίδες και blogs, torrents κλπ.

Σε συνέντευξη που έδωσε στη "Wall Street Journal", ο CEO της Apple, Tim Cook, εξήγησε ότι οι χάκερς κατόρθωσαν είτε να απαντήσουν σωστά στις ερωτήσεις ασφαλείας των θυμάτων με αποτέλεσμα να ανακτήσουν τους κωδικούς από τα Apple IDs και να εισέλθουν στους λογαριασμούς τους, είτε να

μαντέψουν σωστά τα passwords τους κάνοντας χρήση τεχνικών ηλεκτρονικού ψαρέματος (phising).

Αξιοσημείωτο είναι το γεγονός πως γυρνώντας πίσω το χρόνο, ειδικά στο 2012, ένας άνδρας καταδικάστηκε σε 10 χρόνια φυλάκισης για τη λήψη γυμνών φωτογραφιών από το τηλέφωνο της γνωστής ηθοποιού Scarlett Johansson.

4.4 Παραβίαση λογαριασμών χρηστών των κοινωνικών δικτύων

Το Νοέμβριο του 2013 δύο εκατομμύρια λογαριασμοί χρηστών από όλο τον κόσμο κυρίως του Facebook αλλά και της Google, της Yahoo, του LinkedIn και 93.000 άλλων ιστοσελίδων, δέχτηκαν παραβίαση. Η επίθεση ξεκίνησε όταν κακόβουλο λογισμικό τύπου δουρείου ίππου εγκαταστάθηκε στους υπολογιστές των χρηστών το οποίο υπέκλεπτε ονόματα χρηστών και κωδικούς για πάνω από ένα μήνα [36].

Ο server μέσω του οποίου έγινε η επίθεση εντοπίστηκε στην Ολλανδία και περιείχε στοιχεία για πάνω από 93.000 ιστοσελίδων συμπεριλαμβανομένων των εξής:

- 318.000 λογαριασμούς Facebook
- 70.000 λογαριασμούς Gmail, Google+ και YouTube
- 60.000 λογαριασμούς Yahoo
- 22.000 λογαριασμούς Twitter
- 9.000 λογαριασμούς Odnoklassniki (Ρωσικό κοινωνικό δίκτυο)
- 8.000 λογαριασμούς ADP (Αμερικανική εταιρεία επενδύσεων και υπηρεσιών μισθοδοσίας)
- 8.000 λογαριασμούς LinkedIn

Σύμφωνα με την Trustwave οι παραβιάσεις αυτές περιλάμβαναν [37]:

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

4.5 Η μεγαλύτερη κυβερνο-ληστεία τραπεζών του 21ου αιώνα

Σύμφωνα με έκθεση της Kaspersky, εταιρείας ασφάλειας στο διαδίκτυο, μία ομάδα χάκερ έχει κλέψει έως 1 δις δολάρια από τράπεζες και άλλες χρηματοοικονομικές εταιρείες από όλο τον κόσμο σε διάστημα δύο ετών (2013-2014). Η εν λόγω ηλεκτρονική επίθεση ήταν μία από τις πιο προσεγμένες επιθέσεις στην ιστορία εξαιτίας των προσεγμένων κινήσεων των χάκερ για να μην αποκαλυφθούν.

Οι χάκερ χρησιμοποίησαν ένα κακόβουλο λογισμικό το οποίο μπορούσε να γίνει downloaded από τα συνημμένα του e-mail, δίνοντάς τους έτσι τη δυνατότητα πρόσβασης στα συστήματα των υπολογιστών των τραπεζών. Το κακόβουλο αυτό λογισμικό (Carbanak) εξαπλωνόταν στη συνέχεια σε εσωτερικά δίκτυα και επέτρεπε τη βιντεοσκόπηση του προσωπικού ώστε να παρακολουθηθεί η δραστηριότητα των εργαζομένων.

ΚΕΦΑΛΑΙΟ 5
ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

5.1 Cookies

Ο όρος cookie προήλθε από το μαγικό «magic cookie», το οποίο δεν είναι τίποτα άλλο από ένα πακέτο δεδομένων το οποίο λαμβάνει και στέλνει αμετάβλητο ένα πρόγραμμα. Τα magic cookies χρησιμοποιήθηκαν για πρώτη φορά το 1994 από τον προγραμματιστή Lou Montulli, ο οποίος την εποχή εκείνη σχεδίαζε μια εφαρμογή ηλεκτρονικού εμπορίου για την Netscape Communications.

Η πρώτη εμφάνιση των cookies έγινε στην ιστοσελίδα της Netscape Communications, χωρίς οι χρήστες να γνωρίζουν τίποτα για την ύπαρξη και τη σημασία τους μέχρι το 1996, όπου ένα άρθρο των Financial Times, τα έκανε ευρέως γνωστά κυρίως λόγω των πιθανών επιπτώσεών τους στην ιδιωτική ζωή των χρηστών [38].

5.1.1 HTTP Cookies

Τα HTTP cookies είναι μικρά αρχεία δεδομένων που αποθηκεύονται στους υπολογιστές των χρηστών και σκοπός τους είναι να παρέχουν πληροφορίες για τους ιστοτόπους που επισκέπτονται. Περιλαμβάνει λιγότερους από 255 χαρακτήρες συνολικής χωρητικότητας 4KB. Μπορούν να απειλήσουν την ιδιωτικότητα του χρήστη αφού τα προσωπικά του δεδομένα μπορούν να συλλεχθούν από τους διάφορους ιστότοπους και να επεξεργαστούν. Ένα cookie είναι ένα κομμάτι κειμένου το οποίο στέλνεται από έναν διαχειριστή διαδικτύου (web server) στον υπολογιστή του χρήστη μέσω του προγράμματος πλοήγησης που αυτός χρησιμοποιεί. Μόλις ληφθεί, το πρόγραμμα πλοήγησης στέλνει αυτό το cookie κάθε φορά που ο χρήστης ζητάει κάποιο καινούργιο έγγραφο από τον web server. Τα cookies μπορούν επίσης, εκτός από το να καθορίζονται από το διαχειριστή, να ορίζονται και από γλώσσες προγραμματισμού όπως η JavaScript.

Για την απομνημόνευση του χρήστη, το σύστημα χρησιμοποιεί τα cookies τα οποία είναι μικρά αρχεία κειμένου που αποθηκεύονται στο σκληρό

δίσκο του υπολογιστή του χρήστη κατά την πλοήγησή του στο διαδίκτυο. Όταν ο χρήστης πραγματοποιήσει είσοδο και επιλέξει να απομνημονευθεί η ταυτότητά του, τότε μαζί με τη δημιουργία του cookie, δημιουργείται και ένα τυχαίο αλφαριθμητικό μεγάλου μεγέθους. Το όνομα του χρήστη μαζί με το τυχαίο αλφαριθμητικό και την ώρα εισόδου, αποθηκεύονται στη βάση δεδομένων. Επίσης το cookie που δημιουργείται στην πλευρά του χρήστη, περιέχει το username και το τυχαίο αλφαριθμητικό. Όταν ο χρήστης επισκεφθεί ξανά το site και χρησιμοποιήσει το cookie για την είσοδό του, τότε ελέγχεται εάν υπάρχει στη βάση αυτός ο συνδυασμός (όνομα- αλφαριθμητικό) και επίσης εάν είναι έγκυρος χρονικά (διάρκεια 30 ημερών). Εάν πραγματοποιηθεί είσοδος, τότε το αλφαριθμητικό αντικαθίσταται από ένα νέο, ενημερώνεται η βάση και δημιουργείται ένα νέο cookie. Σε περίπτωση που ο χρήστης πραγματοποιήσει αποσύνδεση από το σύστημα, τότε το cookie διαγράφεται όπως και η αντίστοιχη εγγραφή στη βάση [39].

Τα cookies έχουν τόσο πλεονεκτήματα όσο και μειονεκτήματα. Τα πλεονεκτήματα αφορούν την πιο γρήγορη πλοήγηση στο διαδίκτυο ενώ τα μειονεκτήματα την παραβίαση της ιδιωτικότητας του χρήστη. Πιο συγκεκριμένα:

Οι τοποθεσίες δικτύου χρησιμοποιούν τα cookies για να παρέχουν μια εξατομικευμένη εμπειρία στους χρήστες , καθώς και για τη συλλογή πληροφοριών σχετικά με τη χρήση τοποθεσιών δικτύου. Πολλές τοποθεσίες χρησιμοποιούν cookies για την αποθήκευση πληροφοριών που παρέχουν μια εμπειρία με συνέπεια στις διαφορετικές ενότητες της τοποθεσίας, όπως στο καλάθι αγορών ή σε προσαρμοσμένες σελίδες. Σε μια αξιόπιστη τοποθεσία δικτύου τα cookies μπορούν να εμπλουτίσουν την εμπειρία του χρήστη επιτρέποντας στην τοποθεσία να εντοπίζει τις προτιμήσεις του ή επιτρέποντάς του να παραλείπει τη διαδικασία σύνδεσης κάθε φορά που επισκέπτεται την τοποθεσία δικτύου [40].

Τα cookies μπορεί να έχουν διάφορους ρόλους. Επιτρέπουν την αποτελεσματική πλοήγηση στις σελίδες, τη διατήρηση των προτιμήσεων των χρηστών, και γενικότερα την πιο άνετη και ευχάριστη χρήση του ιστότοπου. Τα cookies επιταχύνουν και διευκολύνουν την αλληλεπίδραση με τον ιστότοπο. Αν ένας ιστότοπος δεν χρησιμοποιεί cookies, θεωρεί κάθε χρήστη νέο όποτε αλλάζει σελίδα –για παράδειγμα, όταν κλείνει ένα μενού και περνάει σε άλλη σελίδα δεν θυμάται την επιλογή του και στην επόμενη σελίδα του ξαναεμφανίζει το μενού ανοιχτό [41].

Ωστόσο, τα cookies μπορούν να χρησιμοποιηθούν για να παραβιάσουν την ανωνυμία από τους χρήστες ή να την ενισχύσουν. Δυστυχώς η επιλογή δεν

είναι στα χέρια του χρήστη, αλλά βρίσκεται υπό τον έλεγχο του διαχειριστή δικτύου.

Ιστοσελίδες, δικτυακές επιχειρήσεις και λοιποί πάροχοι συλλέγουν μεγάλο όγκο προσωπικών πληροφοριών, χωρίς απαραίτητα τα άτομα να έχουν συναινέσει ή και να έχουν γνώση της συλλογής, καθώς αυτή μπορεί μάλιστα να λαμβάνει χώρα με αδιαφανή τρόπο. Αν δε ο τεχνολογικά ενήμερος χρήστης μπορεί να περιορίσει τα cookies χρησιμοποιώντας τις σχετικές ρυθμίσεις, θα αντιμετωπίσει τον αποκλεισμό της πρόσβασης σε σελίδες υψηλής ζήτησης, συμπεριλαμβανομένης αυτής της Google ή τη μειωμένη λειτουργικότητά τους. Εναλλακτικά ο χρήστης μπορεί να διαγράψει τα αποθηκευμένα cookies. Ορισμένα προγράμματα περιήγησης, όπως το Mozilla Firefox και το Opera, προσφέρουν τη δυνατότητα διαγραφής των cookies κάθε φορά που ο χρήστης κλείνει το συγκεκριμένο πρόγραμμα.

Τα είδη των HTTP cookies είναι τα κάτωθι:

- ***Third party cookies***

  Τα «Third party cookies» δημιουργούνται και χρησιμοποιούνται από φορέα άλλον από τον ιδιοκτήτη του ιστότοπου. Για παράδειγμα, ένας ιστότοπος μπορεί να χρησιμοποιεί υπηρεσίες άλλης εταιρείας για την ανάλυση του ακροατηρίου του. Η εταιρεία αυτή ορίζει τότε το δικό της cookie για να κάνει την ανάλυση. Ο ιστότοπος μπορεί επίσης να περιλαμβάνει περιεχόμενο ενσωματωμένο από αλλού, για παράδειγμα βίντεο από το YouTube ή προβολές διαφανειών από το Flickr. Οι ιστότοποι αυτοί μπορούν επίσης να προσθέτουν τα δικά τους cookies.

  Ακόμα πιο σημαντικό είναι το γεγονός ότι οι ιστότοποι μπορούν να χρησιμοποιούν διαφημιστικά δίκτυα τρίτων για την προβολή στοχευμένων διαφημίσεων.

- ***Τα cookies συνεδρίας***

  Τα cookies συνεδρίας αποθηκεύονται προσωρινά για τη διάρκεια μιας συνεδρίας πλοήγησης και σβήνονται από τον υπολογιστή όταν κλείσει το πρόγραμμα πλοήγησης.

- ***Τα μόνιμα cookies***

  Τα cookies αυτού του τύπου καταγράφονται στον υπολογιστή του χρήστη για περιορισμένο χρονικό διάστημα (κατά γενικό κανόνα για ένα έτος ή περισσότερο) και δεν σβήνονται όταν κλείνει το πρόγραμμα πλοήγησης.

5.1.2 Flash cookies

Η διαγραφή των HTTP cookies από τους χρήστες, τουλάχιστον μία φορά το μήνα για λόγους ασφαλείας, αύξησε το επίπεδο ανησυχίας των διαφημιστών οι οποίοι ενδιαφέρονται για την online παρακολούθηση των προτιμήσεων των χρηστών του διαδικτύου με αποτέλεσμα τη χρήση των Flash cookies.

Τα Flash cookies ή Local Shared Objects (LSOs) δεν είναι τίποτα άλλο παρά cookies ιστοσελίδων που χρησιμοποιούν Adobe Flash. Βασική διαφορά με τα HTTP cookies αποτελεί το γεγονός πως δεν είναι εύκολα ανιχνεύσιμα και η επιλογή στα περισσότερα προγράμματα περιήγησης να μην δέχονται cookies δεν τα επηρεάζει [42].

Τα Flash cookies αποθηκεύονται σε διαφορετική τοποθεσία από αυτήν των HTTP cookies με αποτέλεσμα ο χρήστης να μην είναι σε θέση να γνωρίζει ποιους φακέλους οφείλει να διαγράψει ούτως ώστε να διαγραφούν και αυτά [43].

Επίσης, τα Flash cookies δεν ελέγχονται από τα προγράμματα περιήγησης, καθώς σβήνοντας το ιστορικό και τα HTTP cookies ή καθαρίζοντας τη μνήμη , αυτά δεν επηρεάζονται ούτε στον ελάχιστο βαθμό. Ακόμα και η επιλογή της ασφαλούς περιήγησης (Secure Browsing) στους περισσότερους περιηγητές, όπως ο Internet Explorer 8 και το Firefox, επιτρέπουν στα Flash cookies να λειτουργούν κανονικά και να ανιχνεύουν τις προτιμήσεις του χρήστη.

Τον Αύγουστο του 2009, το αμερικανικό περιοδικό Wired σε άρθρο του επισήμανε πως περισσότερες από τις μισές μεγαλύτερες σε επισκεψιμότητα ιστοσελίδες χρησιμοποιούσαν Flash cookies (σε σύνολο 100 ιστοσελίδων), ωστόσο, μόνο τέσσερις από αυτές ανέφεραν το συγκεκριμένο γεγονός στην πολιτική ασφαλείας τους.

5.1.3 Evercookies

Το 2013 απόρρητα έγγραφα της Εθνικής Υπηρεσίας Ασφαλείας των Ηνωμένων Πολιτειών της Αμερικής (National Security Agency, NSA) διέρρευσαν από τον Edward Snowden τα οποία περιείχαν πληροφορίες σχετικά με το πρόγραμμα μαζικής παρακολούθησης που εφάρμοζαν οι αμερικανικές και βρετανικές κυβερνήσεις με αξιοσημείωτη αναφορά στα λεγόμενα evercookies [44].

Πρόκειται για εξαιρετικά επίμονα cookies, γραμμένα σε κώδικα JavaScript και δημιουργημένα από τον Samy Kamkar, τα οποία παραμένουν ακόμα και αν ο χρήστης διαγράψει τα HTTP αλλά και τα Flash cookies. Αποθηκεύουν δεδομένα σε διαφορετικές τοποθεσίες μέσα στο πρόγραμμα περιήγησης, συμπεριλαμβανομένου HTTP, Flash, force-cached PNG εικόνες, HTML5 αποθηκευτικά συστήματα , ιστορικό περιήγησης και SQLite. Στην περίπτωση που ένα evercookie ανιχνεύσει την προσπάθεια διαγραφής των cookies από το χρήστη, τότε το πρόγραμμα τα ξαναδημιουργεί από την αρχή [45].

5.2 Δούρειοι Ίπποι (Trojan Horses)

Ένας από τους μεγαλύτερους κινδύνους τους οποίους διατρέχει ένας χρήστης είναι αυτός του δούρειου ίππου. Οι δούρειοι ίπποι δανείστηκαν το όνομά τους από το μυθικό τέχνασμα του Οδυσσέα στη Τροία, καθώς εισβάλλουν με αθώο τρόπο στο εκάστοτε σύστημα και μόλις ενεργοποιηθούν, το αποτέλεσμα της εκτέλεσής τους μπορεί να είναι καταστροφικό. Πρόκειται για προγράμματα που, ενώ εμφανίζονται σαν κανονικά προγράμματα για την εκτέλεση μιας συγκεκριμένης εργασίας στον υπολογιστή, κρυφά εκτελούν κάποια διαφορετική, στην πλειοψηφία της, κακόβουλη [46].

Αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Το πόσο μπορεί να συνεχιστεί ο έλεγχος του επιτιθέμενου στο άλλο μηχάνημα και τι καταστροφές μπορεί να προκαλέσει εξαρτάται από το είδος του δούρειου ίππου και το λόγο για τον οποίο κατασκευάστηκε. Μπορεί να του διαγράψει αρχεία ή ακόμη και να προκαλέσει ζημιές στο υλικό του υπολογιστή του. Μια άλλη ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πατάει το θύμα.

Ο διακομιστής του δούρειου ίππου παρακολουθεί συνεχώς τις κινήσεις του χρήστη.

Από τη στιγμή που ένας δούρειος ίππος θα εγκατασταθεί και θα ενεργοποιηθεί, κατασκοπεύει την κάθε μας κίνηση και την αναφέρει στον δημιουργό του. Οι Keyloggers καταγράφουν και αποθηκεύουν ότι πληκτρολογούμε και το στέλνουν στον ιδιοκτήτη του δούρειου ίππου. Έτσι πολύ εύκολα αποκαλύπτονται κωδικοί, αριθμοί πιστωτικών καρτών κτλ, πράγμα ιδιαίτερα επικίνδυνο για όσους κάνουν online-banking. Ο δούρειος ίππος μετατρέπεται εύκολα σε backdoor (εισβάλλει από την "πίσω πόρτα" του Η/Υ) όταν είναι κατάλληλος σχεδιασμένος ώστε να επιτρέπει στο δημιουργό του να πάρει τον πλήρη έλεγχο του Η/Υ που έχει μολύνει.

Η συμπεριφορά ενός online υπολογιστή που είναι μολυσμένος με ένα ενεργοποιημένο backdoor φαίνεται αλλόκοτη στους ανυποψίαστους : παράθυρα ανοίγουν και κλείνουν, ο υπολογιστής γίνεται πολύ αργός, τα antivirus και τα firewall απενεργοποιούνται. Ένας τέτοιος παραβιασμένος Η/Υ δεν είναι πλέον αξιόπιστος και η μόνη λύση για να εξαλειφθούν όλα τα ίχνη των ιών είναι το format.

Η πλειοψηφία των μολύνσεων από δούρειους ίππους συμβαίνει όταν ο χρήστης προσπαθεί να εγκαταστήσει ένα δωρεάν λογισμικό από το διαδίκτυο ή να εγκαταστήσει προγράμματα antivirus τα οποία στην πραγματικότητα είναι μολυσμένα. Συνήθεις κρυψώνες ενός δούρειου ίππου είναι επίσης κάποιο νέο δωρεάν παιχνίδι στο διαδίκτυο, κάποιο τραγούδι mp3 ή κάποιο πρόγραμμα αρκετά δελεαστικό ώστε να το κατεβάσει ο χρήστης [47].

Υπάρχουν δύο είδη δούρειων ίππων. Το πρώτο αποτελείται από κανονικά προγράμματα, τα οποία κακόβουλοι προγραμματιστές μεταβάλλουν προσθέτοντάς τους κακόβουλο κώδικα. Στη κατηγορία αυτή ανήκουν διάφορα προγράμματα ανταλλαγής αρχείων (peer-to-peer) καθώς και προγράμματα ανακοίνωσης καιρικών συνθηκών. Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν το χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Σε αντίθεση με άλλα κακόβουλα προγράμματα (σκουλήκια, ιούς κτλ), οι δούρειοι ίπποι δεν μπορούν να δράσουν αυτόνομα αλλά εξαρτώνται από τις ενέργειες που θα κάνει το υποψήφιο θύμα. Τέλος, στην επιστήμη της αρχιτεκτονικής υπολογιστών, η λέξη «δούρειος ίππος» δύναται επίσης να αναφέρεται και σε κενά ασφαλείας που επιτρέπουν σε διάφορα προγράμματα να διαβάσουν αρχεία χωρίς εξουσιοδότηση.

5.3 Κερκόπορτα (Backdoor ή Trapdoor)

Η κερκόπορτα είναι η πιο επικίνδυνη κατηγορία δούρειων ίππων επειδή η λειτουργία της θυμίζει κανονικά προγράμματα απομακρυσμένης διαχείρισης. Οι κερκόπορτες εγκαθίστανται εν αγνοία του χρήστη και παρέχουν στον εισβολέα τη δυνατότητα απομακρυσμένης διαχείρισης του υπολογιστή. Έτσι, αυτή η κερκόπορτα είναι μια κρυφή λειτουργία μιας εφαρμογής η οποία έχει προγραμματιστεί με στόχο να εκμεταλλεύεται το σύστημα που θέλει και να αποσπά τις πληροφορίες που θέλει.

5.4 Λογική Βόμβα (Logic bomb)

Η λογική βόμβα αποτελεί έναν από τους παλιότερους τύπους κακόβουλου λογισμικού. Πρόκειται για μικρά προγράμματα τα οποία προστίθενται σε κάποιο υπάρχον ή ακόμα και για τροποποιήσεις σε υπάρχοντες κώδικες. Αποκαλούνται βόμβες διότι ενεργοποιούνται όταν πληρούνται συγκεκριμένες συνθήκες (π.χ. παρουσία ή απουσία κάποιου αρχείου, συγκεκριμένη ημερομηνία, συγκεκριμένος χρήστης). Ένα παράδειγμα που θα μπορούσε να δοθεί είναι ένα τμήμα κώδικα που έχει προστεθεί από προγραμματιστή εταιρείας στο λειτουργικό σύστημα που χρησιμοποιείται. Για όσο ο προγραμματιστής τροφοδοτεί τον υπολογιστή με τον κωδικό πρόσβασής του δε συμβαίνει τίποτα. Σε περίπτωση απόλυσής του, η βόμβα, μετρώντας κάποιο χρονικό διάστημα που δεν έχει δεχτεί κωδικό πρόσβασης, θα εκραγεί προκαλώντας σοβαρά αποτελέσματα όπως καθαρισμός δίσκων, διαγραφή τυχαίων αρχείων ή κρυπτογράφηση βασικών αρχείων.

5.5 Ιοί (Viruses)

Πρόκειται για ένα είδος προγράμματος ή κώδικα που είναι ικανό να δημιουργεί αντίγραφα του εαυτού του και εισάγεται σκοπίμως σε κάποιο πρόγραμμα ηλεκτρονικού υπολογιστή ή σε κάποιο σύστημα. Κάθε ιός έχει μια ταυτότητα/ υπογραφή, η οποία δεν είναι τίποτα άλλο από μια σειρά από bytes [48].

Πρώτος ο Fred Cohen μελέτησε τη συμπεριφορά των ιών. Απέδειξε ότι η μόλυνση είναι δυνατόν να υπάρξει όποτε υπάρχει διαμοιράσιμη πληροφορία ή μη ελεγχόμενη ροή πληροφορίας. «Ο μόνος σίγουρος τρόπος για να εμποδίσουμε τη διάδοση μιας μόλυνσης που οφείλεται σε ιό, είναι να απαγορεύσουμε την ύπαρξη διαμοιράσιμων πόρων και τη ροή πληροφορίας στο σύστημά μας. Τότε όμως, στην ουσία θα καταλήξουμε να έχουμε ένα σύστημα που δε λειτουργεί» [49].

Ένας τυπικός ιός περνάει από τις εξής φάσεις:

- ***Ύπνωση (Dormant):*** Κατά τη φάση αυτή ο ιός είναι ανενεργός και αναμένει τη πυροδότηση κάποιας λειτουργίας ή συνθήκης για να ξεκινήσει τη διάδοσή του. Η ενεργοποίηση αυτή μπορεί να προέλθει από κάποιο γεγονός, όπως η παρουσία ενός άλλου προγράμματος ή η υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους ιούς.
- ***Διάδοση (Propagation):*** Κατά τη φάση αυτή ο ιός τοποθετεί ένα ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε συγκεκριμένες περιοχές του δίσκου. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος με τη σειρά του θα μπει σε φάση διάδοσης.
- ***Ενεργοποίηση (Triggering):*** Όπως και με τη φάση διάδοσης, έτσι και η φάση ενεργοποίησης μπορεί να πυροδοτηθεί από την εμφάνιση κάποιου γεγονότος σχετικού με το σύστημα. Ο ιός ενεργοποιείται για να επιτελέσει τη λειτουργία για την οποία έχει σχεδιαστεί.
- ***Εκτέλεση (Execution):*** Κατά τη φάση αυτή επιτελείται η λειτουργία που προβλέπεται στον κώδικα του ιού. Η λειτουργία ενδέχεται να είναι ουσιαστικά αβλαβής, όπως η εμφάνιση ενός απλού μηνύματος στην οθόνη του χρήστη, ή επιβλαβής, όπως η καταστροφή προγραμμάτων και αρχείων δεδομένων. Σε κάποιες περιπτώσεις μάλιστα είναι δυνατόν να προκληθεί απώλεια δεδομένων, και μάλιστα από ολόκληρα κομμάτια του δίσκου. Επίσης, συχνά, ο υπολογιστής γίνεται ξαφνικά ασταθής, αποτυγχάνει να ξεκινήσει, ή δεν μπορεί να εντοπίσει το σκληρό δίσκο. Σε τέτοιες περιπτώσεις, μηνύματα λάθους όπως «invalid system disk» είναι συχνό φαινόμενο. Η μετάδοση αυτού του είδους ιομορφικού λογισμικού γινόταν συνήθως από μολυσμένους εξωτερικούς δίσκους. Σήμερα, η μετάδοσή τους γίνεται κατά βάση μέσω του διαδικτύου κατά το κατέβασμα αρχείων ή και από μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου.

5.6 Σκουλήκια (Worms)

Η μεγαλύτερη παραβίαση ασφάλειας όλων των εποχών σε υπολογιστές ξεκίνησε το απόγευμα της 2ας Νοεμβρίου 1988, όταν ένας τελειόφοιτος του Πανεπιστημίου Cornell ελευθέρωσε το πρόγραμμα σκουλήκι (worm) στο διαδίκτυο. Αυτή η πράξη είχε ως αποτέλεσμα να καταρρεύσουν χιλιάδες υπολογιστές σε πανεπιστήμια, εταιρείες και κυβερνητικά εργαστήρια σε ολόκληρο τον κόσμο, προτού αποκαλυφθεί και απομακρυνθεί το εν λόγω σκουλήκι [50].

Το σκουλήκι εκμεταλλευόταν ένα σφάλμα που είχε το λειτουργικό Berkeley UNIX, χάρη στο οποίο του επιτρεπόταν να έχει μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές, οι οποίοι ήταν συνδεδεμένοι στο διαδίκτυο. Από τη στιγμή που αποκτούσε πρόσβαση σε ένα νέο υπολογιστή αναπαραγόταν σε αυτόν (αντέγραφε τον εαυτό του) και το αντίγραφό του έψαχνε με τη σειρά του να αποκτήσει πρόσβαση σε άλλους υπολογιστές. Τίποτα όμως στον κώδικα του σκουληκιού δεν υποδήλωνε προσπάθεια για να κλέψει ή να χαλάσει οτιδήποτε στους υπολογιστές που αποκτούσε πρόσβαση. Δεν είναι βέβαια γνωστό, αν η μορφή που είχε το πρόγραμμα στις 2 Νοεμβρίου 1988 προοριζόταν απλώς για έλεγχο και διέρρευσε στο διαδίκτυο κατά λάθος ή ήταν η τελική. Γεγονός πάντως είναι ότι οι μολυσμένοι υπολογιστές μετά από κάποιο διάστημα κατακλύζονταν από αντίγραφα του σκουληκιού και δεν μπορούσαν να λειτουργήσουν.

Ένα σκουλήκι δεν είναι τίποτα άλλο παρά ένα αυτό-αναπαραγόμενο πρόγραμμα ηλεκτρονικού υπολογιστή το οποίο χρησιμοποιεί το δίκτυο για να στείλει αντίγραφα του εαυτού του σε άλλους υπολογιστές στο δίκτυο χωρίς να είναι αναγκαία κάποια παρέμβαση από το χρήστη. Σε αντίθεση με τους ιούς, δεν χρειάζεται να προσκολλάται σε ένα υπάρχον πρόγραμμα. Τα σκουλήκια σχεδόν πάντα προκαλούν βλάβες στο δίκτυο.

Τα σκουλήκια επομένως είναι παρασιτικά προγράμματα που μπορούν και αναπαραγάγουν τον εαυτό τους αλλά δε μολύνουν άλλα αρχεία στον υπολογιστή που προσβάλλουν. Κάνουν χρήση των υπηρεσιών δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται πιο εύκολα και με μεγάλη ταχύτητα λόγω της εύκολης επικοινωνίας των χρηστών. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή , στέλνουν μολυσμένα και καμουφλαρισμένα μηνύματα ηλεκτρονικού ταχυδρομείου σε όλη τη λίστα επαφών του χρήστη. Η μαζική αποστολή ηλεκτρονικού ταχυδρομείου

επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του διαδικτύου, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας.

Σύμφωνα με τον Aycock J. [47], μερικές κατηγορίες του διαδικτυακού σκουληκιού είναι οι ακόλουθες:

- Το σκουλήκι που εξαπλώνεται μέσω του ηλεκτρονικού ταχυδρομείου.
- Το σκουλήκι που εξαπλώνεται μέσω μολυσμένων επισυναπτόμενων αρχείων και παραπέμπουν το χρήστη να μπει σε κακόβουλους ιστότοπους (Instant messaging worm).
- Το σκουλήκι που εξαπλώνεται μέσω φόρουμ και chat rooms (Internet Relay Chat worm)
- Το σκουλήκι που εξαπλώνεται μέσω της πρόσβασης ενός χρήστη σε μια ιστοσελίδα ή σε οποιοδήποτε άλλο διαδικτυακό μέσο (Internet worm).
- Το σκουλήκι που αντιγράφεται μέσα σε ένα διαμοιραζόμενο φάκελο και έπειτα χρησιμοποιεί peer-to-peer μηχανισμούς προκειμένου να ανακοινωθεί η ύπαρξή του με την ελπίδα πως και άλλοι χρήστες θα το κατεβάσουν και θα το εκτελέσουν (File sharing ή peer-to-peer worm).
- Το σκουλήκι που εξαπλώνεται μέσω διαδικτύου και προσβάλλει όλους τους ευπαθείς servers μέσα σε 15 λεπτά από την ενεργοποίησή του (Warhol worm).
- Το σκουλήκι που εξαπλώνεται μέσα σε δευτερόλεπτα από την ενεργοποίησή του σε όλους τους ευπαθείς υπολογιστές στο διαδίκτυο (Flash worm).

Πλέον, όλες οι εταιρείες αντιβιοτικών παρέχουν τακτικές ενημέρωσης ασφαλείας και εφόσον αυτές έχουν εγκατασταθεί σε έναν υπολογιστή, τότε η πλειοψηφία των σκουληκιών δεν είναι σε θέση να εξαπλωθούν σε αυτόν. Εν γένει, ο χρήστης θα πρέπει να είναι δύσπιστος όσον αφορά το άνοιγμα απρόσμενης ηλεκτρονικής αλληλογραφίας και δεν θα πρέπει να τρέχει συνημμένα αρχεία ή προγράμματα ή να επισκέπτεται διαδικτυακούς τόπους που συνδέονται με τέτοιου είδους μηνύματα.

5.7 Rootkits

Ο όρος rootkit προέρχεται από τη συνένωση των όρων «root» (το παραδοσιακό όνομα του προνομιούχου λογαριασμού σε λειτουργικά συστήματα τύπου Unix) και του όρου «kit». Υπό τη γενικότερη έννοια, τα rootkit θεωρούνται εργαλεία λογισμικού τα οποία επιτρέπουν τη μεταμφίεση διεργασιών και αρχείων και συνεπώς την αποφυγή ανίχνευσης από το χρήστη ή, καλύτερα, από το λογισμικό προστασίας από τους ιούς .

Η τεχνολογία rootkit καθ' εαυτή δεν περιλαμβάνει επιζήμιες ενέργειες, ωστόσο λειτουργώντας ως μανδύας μεταμφίεσης για άλλα λογισμικά, κυρίως κακόβουλα, επιτρέπει τη λειτουργία τους στο παρασκήνιο χωρίς να το γνωρίζει ο χρήστης.

Ακόμη και φαινομενικά αβλαβείς, εμπορικές εφαρμογές έχουν χρησιμοποιήσει rootkits. Το γνωστότερο παράδειγμα είναι αυτό της Sony BMG, η οποία χρησιμοποιούσε XCP, το οποίο παρέμενε κρυμμένο σε διάφορα μουσικά CD με τη βοήθεια της τεχνολογίας rootkit.

Ένα rootkit μπορεί να αποκτήσει τον πλήρη έλεγχο ενός συστήματος. Ο σκοπός του είναι συνήθως να αποκρύψει στοιχεία, δικτυακές συνδέσεις ή διευθύνσεις στη μνήμη από άλλα προγράμματα τα οποία χρησιμοποιούνται από τους διαχειριστές των συστημάτων για την ανακάλυψη μη αποδεκτών προσβάσεων στους πόρους ενός συστήματος. Τα rootkits χωρίζονται σε δύο κατηγορίες:

- *User-Level rootkit*, το οποίο αντικαθιστά ή αλλάζει αρχεία και προγράμματα που χρησιμοποιούνται από τους χρήστες και τους διαχειριστές ενός συστήματος ώστε να ικανοποιήσουν τις ανάγκες ενός κακόβουλου χρήστη.
- *Kernel-Level rootkit*, το οποίο μπορεί και παραποιεί τον πυρήνα του λειτουργικού συστήματος με σκοπό την εγκατάσταση κάποιων backdoors ή την απόκρυψη διεργασιών και άλλων στοιχείων.

5.8 Κακόβουλοι Πράκτορες (Bot- Zombie)

Το bot είναι ένα είδος κακόβουλου λογισμικού που επιτρέπει σε έναν εισβολέα να αποκτήσει τον πλήρη έλεγχο στον πληγέντα υπολογιστή. Οι υπολογιστές που έχουν μολυνθεί από ένα bot συνήθως αναφέρονται ως

zombie. Ο επιτιθέμενος καθίσταται αόρατος με στόχο τον πλήρη έλεγχο του υπολογιστή [51].

Πρόκειται για κακόβουλο λογισμικό που προσβάλλει τους υπολογιστές καθιστώντας τους μέλη ενός δικτύου (botnet), το οποίο ελέγχεται εξ' αποστάσεως από τρίτους, με σκοπό τη πραγματοποίηση επιθέσεων κατά τις οποίες ένας αριθμός μολυσμένων υπολογιστών προσπαθεί να συνδεθεί στον υπολογιστή - στόχο μέσω δικτύου. Ο όρος bot προέρχεται από την τσεχικής προέλευσης λέξη «robota» και χρησιμοποιείται για να περιγράψει κάθε είδους αυτοματοποιημένη διαδικασία.

5.9 Προγράμματα παρακολούθησης (Spyware)

Το spyware είναι λογισμικό το οποίο εγκαθίσταται εν αγνοία του χρήστη με σκοπό να σταματήσει ή να λάβει το μερικό έλεγχο της αλληλεπίδρασης του χρήστη με τον υπολογιστή. Μια συνηθισμένη λειτουργία του είναι να κατακλύζει τους προσβεβλημένους υπολογιστές με pop-up διαφημίσεις. Είναι σε θέση να συλλέξει διάφορα είδη πληροφοριών που αφορούν τους χρήστες αλλά και να εγκαθιστά επιπρόσθετο λογισμικό και να προσπελαύνει ιστοσελίδες που μπορούν να προσβάλουν τον υπολογιστή με πολύ πιο επικίνδυνους ιούς.

Σύμφωνα με τον Peterson, ο πιο συνηθισμένος τύπος spyware είναι το keylogger καθώς παίρνει πληροφορίες που εισάγονται από το πληκτρολόγιο, ελέγχει προσωπικές πληροφορίες και κωδικούς παρακολουθώντας ταυτόχρονα και τους ιστότοπους τους οποίους επισκέπτεται ο χρήστης [52].

5.10 Adware

Πρόκειται για λογισμικό υποστήριξης διαφημίσεων καθώς εμφανίζουν διαφημιστικά πλαίσια στο περιβάλλον άλλων προγραμμάτων και ανακατευθύνουν ερωτήματα αναζήτησης σε διαφημιστικούς δικτυακούς τόπους. Επίσης, μεταφέρουν και πληροφορίες με την άδεια του χρήστη.

Η εκτέλεση αυτού του λογισμικού μπορεί να γίνεται νόμιμα, στα πλαίσια μιας εφαρμογής που το ορίζει ρητώς στους όρους χρήσης της, ή με τρόπο μη φανερό. Στη δεύτερη περίπτωση τα λογισμικά τύπου adware θεωρούνται κακόβουλο λογισμικό. Το λογισμικό adware συνήθως συνεργάζεται με λογισμικό spyware.

Οι παρενέργειες ενός λογισμικού adware ποικίλλουν: εμφάνιση ανεπιθύμητων μηνυμάτων, αλλαγή αρχικής σελίδας του browser, αναδρομολόγηση σε λανθασμένο (πλαστό) δικτυακό τόπο (web spoofing).

ΚΕΦΑΛΑΙΟ 6
ΔΙΑΜΟΙΡΑΣΜΟΣ ΑΡΧΕΙΩΝ

6.1 ΟΜΟΤΙΜΗ ΔΙΚΤΥΩΣΗ - PEER-TO-PEER

6.1.1 Αρχιτεκτονική ομότιμων συστημάτων

Τα συστήματα ομότιμων κόμβων (peer-to-peer) λαμβάνουν μεγάλης προσοχής καθώς προσφέρουν δυνατότητες σε προγράμματα για το διαμοιρασμό μεγάλου όγκου δεδομένων. Καθένα από αυτά τα προγράμματα λειτουργεί έτσι ώστε, να κάνει κοινόχρηστο ένα μέρος του σκληρού δίσκου του τοπικού υπολογιστή του χρήστη, σε όλους τους χρήστες, οι οποίοι είναι συνδεδεμένοι στο διαδίκτυο και χρησιμοποιούν το ίδιο πρόγραμμα. Επομένως, κάθε μέλος της ιδιότυπης αυτής κοινότητας, μπορεί να αναζητεί αρχεία στους υπολογιστές των μελών της και να δημιουργεί αντίγραφά τους στο δικό του υπολογιστή. Κατά την αντιγραφή των αρχείων υπάρχει απευθείας, σύγχρονη επικοινωνία μεταξύ υπολογιστών, ως εκ τούτου τα προγράμματα αυτά ονομάζονται και ομότιμης σύνδεσης προγράμματα.

Τα peer-to-peer συστήματα είναι κατανεμημένα συστήματα στα οποία οι κόμβοι (peers) συνδέονται μεταξύ τους με διάφορους τρόπους και τεχνικές. Το χαρακτηριστικό των συστημάτων αυτών είναι ότι όλοι ο κόμβοι είναι ομότιμοι, δηλαδή έχουν τις ίδιες δυνατότητες, κρατούν το ίδιο μέγεθος πληροφορίας και έχουν τις ίδιες ευθύνες. Χαρακτηριστικά παραδείγματα τέτοιων συστημάτων είναι τα Napster, Gnutella και Freenet. Τα συστήματα αυτά είναι κατανεμημένες εφαρμογές που δε χαρακτηρίζονται από το κλασικό μοντέλο πελάτη/ εξυπηρετητή, αλλά χρησιμοποιούν μια διαφορετική προσέγγιση στην υποδομή τους, κατά την οποία όλοι οι μέτοχοι σε αυτήν είναι ισότιμα μέλη. Δηλαδή, έχουν τη δυνατότητα να ενεργούν και ως πελάτες αλλά και ως εξυπηρετητές αιτήσεων. Επομένως, κάθε κόμβος που μετέχει είναι ισότιμος με κάθε άλλο και μπορεί να ενεργήσει είτε σαν πελάτης (client) είτε σαν εξυπηρετητής (server). Κινητήρια δύναμη για ανάπτυξη εφαρμογών peer-to-peer αποτελεί η αποκεντρικοποιημένη και κατανεμημένη δομή τέτοιων συστημάτων που δεν απαιτούν διαχείριση και συντήρηση, οικονομικές αξιώσεις ή άλλους νομικούς περιορισμούς. Οι κόμβοι (πρόκειται για προσωπικούς υπολογιστές, σταθμούς εργασίας κτλ) προσαρμόζονται, αυτο-διοργανώνονται καθώς εισέρχονται ή αποχωρούν από το σύστημα, ικανοποιώντας την ιδιότητα της κλιμάκωσης και της ανοχής στις αποτυχίες. Οι λειτουργίες του είναι κατανεμημένες στους κόμβους που μετέχουν σε ένα

τέτοιο σύστημα, όπου εκατομμύρια χρήστες μπορούν να είναι παρόντες ταυτόχρονα.

Η συμμετοχή σε ένα peer-to-peer σύστημα είναι εθελοντική και δυναμική. Αποσκοπεί στη συνεργασία των peers για την επίτευξη της εκάστοτε ζητούμενης υπηρεσίας και στοχεύει στην ισότιμη συνεισφορά διαθέσιμων πόρων από όλους. Οι προκλήσεις που προκύπτουν κατά το σχεδιασμό τέτοιων συστημάτων, σχετίζονται με την ανάπτυξη των κατάλληλων μηχανισμών, ώστε να επιτυγχάνεται η καλύτερη δυνατή οργάνωση των peers με στόχο τη βελτίωση της ποιότητας της υπηρεσίας. Επιπλέον, το κλειδί της χρηστικότητας ενός peer-to-peer συστήματος διαμοιρασμού δεδομένων είναι οι αποδοτικές τεχνικές για αναζήτηση και απόκτηση των δεδομένων.

Το πιο γνωστό peer-to-peer σύστημα έκανε την εμφάνισή του το 1999 και δημιουργήθηκε από τον Shawn Fanning για ανταλλαγή μουσικών αρχείων τύπου mp3 με τους φίλους του. Μέσα σε πολύ μικρό χρονικό διάστημα όμως, τα μέλη του είχαν ξεπεράσει τα 21 εκατομμύρια. Το όνομά του ήταν Napster και η φιλοσοφία της λειτουργίας του ήταν πολύ απλή. Σε έναν κεντρικό διακομιστή φιλοξενούταν μια βάση δεδομένων με καταχωρίσεις ευρετηρίου για τη θέση αποθήκευσης των μουσικών αρχείων. Ο χρήστης απηύθυνε εκεί την ερώτηση για το αρχείο που επιθυμούσε, ο διακομιστής του απαντούσε που θα βρει αντίγραφο και στη συνέχεια, ο χρήστης το κατέβαζε απευθείας από τον κόμβο που διατηρούσε αντίγραφο. Το αντίγραφο αυτό βρισκόταν στους τοπικούς δίσκους του κάθε μέλους σε κατάλογο. Η ανταλλαγή γινόταν με απευθείας σύνδεση των δύο αυτών μελών βασισμένη σε ένα HTTP πρωτόκολλο ανταλλαγής αρχείων.

Νομικοί περιορισμοί από δισκογραφικές εταιρείες επέβαλαν το σταμάτημα της λειτουργίας του Napster το 2001, όμως το πνεύμα του διαχέεται στα μετέπειτα peer-to-peer συστήματα, όπως αυτό της Gnutella, ένα αδόμητο, δυναμικό σύστημα το οποίο έχει μεταφέρει όλες τις λειτουργίες στο χρήστη, με αποτέλεσμα να μην υπάρχει καμία κεντρική διαχείριση ώστε να μη μπορεί κανείς να θεωρηθεί υπεύθυνος.

6.1.2 Ασφάλεια, Ανωνυμία, Έλεγχος Πρόσβασης

Η ασφάλεια είναι ιδιαίτερη απαίτηση στα peer-to-peer συστήματα, καθώς υπάρχει ανάγκη για διαθεσιμότητα, μυστικότητα, εμπιστοσύνη, ακεραιότητα και αυθεντικότητα. Εξαιτίας της αυτονομίας και της ανοικτής

δομής των συστημάτων αυτών, είναι ιδιαίτερα ευάλωτα σε επιθέσεις. Ο όρος ασφάλεια αναφέρεται «στις πολιτικές, τις διαδικασίες και τα τεχνικά μέτρα που χρησιμοποιούνται προκειμένου να εμποδιστεί η πρόσβαση, η αλλοίωση, η κλοπή ή η υλική ζημιά των peer-to-peer δικτύων από παρείσακτους» [53].

Το ενδιαφέρον επικεντρώνεται στην ασφαλή αποθήκευση δεδομένων και στην ασφαλή δρομολόγηση. Η ασφαλής αποθήκευση επιτυγχάνεται με τη χρήση παραδοσιακών και νέων πρωτοκόλλων και αλγορίθμων κρυπτογραφίας (ψηφιακές υπογραφές, multi-key encryption, firewalls) με σκοπό να χτισθεί εμπιστοσύνη μεταξύ των κόμβων και των κοινόχρηστων αντικειμένων. Η ασφαλή δρομολόγηση επιτυγχάνεται με τεχνικές ελέγχου αυθεντικότητας και ακεραιότητας, την ασφαλή αντιστοίχηση ID, κτλ.

Το χαρακτηριστικό της ανωνυμίας επιτρέπει στους χρήστες να χρησιμοποιούν το peer-to-peer σύστημα διατηρώντας όμως την ανωνυμία τους, αποφεύγοντας έτσι τυχόν νομικούς περιορισμούς. Σύμφωνα με τον Diegledine, η ανωνυμία αναφέρεται στο συγγραφέα (ή εκδότη), στην ταυτότητα του κόμβου και του αντικειμένου και στις λεπτομέρειες της ερώτησης [54].

Για την επίτευξη της ανωνυμίας χρησιμοποιούνται τεχνικές όπως multicasting, cover paths, ανώνυμες συνδέσεις κτλ.

Ο έλεγχος πρόσβασης, η πιστοποίηση, αλλά και η διαχείριση ταυτοτήτων είναι θέματα για τα οποία δεν έχει δοθεί ιδιαίτερη σημασία. Αφού το περιβάλλον είναι κατανεμημένο, είναι δυνατό οι ίδιες φυσικές οντότητες να εμφανίζονται με διαφορετικές ταυτότητες. Τελικά, ο έλεγχος πρόσβασης και η πιστοποίηση προκύπτει από την κατανεμημένη δομή όπου η ευθύνη και ο έλεγχος περνά στους κόμβους.

6.2 Υπολογιστικό νέφος -CLOUD COMPUTING

6.2.1 Τεχνολογία του Cloud

Πριν από λίγα χρόνια, οι άνθρωποι μετέφεραν τα έγγραφά τους με σκληρούς δίσκους. Στη συνέχεια, πιο πρόσφατα, πολλοί άνθρωποι χρησιμοποιούσαν usb sticks. Μια νέα γενιά τεχνολογίας άλλαξε τον κόσμο των υπολογιστών και της πληροφορικής. Η αποθήκευση δεδομένων βασισμένη στο

διαδίκτυο και οι αντίστοιχες υπηρεσίες – επίσης γνωστές σαν cloud computing – είναι ταχέως αναδυόμενες και έχουν στόχο να συμπληρώσουν το παραδοσιακό μοντέλο του εκτελούμενου λογισμικού και των αποθηκευμένων δεδομένων στους σταθμούς εργασίας και τους εξυπηρετητές. Με απλά λόγια, το cloud computing αναφέρεται στην ικανότητα των χρηστών να έχουν πρόσβαση και να διαχειρίζονται εφαρμογές και πληροφορίες που είναι αποθηκευμένες εκτός του προσωπικού υπολογιστή ή κάποιας άλλης ψηφιακής συσκευής του χρήστη, αλλά σε απομακρυσμένους διακομιστές, χρησιμοποιώντας πλατφόρμες βασισμένες στο διαδίκτυο.

Το cloud computing αποτελεί μια νέα τεχνολογία η οποία διευκολύνει την αποθήκευση, επεξεργασία και χρήση δεδομένων σε απομακρυσμένους υπολογιστές που είναι προσβάσιμοι μέσω του διαδικτύου. Πρόκειται αναμφίβολα για έναν από τους ταχύτερα αναπτυσσόμενους κλάδους της παγκόσμιας αγοράς τεχνολογίας, ο οποίος προσφέρει δια μέσω των κέντρων δεδομένων (data servers), οικονομίες κλίμακας, φθηνότερη υπολογιστική ισχύ και ευκολότερη πρόσβαση στα δεδομένα και στις εφαρμογές.

Ένας άλλος παράγοντας που συνέβαλλε στην ανάπτυξη της νέας τεχνολογίας του υπολογιστικού νέφους είναι η εξάπλωση σε αριθμό και σε είδος των ψηφιακών συσκευών. Πλέον, ένα σπίτι διαθέτει περισσότερους του ενός desktop υπολογιστές και συγχρόνως, η αυξανόμενη φορητότητα (laptops, netbooks) και η εμφάνιση μικρότερων συσκευών (tablets, smartphones) δημιούργησε την ανάγκη για υπηρεσίες οι οποίες μπορούν να χρησιμοποιηθούν διασταυρωτικά και συνδετικά, επιτρέποντας στο χρήστη να ελέγχει τα email του, να μεταφορτώνει, να ακούει, να βλέπει βίντεο κτλ, οπουδήποτε και αν βρίσκεται.

Το cloud computing αλλάζει τον τρόπο με τον οποίο γίνεται η διαχείριση πληροφοριών, ιδίως όταν η επεξεργασία αφορά προσωπικά δεδομένα όπου και προκαλείται ανησυχία. Οι τελικοί χρήστες μπορούν να έχουν πρόσβαση σε υπηρεσίες cloud χωρίς την ανάγκη για οποιαδήποτε εξειδικευμένη γνώση της συγκεκριμένης τεχνολογίας. Αυτό είναι ένα βασικό χαρακτηριστικό του cloud computing, το οποίο εγείρει θέματα σχετικά με την ασφάλεια, την εμπιστοσύνη και τους μηχανισμούς της ιδιωτικότητας.

6.2.2 Ζητήματα Ασφάλειας και Εμπιστευτικότητας

Η ιδιωτικότητα, όπως έχει αναλυθεί, αναφέρεται στο δικαίωμα της αυτοδιάθεσης, το δικαίωμα δηλαδή των ατόμων να «γνωρίζουν τι είναι γνωστά για αυτούς», να γνωρίζουν πού αποθηκεύονται οι πληροφορίες σχετικά με αυτούς, να ελέγχουν τον τρόπο με τον οποίο οι πληροφορίες αυτές κοινοποιούνται καθώς και στην πρόληψη κατάχρησης. Με άλλα λόγια,

αναφέρεται σε κάτι περισσότερο από την εμπιστευτικότητα των πληροφοριών. Η προστασία των προσωπικών στοιχείων (ή η προστασία δεδομένων) απορρέει από το δικαίωμα της ιδιωτικής ζωής μέσω του συσχετιζόμενου δικαιώματος της αυτοδιάθεσης. Κάθε άτομο έχει το δικαίωμα να ελέγχει τα δικά του δεδομένων, είτε πρόκειται για ιδιωτικά, δημόσια ή επαγγελματικά.

Χωρίς τη γνώση της φυσικής τοποθεσίας του διακομιστή ή του τρόπου ρύθμισης της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, οι τελικοί χρήστες χρησιμοποιούν τις υπηρεσίες cloud, χωρίς οποιαδήποτε πληροφορία σχετικά με τις διαδικασίες που πραγματοποιούνται. Τα δεδομένα στο cloud είναι πιο εύκολο να διαχειριστούν, αλλά εξίσου εύκολο είναι να χαθεί ο έλεγχός τους. Για παράδειγμα, η αποθήκευση προσωπικών δεδομένων σε ένα διακομιστή κάπου στον κυβερνοχώρο θα μπορούσε να αποτελέσει σημαντική απειλή για την ιδιωτική ζωή. Το cloud computing εγείρει μια σειρά από ερωτήσεις σχετικά με την ιδιωτικότητα καθώς και θέματα ασφάλειας. Ενδεικτικά, κάποιες από τις ανησυχίες των χρηστών είναι οι εξής : μπορεί άραγε κάποιος να εμπιστευτεί έναν πάροχο cloud ή οι cloud διακομιστές είναι αξιόπιστοι ή τι θα συμβεί αν τα δεδομένα χαθούν ή τι συμβαίνει αναφορικά με την ιδιωτικότητα και τέλος η μεταφορά σε άλλο cloud είναι δύσκολη;

Τα θέματα ιδιωτικότητας αποκτούν όλο και μεγαλύτερη σημασία στον ηλεκτρονικό κόσμο. Είναι γενικά αποδεκτό ότι λαμβάνεται δεόντως υπόψη το θέμα της ιδιωτικότητας ώστε να προαχθεί η εμπιστοσύνη των χρηστών. Ωστόσο, η ασφάλεια, η διαχείριση και ο έλεγχος των προσωπικών δεδομένων στο cloud αποτελεί μια τεράστια πρόκληση για όλους τους ενδιαφερόμενους, συμπεριλαμβανομένων των νομικών και εμπορικών παραμέτρων.

6.2.3 Προκλήσεις για την προστασία της ιδιωτικής ζωής στο cloud computing

Οι χρήστες δημιουργούν μια συνεχώς αυξανόμενη ποσότητα των δεδομένων προσωπικού χαρακτήρα. Αυτή η αύξηση της ποσότητας των δεδομένων προσωπικού χαρακτήρα αυξάνει τη ζήτηση για τις υπηρεσίες cloud, ιδιαίτερα αν το cloud computing προσφέρει υποσχέσεις για μείωσης του κόστους για τους πελάτες και την εμφάνιση νέων επιχειρηματικών μοντέλων για τους παρόχους. Μεταξύ των κύριων προκλήσεων της ιδιωτικότητας για το cloud computing είναι:

α. Η πολυπλοκότητα της αξιολόγησης του κινδύνου σε ένα περιβάλλον cloud.
β. Η εμφάνιση νέων επιχειρηματικών μοντέλων και οι επιπτώσεις τους για την προστασία της ιδιωτικότητας των χρηστών.
γ. Η επίτευξη συμμόρφωσης προς τους κανονισμούς.

6.2.4 Η πολυπλοκότητα της αξιολόγησης του κινδύνου

Η πολυπλοκότητα των υπηρεσιών cloud εισάγει μια σειρά από άγνωστες παραμέτρους. Οι πάροχοι υπηρεσιών και οι καταναλωτές είναι επιφυλακτικοί, αντίστοιχα, σχετικά με την παροχή εγγυήσεων για υπηρεσίες που πληρούν τους κανονισμούς και την υιοθέτηση των υπηρεσιών. Με τους παρόχους υπηρεσιών να προωθούν έναν απλό τρόπο για τη διακίνηση προσωπικών δεδομένων, ανεξάρτητα από εθνικά σύνορα, προκύπτει μια πραγματική πρόκληση όσον αφορά τον έλεγχο της επεξεργασίας των δεδομένων του κύκλου ζωής και τη νομική τους συμμόρφωσή.

Σε μια υπηρεσία cloud, υπάρχουν πολλά ζητήματα που πρέπει να αντιμετωπιστούν προκειμένου να προσδιοριστούν οι κίνδυνοι για την ιδιωτικότητα και την ασφάλεια:

- Ποιοι είναι οι φορείς που εμπλέκονται στη λειτουργία;
- Ποιοι είναι οι ρόλοι και οι ευθύνες τους;
- Πού αποθηκεύονται τα δεδομένα;
- Πώς αναπαράγονται τα δεδομένα;
- Ποιες είναι οι σχετικές νομικές διατάξεις για την επεξεργασία δεδομένων;
- Πώς ο φορέας παροχής υπηρεσιών θα παρέχει το αναμενόμενο επίπεδο της ασφάλειας και της ιδιωτικότητας;

Για την αντιμετώπιση αυτών των ζητημάτων, το ψήφισμα της Μαδρίτης (Madrid Resolution, 2009) αναφέρει ότι κάθε υπεύθυνος πρέπει να έχει διάφανη πολιτική έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Οι ενδιαφερόμενοι πρέπει να καθορίσουν απαιτήσεις για το cloud computing οι οποίες θα πληρούν το αναμενόμενο επίπεδο της ασφάλειας και της ιδιωτικής ζωής. Στην Ευρώπη, ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών (European Network and Information Security Agency, ENISA) παρέχει συστάσεις για την κατανόησης της μετατόπισης της ισορροπίας μεταξύ της ευθύνης και της λογοδοσίας για τις βασικές λειτουργίες, όπως η διακυβέρνηση και ο έλεγχος των δεδομένων και τις λειτουργίες και τη συμμόρφωση με τους νόμους και τους κανονισμούς.

ΚΕΦΑΛΑΙΟ 7
ΥΠΗΡΕΣΙΕΣ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (Social Networking)

7.1 Ορισμός

Τα μέσα κοινωνικής δικτύωσης (social media) και τα κοινωνικά δίκτυα (ή ψηφιακά κοινωνικά δίκτυα (social networks) κατακτούν με εκπληκτικά αυξανόμενους ρυθμούς όλο και περισσότερους χρήστες [55].

Οι δυνατότητες των μέσων κοινωνικής δικτύωσης είναι πολλές καθώς πρόκειται για την πιο σύγχρονη αντίληψη και εξέλιξη στο χώρο του διαδικτύου που επιτρέπει, υποστηρίζει και στηρίζεται στην ενεργό συμμετοχή και την αλληλεπίδραση μεταξύ των χρηστών.

Οι όροι social media και social networks χρησιμοποιούνται ευρύτατα αλλά συχνά ταυτίζονται παρόλη τη σημαντική διαφοροποίησή τους. Σύμφωνα με τη Wikipedia, ο όρος social media αναφέρεται στα μέσα που χρησιμοποιούνται για την κοινωνική αλληλεπίδραση παρέχοντας υψηλή προσβασιμότητα και τεχνικές δυνατότητες. Τα μέσα κοινωνικής δικτύωσης αξιοποιούν τεχνολογίες που βασίζονται στο διαδίκτυο (web-based) με στόχο την επικοινωνία και την ενεργοποίηση του κοινωνικού διαλόγου. Οι Kaplan & Haenlein (2010) στο άρθρο τους «Users of the world, unite! The challenges and opportunities of Social Media», ορίζουν τα μέσα κοινωνικής δικτύωσης σαν ένα σύνολο από διαδικτυακές εφαρμογές που βασίζονται στα ιδεολογικά και τεχνολογικά θεμέλια του διαδικτύου δεύτερης γενιάς Web 2.0 και επιτρέπουν τη δημιουργία και ανταλλαγή περιεχομένου. Τα social media είναι δηλαδή απόρροια της δεύτερης γενιάς του διαδικτύου, στην οποία ο κάθε χρήστης έχει τη δυνατότητα όχι μόνο να δημοσιεύει το περιεχόμενο που επιθυμεί άμεσα, αλλά και να αλληλεπιδρά με άλλους χρήστες, μιλώντας και συμμετέχοντας [56].

Τα social media, κατά τον Evans (2008), αποτελούν τον εκδημοκρατισμό της πληροφορίας, αφού μέσα από την χρήση τους οι άνθρωποι γίνονται εκδότες ενός περιεχομένου και δεν παραμένουν απλοί αναγνώστες, ενώ παράλληλα αποτελούν ένα πολύπλευρο μέσω επικοινωνίας μεταξύ των χρηστών. Επιπλέον, τα μέσα κοινωνικής δικτύωσης παρέχουν κοινωνική και συναισθηματική υποστήριξη και αποτελούν πηγές πληροφόρησης για τους χρήστες [57].

Τα μέσα κοινωνικής δικτύωσης είναι μια αντανάκλαση των συνομιλιών που συμβαίνουν κάθε μέρα, είτε σε ένα σουπερ μάρκετ, είτε σε μια παιδική χαρά, είτε σε ένα κέντρο διασκέδασης με την διαφορά ότι επιτρέπουν σε αυτές τις συνομιλίες να είναι προσβάσιμες σε ένα ευρύτερο ακροατήριο μέσω του ψηφιακού «μεγαφώνου» [58].

7.2 Τα βασικά χαρακτηριστικά των Μέσων Κοινωνικής Δικτύωσης

Τα μέσα κοινωνικής δικτύωσης κατά τον Mayfield(2008) παρουσιάζουν κάποια βασικά χαρακτηριστικά [59]:

- ***Συμμετοχή (Participation):*** τα μέσα κοινωνικής δικτύωσης ενθαρρύνουν τη συνεισφορά και τα σχόλια από τους ενδιαφερόμενους. Η συμμετοχή των χρηστών θολώνει τα όρια μεταξύ των μέσων ενημέρωσης και του κοινού.
- ***Διαφάνεια (Openness)*** : οι περισσότερες υπηρεσίες των social media είναι ανοιχτές σε ανατροφοδότηση και συμμετοχή, ενώ σπάνια υπάρχουν εμπόδια στην πρόσβαση και στη χρήση του περιεχομένου.
- ***Συνομιλία (Conversation):*** σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης που αφορούν μόνο τη μετάδοση (broadcasting) ενός περιεχομένου σε ένα ακροατήριο, τα social media αποτελούν μια συνομιλία διπλής κατεύθυνσης.
- ***Κοινότητα (Community):*** τα social media επιτρέπουν την εύκολη και άμεση δημιουργία κοινοτήτων που μοιράζονται κοινά ενδιαφέροντα, όπως την αγάπη τους για τη φωτογραφία ή μια τηλεοπτική εκπομπή.
- ***Συνεκτικότητα (Connectedness)*** **:** Τα περισσότερα είδη των μέσων κοινωνικής δικτύωσης αναπτύσσουν τη συνεκτικότητά τους κάνοντας χρήση συνδέσεων με άλλες ιστοσελίδες , πόρους και ανθρώπους.

7.3 Κατηγοριοποιήσεις των Μέσων Κοινωνικής Δικτύωσης

Καθώς η χρήση των μέσων κοινωνικής δικτύωσης εξαπλώνεται, πολλοί ερευνητές προσπάθησαν να τα κατηγοριοποιήσουν χρησιμοποιώντας διαφορετικές βάσεις. Οι Kaplan & Heinlein (2010) βασίστηκαν στο συνδυασμό

δύο κύριων στοιχείων των social media, της κοινωνικής διεργασίας και της θεωρίας των μέσων μαζικής ενημέρωσης, οι Boyd & Ellison [60] στην αλληλεπίδραση και την κοινωνικοποίηση που προσφέρει κάθε μέσο και ο Owyang (2009) στις δυνατότητες του κάθε μέσου.

Οι Kaplan & Heinlein (2010) διακρίνουν 6 βασικές κατηγορίες:

1. ***Συνεργατικά έργα (Collaborative projects)***

   Σε αυτή τη κατηγορία εντάσσονται οι ιστοσελίδες στις οποίες οι τελικοί χρήστες συνεργατικά μπορούν να επεξεργαστούν ή και να προσθέσουν περιεχόμενο προς ένα συγκεκριμένο θέμα ή στόχο. Η θεμελιώδης ιδέα στην οποία βασίζεται η ύπαρξη των συνεργατικών έργων είναι ουσιαστικά η ισχύς εν τη ενώσει. Η κοινή προσπάθεια πολλών παραγόντων οδηγεί σε ένα καλύτερο αποτέλεσμα από ότι κάποιος παράγοντας θα μπορούσε να επιτύχει μεμονωμένα. Τα συνεργατικά έργα διαφοροποιούνται μεταξύ τους και περιλαμβάνουν τα wikis και το social bookmarking.

   Τα Wikis είναι ιστοσελίδες που επιτρέπουν στους χρήστες να προσθέσουν, να αφαιρέσουν ή να επεξεργαστούν ένα περιεχόμενο κειμένου. Η online εγκυκλοπαίδεια Wikipedia αποτελεί ίσως το πλέον αντιπροσωπευτικό παράδειγμα της κατηγορίας των wikis.

   Μέσω του social bookmarking δίνεται η δυνατότητα σχολιασμού, διαμοιρασμού, συλλογής, κατάταξης και επισήμανσης ιστοσελίδων (Links) που ενδιαφέρουν τους χρήστες. Χαρακτηριστικό παράδειγμα αποτελεί η σελίδα Reddit η οποία δίνει τη δυνατότητα στους χρήστες να τοποθετήσουν κάποιο ενδιαφέρον άρθρο στους σελιδοδείκτες τους (bookmarks) κάνοντάς το έτσι δημοφιλέστερο και κατά κάποιο τρόπο παροτρύνοντας και άλλους να το διαβάσουν. Ένα σημαντικό γνώρισμα των συστημάτων κοινωνικής σελιδοσήμανσης αποτελεί ο όρος tagging. Το tagging επιτρέπει στους χρήστες να οργανώσουν τους σελιδοδείκτες τους με ευέλικτο τρόπο και να αναπτύξουν κοινά λεξιλόγια.

2. ***Ιστολόγια (Blogs)***

   Τα ιστολόγια είναι διαδικτυακοί τόποι οι οποίοι ενημερώνονται συχνά από καταχωρήσεις κειμένου, όπως απόψεις, πληροφορίες, προσωπικές καταχωρήσεις ημερολογίου κτλ. Τα ιστολόγια διαχειρίζονται συνήθως

από ένα άτομο αλλά παρέχουν τη δυνατότητα αλληλεπίδρασης με άλλους με την προσθήκη παρατηρήσεων [56].

Τα πλέον δημοφιλή blogs σήμερα είναι το Blogger και το Twitter.

3. ***Κοινότητες περιεχομένου (Content communities)***

Ο κύριος στόχος των κοινοτήτων αυτών είναι η δημιουργία και η ανταλλαγή περιεχομένου όπως αρχεία ήχου εικόνας και βίντεο, ενώ παράλληλα δίνεται η δυνατότητα στους χρήστες να τα σχολιάσουν. Στις κοινότητες περιεχομένου οι χρήστες δεν είναι υποχρεωτικό να δημιουργήσουν κάποιο προφίλ [56].

Τα πιο αντιπροσωπευτικά παραδείγματα αυτής της κατηγορίας αποτελούν το YouTube που επιτρέπει το διαμοιρασμό βίντεο καθώς και το Instagram το οποίο αφορά φωτογραφίες.

Η αρνητική πλευρά της υπόθεσης είναι ότι σε αυτές τις σελίδες συχνά δημοσιεύονται παράνομα περιεχόμενα τα οποία έχουν προστασία πνευματικών δικαιωμάτων [56].

4. ***Ιστοσελίδες Κοινωνικής Δικτύωσης (social networking sites)***

Αποτελούν εικονικές κοινότητες [61] όπου μέσα σε αυτές ο χρήστης έχει την δυνατότητα να αλληλεπιδρά με φίλους ή να συμμετέχει σε ομάδες κοινών ενδιαφερόντων, δημιουργώντας αρχικά ένα προφίλ με προσωπικές πληροφορίες. Τα πιο δημοφιλή κοινωνικά δίκτυα είναι το Facebook και το My space. Τα δίκτυα αυτά αποτελούν την πιο διαδεδομένη μορφή των social media και ιστορικά προϋπήρχαν των υπολοίπων μορφών μέσων κοινωνικής δικτύωσης. Οι σελίδες Classmates.Com και SixDegrees.com αποτελούν τις πρώτες επίσημες ιστοσελίδες κοινωνικής δικτύωσης, οι οποίες εμφανίστηκαν το 1995 και το 1997 αντίστοιχα [62].

5. ***Εικονικοί κόσμοι (virtual words)***

Οι εικονικοί κόσμοι είναι πλατφόρμες που αναπαράγουν ένα τρισδιάστατο περιβάλλον στο οποίο οι χρήστες μπορούν να εμφανιστούν υπό μορφή εξατομικευμένων ειδώλων και να αλληλεπιδρούν ο ένας με τον άλλον, όπως θα έκαναν και στην πραγματική ζωή. Αποτελούν το απόλυτο μανιφέστο των social media αφού παρέχουν το υψηλότερο επίπεδο κοινωνικής παρουσίας μέσα από εξαιρετικά εξελιγμένες τεχνολογικές δυνατότητες [56].

Οι εφαρμογές αυτές διακρίνονται σε δυο μεγάλες κατηγορίες. Στα παιχνίδια εικονικής πραγματικότητας (virtual games world) όπως το World of War Craft και στους εικονικούς κοινωνικούς κόσμους όπως το Second Life. Ειδικά η τελευταία κατηγορία είναι αρκετά σημαντική αφού οι συμπεριφορές και οι ενέργειες των χρηστών καθρεπτίζουν την ύπαρξή τους στην πραγματική τους ζωή.

Μια πιο συνοπτική κατηγοριοποίηση των μέσων κοινωνικής δικτύωσης είναι η κατηγοριοποίηση κατά Zhang [55]:

- Ιστολόγια (blogging).
- Κοινωνικά δίκτυα (social networking).
- Κοινωνική σελιδοσήμανση (social bookmarking)
- Συνεργατική συγγραφή (collaborative authoring)
- Διαμοιρασμός πολυμέσων (multimedia sharing)
- Διαδικτυακές τηλεδιασκέψεις (web conferencing)

Από την ανασκόπηση της διεθνούς βιβλιογραφίας προέκυψε πως πολύ συχνά, οι όροι social media και social network συγχέονται.

Σύμφωνα με τον Stelzner [63] τα μέσα κοινωνικής δικτύωσης αποτελούν εργαλεία για ανταλλαγή πληροφοριών και συζήτηση. Από την άλλη ο όρος κοινωνική δικτύωση αναφέρεται στη δημιουργία μιας διαδικτυακής κοινότητας, η οποία συγκροτείται από ανθρώπους με κοινά ενδιαφέροντα, φίλους συνεργάτες κτλ. Ένα κοινωνικό δίκτυο είναι μία κοινωνική δομή αποτελούμενη από κόμβους (συνήθως άτομα ή επιχειρήσεις) οι οποίοι συνδέονται μεταξύ τους με έναν ή περισσότερους τύπους αλληλεξάρτησης, όπως αξίες, οράματα, ιδέες, οικονομικές συναλλαγές, φιλία, συγγένεια, αντιπάθεια, συγκρούσεις, σεξουαλικές επαφές, κλπ.

Οι κύριοι τύποι κοινωνικών υπηρεσιών δικτύωσης είναι εκείνοι που περιέχουν τα εξής χαρακτηριστικά: υποδιαίρεση των χρηστών σε κατηγορίες (αναλόγως με το σχολείο φοίτησης, το χώρο εργασίας κλπ), τρόπους σύνδεσης με φίλους (συνήθως με δημιουργία προσωπικών profile) και ένα έμπιστο σύστημα εύρεσης φίλων. Τα δημοφιλέστερα κοινωνικά δίκτυα συνδυάζουν τα παραπάνω χαρακτηριστικά , με κύριο το Facebook και το Twitter χρησιμοποιούμενα ευρέως παγκοσμίως , το MySpace, και το LinkedIn που χρησιμοποιούνται στη Βόρεια Αμερική, το Nexopia στον Καναδά, τα Bebo, dol2day, Tagged, XING, και Skyrock σε χώρες της Ευρώπης, το Orkut και το Hi5 χρησιμοποιούνται στη Νότια και Κεντρική Αμερική και τέλος τα Friendster,

Multiply, Orkut, Xiaonei και Cyworld στην Ασία και τα νησιά του Ειρηνικού Ωκεανού [64].

Οι Walker, MacBride και Vachon (1977) όρισαν ως κοινωνικό δίκτυο το άθροισμα των προσωπικών επαφών μέσω των οποίων το άτομο διατηρεί την κοινωνική του ταυτότητα, λαμβάνει συναισθηματική υποστήριξη, υλική ενίσχυση και συμμετοχή στις υπηρεσίες, έχει πρόσβαση στις πληροφορίες και δημιουργεί νέες κοινωνικές επαφές.

Σύμφωνα με τον Αριστοτέλη, ο άνθρωπος είναι από τη φύση του κοινωνικό ον. Η αίσθησή του να ανήκει σε μια κοινότητα ήταν πάντα το ζητούμενο. Η έμφυτη αυτή τάση του για επικοινωνία και η ανάγκη του για αλληλεπίδραση με τους ομοίους του, βρήκε διέξοδο μέσα από την κοινωνική δικτύωση. Σύμφωνα με τους Gunawardena, Hermans και Sanchez (2009), ως κοινωνική δικτύωση ορίζεται η πρακτική της επέκτασης της γνώσης μέσα από τη δημιουργία συνδέσεων με άτομα με παρόμοια ενδιαφέροντα.

Σύμφωνα με άρθρο στο Social Networks του Mitchell [65], ο Barnes ήταν ο πρώτος που εισήγαγε την έννοια των κοινωνικών δικτύων το 1954 τονίζοντας πως το κοινωνικό δίκτυο αποτελεί μια κοινωνική δομή που περιλαμβάνει μεμονωμένους ανθρώπους αλλά και ομάδες, τους οποίους συνδέουν κοινές δραστηριότητες, ιδέες, φιλίες και σχέσεις.

Οι Walker, MacBride και Vachon (1977) όρισαν ως κοινωνικό δίκτυο το άθροισμα των προσωπικών επαφών μέσω των οποίων το άτομο διατηρεί την κοινωνική του ταυτότητα, λαμβάνει συναισθηματική υποστήριξη, υλική ενίσχυση και συμμετοχή στις υπηρεσίες, έχει πρόσβαση στις πληροφορίες και δημιουργεί νέες κοινωνικές επαφές.

7.4 Θέματα Ασφάλειας στα Κοινωνικά Δίκτυα

7.4.1 Ιδιωτικότητα και Ασφάλεια Προσωπικών Δεδομένων

Ωστόσο, οι χρήστες των μέσων κοινωνικής δικτύωσης και των κοινωνικών δικτύων εν γένει, θα πρέπει να έχουν κατά νου όλους τους κινδύνους που καραδοκούν ενώ θυσιάζουν στοιχεία και πληροφορίες της προσωπικής τους ζωής με στόχο περισσότερες υπηρεσίες και καλύτερη διαδικτυακή δραστηριότητα. Και αυτό διότι, υπάρχουν παραδείγματα όπου τα δεδομένα είναι ευαίσθητα και ο ανοιχτός χαρακτήρας τους σίγουρα δεν ευνοεί

την ιδιωτική ζωή και την προστασία της. Τα προβλήματα που ενδέχεται να προκύψουν στις ιστοσελίδες κοινωνικής δικτύωσης δε διαφέρουν ως προς τη φύση ή τη μορφή από τα προβλήματα που μπορεί να προκύψουν από τη γενικότερη χρήση του διαδικτύου, διαφοροποιούνται όμως ως προς την ένταση και το μέγεθος των συνεπειών τους. Τέτοια προβλήματα σχετίζονται με καταδίωξη (stalking), κλοπή ταυτότητας και σεξουαλική παρενόχληση, όπως επίσης και με την ηθική, αναφορικά με την αποθήκευση, διαχείριση και δημοσίευση προσωπικών δεδομένων. Επίσης, θέματα ασφαλείας προκύπτουν όταν ένας hacker αποσπά μη εξουσιοδοτημένη πρόσβαση στην προστατευμένη κωδικοποίηση ή σε κείμενο μιας ιστοσελίδας.

Παρόλα αυτά, τα θέματα ιδιωτικότητας προσωπικών δεδομένων δεν έχουν να κάνουν απαραίτητα με παραβιάσεις ασφαλείας στα κοινωνικά δίκτυα. Ενδεχόμενη απειλή των δεδομένων ενός χρήστη εξαρτάται από το πόσο ο χρήστης ασχολείται με τα κοινωνικά δίκτυα καθώς επίσης και με την ποσότητα των πληροφοριών που προτίθεται να μοιραστεί και να δημοσιεύσει. Ένας χρήστης με περισσότερη online δραστηριότητα είναι πιο πιθανόν να υποστεί παραβίαση των προσωπικών του δεδομένων σε σχέση με κάποιον άλλον χρήστη ο οποίος αρκείται σε φειδωλή χρήση των κοινωνικών δικτύων.

Η σχέση μεταξύ της ιδιωτικότητας και του κοινωνικού δικτύου ενός ατόμου είναι πολυπρόσωπη. Σε συγκεκριμένες περιπτώσεις ο χρήστης επιλέγει να παρέχει προσωπικές πληροφορίες μόνο σε ένα μικρό κύκλο κοντινών φίλων και όχι σε ξένους. Σε άλλες περιπτώσεις, ο χρήστης επιθυμεί να τις αποκαλύψει σε ξένους αλλά όχι σε αυτούς που τον γνωρίζουν καλά.

Τα κοινωνικά δίκτυα εκτός διαδικτύου αποτελούνται από δεσμούς που μπορούν να κατηγοριοποιηθούν ως δυνατοί ή ασθενείς αλλά στην πραγματικότητα είναι πολύ διαφορετικοί σε όρους του πόσο κοντινή και τίμια αξιολογεί κάποιος μια σχέση. Τα κοινωνικά δίκτυα εντός διαδικτύου από την άλλη, συχνά μειώνουν αυτές τις περίπλοκες συνδέσεις σε απλές δυαδικές σχέσεις: «φίλος ή μη φίλος» [66]. Δεν υπάρχει κανένας τρόπος να αποφασίσεις τη μετρική που χρησιμοποιήθηκε ή το ρόλο και το βάρος μιας σχέσης. Ενώ μερικοί άνθρωποι επιθυμούν να αναφέρουν οποιονδήποτε ως φίλο και άλλοι προσκολλούνται σε έναν ασαφή προσδιορισμό, οι περισσότεροι τείνουν να θεωρούν ως φίλο οποιονδήποτε γνωρίζουν και απλά δεν αντιπαθούν. Αυτό συχνά σημαίνει ότι κάποιοι θεωρούνται ως φίλοι παρ' όλο που ο χρήστης δεν τους γνωρίζει ή εμπιστεύεται απόλυτα.

Επίσης, ενώ ο αριθμός των δυνατών δεσμών που κάποιος μπορεί να διατηρεί σε έναν ιστότοπο κοινωνικού δικτύου μπορεί να μην αυξάνεται σημαντικά μέσω τεχνολογίας κοινωνικών δικτύων, οι Donath και Boyd

σημειώνουν ότι «ο αριθμός των ασθενών δεσμών που κάποιος μπορεί να σχηματίσει και να διατηρήσει δύναται να αυξηθεί ουσιαστικά, επειδή το είδος της επικοινωνίας που μπορεί να γίνει πιο εύκολα και φθηνά με τη νέα τεχνολογία ταιριάζει πολύ καλά στους δεσμούς αυτούς [67].

Πρακτικά, το παραπάνω γεγονός συνιστά ότι τα κοινωνικά δίκτυα εντός διαδικτύου είναι περισσότερο αχανή και έχουν περισσότερους ασθενείς δεσμούς, κατά μέσο όρο, από τα κοινωνικά δίκτυα εκτός διαδικτύου. Με άλλα λόγια, οι χρήστες μπορούν να κατηγοριοποιηθούν ως φίλοι φίλων ενός χρήστη και να αποκτήσουν πρόσβαση στις προσωπικές πληροφορίες του, ενώ την ίδια στιγμή το όριο για να αξιολογηθεί κάποιος ως φίλος στο δίκτυο κάποιου είναι πολύ χαμηλό. Κάτι τέτοιο όμως μπορεί να κάνει ένα κοινωνικό δίκτυο μια φανταστική κοινότητα. Και όμως, η εμπιστοσύνη μέσα στα κοινωνικά δίκτυα του διαδικτύου απονέμεται διαφορετικά και έχει διαφορετικό νόημα από τα αντίστοιχα δίκτυα εκτός διαδικτύου. Τα δίκτυα εντός διαδικτύου έχουν περισσότερα επίπεδα, λόγω του ότι η ίδια πληροφορία παρέχεται σε περισσότερους φίλους.

Και εδώ βρίσκεται ένα παράδοξο. Ενώ η ιδιωτικότητα μπορεί να θεωρηθεί αναγκαία και προϋπάρχουσα για την οικειότητα, η εμπιστοσύνη μπορεί να μειώνεται μέσα σε ένα κοινωνικό δίκτυο του διαδικτύου. Την ίδια στιγμή μια νέα μορφή οικειότητας γίνεται ευρέως γνωστή: το μοίρασμα προσωπικών πληροφοριών σε μεγάλο και πιθανώς άγνωστο αριθμό φίλων και αγνώστων μαζί.

Οι ιστοσελίδες κοινωνικής δικτύωσης ποικίλλουν σημαντικά στα επίπεδα προστασίας των δεδομένων που προσφέρονται ή απαιτούνται. Σε διάφορες ιστοσελίδες όπως το Facebook ενθαρρύνεται η χρήση πραγματικών προσωπικών πληροφοριών στο προφίλ του χρήστη. Αυτές οι πληροφορίες δύναται να περιλαμβάνουν ονόματα, διευθύνσεις, τηλέφωνα, γενέθλια, γενέτειρα πόλη, ενδιαφέροντα, αγαπημένη μουσική, κατάσταση σχέσης αλλά και σεξουαλικές προτιμήσεις. Η χρήση αληθινών ονομάτων μπορεί να είναι ανεκτή αλλά να φιλτράρεται σε ιστότοπους ραντεβού ή σχέσεων όπως το Friendster που δημιουργεί μια λεπτή ασπίδα μιας ανίσχυρης ψευδωνυμίας μεταξύ της δημόσιας ταυτότητας ενός ατόμου και της διαδικτυακής αναπαράστασής του, με το να αποκαλύπτει μόνο το όνομα και όχι το επώνυμο του συμμετέχοντα. Σε άλλες ιστοσελίδες όπως το match.com όπου κάποιος μπορεί να βρει το ταίρι του, ενθαρρύνεται η ανωνυμία. Αλλά ακόμα και σε αυτές τις περιπτώσεις η αναγνώριση καθίσταται εύκολη μέσω της αναγνώρισης του προσώπου τους από δημοσιευμένες φωτογραφίες.

7.4.2 Αποθήκευση Δεδομένων

Τα περισσότερα από τα κοινωνικά δίκτυα απαιτούν από τους χρήστες να συμφωνήσουν με την πολιτική χρήσης τους πριν χρησιμοποιήσουν τις υπηρεσίες τους, η οποία βέβαια εμπεριέχει ρήτρες που επιτρέπουν στους διαχειριστές των δικτύων να αποθηκεύουν τα δεδομένα των χρηστών ακόμα και να τα μοιράζονται με τρίτους.

Αναφορικά με τις πληροφορίες, αυτές είτε μοιράζονται από τους ίδιους τους χρήστες είτε προέρχονται από online παρακολούθηση.

Σύμφωνα με τους Gross και Acquisti [68], οι πληροφορίες αυτές αποκαλύπτονται από το χρήστη είτε εν γνώσει είτε εν αγνοία του. Η εν γνώσει πληροφορία περιλαμβάνει δεδομένα τα οποία αντλούνται από «liking» και «posting» ενώ η εν αγνοία πληροφορία περιλαμβάνει δεδομένα από cookies, το είδος της συσκευής αλλά και τη μηχανή αναζήτησης που χρησιμοποιήθηκε.

Το είδος της πληροφορίας που αποκαλύπτεται ή αποκρύπτεται, συχνά περιστρέφεται γύρω από χόμπυ και ενδιαφέροντα αλλά μπορεί να πάρει από εκεί και πέρα διάφορες κατευθύνσεις. Αυτές περιλαμβάνουν: ημι-δημόσιες πληροφορίες όπως τρέχοντα ή πρώην σχολεία και εργασίες, ιδιωτικές πληροφορίες όπως προτιμήσεις κατανάλωσης αλκοόλ και σεξουαλικός προσανατολισμός και εντελώς ανοιχτές καταχωρήσεις προσωπικών πληροφοριών.

Σημαντική παράμετρος αποτελεί το ποιος έχει πρόσβαση στις πληροφορίες αυτές εκτός από τον ίδιο το χρήστη. Τόσο το ίδιο το μέσο κοινωνικής δικτύωσης όσο και άλλα δίκτυα μπορούν να εισέλθουν στα προσωπικά δεδομένα των χρηστών.

7.4.3 Πιθανοί Κίνδυνοι

- ***Κλοπή Ταυτότητας***

  Εξαιτίας του μεγάλου όγκου προσωπικών πληροφοριών που συχνά επιδεικνύεται στις ιστοσελίδες κοινωνικής δικτύωσης, είναι δυνατό να γίνουν και περαιτέρω εκτιμήσεις για ένα χρήστη όπως ο αριθμός

κοινωνικής ασφάλισης που μπορεί μετά να χρησιμοποιηθεί για την επίτευξη κλοπής ταυτότητας.

- ***Ηλεκτρονική Παρενόχληση***

Με τον όρο «ηλεκτρονική παρενόχληση» ή «ηλεκτρονικός εκφοβισμός» (cyberbullying) περιγράφεται η επιθετική συμπεριφορά από πρόθεση με τη χρήση ηλεκτρονικών μέσων. Τέτοιου είδους περιστατικά μπορούν να εμφανιστούν με πολύ διαφορετικές μορφές. Η Μονάδα Εφηβικής Υγείας τις κωδικοποιεί συνοπτικά στις εξής:

- Αποστολή κειμένων, e-mail ή άμεσων μηνυμάτων με απειλητικό περιεχόμενο.
- Ανάρτηση εξευτελιστικών φωτογραφιών ή βίντεο σε ιστοσελίδες όπου και άλλα άτομα έχουν πρόσβαση.
- Διάδοση φημών στο περιβάλλον του θύματος με τη χρήση κινητού, ηλεκτρονικού ταχυδρομείου ή άλλων υπηρεσιών ηλεκτρονικής επικοινωνίας.
- Δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύουν μηνύματα μίσους.
- Χρήση των προσωπικών στοιχείων κάποιων ανθρώπων (κλοπή ταυτότητας) με απώτερο σκοπό να κατηγορηθούν τελικά ως υπεύθυνοι παραβατικών συμπεριφορών.

Πολλή κριτική έχει ασκηθεί στο Facebook λέγοντας ότι αποτελεί ένα πιθανό εργαλείο εκφοβισμού του διαδικτύου εξαιτίας της ευκολίας δημιουργίας ανώνυμων προφίλ και τη δημιουργία ομάδων που επιτρέπουν σε «bullies» να εντοπίζουν άτομα προς εκφοβισμό online. Στις 21 Αυγούστου του 2009, η Keeley Houghton, 18 χρονών από το Malvern Worcestershire, καταδικάστηκε σε 3 μήνες έγκληση σε αναμορφωτήριο αφότου βρέθηκε ένοχη για εκφοβισμό ενός συμμαθητή της στο Facebook, κάνοντάς την το πρώτο άτομο στη Μεγάλη Βρετανία που καταδικάζεται για εκφοβισμό σε ιστοσελίδα κοινωνικής δικτύωσης.

Επιπρόσθετα, έχει παρατηρηθεί η δυνατότητα παρακολούθησης και καταδίωξης χρηστών στις ιστοσελίδες κοινωνικής δικτύωσης, καθώς οι χρήστες επιτρέπουν στους άλλους χρήστες να γνωρίζουν την ακριβή τοποθεσία τους σε συγκεκριμένες ώρες.

- ***Προσηλυτισμός-Ρατσισμός-Εγκλήματα μίσους***

Το διαδίκτυο είναι και αυτό μια σύγχρονη μορφή κοινωνίας και μάλιστα μπορεί να θεωρηθεί ως ένας καθρέφτης της. Στον κόσμο του βρίσκουν έφορο έδαφος πληθώρα παραθρησκευτικών ομάδων, οι οποίες έντεχνα αποκρύπτουν το πραγματικό τους πρόσωπο και διαπιστωμένα προσπαθούν να προσηλυτίσουν άτομα, νεαρής κυρίως ηλικίας, μιλώντας για «θετική σκέψη», «αυτοΐαση», μεθόδους διαλογισμού κτλ. Παράλληλα, η διάδοση ρατσιστικής και ξενοφοβικής προπαγάνδας είτε από μεμονωμένα άτομα είτε μεθοδικά από διάφορες οργανώσεις, εμφανίζει αυξητικούς ρυθμούς. Το διαδικτυακό περιβάλλον δίνει την ευκαιρία σε φορείς τέτοιων αντιλήψεων, εκμεταλλευόμενοι την ανωνυμία που τους προσφέρει η χρήση ψευδωνύμου, να προσεγγίσουν άτομα και να προσπαθήσουν να τα χειραγωγήσουν με τις επικίνδυνες ιδέες τους. Χρησιμοποιούν διάφορους τρόπους συγκάλυψης ισχυριζόμενοι συνήθως πως παρέχουν πληροφορίες για την Ιστορία ή τη Θρησκεία, τις οποίες όμως ερμηνεύουν μέσα από τη δική τους, ξεχωριστή, οπτική ματιά. Με τον τρόπο αυτό προβάλλουν τα μηνύματά τους στο ευρύ κοινό, προσελκύουν νέους οπαδούς, συγκεντρώνουν πόρους και καλούν τους επισκέπτες τους σε «συστράτευση» και «ιερούς πολέμους» [69]. Πολλές φορές μάλιστα εμπλουτίζουν το περιεχόμενό τους με διαδικτυακά παιχνίδια, στα οποία ο χρήστης μπορεί να εξοντώσει μετανάστες ή άλλες θρησκευτικές και φυλετικές μειονότητες. Μέσα σε αυτό το πλαίσιο, το διαδικτυακό μίσος μπορεί να καλλιεργήσει εχθρικό κλίμα εναντίον συγκεκριμένων ομάδων, να πυροδοτήσει τη βία και τελικά να οδηγήσει σε πραγματικά εγκλήματα μίσους [70].

- ***Σεξουαλική Εκμετάλλευση***

I. <u>Εγκλήματα κατά της γενετήσιας αξιοπρέπειας</u>

Οι περισσότερες ιστοσελίδες κοινωνικής δικτύωσης είναι δεσμευμένες να διαβεβαιώσουν ότι η χρήση των υπηρεσιών τους είναι όσο το δυνατόν πιο ασφαλή. Παρόλα αυτά, λόγω της υψηλής περιεκτικότητας προσωπικών δεδομένων που εκτίθενται σε αυτές, καθώς επίσης και της δυνατότητας απόκρυψης της πραγματικής ταυτότητας των χρηστών, τέτοιου είδους ιστοσελίδες έχουν γίνει ολοένα και πιο δημοφιλείς για δράστες σεξουαλικών αδικημάτων. Το 2009 αποκαλύφθηκε ότι στο MySpace είχαν εκδιωχθεί 90.000 καταγεγραμμένοι δράστες σεξουαλικών αδικημάτων από τα προηγούμενα δύο χρόνια. Ωστόσο, έχει σημειωθεί ότι ο αριθμός των δραστών τέτοιων αδικημάτων έχει

αυξηθεί σημαντικά και έχει φτάσει στις μέρες μας σε εβδομαδιαία βάση. Οι βασικοί τρόποι με τους οποίους οι σεξουαλικοί δράστες χρησιμοποιούν το διαδίκτυο είναι [71]:

- Εμπόριο πορνογραφίας.
- Εντοπισμός θυμάτων με σκοπό τη σεξουαλική κακοποίηση.
- Συνομιλία με άλλους σεξουαλικούς δράστες.
- Αποπλάνηση μέσω σεξουαλικών συνομιλιών.

Τα χαρακτηριστικά του διαδικτύου που ευνοούν την ανάπτυξη του φαινομένου μπορούν να συνοψιστούν στα εξής:

- Η ευκολία δημιουργίας ψευδών προφίλ.
- Η ανωνυμία διευκολύνει τη χαλάρωση των κοινωνικών αναστολών και περιορισμών τόσο από την πλευρά του δράστη όσο και από την πλευρά του θύματος.
- Ο διασκεδαστικός χαρακτήρας του προωθεί μορφές συμπεριφοράς που στο πραγματικό περιβάλλον μπορεί να μην εκδηλώνονταν.
- Οι υπηρεσίες κοινωνικής δικτύωσης καθιστούν την επικοινωνία ανάμεσα στα θύματα και στους δράστες άμεση, εύκολη και γρήγορη.

II. Το φαινόμενο «Grooming»

Η ψηφιακή εποχή έχει επιφέρει τόσο βαθιές κοινωνικές αλλαγές, τέτοιες που πιθανόν μόνο η ανακάλυψη της φωτιάς είχε ως αποτέλεσμα [72]. Το διαδίκτυο αποτελεί μια ανεξάντλητη πηγή μάθησης, εκπαίδευσης και πληροφόρησης. Ωστόσο, η λαμπρότητα του διαδικτύου δύναται να επισκιαστεί από κρυμμένους κινδύνους απαιτώντας την προσεκτική χρήση του. Υπό αυτό το πρίσμα, το διαδίκτυο αποτελεί ένα ιδανικό περιβάλλον για τους σεξουαλικούς δράστες καθώς προσφέρει πληροφορίες που αφορούν τα υποψήφια θύματά τους.

Ακόμα, η ολοένα και αυξανόμενη χρήση των υπηρεσιών κοινωνικής δικτύωσης από τα παιδιά και τους εφήβους καθιστούν την επικοινωνία άμεση, εύκολη και γρήγορη τόσο για τα παιδιά και τους εφήβους όσο και για τους δράστες. Η ανωνυμία που προσφέρει το διαδίκτυο επιτρέπει τη δημιουργία ψευδών προφίλ από την πλευρά των δραστών και την «μεταμφίεση» τους σε παιδιά, προκειμένου να κερδίσουν την εμπιστοσύνη των θυμάτων και βαθμιαία να τα εισάγουν σε σεξουαλικές

διαδικτυακές συζητήσεις, να τα αποπλανήσουν και ίσως να τα καταστήσουν θύματα εμπορικής εκμετάλλευσης.

Υπάρχουν τέσσερις τρόποι με τους οποίους οι δράστες, με θύματα τα παιδιά, μπορούν να χρησιμοποιήσουν το διαδίκτυο. Αυτοί είναι: το εμπόριο παιδικής πορνογραφίας (σεξουαλική εκμετάλλευση), ο εντοπισμός των παιδιών με σκοπό τη σεξουαλική κακοποίηση, η συνομιλία με άλλους δράστες (παιδόφιλους), και η αποπλάνηση των ανηλίκων μέσω σεξουαλικών συνομιλιών (grooming). Οι παραβάτες διακινούν παιδική πορνογραφία, εντοπίζουν παιδιά και τα παρενοχλούν σεξουαλικά κάνοντάς τους ανάρμοστες προτάσεις, ενώ παρουσιάζονται στο διαδίκτυο σε ομάδες συζητήσεων (chat rooms) ως παιδιά και ως ενήλικες συγχρόνως.

Ο όρος «grooming» (ή cybergrooming) , σύμφωνα με το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου [73] περιγράφει τη συμπεριφορά εκείνη του διαδικτυακού χρήστη που σκοπό έχει να εμπνεύσει εμπιστοσύνη στο θύμα του, για να πραγματοποιήσει μαζί του μια συνάντηση. Αποτελεί ένα είδος ψυχολογικού και πνευματικού χειρισμού. Συνήθως εκτυλίσσεται σε δωμάτια συνομιλιών, υπηρεσίες ανταλλαγής μηνυμάτων ή υπηρεσίες κοινωνικής δικτύωσης χωρίς να αποκλείονται και άλλοι δίοδοι (π.χ. διαδικτυακοί τόποι ανεύρεσης εργασίας όπως παιδικό μόντελινγκ κλπ). Συχνά, τέτοιου είδους ιστόχωροι θεωρούνται από τα θύματα ασφαλείς τόποι συνομιλίας τόσο εξαιτίας της δημόσιας φύσης της συζήτησης όσο και της λανθασμένης εκτίμησης ότι διατηρείται η ανωνυμία τους. Οι Craven, Brown και Gilchrist, ορίζουν το φαινόμενο «grooming» ως μια διαδικασία προετοιμασίας του παιδιού από ένα σεξουαλικό δράστη, αλλά και του περιβάλλοντος του [74]. Οι στόχοι του σεξουαλικού δράστη είναι να πλησιάσει το παιδί και να κερδίσει τη συναίνεση και την εμπιστοσύνη του, έτσι ώστε να μην αποκαλυφθεί το κοινό «μυστικό» τους. Με αυτόν τον τρόπο οι σεξουαλικοί δράστες μπορούν να δικαιολογήσουν ή να αρνηθούν τις πράξεις τους όταν θα βρεθούν αντιμέτωποι με το νόμο. Η σεξουαλική κακοποίηση του θύματος, η σωματική βία ή η παιδική πορνεία και η κακοποίηση μέσω πορνογραφικού υλικού, μπορεί να είναι το αποτέλεσμα αυτής της συνάντησης κάτι που καθιστά το grooming ένα είδος ψυχολογικού χειρισμού που διεξάγεται μέσω του διαδικτύου, κινητών τηλεφώνων ή άλλων τεχνολογιών.

Ουσιαστικά, πρόκειται για μια σταδιακή διαδικασία αποκάλυψης πληροφοριών - οικοδόμησης σχέσης εμπιστοσύνης, ανάμεσα στο θύτη και το θύμα του, που συνήθως κρατάει αρκετό χρονικό διάστημα και

ποικίλει ανάλογα τον τύπο του χειρισμού και την ευπιστία του θύματος. Η καθαυτή σωματική επαφή δεν είναι οπωσδήποτε απαραίτητη σε αντίθεση με την πλειοψηφία των φαινομένων αποπλάνησης. Άλλωστε το διαδίκτυο διευκολύνει την μακροπρόθεσμη θυματοποίηση (π.χ. διανομή φωτογραφιών, οι οποίες μπορούν να μείνουν αναρτημένες για πάντα μεταφερόμενες από ιστοσελίδα σε ιστοσελίδα).

Η διαδικασία της αποπλάνησης του παιδιού περνά συνήθως από τέσσερα στάδια κατά τη διάρκεια των οποίων ο θύτης χρησιμοποιεί μια σειρά από τεχνικές. Το πρώτο στάδιο είναι η προετοιμασία της επαφής, το δεύτερο στάδιο είναι η επαφή με το θύμα και η δημιουργία σχέσης εμπιστοσύνης, το τρίτο στάδιο είναι η προετοιμασία για την προσωπική συνάντηση. Στο τέταρτο στάδιο, πλέον, πραγματοποιείται η προσωπική συνάντηση με σκοπό τη σεξουαλική κακοποίηση του παιδιού. Πιο συγκεκριμένα:

Τα στάδια

1. ***Προετοιμασία της επαφής.*** Μια από τις πιο συχνές πρακτικές που χρησιμοποιεί ο θύτης είναι η δημιουργία ψεύτικης ταυτότητας, παρέχοντας με αυτόν τον τρόπο ψεύτικες πληροφορίες όσον αφορά το όνομά του, την ηλικία του και ακόμη δίνοντας παραπλανητική φωτογραφία. Έτσι, οι άμυνες του διαδικτυακού συνομιλητή του δεν είναι ενεργοποιημένες. Η ψευδής αυτή ταυτότητα μπορεί να είναι στατική, με την έννοια ότι χρησιμοποιείται η ίδια σε όλη τη διάρκεια της προσέγγισης. Υπάρχει όμως και το ενδεχόμενο ο θύτης να αλλάζει συνεχώς το διαδικτυακό του προφίλ ή να διατηρεί πολλά και διαφορετικά με άλλα ονόματα. Αυτό του δίνει την ικανότητα να προσαρμόζει τα ενδιαφέροντα, τα γούστα και όλα όσα θεωρεί απαραίτητα για την προσέγγιση του θύματος που έχει επιλέξει.

2. ***Επαφή με το θύμα και δημιουργία σχέσης εμπιστοσύνης.*** Ένα βασικό χαρακτηριστικό της συμπεριφοράς του θύτη είναι το «καθρέφτισμα» (mirroring), διαδικασία κατά την οποία αντιγράφει ακριβώς το θύμα του (συναισθηματική κατάσταση, ενδιαφέροντα κλπ) με σκοπό να μειώσει τις άμυνες του και να το κάνει να νιώσει πως ταυτίζεται μαζί του. Ακολούθως επιδιώκει να μάθει όσο το δυνατόν περισσότερες λεπτομέρειες για τη ζωή του, να κάμψει κι άλλο τις αναστολές του και βαθμιαία να εισάγει το σεξουαλικό στοιχείο στην επικοινωνία τους. Οι συζητήσεις αυτού του είδους μπορεί να ξεκινήσουν γενικά με θέμα την

ανθρώπινη σεξουαλικότητα και να καταλήξουν με την αποστολή πορνογραφικού υλικού ή τη φωτογράφιση του θύματος σε σεξουαλικές στάσεις με σκοπό να μειωθεί η ντροπή, να εισαχθεί το στοιχείο της γυμνότητας και να οξυνθεί η περιέργεια.

3. ***Προετοιμασία για την προσωπική συνάντηση.***

4. ***Προσωπική συνάντηση.***

Καθώς το διαδίκτυο και οι τεχνολογίες επικοινωνίας θα συνεχίζουν να εξελίσσονται, οι περιπτώσεις σεξουαλικής εκμετάλλευσης και αποπλάνησης θα αυξάνονται. Είναι λοιπόν απαραίτητη η επαγρύπνηση όλων σχετικά με τους πιθανούς κινδύνους που προκύπτουν διαδικτυακά [75].

<u>Σημάδια ότι ο ανήλικος εκτίθεται σε κίνδυνο στο διαδίκτυο:</u>

- Υπάρχει πορνογραφικό υλικό στον υπολογιστή του.
- Δέχεται τηλεφωνήματα από αγνώστους.
- Δέχεται δώρα από αγνώστους.
- Κλείνει τον υπολογιστή του όταν μπαίνουν οι γονείς στο δωμάτιο.
- Χρησιμοποιεί λογαριασμό που ανήκει σε άλλον.

▪ ***Εργοδοσία***

Τα μέσα κοινωνικής δικτύωσης παίζουν καθοριστικό ρόλο στην αγορά εργασίας και μάλιστα αναμένεται ο ρόλος τους να γίνεται ολοένα και σημαντικότερος τα επόμενα χρόνια, αλλά οι καλύτερες πρακτικές και η επιρροή τους δεν είναι πάντα σαφείς τόσο στα άτομα που αναζητούν εργασία όσο και στους εργοδότες, όπως προκύπτει από σχετική παγκόσμια έρευνα που πραγματοποίησε η εταιρεία συμβούλων επιχειρήσεων Adecco. Η μελέτη της Adecco που διεξήχθη σε συνεργασία με το Catholic University of Milan της Ιταλίας (2013), προσφέρει εξειδικευμένες συμβουλές για την επιτυχημένη διασύνδεση με την αγορά εργασίας [76].

Σύμφωνα με τη μελέτη, καθοριστικό ρόλο στη στελέχωση επιχειρήσεων αλλά και στην εύρεση εργασίας διαδραματίζει πλέον η «ψηφιακή φήμη». Επτά στους δέκα εργοδότες χρησιμοποιούν κυρίως το Linkedin και το

Facebook για την επιλογή ανθρωπίνου δυναμικού, ενώ πέντε στους δέκα υποψηφίους αναζητούν εργασία μέσω αυτών.

Περισσότεροι από 17.000 υποψήφιοι και πάνω από 1.500 εργοδότες από 24 χώρες συμμετείχαν στην έρευνα, σύμφωνα με την οποία το 53% των διαδικασιών αναζήτησης και πρόσληψης εργαζομένων, το 2013 πραγματοποιήθηκε με τη χρήση ή και την αξιοποίηση του διαδικτύου. Το ποσοστό για το 2014 αναμένεται να ανέλθει στο 61%. Επτά στους 10 εργοδότες δήλωσε ότι χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης στη διαδικασία επιλογής ανθρώπινου δυναμικού και 5 στους 10 υποψηφίους απάντησαν πως τα χρησιμοποιούν στην αναζήτηση εργασίας. Στην Ελλάδα το ποσοστό των υποψηφίων που αναζητούν εργασία μέσω των μέσων κοινωνικής δικτύωσης ανέρχεται στο 65%. Επιπλέον, το 34% των υποψηφίων στην Ελλάδα δηλώνει πως τουλάχιστον μια φορά κάποιος εργοδότης τούς προσέγγισε μέσω ενός από τα κανάλια κοινωνικής δικτύωσης και το 6% αυτών έλαβε μάλιστα και προσφορά εργασίας. Τα αντίστοιχα ποσοστά της παγκόσμιας μελέτης είναι 30% και 9%.

Αντίθετα με ό,τι θα θεωρούνταν αναμενόμενο, η αναζήτηση εργασίας μέσω των καναλιών κοινωνικής δικτύωσης δεν είναι πλέον αποκλειστικό προνόμιο των έμπειρων υποψηφίων που διαθέτουν εξαιρετικά προσόντα. Η πλειοψηφία των υποψηφίων που αναζητούνται για κάλυψη θέσεων σήμερα μέσω των μέσων κοινωνικής δικτύωσης δεν αφορούν σε υψηλόβαθμα/διευθυντικά στελέχη.

Η μελέτη επιβεβαιώνει επίσης ότι η φήμη των υποψηφίων στα μέσα κοινωνικής δικτύωσης παίζει σημαντικό ρόλο και οι εργοδότες χρησιμοποιούν σε μεγάλο βαθμό τα κοινωνικά δίκτυα για να την αξιολογήσουν. Για τον σκοπό αυτό, η χρήση του LinkedIn σε παγκόσμιο επίπεδο αλλά και στην Ελλάδα παραμένει κυρίαρχη (68% σε παγκόσμιο επίπεδο, 48% στην Ελλάδα), αλλά και το Facebook είναι επίσης σημαντικό (52% σε παγκόσμιο επίπεδο, 25% στην Ελλάδα), παρόλο που γενικά θεωρείται ως μια πιο προσωπική ιστοσελίδα κοινωνικής δικτύωσης. Όταν εξετάζουν τα διάφορα στοιχεία στα προφίλ των πιθανών υποψηφίων, οι εργοδότες δίνουν κυρίως σημασία στην προηγούμενη επαγγελματική εμπειρία. Πληροφορίες που αφορούν σε βραβεία ή άλλα επιτεύγματα είναι επίσης σημαντικές για τους εργοδότες, αλλά συχνά παραλείπονται στα προφίλ των υποψηφίων.

Οι εργοδότες επίσης εξετάζουν στοιχεία που αφορούν στην προσωπικότητα των υποψηφίων. Περίπου ένας στους τρεις παραδέχεται ότι έχει απορρίψει έναν πιθανό υποψήφιο ως συνέπεια του

περιεχόμενου ή των εικόνων που δημοσιεύτηκαν στο προφίλ του. Ωστόσο, η συντριπτική πλειοψηφία των υποψηφίων που αναζητούν εργασία υποτιμούν την επίδραση των προσωπικών τους σελίδων σε μέσα κοινωνικής δικτύωσης στην επαγγελματική τους πορεία.

Θέματα σχετικά με την ιδιωτικότητα αυξάνονται ολοένα για τους χρήστες που ήδη εργάζονται. Ένας μεγάλος αριθμός περιπτώσεων έχουν εμφανιστεί κατά τις οποίες οι υπάλληλοι έχουν απολυθεί λόγω δημοσίευσης σχολίων σε ιστοσελίδες κοινωνικής δικτύωσης τα οποία έχουν θεωρηθεί ως δυσφήμιση προς τους συναδέλφους τους ή την εταιρεία εργασίας τους. Το 2009 ο 16χρονος Kimberley Swann απολύθηκε από τη θέση του στην εταιρεία Ivell Marketing and Logistics Limited διότι περιέγραψε τη δουλειά του ως βαρετή. Το 2008 η αεροπορική εταιρεία Virgin Atlantic απέλυσε 13 εργαζόμενους του προσωπικού του πληρώματός της επειδή κατέκριναν τα πρότυπα ασφαλείας της εταιρείας και αποκάλεσαν τους επιβάτες ως «πρόβατα προς σφαγή» στο Facebook. Ωστόσο, ομάδες ανθρωπίνων δικαιωμάτων και συνδικάτα εκφράζουν τα παράπονά τους σχετικά με αυτήν την επεμβατική προσέγγιση που έχει υιοθετηθεί από πολλούς εργοδότες υποστηρίζοντας πως επειδή δίνεται η δυνατότητα να κρυφακούμε προσωπικές συνομιλίες μέσω κοινωνικών δικτύων, δε σημαίνει ότι είναι και υγιές πρακτική.

Συμπερασματικά, το θέμα της ιδιωτικότητας και της προστασίας της μέσω των υπηρεσιών κοινωνικής δικτύωσης απασχόλησε και απασχολεί τις Αρχές Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης. Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (European Union Agency of Network and Information Security, ENISA) εξέδωσε αναφορά στην οποία παραθέτει τα βασικότερα σημεία που θα πρέπει να προσέξουν οι χρήστες των ιστοσελίδων κοινωνικής δικτύωσης, και παράλληλα προτείνει πολιτικές που πρέπει να ακολουθηθούν από τους αρμόδιους φορείς για την αντιμετώπισή τους [77].

- ***Ψηφιακοί φάκελοι προσωπικών δεδομένων:*** Τα ηλεκτρονικά προφίλ στις ιστοσελίδες κοινωνικής δικτύωσης μπορούν να αποθηκευτούν από τρίτους και να αποτελέσουν μέρος ψηφιακών φακέλων προσωπικών δεδομένων. Μάλιστα κάποιες προσωπικές πληροφορίες μπορούν να συλλεχθούν μέσω μιας απλής αναζήτησης εκτός και αν οι χρήστες αλλάξουν τις προεπιλεγμένες ρυθμίσεις ασφάλειας στο προφίλ τους.

- ***Δευτερεύοντα δεδομένα***: Εκτός των πληροφοριών τις οποίες οι χρήστες αναρτούν με τη θέλησή τους, τα μέλη τέτοιου είδους ιστοσελίδων αποκαλύπτουν αυτόματα δευτερεύοντα στοιχεία τα οποία αφορούν τον τρόπο που χρησιμοποιούν τις προσφερόμενες υπηρεσίες: π.χ. τη χρονική διάρκεια μιας επικοινωνίας, τις επισκέψεις σε προφίλ άλλων χρηστών και τα μηνύματα που έχουν αποσταλεί μέσω του δικτύου. Στις πολιτικές απορρήτου γνωστών ιστοσελίδων κοινωνικής δικτύωσης που επισκέφθηκε ο Ελληνικός Κόμβος Ασφαλούς Διαδικτύου, παρατηρείται ότι δεν διευκρινίζεται επαρκώς ποιος μπορεί να έχει πρόσβαση στα δεδομένα αυτά και δεν είναι σαφώς καθορισμένο τι αποτελεί προσωπικό δεδομένο και τι όχι. Τα δεδομένα αυτά είναι πολύ πιθανό να χρησιμοποιηθούν για την απόκτηση οικονομικού οφέλους από την μεταπώλησή τους σε τρίτους.

- ***Αναγνώριση προσώπου:*** Οι φωτογραφίες που χρησιμοποιούνται στα εικονικά προφίλ αποτελούν μια ψηφιακή ταυτότητα του εκάστοτε χρήστη. Μέσω των προηγμένων τεχνολογιών αναγνώρισης προσώπου (face recognition) μπορούν αυτές οι φωτογραφίες να συνδεθούν με πληροφορίες από άλλους ιστοχώρους και υπηρεσίες, όπου ο ίδιος χρήστης έχει δημοσιεύσει άλλα στοιχεία του, οδηγώντας τελικά στη συλλογή πολύ περισσότερων προσωπικών δεδομένων για το χρήστη από ότι ο ίδιος είχε στο μυαλό του να αποκαλύψει μέσα από την κοινωνική δικτύωση.

- ***Εντοπισμός στο φυσικό κόσμο***: Μέσω νέων τεχνολογικών επιτευγμάτων, από τις φωτογραφίες που δημοσιεύονται είναι δυνατή η άντληση δεδομένων που παραπέμπουν στον εντοπισμό του χρήστη στον πραγματικό κόσμο (όπως για παράδειγμα μια φωτογραφία μπροστά από το σπίτι του). Οι χρήστες δεν αντιλαμβάνονται συχνά πόσο σημαντικό είναι να μη δημοσιεύουν φωτογραφίες όπου η τοποθεσία γίνεται εύκολα αντιληπτή.

- ***Μεταδεδομένα:*** Πολλές πλατφόρμες κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες τους να μαρκάρουν με μεταδεδομένα (τα λεγόμενα metadata) τις φωτογραφίες τους. Τα μεταδεδομένα μπορούν να είναι σύνδεσμοι σε προφίλ ή διευθύνσεις e-mail. Αυτό ενέχει κινδύνους για ανεπιθύμητη διασύνδεση των φωτογραφιών με προσωπικά δεδομένα. Ακόμα και αν οι χρήστες τηρούν τα μέτρα ασφάλειας σε ότι αφορά τις προσωπικές τους φωτογραφίες, οι ιστοσελίδες κοινωνικής δικτύωσης δίνουν τη δυνατότητα στους χρήστες τους να μαρκάρουν τις φωτογραφίες άλλων χρηστών, μάλιστα όχι πάντα με τη συναίνεσή τους. Επιπλέον, αρκετές φωτογραφίες περιλαμβάνουν δεδομένα, όπως τον σειριακό αριθμό της

φωτογραφικής μηχανής, κάτι που μπορεί να αποτελέσει απειλή προς την ιδιωτική ζωή του χρήστη.

- ***Αδυναμία πλήρους διαγραφής του προφίλ:*** Οι χρήστες που επιθυμούν να διαγράψουν το λογαριασμό τους από μια ιστοσελίδα κοινωνικής δικτύωσης δεν μπορούν να διαγράψουν τις δευτερεύουσες πληροφορίες που συνδέονται με το προφίλ τους, όπως τα δημόσια σχόλια.

- ***Social Networking Spam:*** Είναι ένα πολύ διαδεδομένο φαινόμενο. Ανεπιθύμητα μηνύματα προωθούνται στους χρήστες μέσω των εφαρμογών που προσφέρονται στις ιστοσελίδες κοινωνικής δικτύωσης. Για παράδειγμα, υπάρχουν μηχανισμοί που αποστέλλουν μαζικά στους χρήστες αίτημα για να τους εντάξουν στους «φίλους» τους, ώστε να έχουν δικαίωμα ανάρτησης σχολίων στο προφίλ τους. Τα σχόλια αυτά συχνά έχουν διαφημιστικό περιεχόμενο ή αποτελούν συνδέσμους προς ιστοσελίδες με πορνογραφικό περιεχόμενο.

- ***Social Networking phishing***: Η ύπαρξη προσωπικών προφίλ και εικονικών φιλικών κύκλων που δεν έχουν περιορίσει την πρόσβαση τρίτων και είναι πολύ εύκολα προσβάσιμα στους ιστοχώρους κοινωνικής δικτύωσης, ευνοεί την άντληση πολλών έγκυρων προσωπικών δεδομένων και πληροφοριών από επιτήδειους οι οποίοι τα χρησιμοποιούν για εξειδικευμένη επίθεση ηλεκτρονικού ψαρέματος. Η επιτυχία της μεθόδου είναι μεγάλη.

- ***Παρενόχληση:*** Οι επιτήδειοι έχουν τη δυνατότητα να επικοινωνούν επανειλημμένα με τα εν δυνάμει θύματά τους με τα ηλεκτρονικά μέσα που τους προσφέρονται μέσα από τις ιστοσελίδες κοινωνικής δικτύωσης. Πολλές από τις εφαρμογές που φιλοξενούν αυτές οι πλατφόρμες ενδέχεται να διευκολύνουν περιστατικά παρενόχλησης. Η απειλή της κλοπής ταυτότητας είναι επίσης ιδιαίτερα σημαντική: ψεύτικα προφίλ δημιουργούνται με σκοπό την προσβολή και τον εξευτελισμό άλλων ατόμων. Ακόμη, δημιουργούνται προφίλ που χρησιμοποιούν ονόματα γνωστών εταιρειών ή προσωπικοτήτων με σκοπό την απόκτηση κέρδους από την εκμετάλλευση της φήμης τους.

- ***Βλαβερό Λογισμικό:*** Οι ιστοσελίδες κοινωνικής δικτύωσης περιλαμβάνουν μικρές εφαρμογές «widgets», οι δημιουργοί των οποίων δεν έχουν πάντα επαρκείς πιστοποιήσεις. Σε τέτοια περίπτωση, αυτές οι εφαρμογές ενδέχεται να περιέχουν κακόβουλο λογισμικό, ιούς και σκουλήκια.

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών προτείνει την ανάληψη δράσεων από μέρους των αρμόδιων φορέων, έτσι ώστε να καταστεί πιο ασφαλής η χρήση των ιστοσελίδων κοινωνικής δικτύωσης:

- Αναθεώρηση και εκ νέου ερμηνεία του νομοθετικού πλαισίου: η κοινωνική δικτύωση είναι ένα πολύ πρόσφατο φαινόμενο και δεν έχει ληφθεί υπόψη στη σύνταξη των ισχυουσών νομοθεσιών, ειδικότερα σε ότι αφορά τους νόμους περί προστασίας προσωπικών δεδομένων.
- Μεγαλύτερη διαφάνεια στις πρακτικές διαχείρισης των προσωπικών δεδομένων από μέρους των ιστοσελίδων κοινωνικής δικτύωσης.
- Ανάληψη πρωτοβουλιών με σκοπό την επαγρύπνηση και την εκπαίδευση κυρίως με εκστρατείες ενημέρωσης σε μαθητές και εκπαιδευτικούς.
- Αποθάρρυνση της απαγόρευσης χρήσης των ιστοσελίδων κοινωνικής δικτύωσης στα σχολεία. Αντιθέτως, προτείνεται η ενθάρρυνση της χρήσης τους στο σχολικό περιβάλλον με σκοπό την εξοικείωση μαθητών και εκπαιδευτικών με την ασφαλή χρήση των ιστοσελίδων αυτών.

ΚΕΦΑΛΑΙΟ 8
ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΣΦΑΛΙΣΗΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ
(PET ENHANCING TECHNOLOGIES, PETs)

Οι τεχνολογίες διασφάλισης ιδιωτικότητας ορίζονται ως τεχνικές και οργανωσιακά λειτουργικά πρότυπα που στοχεύουν στην προστασία της προσωπικής ταυτότητας και των προσωπικών δεδομένων που αποκαλύπτονται κατά τη χρήση δικτύων ηλεκτρονικών υπολογιστών.

8.1 Απαιτήσεις Ιδιωτικότητας

Στη σημερινή ψηφιακή κοινωνία, οι νόμοι και οι κανονισμοί δεν επαρκούν για να καλύψουν την ιδιωτικότητα. Τα πληροφοριακά συστήματα που συλλέγουν δεδομένα θα πρέπει να αποτρέπουν την παραβίαση της ιδιωτικότητας και για το λόγο αυτό θα πρέπει να λαμβάνεται υπόψη σαν μια βασική παράμετρος που θα πρέπει να υλοποιηθεί.

Οι υπεύθυνοι για την προστασία δεδομένων απαιτούν πλέον από τους αναλυτές και προγραμματιστές πληροφοριακών συστημάτων να συμπεριλαμβάνουν την ιδιωτικότητα ως τεχνική απαίτηση που πρέπει να λαμβάνεται υπόψη στο υπο ανάπτυξη σύστημα και πιο συγκεκριμένα θα πρέπει να λαμβάνεται υπόψη από τη φάση της σχεδίασης του συστήματος αποτελώντας ξεχωριστό κριτήριο που πρέπει να υλοποιηθεί.

Για τη μετατροπή της ιδιωτικότητας από μια γενική έννοια σε τεχνική απαίτηση, θα πρέπει να ικανοποιούνται κάποιες απαιτήσεις οι οποίες αναλύονται παρακάτω.

8.1.1 Αυθεντικοποίηση (Authentication)

Η διαδικασία μέσω της οποίας επιβεβαιώνεται η ταυτότητα του χρήστη. Σε ιδιωτικά και δημόσια δίκτυα, η αυθεντικοποίηση υλοποιείται συνήθως με τη χρήση κωδικών πρόσβασης. Αποτελεί κυρίως απαίτηση ασφάλειας παρά ιδιωτικότητας, ωστόσο έχει σημαντική συνεισφορά και στην ικανοποίηση απαιτήσεων ιδιωτικότητας.

8.1.2 Εξουσιοδότηση (Authorization)

Η διαδικασία μέσω της οποίας ο χρήστης αποκτά δικαιώματα-πρόσβαση σε μια μεμονωμένη υπηρεσία ή σε συγκεκριμένες υπηρεσίες ενός πληροφοριακού συστήματος. Αν σε ένα σύστημα υπάρχουν πολλοί χρήστες, τότε ο διαχειριστής του συστήματος φροντίζει να εξουσιοδοτεί τον καθένα από αυτούς με τα αντίστοιχα δικαιώματα, ανάλογα με το ρόλο τους και τις υποχρεώσεις τους στο σύστημα.

8.1.3 Αναγνώριση (Identification)

Η διαδικασία μέσω της οποίας ελέγχεται αν η υπηρεσία ή τα δεδομένα που ζητούνται απαιτούν αυθεντικοποίηση και στη συνέχεια εξουσιοδότησή της ή όχι.

8.1.4 Προστασία Δεδομένων (Data Protection)

Η διαδικασία μέσω της οποίας διασφαλίζονται σύμφωνα και με την Ευρωπαϊκή Οδηγία 1995/46/ΕΚ, οι κάτωθι αρχές:

- Αρχή της νομιμότητας και της δικαιοσύνης.
- Αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν.
- Αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων.
- Παροχή πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων.
- Αρχή της ασφάλειας και της ακεραιότητας.
- Εποπτεία και Επικύρωση.

8.1.5 Ανωνυμία (Anonymity)

Η διαδικασία μέσω της οποίας διασφαλίζεται ότι ένας χρήστης μπορεί να χρησιμοποιήσει μια υπηρεσία ή να επικοινωνήσει με έναν άλλο χρήστη, χωρίς να αποκαλύψει την ταυτότητά του. Σύμφωνα με τους Pfitzmann και Hansen (2007), ανωνυμία μιας οντότητας σημαίνει ότι αυτή δεν είναι αναγνωρίσιμη μέσα σε ένα σύνολο οντοτήτων. Το σύνολο αυτό περιλαμβάνει όλες τις οντότητες που μετέχουν σε μια επικοινωνία και που πιθανόν θα μπορούσαν να αναγνωρισθούν από διάφορους επιτιθέμενους [78].

Ανάλογα με το ρόλο που έχει ο χρήστης στην επικοινωνία, έχουν καθοριστεί δύο μορφές ανωνυμίας: η ανωνυμία του αποστολέα (sender anonymity) και η ανωνυμία του παραλήπτη (receiver anonymity). Η ανωνυμία του αποστολέα σημαίνει ότι σε μια επικοινωνία ο χρήστης που έχει το ρόλο του αποστολέα παραμένει ανώνυμος ενώ ο παραλήπτης όχι. Το αντίστοιχο συμβαίνει στην ανωνυμία του παραλήπτη.

8.1.6 Ψευδωνυμία (Pseydonymity)

Η διαδικασία μέσω της οποίας προστατεύεται η αναγνώριση του χρήστη από μη εξουσιοδοτημένους τρίτους χρήστες. Η Fischer-Hubner (2001) ορίζει τη ψευδωνυμία ως την απαίτηση που διασφαλίζει την απόκρυψη της ταυτότητας του χρήστη όταν αυτός ενεργεί στα πλαίσια μίας επικοινωνίας χρησιμοποιώντας ένα ή περισσότερα ψευδώνυμα. Η ψευδωνυμία υλοποιείται όταν δεν μπορεί να υλοποιηθεί η ανωνυμία [78].

8.1.7 Μη συνδεσιμότητα (Unlinkability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να συνδέσουν τμήματα σχετικών πληροφοριών μεταξύ τους, οδηγώντας έτσι στην αποκάλυψη της ταυτότητάς του χρήστη. Στην ουσία, μη συνδεσιμότητα σημαίνει πως ο επιτιθέμενος δεν είναι σε θέση να διακρίνει αν τα στοιχεία που

τον ενδιαφέρουν μέσα σε ένα σύστημα (χρήστες, μηνύματα που εστάλησαν κτλ), σχετίζονται μεταξύ τους ή όχι.

8.1.8 Μη παρατηρησιμότητα (Unobservability)

Η διαδικασία μέσω της οποίας προστατεύεται η ιδιωτικότητα του χρήστη από πιθανούς επιτιθέμενους απαγορεύοντας στους δεύτερους να παρατηρήσουν ή να εντοπίσουν ίχνη του πρώτου. Σύμφωνα με τους Pfitzmann και Hansen (2007), μία οντότητα (π.χ. χρήστης, μήνυμα, ενέργεια) είναι μη-παρατηρήσιμη σε ένα σύνολο οντοτήτων όταν: α) ο επιτιθέμενος δεν μπορεί να εντοπίσει την οντότητα αυτή και β) ο κάτοχος της οντότητας αυτής παραμένει ανώνυμος σε σχέση με τους άλλους κατόχους των υπόλοιπων οντοτήτων.

8.2 Τρόποι Προστασίας της Ιδιωτικότητας

Η προστασία των προσωπικών δεδομένων είναι μια εξαιρετικά πολύπλοκη διαδικασία στην οποία, εκτός από τον ίδιο το χρήστη, εμπλέκονται αρκετοί παράγοντες. Οι τεχνικές ρύθμισης της ιδιωτικότητας στο διαδίκτυο (Privacy Enhancing Technologies) αποτελούν ένα ευρύ φάσμα τεχνικών μέσων εξαλείφοντας ή εμποδίζοντας την περιττή ή/και ανεπιθύμητη επεξεργασία προσωπικών δεδομένων χωρίς να υπάρξει απώλεια της λειτουργικότητας του συστήματος πληροφοριών και για αυτό το λόγο έχουν αποκτήσει σημαντική δυναμική στον ακαδημαϊκό χώρο και τη βιομηχανία. Οι τεχνολογίες αυτές πολλές φορές θεωρούνται λανθασμένα ως υποκατάστατα άλλων μέσων προστασίας των προσωπικών δεδομένων (όπως η νομοθεσία). Στην πραγματικότητα, όμως, δρουν συμπληρωματικά με τους υφιστάμενους νόμους ώστε να εξασφαλίζεται η όσο το δυνατόν μεγαλύτερη ασφάλεια δεδομένων.

8.2.1 Πολιτικές Ιδιωτικότητας των Ιστοτόπων

Τα μέτρα πολιτικής τα οποία θα πρέπει να λάβουν οι οργανισμοί και οι υπηρεσίες που συλλέγουν προσωπικές πληροφορίες στο διαδίκτυο, είναι αναμφισβήτητα το πιο σημαντικό εργαλείο για την προστασία της ιδιωτικής ζωής. Οι πολιτικές ιδιωτικότητας που αναγράφουν οι ιστότοποι στις αρχικές τους σελίδες, αποτελούν στην ουσία ένα είδος υπόσχεσης της διαδικτυακής εταιρείας να επεξεργαστεί τα ιδιωτικά δεδομένα των χρηστών της με ένα συγκεκριμένο τρόπο. Περιλαμβάνουν προτάσεις που αναφέρονται στον τρόπο συλλογής των ιδιωτικών δεδομένων, στη μη χρησιμοποίηση των δεδομένων αυτών για άλλους σκοπούς εκτός της παρούσας συναλλαγής και στη μη παροχή των δεδομένων αυτών προς τρίτα μη εξουσιοδοτημένα μέρη.

Ωστόσο, αν και οι προτάσεις αυτές κινούνται προς τη σωστή κατεύθυνση, εντούτοις, οι πολιτικές ιδιωτικότητας εμφανίζουν σημαντικά μειονεκτήματα, τα οποία είναι τα εξής [79]:

- Ο χρήστης πρέπει να διαβάσει ολόκληρη την πολιτική ιδιωτικότητας του ιστοτόπου πριν αποφασίσει να δώσει κάποιο μέρος των ιδιωτικών δεδομένων του. Σε περίπτωση διαφωνίας θα πρέπει να επικοινωνήσει και να διαπραγματευτεί με τη διαδικτυακή επιχείρηση, διαδικασία ιδιαιτέρως επίπονη και χρονοβόρα.
- Η πολιτική ιδιωτικότητας μιας επιχείρησης μπορεί να αλλάξει ανά πάσα στιγμή και μάλιστα να αφορά και ιδιωτικές πληροφορίες που έχουν ήδη συλλεχθεί. Επίσης, δεν υπάρχει κάποιος αυτόματος μηχανισμός που να ενημερώνει διαρκώς το χρήστη για τις συγκεκριμένες αλλαγές.
- Σε περίπτωση μη τήρησης της πολιτικής ιδιωτικότητας από τη μεριά της διαδικτυακής επιχείρησης, ο χρήστης θα πρέπει να το εντοπίσει από μόνος του και να λάβει τα αναγκαία νομικά μέτρα. Όμως στην πράξη είναι σχεδόν αδύνατο ο απλός χρήστης να έχει τη δυνατότητα να εποπτεύει το τι πραγματικά συμβαίνει με τα ιδιωτικά του δεδομένα και πως αυτά διαχειρίζονται από τις επιχειρήσεις. Επομένως, η τήρηση και αντίστοιχα, η μη τήρηση της πολιτικής ιδιωτικότητας, επαφίεται στην αυτορρύθμιση των ίδιων των εταιρειών και στο βαθμό εμπιστοσύνης και αξιοπιστίας που καλλιεργούν στους χρήστες/ πελάτες τους.

Σημαντικό είναι επίσης το γεγονός πως οι συγκεκριμένες πολιτικές αφορούν κυρίως τις συμμετέχουσες οντότητες που επεξεργάζονται τα δεδομένα προκειμένου να παρέχουν εξατομικευμένες υπηρεσίες στο χρήστη. Εντούτοις, δεν επαρκούν ενάντια σε μια τρίτη, κακόβουλη οντότητα η οποία επιθυμεί να υποκλέψει τα δεδομένα αυτά.

Παράλληλα, ο καθορισμός μιας τέτοιας πολιτικής βρίσκεται στην ευχέρεια του κάθε φορέα παροχής υπηρεσιών, με αποτέλεσμα να μην υπάρχει μια κοινή πολιτική προστασίας της ιδιωτικότητας. Τέλος, δεδομένου ότι οι εφαρμογές αυτές είναι σχετικά νέες, είναι αμφισβητήσιμο το πόσο αποτελεσματικά είναι αυτά τα μέτρα για την προστασία των χρηστών. Για το λόγο αυτό, δεν επαρκεί να ορίζονται μόνο οι πολιτικές ιδιωτικότητας αλλά θα πρέπει να λαμβάνονται και άλλα μέτρα προστασίας των δεδομένων.

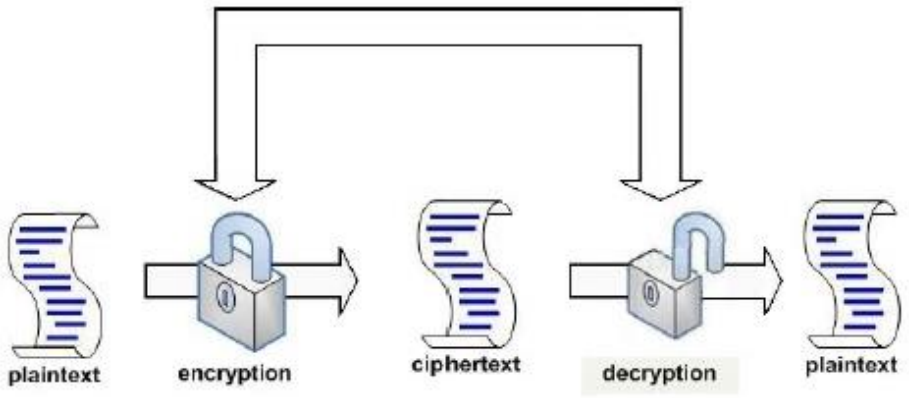
8.2.2 Κρυπτογραφία

Η κρυπτογραφία (Encryption) είναι μια από τις βασικότερες τεχνικές προκειμένου να επιτευχθεί η αυθεντικοποίηση του χρήστη καθώς και η προστασία των δεδομένων από πιθανή κακόβουλη χρήση. Πρόκειται για μια μέθοδο παραλλαγής του απλού κειμένου (plaintext) σε μη αναγνώσιμη μορφή χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης με αποτέλεσμα τη δημιουργία του cipher text. Με αυτό τον τρόπο, οι πληροφορίες μετατρέπονται από έναν αλγόριθμο και γίνονται δυσανάγνωστες. Σκοπός της κρυπτογράφησης είναι να εξασφαλίσει το απόρρητο των δεδομένων κρατώντας τα κρυφά από όλους όσους έχουν πρόσβαση σε αυτά.

Στο plaintext τα δεδομένα είναι ευανάγνωστα και κατανοητά. Στο cipher text τα δεδομένα προκύπτουν αν στο plaintext εφαρμοστεί ένας αλγόριθμος κρυπτογράφησης. Κλειδί (key) ονομάζεται ένα κομμάτι πληροφορίας το οποίο υπολογίζει την έξοδο ενός αλγορίθμου και καθορίζει την αλλαγή από το plaintext στο cipher text.

Στόχος, επομένως, της κρυπτογραφίας είναι να επικοινωνούν δύο άνθρωποι από ένα μη ασφαλές κανάλι χωρίς να υποκλαπεί το μήνυμά τους. Έτσι, ένα κρυπτοσύστημα αποτελείται από τις εξής πέντε παραμέτρους:

1. Τα plaintexts
2. Τα cipher texts
3. Τα κλειδιά
4. Την κρυπτογραφική μετατροπή ή κρυπτογραφική συνάρτηση
5. Την αντίθετη συνάρτηση ή αποκρυπτογραφική μετατροπή



Σχήμα 2: Κρυπτογράφηση και αποκρυπτογράφηση

8.2.2.1 Ασύμμετρη Κρυπτογραφία ή Κρυπτογραφία Δημοσίου-Ιδιωτικού κλειδιού

Η ασύμμετρη κρυπτογραφία (Public Key Cryptography) είναι ένα από τα βασικότερα είδη κρυπτογράφησης η οποία εγγυάται την αυθεντικοποίηση των χρηστών ενός συστήματος. Αυτό το είδος κρυπτογράφησης απαιτεί την ύπαρξη δύο κλειδιών, ενός δημοσίου (public key) και ενός ιδιωτικού (private key).

Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κρατείται πάντοτε μυστικό. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη να μοιράζεται ο αποστολέας με τον παραλήπτη το ίδιο κλειδί εξαφανίζεται. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η διαπιστευμένη και επιβεβαιωμένη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους, ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστογραφία.

Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να «σπάσει» ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στο χρήστη Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει

χρήση του ιδιωτικού του κλειδιού για να το αποκρυπτογραφήσει. Κάποιος που παρακολουθεί τη σύνδεση, δε μπορεί να αποκρυπτογραφήσει το μήνυμα. Όποιος έχει το δημόσιο κλειδί του Β, μπορεί να του στείλει μήνυμα, ενώ μόνο ο Β μπορεί να το διαβάσει, γιατί είναι ο μόνος που γνωρίζει το ιδιωτικό κλειδί.

Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί έναν υπολογισμό που απαιτεί το ιδιωτικό του κλειδί και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας το δημόσιο κλειδί του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα βγει θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά, η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

Η βασική αυτή αρχή της κρυπτογραφίας δημοσίου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι στις αρχές της θεωρίας των πεπερασμένων πεδών, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού. Εξ ου και οι κυριότεροι αλγόριθμοι που χρησιμοποιούνται είναι ο Diffie-Hellman, ο RSA και ο El-Gamal.

Πιο συγκεκριμένα, ο αλγόριθμος RSA, όντας ο πιο διαδεδομένος χρησιμοποιείται σε μια μεγάλη ποικιλία από προϊόντα και εφαρμογές, όπως σε εφαρμογές λογισμικού και σε λειτουργικά συστήματα γνωστών εταιρειών όπως της Microsoft, της Sun, της Apple και της Novell. Όσο αφορά το hardware, συναντούμε τον RSA σε έξυπνες κάρτες καθώς και σε κάρτες δικτύου Ethernet.

8.2.2.2 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογραφία (Symmetric Cryptography ή Secret-Key Cryptography) ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να το αποκρυπτογραφήσει. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση αλλά και για πιστοποίηση ταυτότητας.

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα

κρυπτογραφεί και αποκρυπτογραφεί όλη τη διακινούμενη πληροφορία, χωρίς κάποιον άλλον να λάβει γνώση αυτού. Σε γενικές γραμμές, οι αλγόριθμοι ασύμμετρου κλειδιού είναι πιο αργοί από τους αλγόριθμους συμμετρικού κλειδιού. Για το λόγο αυτό, χρησιμοποιούνται κυρίως για ασφαλή μετάδοση συμμετρικών κλειδιών και για κρυπτογράφηση δεδομένων μικρού μεγέθους (PINs και αριθμούς πιστωτικών καρτών). Τέλος, λόγω των πλεονεκτημάτων που παρουσιάζουν, χρησιμοποιούνται ευρέως και σε πρωτόκολλα όπως TLS (Transport Layer Security), IPSec (IP Security) και SSH (Secure Shell).

8.2.3 Ψηφιακές υπογραφές

Ο σκοπός της τεχνικής των ψηφιακών υπογραφών είναι να συνδυάσει μοναδικά την πληροφορία με την ταυτότητα του κατόχου της. Πρόκειται για ένα εργαλείο που παρέχει ακεραιότητα των δεδομένων και πιστοποίηση ταυτότητας. Η έννοια πιστοποίηση ταυτότητας περιλαμβάνει όλες εκείνες τις διαδικασίες που είναι απαραίτητες για την επαλήθευση συγκεκριμένων ευαίσθητων πληροφοριών, όπως την ταυτότητα του αποστολέα ενός μηνύματος, την αυθεντικότητα ενός εγγράφου, ακεραιότητα δεδομένων και την ταυτοποίηση ενός υπολογιστή. Οι ψηφιακές υπογραφές επιτυγχάνουν την πιστοποίηση ταυτότητας, παράγοντας ένα σύνολο πληροφοριών που βασίζεται στο έγγραφο και σε ιδιωτικά στοιχεία το αποστολέα. Το σύνολο αυτό δημιουργείται μέσω μιας συνάρτησης κατακερματισμού και του ιδιωτικού κλειδιού του αποστολέα.

Η σωστή εφαρμογή της ψηφιακής υπογραφής σε ένα κρυπτογραφημένο σύστημα διασφαλίζει θεμελιώδεις απαιτήσεις ασφαλείας όπως την αυθεντικότητα των δεδομένων και της πηγής (data origin authentication, data source authentication), την ακεραιότητα της πληροφορίας (data integrity) την εξουσιοδότηση του υπογράφοντα (authorization) και την αποφυγή άρνησης αποστολής της από αυτόν (non-repudiation). Η απαίτηση για non-repudiation προσθέτει ένα επιπλέον επίπεδο ασφαλείας σε ένα κρυπτογραφημένο σύστημα καθώς, εάν ο δημιουργός μιας υπογραφής την αποστείλει και στη συνέχεια το αρνηθεί, αυτό σημαίνει ότι ψεύδεται διότι η υπογραφή θα επικυρώνεται με τη χρήση του δημοσίου κλειδιού.

8.2.3.1 Εφαρμογές της Ψηφιακής Υπογραφής

Καθώς η τεχνολογία εξελίσσεται, και δη των ψηφιακών υπογραφών, πολλές εφαρμογές έχουν ενσωματώσει το συγκεκριμένο εργαλείο. Στη συνέχεια θα αναφερθούμε συνοπτικά στις κυριότερες εξ αυτών:

Ασφάλεια Ηλεκτρονικού Ταχυδρομείου (E-mail)

Το ηλεκτρονικό ταχυδρομείο είναι απαραίτητο να υποστηρίζει τη δυνατότητα της ψηφιακής υπογραφής, ιδιαίτερα σε περιπτώσεις όπου μεταδίδονται ευαίσθητες πληροφορίες. Το πρωτόκολλο PGP (Pretty Good Privacy) προσφέρει υπηρεσίες ασφαλείας για την αποστολή μηνυμάτων και αρχείων χρησιμοποιώντας τεχνικές ψηφιακής υπογραφής, κρυπτογράφησης και συμπίεσης (zip).

Ασφάλεια Οικονομικών Συναλλαγών

Η ασφάλεια των οικονομικών συναλλαγών μέσω διαδικτύου συνιστά ένα θέμα μείζονος σημασίας, καθώς το ηλεκτρονικό εμπόριο και οι κάθε λογής οικονομικές συναλλαγές εξελίσσονται ραγδαία τα τελευταία χρόνια. Η ηλεκτρονική μεταφορά κεφαλαίων (Electronic Funds Transfer) επωφελείται σε σημαντικό βαθμό με τη χρήση της ψηφιακής υπογραφής. Το πιο γνωστό πρωτόκολλο που σχετίζεται με το ηλεκτρονικό εμπόριο είναι το SET (Secure Electronic Transaction). Το SET εισήγαγε ένα νέο μοντέλο ψηφιακών υπογραφών, το λεγόμενο dual signatures (διπλές υπογραφές), που αφορά τόσο την παραγγελία όσο και την αντίστοιχη πληρωμή. Το πρωτόκολλο SET χρησιμοποιεί τις ανωτέρω κρυπτογραφικές τεχνικές για να παρέχει τη μυστικότητα της πληροφορίας, για να διασφαλίζει την ακεραιότητα της πληρωμής και την πιστοποίηση της ταυτότητας αυτών που εμπλέκονται στη συναλλαγή.

Προστασία του software

Μέσω της ψηφιακής υπογραφής του software διασφαλίζεται η ακεραιότητα κατά τη διανομή του. Η υπογραφή επικυρώνεται όταν εγκαθίσταται το προϊόν στον υπολογιστή του αγοραστή και με αυτόν τον τρόπο είναι σίγουρος ότι δεν έχει υποστεί καμία ανεπιθύμητη αλλοίωση κατά τη διανομή του.

Ασφάλεια της Ηλεκτρονικής Αρχειοθέτησης (Electronic Filing)

Για την υπογραφή ενός συμβολαίου χρειάζεται η υποβολή κάποιων πιστοποιητικών από τα συμβαλλόμενα μέρη. Είναι απαραίτητη λοιπόν, η

αρχειοθέτηση των πιστοποιητικών επικυρωμένα με μία γραπτή υπογραφή. Σήμερα όμως, η αρχειοθέτηση αυτή πραγματοποιείται με ηλεκτρονικό τρόπο και η γραπτή υπογραφή δύναται να αντικατασταθεί από τη ψηφιακή διασφαλίζοντας υπηρεσίες ασφάλειας και ιδιωτικότητας, όπως ακεραιότητα και πιστοποίηση της αυθεντικότητας.

8.2.3.2 Επιθέσεις εναντίον των Ψηφιακών Υπογραφών

Ο στόχος μιας κακόβουλης επίθεσης είναι να πλαστογραφήσει μία ψηφιακή υπογραφή. Στη συνέχεια αναφέρονται τύποι επιτυχών επιθέσεων σε ψηφιακές υπογραφές:

- ***Συνολική κατάρρευση της υπογραφής (total break)***, στην οποία το κακόβουλο άτομο έχει καταφέρει να δημιουργήσει την πληροφορία του ιδιωτικού κλειδιού του κατόχου, ή έχει καταφέρει να δημιουργήσει έναν αποδοτικό αλγόριθμο ψηφιακής υπογραφής ο οποίος είναι όμοιος με αυτόν που χρησιμοποίησε ο κάτοχος.
- ***Επιλεκτική πλαστογράφηση της ψηφιακής υπογραφής (selective forgery),*** κατά την οποία το κακόβουλο άτομο έχει καταφέρει να δημιουργήσει μια αποδεκτή υπογραφή ενός συγκεκριμένου μηνύματος ή περισσοτέρων, που έχει επιλέξει ο ίδιος.
- ***Πλαστογράφηση υπάρχοντος μηνύματος (existential forgery),*** κατά την οποία το κακόβουλο άτομο καταφέρνει να δημιουργήσει μια αποδεκτή υπογραφή ενός ή περισσοτέρων μηνυμάτων, τα οποία δεν έχει επιλέξει ο ίδιος, αλλά ο νόμιμος υπογράφων.

Επίσης, το κακόβουλο άτομο ενδέχεται να γνωρίζει μόνο το δημόσιο κλειδί του υπογράφοντα και να πραγματοποιεί key-only attacks ή να πραγματοποιεί message attacks, σε περίπτωση που εξετάζει υπογραφές μηνυμάτων που ο ίδιος είτε γνωρίζει είτε έχει ο ίδιος δημιουργήσει προηγουμένως.

8.2.4 Ασφάλεια Περιμέτρου

Ως Περίμετρος Δικτύου ορίζονται όλα τα σημεία πρόσβασης του δικτύου του παρόχου σε εξωτερικά δίκτυα (διαδίκτυο, δίκτυα άλλων υποκαταστημάτων του παρόχου, δίκτυα συνεργατών του, ασύρματα δίκτυα, κλπ). Ο πρωταρχικός σκοπός της πολιτικής ασφαλείας περιμέτρου είναι να προστατεύσει τους διάφορους δικτυακούς πόρους του παρόχου διαδικτύου από εισβολείς, δηλαδή να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση σε στοιχεία του δικτύου του παρόχου, καθώς και τη διακοπή της ομαλής παροχής των υπηρεσιών του. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΕΑ) υποχρεώνει κάθε πάροχο διαδικτύου, συνεπώς έμμεσα και κάθε οργανισμό ηλεκτρονικού εμπορίου, να χρησιμοποιεί συστήματα firewall για την προστασία των συνδέσεων του δικτύου του με το διαδίκτυο και επιπλέον τον υποχρεώνει να χρησιμοποιεί συστήματα ανίχνευσης εισβολών για την ενίσχυση της προστασίας του δικτύου [80].

Ένα σύστημα firewall (τοίχος προστασίας) καλείται να λειτουργήσει ως μηχανισμός «περιμετρικής άμυνας», ο οποίος δρα συμπληρωματικά με τους υπόλοιπους μηχανισμούς ασφάλειας. Σκοπός του είναι ο έλεγχος και η καταγραφή όλων των προσπαθειών προσπέλασης οι οποίες κατευθύνονται προς το προστατευμένο σύστημα, με το να επιτρέπει, να απαγορεύει ή να ανακατευθύνει τη ροή των δεδομένων μέσω των μηχανισμών του. Η κύρια λειτουργία του είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το διαδίκτυο και το τοπικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο ή το δίκτυο ενός σπιτιού διαθέτει το μέγιστο βαθμό εμπιστοσύνης.

Άλλα συστήματα που χρησιμοποιούνται είναι τα εξής: Σύστημα Προστασίας Αποστρατιωτικοποιημένης Ζώνης (Demilitarized Zone System) και Σύστημα Ανίχνευσης Επισυνδέσεων (Intrusion Detection System).

ΚΕΦΑΛΑΙΟ 9
ΑΝΩΝΥΜΟΠΟΙΗΣΗ ΔΕΔΟΜΕΝΩΝ

Οι περισσότερες ανθρώπινες δραστηριότητες τα τελευταία χρόνια προκαλούν κάποια καταγραφή δεδομένων. Αρκετοί οργανισμοί είτε ιδιωτικοί είτε κρατικοί, καταγράφουν τις ανθρώπινες αυτές δραστηριότητες, η μελέτη των οποίων είναι πολύτιμη σε διάφορους τομείς ώστε να γίνονται πιο αποδοτικές οι υπηρεσίες που οι ίδιοι προσφέρουν αλλά και για εξαγωγή στατιστικών δεδομένων. Χαρακτηριστικό παράδειγμα είναι οι οργανισμοί που διαχειρίζονται δεδομένα νοσηλείας αλλά και τα συστήματα εξ αποστάσεως εκπαίδευσης στα οποία η καταγραφή πληθώρας προσωπικών δεδομένων τόσο των εκπαιδευομένων όσο και των εκπαιδευτικών είναι μια συνήθης διαδικασία, καθώς οι πληροφορίες που απορρέουν από την καταγραφή του ιστορικού της απόδοσης των χρηστών, των προτιμήσεων τους, των κινήσεων τους μέσα στο σύστημα και από τη δόμηση του προσωπικού τους προφίλ, είναι απαραίτητες στην εκπαιδευτική διαδικασία, ώστε να μπορέσουν να προσφέρουν μια καλύτερη μορφή εξατομικευμένης μάθησης, συστάσεων και καθοδήγησης.

Παράλληλα, όμως, δημιουργείται ένα νέο πρόβλημα, αυτό της προστασίας της ταυτότητας των ατόμων από τα οποία προέρχονται οι καταγραφές. Επιθυμία, λοιπόν, των οργανισμών είναι, η διαφύλαξη της ιδιωτικότητας σε δημοσιευμένα δεδομένα, προσφέροντας εγγυήσεις ανωνυμίας.

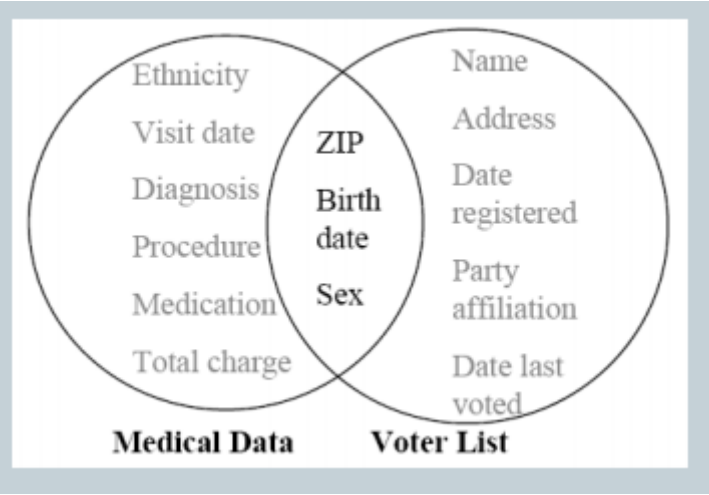
Αποκρύπτοντας, απλά, στοιχεία που συνδέουν άμεσα την ταυτότητα ενός προσώπου με ένα σύνολο από δεδομένα, όπως το ονοματεπώνυμο ή το ΑΦΜ, δεν εξασφαλίζεται ότι η σύνδεση αυτή δεν θα αποκαλυφθεί. Μέσω διασταύρωσης των δημοσιευμένων δεδομένων με άλλες πηγές γνώσης (εξωτερικούς καταλόγους δεδομένων, διαδίκτυο, κλπ), μπορεί να αναγνωριστούν με μεγάλη βεβαιότητα οι εγγραφές που αφορούν στην ταυτότητα ενός συγκεκριμένου προσώπου μέσω επιθέσεων συσχέτισης.

Συνεπώς, δεδομένα που προέρχονται από την καταγραφή του ιστορικού των χρηστών, των προτιμήσεων και των ενδιαφερόντων τους, δύναται να είναι προσβάσιμα από όλους τους εμπλεκόμενους φορείς. Οι πληροφορίες που απορρέουν από τα αρχεία αυτά για τους χρήστες, δίνουν τη δυνατότητα να κατασκευαστεί μια γενική εικόνα τους. Επίσης, με κατάλληλη επεξεργασία αυτών των αρχείων και σε συνδυασμό με αρχεία που προέρχονται από εξωτερικές πηγές και είναι εύκολο να ανακτηθούν, για παράδειγμα μέσω του διαδικτύου, θα μπορούσε να κατασκευαστεί επιπλέον μία πιο εξειδικευμένη εικόνα των χρηστών. Μέσα από αυτούς τους τρόπους, είναι δυνατόν να αποκαλυφτούν πολιτικές και θρησκευτικές πεποιθήσεις, αξίες, φιλοδοξίες, ευαίσθητα ιατρικά δεδομένα, και ακόμη, ένα μεγάλο μέρος των προτιμήσεων και ενδιαφερόντων των χρηστών ως καταναλωτές, γεγονός που αποκτά μεγάλη αξία για εμπορικούς σκοπούς.

9.1 Ιδιωτικότητα και Ανωνυμία δημοσιευμένων δεδομένων

Τα τελευταία χρόνια, έχει σημειωθεί εκθετική αύξηση του όγκου των πληροφοριών που είναι διαθέσιμες στο ευρύ κοινό, καθώς οι ταχύτητες και η συνδεσιμότητα στο διαδίκτυο αλλά και ο αποθηκευτικός χώρος γίνονται ολοένα και πιο διαθέσιμα. Το γεγονός αυτό, σε συνδυασμό με την προσωπική φύση του μεγαλύτερου όγκου αυτής της πληροφορίας, αλλά και της αυξανόμενης δημοσίευσης προσωπικών δεδομένων από τους ίδιους τους χρήστες, έχουν οδηγήσει στην ανάπτυξη τόσο νομοθεσίας, όσο και τεχνικών ανωνυμοποίησης των δεδομένων προς δημοσίευση με σκοπό την προστασία της ταυτότητας του ατόμου, αλλά και πιθανών ευαίσθητων γνωρισμάτων (sensitive attributes ή sensitive data), όπως για παράδειγμα η ασθένεια σε μία δημοσιευμένη βάση ενός νοσοκομείου. Τεχνικές όπως αυτή της απαλοιφής ορισμένων γνωρισμάτων δεν ήταν αρκετή για την προστασία των προσωπικών δεδομένων.

Το χαρακτηριστικότερο παράδειγμα αυτής της κατηγορίας είναι ο συνδυασμός δημοσίων εκλογικών καταλόγων και δημοσιευθέντων ιατρικών δεδομένων του οργανισμού GIC ο οποίος είναι υπεύθυνος για την ιατρική ασφάλιση των εργαζομένων της πολιτείας, δύο δημοσιευμένα και φαινομενικά ανεξάρτητα σύνολα δεδομένων, για να ανευρεθεί ο ιατρικός φάκελος του κυβερνήτη της πολιτείας Μασαχουσέτης William Weld . Συγκεκριμένα, τα στοιχεία του τότε κυβερνήτη της Μασαχουσέτης ήταν καταχωρημένα στον οργανισμό ασφάλισης για την υγεία. Ο κυβερνήτης ζούσε στο Cambridge της Μασαχουσέτης. Σύμφωνα με τους καταλόγους ψηφοφορίας, έξι άτομα ήταν γεννημένα την ίδια ημερομηνία με τον κυβερνήτη, μόνο τρία από αυτά ήταν άντρες και μόνο ο κυβερνήτης είχε το συγκεκριμένο ταχυδρομικό κώδικα.



Σχήμα 3: Συνδυασμός δεδομένων

Η συγκεκριμένη υπόθεση δείχνει πόσο εύκολα μπορεί να προσδιοριστεί μοναδικά μια εγγραφή με απευθείας σύνδεση κοινών χαρακτηριστικών δύο πινάκων. Πιο σύγχρονο παράδειγμα αποτελεί η δυνατότητα αναγνώρισης ενός χρήστη μέσω της διασταύρωσης λογαριασμών του στα κοινωνικά δίκτυα.

Ως αποτέλεσμα στις αρχές της δεκαετίας του 2000, άρχισαν να αναπτύσσονται πολυπλοκότερες μέθοδοι προστασίας της ιδιωτικότητας με πρώτη αυτή της *k*-ανωνυμίας από την Latanya Sweeney (2002) [81]. Τα επόμενα χρόνια χαρακτηρίστηκαν τόσο από επεκτάσεις της *k*-ανωνυμίας όσο και από τη δημιουργία νέων τεχνικών για τη διασφάλιση της ιδιωτικότητας των προσώπων σε σύνολα δεδομένων, έχοντας ως συνέπεια τη δημιουργία ενός νέου κλάδου της επιστήμης των υπολογιστών και ειδικότερα των βάσεων δεδομένων ο οποίος είναι πλέον γνωστός ως κλάδος «ιδιωτικότητας δεδομένων – ανωνυμοποίησης δεδομένων» (data privacy – data anonymization).

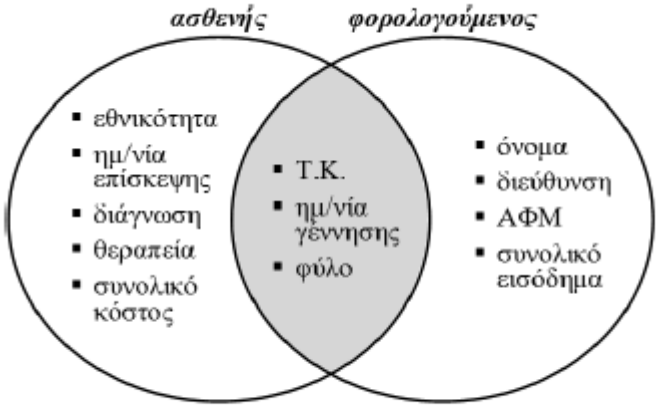
Βασική ιδέα του κλάδου της ανωνυμοποίησης δεδομένων είναι ο μετασχηματισμός των αρχικών αυτών δεδομένων σε μία μορφή που αντιμετωπίζει τους κινδύνους περιορίζοντας την απώλεια πληροφορίας. Οι εν λόγω κίνδυνοι αφορούν τρεις παραμέτρους. Πρώτον, την αποκάλυψη συμμετοχής, όταν και μόνο όταν η συμμετοχή στα δημοσιευμένα δεδομένα είναι ευαίσθητη πληροφορία. Δεύτερον, την αναγνώριση, όταν εντοπίζουμε μια εγγραφή που αναφέρεται σε ένα πρόσωπο. Και τρίτον, τη συσχέτιση, όταν συσχετίζουμε μια ευαίσθητη τιμή με ένα πρόσωπο.

9.2 Επιθέσεις σύνδεσης (linking attacks) και η τεχνική της *k*-Ανωνυμίας

Η πρώτη τεχνική προστασίας που προτάθηκε για την ανωνυμοποίηση δεδομένων ήταν αυτή της *k*-ανωνυμίας, η οποία σχεδιάστηκε για την προστασία από μία κατηγορία επιθέσεων που χαρακτηρίζονται ως «επιθέσεις σύνδεσης».

Ορισμός: Μια βάση δεδομένων ονομάζεται *k*-ανώνυμη εάν δεν υπάρχει καμία ερώτηση που να μπορεί να εξάγει λιγότερες από *k* εγγραφές από αυτή.

Η τιμή του *k* καθορίζει την αναλογία μεταξύ της απώλειας πληροφορίας και ισχύος της ανωνυμίας των ανωνυμοποιημένων δεδομένων.



Σχήμα 4: *k*-ανώνυμη βάση δεδομένων

Ένας προς δημοσίευση πίνακας RT(A1, A2,….An) με ψευδο-αναγνωριστικό QI_{RT}= (A1, A2,….Aj) το σύνολο των γνωρισμάτων A1, A2,…., Aj, ικανοποιεί την *k*-ανωνυμία αν κάθε ακολουθία τιμών στον πίνακα RT[QI_{RT}] του ψευδο-αναγνωριστικού εμφανίζεται τουλάχιστον *k* φορές.

Ως ψευδο-αναγνωριστικό του πίνακα δεδομένων RT ορίζεται το ελάχιστο σύνολο γνωρισμάτων του, τα οποία σε συνδυασμό με την εξωτερική πληροφορία μπορούν να οδηγήσουν στην αναγνώριση της ταυτότητας κάποιας εγγραφής.

Κάτι τέτοιο πράγματι αποτρέπει σε ικανοποιητικό βαθμό επιθέσεις κατά τις οποίες επιχειρείται η αναγνώριση της ταυτότητας ενός ατόμου που συμμετέχει στα δεδομένα. Όταν τα δεδομένα που δημοσιεύονται ικανοποιούν την *k*-ανωνυμία, για κάθε συνδυασμό τιμών στα γνωρίσματα του ψευδο-

αναγνωριστικού, θα υπάρχουν το λιγότερο *k* εγγραφές που θα τον περιέχουν. Κάθε ομάδα από πλειάδες που εμφανίζουν ταυτόσημες τιμές στα γνωρίσματα του ψευδο-αναγνωριστικού, ονομάζεται κλάση ισοδυναμίας. Συνεπώς, ένας πίνακας από δεδομένα όταν ικανοποιεί την *k*-ανωνυμία αποτελείται από κλάσεις ισοδυναμίας (κάθε σύνολο εγγραφών που έχουν ίδιες τιμές ψευδο-αναγνωριστικών) όπου σε καθεμία εμφανίζεται ένας συνδυασμός τιμών στα γνωρίσματα του ψευδο-αναγνωριστικού. Ο επιτιθέμενος πάνω σε δεδομένα που δημοσιεύονται σε τέτοια μορφή δεν μπορεί με βεβαιότητα να αναγνωρίσει μοναδικά μια εγγραφή, μέσω αυτών των τιμών των γνωρισμάτων, καθώς θα οδηγείται κάθε φορά σε τουλάχιστον *k* εγγραφές που παίρνουν τις ζητούμενες τιμές στα γνωρίσματα αυτά.

Στόχος, λοιπόν, της προστασίας ιδιωτικότητας είναι να μειωθεί η πιθανότητα να προσδιοριστεί μοναδικά μια συγκεκριμένη οντότητα, ακόμα και με τη διασταύρωση δημοσιευμένων εγγράφων που μπορεί να είναι ανωνυμοποιημένες. Για να γίνει αυτό, πρέπει ουσιαστικά να υπάρχει μία μέγιστη πιθανότητα το πολύ *k*, ένας επιτιθέμενος να μπορεί να ανακαλύψει με κάποια σύνδεση πινάκων, σε ποιο άτομο ανήκει μια εγγραφή ή σύνολο εγγραφών.

Με τη μέθοδο της *k*-ανωνυμίας εξασφαλίζεται ότι, η πιθανότητα ανακάλυψης της ταυτότητας μιας εγγραφής είναι το πολύ 1/*k*.

Επειδή είναι σπάνια τα σύνολα δεδομένων που συλλέγονται να ικανοποιούν την *k*-ανωνυμία στην αρχική τους μορφή, ο τομέας της προστασίας της ιδιωτικότητας έχει αναπτύξει τεχνικές και αλγορίθμους ώστε να τροποποιούνται τα δεδομένα προς μία μορφή τέτοια ώστε να ικανοποιείται η *k*-ανωνυμία. Συνήθως, από τις διαδικασίες αυτές προκύπτει μια νέα έκδοση του πίνακα δεδομένων. Εξάλλου η *k*-ανωνυμία έχει μελετηθεί κυρίως για δεδομένα πινάκων.

Οι μετασχηματισμοί δεδομένων που χρησιμοποιούνται κατά την ανωνυμοποίηση με την τεχνική της *k*-ανωνυμίας είναι οι κάτωθι:

- **Η μέθοδος της Γενίκευσης (Generalization)**

  Η μέθοδος της γενίκευσης συνιστά μια πολύ χρήσιμη τεχνική στο χώρο της προστασίας της ιδιωτικότητας. Με τη χρήση της επιτυγχάνεται η αντικατάσταση της αρχικής τιμής ενός πεδίου με μια άλλη τιμή πιο γενική. Αυτό έχει ως αποτέλεσμα να διατηρείται μέρος της πληροφορίας που περιέχει η αρχική τιμή, χωρίς να αλλοιώνεται πλήρως. Με τη σειρά

της αυτή η γενικευμένη τιμή μπορεί να γενικευτεί ξανά σε μια πιο γενικευμένη τιμή διατηρώντας πάλι την ίδια σημασιολογία με την αρχική τιμή του πεδίου κοκ. Για τη γενίκευση ακολουθείται ένα δέντρο ιεραρχίας όπου τα φύλλα απεικονίζονται στην τιμή του γονέα, αυτή στου δικού του γονέα πηγαίνοντας μέχρι τη ρίζα του δέντρου που σημασιολογικά αντιστοιχεί σε όλες τις τιμές.

- **Η μέθοδος της Απόκρυψης (Suppression)**

Σε αυτήν την περίπτωση αφαιρούνται δεδομένα από το σύνολο εγγραφών προκειμένου να ελαχιστοποιηθεί το επίπεδο γενίκευσης και να μειωθεί η απώλεια πληροφορίας στα δεδομένα.

Ημερομηνία Γεννήσεως	Φύλο	Ταχυδρ. Κώδικας
1988	Άρρεν	53771
1978	Θήλυ	53772
1987	Άρρεν	53771
1966	Άρρεν	53710
1999	Άρρεν	43654
1976	Θήλυ	53712
1966	Άρρεν	53711

Suppression + Generalization

Ημερομηνία Γεννήσεως	Φύλο	Ταχυδρ. Κώδικας
198*	Άρρεν	53771
197*	Θήλυ	53772
198*	Άρρεν	53771
1966	Άρρεν	5371*
197*	Θήλυ	53772
1966	Άρρεν	5371*

Σχήμα 5 : Απόκρυψη εγγραφών κατά τη διαδικασία ανωνυμοποίησης

9.3 Επιθέσεις ομογενών δεδομένων και η τεχνική της ℓ -πολυμορφίας

Η *k*-ανωνυμία δέχεται δύο ειδών επιθέσεων: την επίθεση ομοιογένειας ή ομοιότητας (similarity ή homogeneity attack) και την επίθεση γνωστικού υποβάθρου (background knowledge attack).

- ***Επίθεση ομοιογένειας***: έστω ότι δύο γείτονες με διαφορετικά χαρακτηριστικά. Ο Α αρρωσταίνει και πηγαίνει στο νοσοκομείο με ασθενοφόρο. Ο Β θέλει να μάθει τι συνέβη στο γείτονά του. Μέσω των δεδομένων του νοσοκομείου και κάνοντας συσχετίσεις με παρόμοιες τιμές, μπορεί να συμπεράνει το πρόβλημα υγείας του γείτονά του.
  Η επίθεση αυτή μπορεί επομένως να συμβεί όταν υπάρχει μικρή ποικιλομορφία στα ευαίσθητα χαρακτηριστικά μέσα σε μια κλάση ισοδυναμίας. Στη περίπτωση αυτή, το ευαίσθητο χαρακτηριστικό όλων των χρηστών στην κλάση ισοδυναμίας γίνεται γνωστό με μεγάλη βεβαιότητα.

- ***Επίθεση γνωστικού υποβάθρου***: έστω ότι ο Α που εισήχθη στο νοσοκομείο είναι Ιάπωνας. Τα στοιχεία του βρίσκονται στον πίνακα του νοσοκομείου καθώς γνωρίζει την ηλικία του και τον ταχυδρομικό του κώδικα. Σύμφωνα με τις εγγραφές ο Α μπορεί να πάσχει είτε από καρδιοπάθεια είτε από αμυγδαλίτιδα. Είναι όμως γνωστό ότι οι Ιάπωνες δεν αντιμετωπίζουν συχνά προβλήματα με καρδιοπάθειες, οπότε εύκολα συμπεραίνεται ότι ο Α εισήχθη στο νοσοκομείο με αμυγδαλίτιδα.
  Η επίθεση αυτή μπορεί επομένως να συμβεί όταν υπό την παρουσία βασικών γνώσεων και ιδιοτήτων μπορεί να συμβεί αποκάλυψη ταυτότητας. Για παράδειγμα, γνωρίζοντας ότι οι φίλοι ενός ατόμου είναι φιλελεύθεροι, τότε καθίσταται πολύ πιθανό ότι αυτό το άτομο είναι επίσης φιλελεύθερο.

Η μεθοδολογία που έχει προταθεί για την επίλυση των πιο πάνω αδυναμιών της *k*-ανωνυμίας και μετριάζει το πρόβλημα της αποκάλυψης ευαίσθητων χαρακτηριστικών είναι η ℓ -πολυμορφία (ℓ -diversity) που είναι εγγενές στοιχείο της *k*-ανωνυμίας και εισήχθη ως μια ισχυρότερη έννοια διασφάλισης της ιδιωτικότητας.

Η ℓ-πολυμορφία προσφέρει ισχυρή προστασία της ιδιωτικότητας ακόμα και όταν αυτός που δημοσιεύει τα δεδομένα δεν ξέρει τι είδους γνώση έχει ο αντίπαλος. Η *k*-ανωνυμία δεν είναι σε θέση να μας εξασφαλίσει ότι ο επιτιθέμενος δεν θα μπορέσει να εξάγει με επιτυχία κάποιες πληροφορίες για κάποιες εγγραφές. Οι ιδιότητες, τις οποίες δεν θέλουμε να ανακαλύψει ο

αντίπαλος, λέγονται ευαίσθητες. Η κύρια ιδέα είναι η απαίτηση ότι οι τιμές των ευαίσθητων χαρακτηριστικών σε κάθε ομάδα παρουσιάζονται με τέτοιο τρόπο ώστε να μην αφήνουν περιθώρια ανακάλυψής τους. Ο στόχος επομένως της ℓ -πολυμορφίας δεν είναι μόνο η ασφάλεια της ταυτότητας μίας εγγραφής, αλλά και η διασφάλιση, ότι από ένα σύνολο εγγραφών δεν θα μπορούμε να βρούμε εύκολα κάποια συγκεκριμένα στοιχεία για ένα άτομο. Η μεθοδολογία της ℓ -πολυμορφίας επιτρέπει σε ένα εξωτερικό παράγοντα να ανακαλύψει με πιθανότητα περίπου $1/\ell$ τα ευαίσθητα δεδομένα ενός ατόμου, ανεξάρτητα σε ποια εγγραφή ανήκει αυτό το άτομο.

Σε ότι αφορά την αλγοριθμική υλοποίηση της προσέγγισης αυτής, τροποποιείται ο αλγόριθμος της *k*-ανωνυμίας ώστε αντί να ελέγχεται αν η γενίκευση ενός πίνακα πληροί την *k*-ανωνυμία, ελέγχεται εν πληροί την ℓ-πολυμορφία. Επειδή αυτό στηρίζεται στη μέτρηση των ευαίσθητων γνωρισμάτων στις κλάσεις ισοδυναμίας, ο αλγόριθμος αυτός είναι πιο αποδοτικός.

9.4 Η τεχνική της ανατομίας

Με την ανωνυμοποίηση των δεδομένων χάνεται ένα μεγάλο μέρος της πληροφορίας που περιέχουν, με αποτέλεσμα να μην μπορούν να αξιοποιηθούν λόγω της γενίκευσης των τιμών που πραγματοποιείται ούτως ώστε να δημιουργηθούν κλάσεις ισοδυναμίας. Εκτός αυτού πολλές φορές δεν προστατεύεται η συσχέτιση της κάθε εγγραφής με την ευαίσθητη τιμή της.

Η τεχνική της ανατομίας προστατεύει την ιδιωτικότητα γατί με τον τρόπο αυτό, αν και δημοσιεύονται οι ακριβείς τιμές των χαρακτηριστικών, δεν υπάρχει στα δημοσιευμένα δεδομένα η ακριβής αντιστοίχησή τους με το ευαίσθητο γνώρισμα, ικανοποιώντας ταυτόχρονα την ℓ -πολυμορφία με ό,τι προστασία αυτή συνεπάγεται.

Σύμφωνα με την τεχνική της ανατομίας δημοσιεύονται δύο ξεχωριστοί πίνακες, ένας πίνακας ψευδο-αναγνωριστικών και ένας με το ευαίσθητο χαρακτηριστικό. Αρχικά χωρίζονται τα δεδομένα σε κλάσεις ισοδυναμίας και αποδίδεται ένας αριθμός σε κάθε μία από αυτές. Έπειτα κατασκευάζεται ένας πίνακας που περιέχει όλες τις τιμές των ψευδο-αναγνωριστικών και έναν αριθμό που προσδιορίζει σε ποια κλάση ισοδυναμίας ανήκει η εγγραφή και ένας πίνακας που περιέχει για κάθε κλάση ισοδυναμίας τις τιμές του

ευαίσθητου γνωρίσματος που συναντώνται μέσα στην κλάση αλλά και το σύνολο των εγγραφών της κλάσης που αντιστοιχούν σε κάθε μία. Οι παραπάνω πίνακες είναι εύκολο να κατασκευαστούν, δίνοντας έτσι στη μέθοδο μια απλή υλοποίηση με μικρή πολυπλοκότητα συγκριτικά με τις υπόλοιπες μεθόδους.

Με αυτόν τον τρόπο, ο επιτιθέμενος γνωρίζοντας κάποιες τιμές του ψευδο-αναγνωριστικού, μπορεί μεν να προσδιορίσει αν το άτομο που αναζητά ανήκει σε κάποια εγγραφή, αλλά δεν μπορεί να συσχετίσει με απόλυτη ακρίβεια και βεβαιότητα καμία εγγραφή με ευαίσθητη τιμή της κλάσης ισοδυναμίας που ανήκει, αφού κάθε ομάδα ικανοποιεί την ℓ -πολυμορφία.

Ωστόσο, παρά την αποδοτικότητα και τη μη απώλεια δεδομένων, η τεχνική αυτή της ανάλυσης παρουσιάζει ένα σημαντικό μειονέκτημα καθ' ότι ο επιτιθέμενος δύναται να αποκτήσει περισσότερη και πιο ακριβή γνώση από ότι ήδη έχει για τα γνωρίσματα του ψευδο-αναγνωριστικού με τον κίνδυνο να την χρησιμοποιήσει σε μία επίθεση σύνδεσης ή απλά για να επιβεβαιώσει την παρουσία κάποιου ατόμου στον πίνακα που δημοσιεύθηκε. Το μειονέκτημα αυτό παρουσιάζεται γιατί ουσιαστικά η ανάπτυξη της τεχνικής της ανάλυσης στηρίχθηκε σε δυο υποθέσεις. Κατά πρώτον, θεωρείται ότι ο επιτιθέμενος έχει γνώση όλων των τιμών του ψευδο-αναγνωριστικού και αναζητά την τιμή του ευαίσθητου δεδομένου, και κατά δεύτερον, ο επιτιθέμενος γνωρίζει με βεβαιότητα ότι το άτομο που αναζητά σχετίζεται με αυτά τα δεδομένα και υπάρχει σε κάποια εγγραφή [82].

9.5 Η τεχνική της δ -παρουσίας

Μια άλλη τεχνική η οποία χρησιμοποιείται για την προστασία της ιδιωτικότητας σε βάσεις δεδομένων είναι η δ -παρουσία. Μέχρι τώρα ο επιτιθέμενος γνώριζε πληροφορίες για ένα άτομο και ήταν σίγουρος ότι τα στοιχεία του ατόμου αυτού ήταν δημοσιευμένα στο σύνολο εγγραφών. Σε κάποιες περιπτώσεις όμως αυτό δεν συμβαίνει. Σχετικό παράδειγμα αποτελεί η βάση η οποία περιλαμβάνει όλους τους διαβητικούς μιας χώρας. Ο επιτιθέμενος δε μπορεί να είναι σίγουρος αν το θύμα περιλαμβάνεται σε αυτή τη βάση καθώς δε γνωρίζει αν πάσχει από τη συγκεκριμένη ασθένεια.

Η τεχνική της δ -παρουσίας εγγυάται ότι με την ανωνυμοποίηση της βάσης δεδομένων, ο επιτιθέμενος δεν θα είναι σε θέση να προσδιορίσει αν

κάποιο άτομο συμπεριλαμβάνεται στη συγκεκριμένη βάση με βεβαιότητα μεγαλύτερη από δ.

Οι δύο αλγόριθμοι για την τεχνική της δ-παρουσίας είναι αυτός της μονοδιάστατης παρουσίας (Single-Dimensional Presence Algorithm- SPALM) και ο αλγόριθμος πολυδιάστατης παρουσίας (Multi-Dimensional Presence Algorithm- MPALM).

9.6 Επιθέσεις ανομοιόμορφων δεδομένων/ομοιότητας - Η τεχνική της *t* -εγγύτητας

Πάρα ταύτα, ένα πρόβλημα που υφίσταται η ℓ -πολυμορφία είναι ότι έχει περιορισμούς στις προϋποθέσεις για τις γνώσεις των αντιπάλων. Η *t* -εγγύτητα τυποποιεί την ιδέα του γνωστικού υπόβαθρου απαιτώντας η κατανομή του κάθε ευαίσθητου χαρακτηριστικού σε κάθε κλάση ισοδυναμίας να είναι κοντά στην κατανομή του χαρακτηριστικού στο γενικό πίνακα, δηλαδή η απόσταση μεταξύ των δύο κατανομών να μην υπερβαίνει ένα όριο *t*. Σαν αποτέλεσμα, περιορίζεται αισθητά η ποσότητα των σημαντικών πληροφοριών ενός χρήστη που μπορεί να μάθει ένας παρατηρητής.

Η *t*-εγγύτητα χρησιμοποιείται σε περιπτώσεις επιθέσεων ανομοιόμορφων δεδομένων (skewness attack) στις οποίες ο επιτιθέμενος κερδίζει πληροφορίες για ένα ευαίσθητο χαρακτηριστικό γνωρίζοντας τη συνολική κατανομή των τιμών του γνωρίσματος αυτού στον πληθυσμό που μελετάται.

Η τεχνική της *t*-εγγύτητας είναι ιδιαίτερα αποτελεσματική και σε επιθέσεις ομοιότητας, οι οποίες αφορούν την περίπτωση όπου οι τιμές του ευαίσθητου γνωρίσματος είναι διαφορετικές αλλά νοηματικά όμοιες και επομένως ο επιτιθέμενος μπορεί να μάθει σημαντικές πληροφορίες.

9.7 Επιθέσεις γνώσης σε πίνακες με δυναμικά δεδομένα - Η τεχνική της *m* -αμεταβλητότητας

Η τεχνική της *m* -αμεταβλητότητας αποτελεί μία επέκταση της *ℓ* -πολυμορφίας ούτως ώστε να γίνει σωστός χειρισμός των δυναμικών δεδομένων, στην περίπτωση δηλαδή που εισάγονται εγγραφές στη βάση ή στην περίπτωση που διαγράφονται. Αυτό αποτελεί σημαντικό πρόβλημα για μία βάση η οποία πρέπει να μένει πάντα ενημερωμένη.

Έστω ότι ένα νοσοκομείο δημοσιεύει τα δεδομένα των ασθενών του στον πίνακα Τ (1). Στη συνέχεια τα ανωνυμοποιεί δημοσιεύοντας τον πίνακα Τ* (1). Μετά από έξι μήνες με βάση τα δεδομένα του πίνακα Τ (2) δημοσιεύεται ο Τ *(2). Παρόλο όμως που και οι δύο αυτοί πίνακες ικανοποιούν τόσο την *k*-ανωνυμία όσο και την *ℓ* -πολυμορφία, ο επιτιθέμενος μπορεί να προσδιορίσει μοναδικά την ταυτότητα ενός ασθενή.

ΠΙΝΑΚΑΣ ΔΕΔΟΜΕΝΩΝ Τ (1) ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ			
Όνομα	Ηλικία	Ταχ. Κώδικας	Ασθένεια
Νίκος	22	12000	Έλκος
Ευγενία	23	14000	Διαβήτης
Βασίλης	24	18000	Γρίπη
Δημήτρης	25	25000	Πυρετός
Γιώργος	45	20000	Γρίπη
Κατερίνα	38	27000	Πυρετός
Θοδώρα	39	25000	Έλκος
Αλέξης	49	35000	Γρίπη
Ματίνα	45	26000	Πυρετός
Αντώνης	60	33000	Έλκος
Μιχάλης	52	34000	Πυρετός

ΓΕΝΙΚΕΥΜΕΝΟΣ ΠΙΝΑΚΑΣ Τ* (1) ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ			
Κλάση	Ηλικία	Ταχ. Κώδικας	Ασθένεια
1	[22,23]	[12K-14K]	Έλκος
1	[22,23]	[12K-14K]	Διαβήτης
2	[24,25]	[18K-25K]	Γρίπη
2	[24,25]	[18K-25K]	Πυρετός
3	[38,45]	[20K-27K]	Γρίπη
3	[38,45]	[20K-27K]	Πυρετός
3	[38,45]	[20K-27K]	Έλκος
4	[45,49]	[26K-35K]	Γρίπη
4	[45,49]	[26K-35K]	Πυρετός
5	[52,60]	[33K-34K]	Έλκος
5	[52,60]	[33K-34K]	Πυρετός

Σχήμα 6: Αρχικός και γενικευμένος πίνακας κατά την πρώτη δημοσίευση

ΠΙΝΑΚΑΣ ΔΕΔΟΜΕΝΩΝ Τ (2) ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ			
Όνομα	Ηλικία	Ταχ. Κώδικας	Ασθένεια
Νίκος	22	12000	Έλκος
Νιόβη	25	21000	Γρίπη
Θανάσης	54	31000	Έλκος
Δημήτρης	25	25000	Πυρετός
Γιώργος	45	20000	Γρίπη
Μαρία	46	30000	Πυρετός
Θοδώρα	39	25000	Έλκος
Γιώργος	60	44000	Πυρετός
Ματίνα	47	26000	Πυρετός
Μαρίνος	65	36000	Πυρετός
Μιχάλης	52	34000	Πυρετός

ΓΕΝΙΚΕΥΜΕΝΟΣ ΠΙΝΑΚΑΣ Τ* (2) ΙΑΤΡΙΚΑ ΔΕΔΟΜΕΝΑ			
Κλάση	Ηλικία	Ταχ. Κώδικας	Ασθένεια
1	[22,25]	[12K-25K]	Έλκος
1	[22,25]	[12K-25K]	Γρίπη
1	[22,25]	[12K-25K]	Πυρετός
2	[39,45]	[20K-25K]	Έλκος
2	[39,45]	[20K-25K]	Γρίπη
3	[46,47]	[26K-30K]	Πυρετός
3	[46,47]	[26K-30K]	Πυρετός
4	[52,54]	[31K-34K]	Έλκος
4	[52,54]	[31K-34K]	Πυρετός
5	[60,65]	[36K-44K]	Πυρετός
5	[60,65]	[36K-44K]	Πυρετός

Σχήμα 7: Αρχικός και γενικευμένος πίνακας κατά τη δεύτερη δημοσίευση

Στον πίνακα δεδομένων Τ (2) έχουν διαγραφεί οι ασθενείς Ευγενία, Βασίλης, Κατερίνα, Αλέξης και Αντώνης και έχουν προστεθεί οι ασθενείς Νιόβη, Θανάσης, Μαρία, Γιώργος και Μαρίνος. Παρατηρούμε πως παρόλο που και οι δύο δημοσιευμένοι πίνακες ικανοποιούν την 2-ανωνυμία και την 2-πολυμορφία, ο επιτιθέμενος μπορεί να προσδιορίσει μοναδικά την ταυτότητα ενός ασθενή με συσχέτιση των δύο πινάκων. Για παράδειγμα γνωρίζοντας πως ο Νίκος με ηλικία 22 ετών και ταχυδρομικό κώδικα 12000 εισήχθη στο νοσοκομείο και η θεραπεία του κράτησε πάνω από έξι μήνες, μπορεί να βγάλει συμπέρασμα για την ασθένειά του. Από τον πρώτο πίνακα ο επιτιθέμενος γνωρίζει πως ο Νίκος πάσχει είτε από έλκος είτε από διαβήτη και από το δεύτερο πίνακα γνωρίζει πως ο Νίκος πάσχει είτε από έλκος είτε από γρίπη είτε απλά έχει πυρετό. Εύκολα συμπεραίνει επομένως, πως ο Νίκος πάσχει από έλκος.

Καταλήγουμε επομένως πως οι μέχρι τώρα τεχνικές ανωνυμοποίησης δεν έχουν προβλέψει τα μη στατικά, δυναμικά δεδομένα. Για αυτό το σκοπό διατυπώθηκε η τεχνική της *m*-αμεταβλητότητας, σύμφωνα με την οποία ο πίνακας Τ *(2) αντικαθίσταται από έναν Τ (3) ο οποίος περιλαμβάνει και δύο πλαστές εγγραφές. Για την ακρίβεια η *m*-αμεταβλητότητα απαιτεί την ικανοποίηση της ℓ -πολυμορφίας και ταυτόχρονα μια εγγραφή να ανήκει πάντα σε μία κλάση ισοδυναμίας, η οποία έχει το ίδιο σύνολο ευαίσθητων δεδομένων για όλες τις δημοσιεύσεις.

Είναι σημαντικό, ωστόσο, να μην αλλοιωθεί η πραγματική πληροφορία καθώς σε αυτήν θα στηριχθούν οι μετέπειτα έρευνες. Έτσι, μαζί με τον πίνακα Τ (3) δημοσιεύεται και ένας ακόμα πίνακας, ο οποίος αντιστοιχεί σε κάθε κλάση ισοδυναμίας με τον αριθμό των πλαστών εγγράφων που περιέχονται σε αυτήν.

Ωστόσο, ακριβώς επειδή πρόκειται για μία τεχνική με συνεχείς γενικεύσεις των τιμών των γνωρισμάτων αλλά και συσσώρευση πλαστών εγγράφων, χρήζει ιδιαίτερης προσοχής.

9.8 Επιθέσεις γνώσης σε πίνακες με πληροφορίες οργανωμένες σε σύνολα - Η τεχνική της k^m-ανωνυμίας

Μια νέα τεχνική διαφύλαξης της ιδιωτικότητας είναι εκείνη της k^m-ανωνυμίας, όπου τα δεδομένα δεν διακρίνονται σε ευαίσθητα και μη-ευαίσθητα, αλλά μπορούν να λειτουργήσουν ταυτόχρονα και σαν ψευδο-αναγνωριστικά και σαν ευαίσθητα δεδομένα, ανάλογα με την προοπτική του αντιπάλου [83]. Και αυτό συμβαίνει διότι η διαθέσιμη πληροφορία που μπορεί να κατέχει ο επιτιθέμενος ενδέχεται να έχει πολλές μορφές. Παράλληλα, τα μοντέλα των δημοσιευμένων δεδομένων μπορεί να διαφέρουν κάθε φορά, με αποτέλεσμα η κάθε περίπτωση να απαιτεί διαφορετική επεξεργασία προκειμένου να εξασφαλίζεται η ιδιωτικότητα των βάσεων δεδομένων.

Ορισμός (k^m-ανωνυμία)

Έστω ότι ένας επιτιθέμενος έχει γνώση m το πολύ αντικειμένων, σε δεδομένα οργανωμένα σε σύνολα. Αν για κάθε σύνολο m ή λιγότερων αντικειμένων, υπάρχουν τουλάχιστον k δοσοληψίες που να περιέχουν αυτό το σύνολο, θα λέμε πως τα δεδομένα ικανοποιούν την αρχή της k^m-ανωνυμίας.

Για την διαδικασία της k^m-ανωνυμίας επιλέγεται η τεχνική της ιεραρχικής γενίκευσης, σύμφωνα με την οποία μια τιμή στη βάση δεδομένων αντικαθίσταται με μια πιο γενική τιμή η οποία περιέχει την αρχική, χωρίς να αλλάζει η σημασιολογία της.

Ένα παράδειγμα όπου εφαρμόζεται η συγκεκριμένη τεχνική ανωνυμοποίησης αποτελεί μία βάση η οποία αποθηκεύει τις καθημερινές αγορές των πελατών μιας υπεραγοράς. Αν ο επιτιθέμενος γνωρίζει ένα μέρος των αγορών ενός πελάτη, μπορεί με ευκολία να προσδιορίσει τις υπόλοιπες αγορές του. Έστω η παρακάτω δημοσιευμένη βάση δεδομένων.

Δημήτρης	{φέτα, σαμπουάν, ρύζι}
Βάσω	{γιαούρτι, σαμπουάν}
Νίκος	{γιαούρτι, σαμπουάν, ρύζι}
Μάγδα	{φέτα,ρύζι}

Σχήμα 8: Βάση δεδομένων υπεραγοράς

Αν ο Νίκος έτυχε να βρεθεί την ίδια μέρα και ώρα στην υπεραγορά με τον Δημήτρη και είδε στο καλάθι του την φέτα και το ρύζι, μπορεί να συμπεράνει και τις υπόλοιπες αγορές του [84].

Σύμφωνα με την τεχνική της k^m-ανωνυμίας υποθέτουμε πως έχουμε μία ιεραρχία γενίκευσης ως εξής: {φέτα, γιαούρτι} → {γαλακτοκομικά προϊόντα}. Τα δεδομένα μας σύμφωνα με τον ορισμό είναι 3^2- ανώνυμα. Πλέον από τη νέα βάση δεδομένων ο επιτιθέμενος δεν είναι σε θέση να γνωρίζει ποια από τις τρείς δοσοληψίες ανήκει στο Δημήτρη.

Δημήτρης	{γαλακτομικά προϊόντα, σαμπουάν, ρύζι}
Βάσω	{γαλακτομικά προϊόντα, σαμπουάν,}
Νίκος	{γαλακτομικά προϊόντα, σαμπουάν, ρύζι}
Μάγδα	{γαλακτοκομικά προϊόντα, ρύζι}

Σχήμα 9: k^m-ανωνυμοποιημένη βάση δεδομένων υπεραγοράς

ΕΠΙΛΟΓΟΣ

Με την πάροδο του χρόνου και υπό την επίδραση της εξέλιξης των νέων τεχνολογιών, γίνεται όλο και περισσότερο κατανοητό ότι η ιδιωτικότητα ως αξίωση σεβασμού του απορρήτου παρέχει αναγκαία μεν, επαρκή ωστόσο προστασία στο άτομο. Είναι προφανές ωστόσο πως μέσω της κασσάνδρειας προφητείας του Orwell (1948) και του Μεγάλου Αδελφού, η γεωμετρική αύξηση των δυνατοτήτων επεξεργασίας και συσχέτισης της προσωπικής πληροφορίας τελεί σε σχέση αντιστρόφως ανάλογη προς την ικανότητα του ατόμου να έχει εποπτεία της χρήσης των πληροφοριών που το αφορούν.

Πλέον, ο όγκος των πληροφοριών είναι τεράστιος. Κάθε δύο χρόνια δημιουργούνται τόσες πληροφορίες από τους χρήστες του διαδικτύου όσες από την αρχή της ανθρώπινης ύπαρξης ως το 2003 [85]. Υπολογίζεται ότι περίπου 2,5 πεντάκις εκατομμύρια bytes δεδομένων δημιουργούνται καθημερινά σε οποιαδήποτε αδόμητη ή δομημένη μορφή, είτε αυτή είναι κείμενο, δεδομένα κίνησης, ήχος, βίντεο και πολλά ακόμα, προερχόμενα από διάφορες και διαφορετικές πηγές όπως αισθητήρες συλλογής πληροφοριών, δημοσιεύσεις σε κοινωνικά δίκτυα, ψηφιακές φωτογραφίες, εγγραφές, αγοραπωλησίες, κινητά τηλέφωνα και σήματα γεωγραφικού εντοπισμού [86].

Σύμφωνα με την ετήσια μελέτη «Visual Networking Index Global Forecast and Service Adoption» της αμερικανικής εταιρείας Cisco για την παγκόσμια διακίνηση δεδομένων κατά την περίοδο 2014-2019, η παγκόσμια διακίνηση δεδομένων θα αυξηθεί σχεδόν τρεις φορές, κυρίως λόγω του αυξημένου αριθμού χρηστών του διαδικτύου και των «έξυπνων» συσκευών, αλλά και της αύξησης των ευρυζωνικών ταχυτήτων.

Επίσης, μέσα στα επόμενα πέντε χρόνια αναμένεται να δεκαπλασιαστεί η διακίνηση δεδομένων μέσω των δικτύων κινητής τηλεφωνίας σε παγκόσμιο επίπεδο. Έως το 2019, οι «έξυπνες» αυτές συνδέσεις θα αντιπροσωπεύουν το 97% της παγκόσμιας διακίνησης δεδομένων μέσω των δικτύων κινητής [87].

Το πρόβλημα για την ιδιωτικότητα στην περίπτωση του τεράστιου αυτού όγκου δεδομένων (Big Data) είναι σύνθετο κυρίως διότι το σημαντικό ερώτημα δεν είναι αν τα δεδομένα αυτά αυξάνουν τον κίνδυνο για την ιδιωτικότητα, αλλά αν αλλάζουν αυτόν τον κίνδυνο. Το πρόβλημα επομένως έγκειται όχι στο σκοπό για τον οποίο συλλέχθηκαν, αλλά στην αυξανόμενη δεύτερη χρήση τους και αυτό διότι ακόμα και μετά την ανωνυμοποίησή τους, αποδεικνύεται εύκολος ο επαναπροσδιορισμός των υποκειμένων της επεξεργασίας.

Καταρχάς βασική παράμετρος για την εξασφάλιση και την προστασία της ιδιωτικότητας είναι η θέσπιση νόμων και η ύπαρξη εποπτικών αρχών για τον έλεγχο της τήρησής τους. Αν και ο αριθμός των νομοθετημάτων αυξάνεται, η προστασία των προσωπικών δεδομένων παραμένει μάλλον εξαίρεση στο διεθνές περιβάλλον, καθώς ουσιαστικά εκτός Ευρώπης, λίγες μόνο χώρες έχουν εισαγάγει δεσμευτικούς κανόνες προστασίας προσωπικών δεδομένων. Ωστόσο, το διαδίκτυο εξελίσσεται και πλέον επαφίεται σε εταιρείες όπως το Facebook και η Google να ρυθμίζουν την αγορά. Εδώ και πολλά όμως χρόνια, αρκετές εταιρείες λειτουργούν ενάντια στην προστασία των προσωπικών δεδομένων. Η διεθνοποίηση των διαδικτυακών υπηρεσιών αυξάνει συνεχώς το βαθμό δυσκολίας επιβολής της νομιμότητας [88].

Ο Επίτροπος Ανθρωπίνων Δικαιωμάτων του Συμβουλίου της Ευρώπης Nils Muiznieks υποστηρίζει πως οι εθνικές κυβερνήσεις θα πρέπει να σταματήσουν να κρύβονται πίσω από τις ιδιωτικές εταιρείες που ελέγχουν το διαδίκτυο, για την επιβολή πρακτικών που παραβιάζουν τα ανθρώπινα δικαιώματα. Η ανάγκη για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο και της τρομοκρατίας είναι αδιαμφισβήτητη. Ωστόσο, αυτό δεν μπορεί να γίνει εις βάρος των ανθρωπίνων δικαιωμάτων. Οι κυβερνήσεις θα πρέπει να δείχνουν τόση αποφασιστικότητα στην προάσπιση των προσωπικών δεδομένων, όση δείχνουν και στην καταπολέμηση της τρομοκρατίας.

Μέσα σε αυτό το πλαίσιο ο Πρωθυπουργός της Βρετανίας David Cameron εξετάζει το ενδεχόμενο απαγόρευσης εφαρμογών όπως το WhatsApp και το Snapchat στη χώρα του αν κερδίσει τις ερχόμενες εκλογές του Μαΐου του 2015, όπου κατεβαίνει ως υποψήφιος με το κόμμα των Συντηρητικών. Με δήλωσή του καταδίκασε την ύπαρξη μέσων επικοινωνίας με ισχυρό σύστημα κρυπτογράφησης (end-to-end encryption), τα οποία δεν μπορούν να αποτελέσουν αντικείμενο υποκλοπής από τις αρχές. Τόσο τα κοινωνικά δίκτυα όσο και μεγάλα ειδησεογραφικά μέσα καταδίκασαν το συγκεκριμένο μέτρο υποστηρίζοντας πως θα αποτελέσει απειλή για τη θεμέλιο λίθο του διαδικτύου, την ελευθερία του λόγου.

Ωστόσο, ο Πρωθυπουργός υποστηρίζει πως η συνεργασία των υπηρεσιών ασφαλείας με τεχνολογικούς κολοσσούς και κοινωνικά δίκτυα δύναται να αποτρέψει το βίαιο εξτρεμισμό του διαδικτύου.

Στην άλλη μεριά του Ατλαντικού η κυβέρνηση των Ηνωμένων Πολιτειών της Αμερικής προχωρά στη δημιουργία μιας νέας υπηρεσίας για την παρακολούθηση απειλών στον κυβερνοχώρο, η οποία θα συγκεντρώνει και θα αναλύει πληροφορίες για ένα ευρύ φάσμα κινδύνων. Σκοπός του Κέντρου Συγκέντρωσης και Αξιολόγησης Πληροφοριών και Αντιμετώπισης Απειλών στο

διαδίκτυο (Cyber Threat Intelligence Integration Center, CTIIC) θα είναι η απρόσκοπτη ροή πληροφοριών μεταξύ των υπηρεσιών, συμπεριλαμβανομένων αυτών που είναι υπεύθυνες για το διαμοιρασμό με τον ιδιωτικό τομέα, ούτως ώστε να προστατευθεί η ασφάλεια και ιδιωτικότητα των χρηστών [89].

Παρόλα αυτά, η ασφάλεια στο διαδίκτυο από τις διαρροές, τις παρακολουθήσεις και τις παραβιάσεις των προσωπικών δεδομένων των χρηστών αποτελεί ένα μείζον θέμα όχι μόνο σε κυβερνητικό επίπεδο αλλά και σε επίπεδο εταιρειών. Για το λόγο αυτό, αυτές προχωρούν στην κρυπτογράφηση δεδομένων για να μη μπορούν ούτε και οι ίδιες να έχουν πρόσβαση. Η Apple έκανε by default την κρυπτογράφηση στο IOS8 και στη συνέχεια ακολούθησε η Google με την κρυπτογράφηση του Android Lollipop. Επιπρόσθετα, παρέχουν ολοένα και περισσότερες εγγυήσεις προστασίας της ιδιωτικότητας των χρηστών τους μέσω των πολιτικών ασφάλειάς τους αλλά και νέων λογισμικών και εφαρμογών.

Η ιδιωτική περιήγηση (incognito mode) παρέχει τη δυνατότητα επιλογής στο χρήστη να μην αποθηκεύονται οι ιστότοποι που επισκέπτεται και τα αρχεία που κατεβάζει, οδηγώντας έτσι σε περιήγηση υπό κατάστασης ανωνυμίας.

Σημαντικό ρόλο στη δυνατότητα ανωνυμίας στο διαδίκτυο διαδραματίζει το Tor (The Onion Router), ένα δίκτυο που δημιουργήθηκε προκειμένου να επιτρέπει όχι μόνο την απολύτως μη ανιχνεύσιμη «περιήγηση» των χρηστών στο διαδίκτυο (η ταυτότητα και η γεωγραφική προέλευση του χρήστη αποκρύπτονται μέσω ειδικής τεχνολογίας παραπλάνησης), αλλά και τη δημιουργία αφανών ιστοσελίδων, οι οποίες δεν εμφανίζονται καν στις μηχανές αναζήτησης όπως της Google και των οποίων οι διευθύνσεις λήγουν σε .onion. Με αυτόν τον τρόπο η δυνατότητα ανίχνευσης της δραστηριότητας ενός χρήστη γίνεται εξαιρετικά δύσκολη.

Το Tor απαιτεί ένα ειδικό λογισμικό πλοήγησης, το Tor Browser, για την αξιοποίηση των δυνατοτήτων του. Μάλιστα, όπως σε ένα κρεμμύδι υπάρχουν διαδοχικά στρώματα, έτσι και στο «σκοτεινό» Tor υπάρχουν αλλεπάλληλα στρώματα κρυπτογράφησης.

Το Facebook είναι η πρώτη μεγάλη εταιρεία της Σίλικον Βάλεϊ, η οποία επίσημα ανακοίνωσε την υποστήριξή της στο Tor. Στην περίπτωση αυτή, οι χρήστες θα πρέπει πάντα να συνδέονται με το όνομά τους. Όμως δεν θα είναι δυνατό να εντοπιστεί η τοποθεσία τους ή άλλη πληροφορία σχετική με αυτούς. Η πρόσβαση θα γίνεται στη διεύθυνση facebookcorewwwi.onion.

Αναφορικά με το Facebook, το οποίο παραμένει η πιο δημοφιλής ιστοσελίδα κοινωνικής δικτύωσης παγκοσμίως, η προσπάθεια αυτή ενίσχυσης της ιδιωτικότητας έρχεται σε αντίθεση με τις περισσότερες τεχνικές του. Όπως διαπιστώθηκε πρόσφατα από ερευνητές του Πανεπιστημίου του Κέμπριτζ και του Πανεπιστημίου Στάνφορντ στις ΗΠΑ, ακόμα και τα «likes» είναι σε θέση να εξάγουν συμπεράσματα για την προσωπικότητα ενός χρήστη και να προβλέψουν κάποιες προσωπικές πληροφορίες όπως ο σεξουαλικός προσανατολισμός και οι πολιτικές πεποιθήσεις [90].

Ανεξάρτητα όμως από τις προσπάθειες προστασίας της ιδιωτικότητας των μέσων κοινωνικής δικτύωσης, τα ίδια αυτά μέσα ενθαρρύνουν την αυτοέκθεση και παρέχουν τη δυνατότητα σε άτομα που ίσως δεν είναι στο άμεσο περιβάλλον του χρήστη ή/και βρίσκονται μακριά ή ακόμα και σε άγνωστους, να έχουν πρόσβαση σε πληροφορίες για τους χρήστες τις οποίες ένα δεν ήταν συνδεδεμένοι με αυτούς δε θα μάθαιναν ποτέ.

Οι ίδιοι οι χρήστες παρά τις ανησυχίες ή τις επιφυλάξεις τους σχετικά με τον τρόπο που διαχειρίζονται τα προσωπικά τους δεδομένα από το μέσο κοινωνικής δικτύωσης, θεωρούν ότι διατηρούν τον έλεγχο αυτών μέσα από την αξιοποίηση τω εκάστοτε ρυθμίσεων απορρήτου και παράλληλα γιατί οι ίδιοι αισθάνονται ότι ελέγχουν ταυτόχρονα και το περιεχόμενο που δημοσιεύουν. Υπό αυτή την έννοια, παρόλο που οι ίδιοι αναγνωρίζουν ότι δημοσιεύουν προσωπικά τους δεδομένα, αυτό δεν φαίνεται να τους προσφέρει μεγάλη ανασφάλεια. Αυτό ίσως συμβαίνει γιατί αισθάνονται ότι «δραστηριοποιούνται» σε ένα – θεωρητικά ελεγχόμενο από αυτούς – οικείο περιβάλλον ή γιατί έχουν εμπιστοσύνη στην ικανότητά τους να διαχειριστούν οι ίδιοι τα προσωπικά τους δεδομένα. Τα τελευταία χρόνια αρκετές μελέτες έχουν μελετήσει τη φύση της αυτοέκθεσης αυτής σε σχέση με το κοινωνικό κεφάλαιο (Bourdieu, 1985) που αποκομίζεται (Ellison, Lampe, Steinfeild, Vitak, 2010), τις ανησυχίες για την ιδιωτικότητα και τη φθίνουσα διάκριση δημόσιου/ιδιωτικού (Boyd & Ellison, 2007). Άλλες μελέτες τονίζουν ότι οι αντιλήψεις για την ιδιωτικότητα επηρεάζουν την αυτο-αποκάλυψη στα κοινωνικά μέσα (Krasnova, Spiekermann, Koroleva και Hildebrand, 2010, όπως και Stutzman, Capra και Thompson, 2011). Πιο συγκεκριμένα, επισημαίνουν ότι η ανησυχία για απειλές που έχουν σχέση με την ιδιωτικότητα οδηγεί σε μικρότερο βαθμό αυτο-αποκάλυψης σε αυτά. Οι Thelwall και Wilkinson (2010) σημειώνουν ότι οι χρήστες κοινωνικών μέσων προσαρμόζουν την ορατότητα της διαδικτυακής τους συμπεριφοράς ή περιορίζουν την πρόσβαση στα προφίλ τους. Επιπλέον, η ανησυχία για την ιδιωτικότητα βρέθηκε να έχει μικρή ή καμία συσχέτιση με την αποκάλυψη πληροφοριών στο διαδίκτυο (Taddicken, 2014). Σύμφωνα δε με τους Christofides, Muise και Desmarais (2009) η ανάγκη για δημοφιλία αποτελεί καθοριστικό παράγοντα για την αυτο-αποκάλυψη και ο βαθμός εμπιστοσύνης

και αυτο-εκτίμησης καθορίζουν τον έλεγχο των πληροφοριών. Σε άλλη συναφή μελέτη, οι Liu, Ang και Lwin (2013) ανακάλυψαν ότι ο ναρκισσισμός είναι καθοριστικός παράγοντας που αυξάνει την αποκάλυψη προσωπικών πληροφοριών. Οι Blank, Bolsover και Dubois (2013) υποστηρίζουν, τέλος, ότι «τα νεαρά άτομα είναι πολύ πιθανότερο σε σύγκριση με τους μεγαλύτερους να έχουν πάρει μέτρα να διαφυλάξουν την ιδιωτικότητά τους στις ιστοσελίδες κοινωνικής δικτύωσης» [91].

Πάρα ταύτα, τα τελευταία χρόνια ολοένα και περισσότερα προσωπικά δεδομένα συλλέγονται από διάφορους οργανισμούς προκειμένου να δημοσιοποιηθούν για σκοπούς έρευνας. Ιδιαίτερα με τη ραγδαία ανάπτυξη του διαδικτύου, η συλλογή τέτοιας πληροφορίας στις μέρες μας παρουσιάζεται σε μεγάλο βαθμό και μπορεί να αφορά σε κοινωνικές σχέσεις από διάφορα κοινωνικά δίκτυα, σε ιατρικής φύσης δεδομένα, είτε ακόμα και σε επιχειρηματική και εμπορική δραστηριότητα. Η διαθεσιμότητα όμως τόσο αναλυτικών προσωπικών δεδομένων θέτει σημαντικούς κινδύνους στην ιδιωτικότητα του καθενός. Ακόμη και με την απόκρυψη στοιχείων που προσδιορίζουν μοναδικά ένα άτομο όπως είναι το ονοματεπώνυμο ή ο Αριθμός Φορολογικού Μητρώου (ΑΦΜ), ο συνδυασμός άλλων στοιχείων όπως ο ταχυδρομικός κώδικας, το φύλο και η ηλικία του, θα μπορούσαν να λειτουργήσουν σαν ψευδο-αναγνωριστικά και να οδηγήσουν στην ταυτοποίηση του ατόμου αποκαλύπτοντας ευαίσθητα προσωπικά δεδομένα (ασθένεια, μηνιαία έσοδα κλπ). Ο Paul Ohm, αναπληρωτής καθηγητής στη Νομική σχολή του πανεπιστημίου του Κολοράντο δηλώνει ότι, σχεδόν για κάθε άνθρωπο πάνω στη γη, υπάρχει τουλάχιστον μια πληροφορία αποθηκευμένη σε μια βάση δεδομένων η οποία καταγράφει κάποιο γεγονός της ζωής του. Η πληροφορία αυτή μπορεί εύκολα να χρησιμοποιηθεί από κάποιο κακόβουλο πρόσωπο, προκειμένου να βλάψει το θύμα νομικά και ηθικά. Είτε αυτό πρόκειται για εκβιασμό, είτε για παρενόχληση ή ακόμα και για κλοπή ταυτότητας. Ο τομέας της προστασίας της ιδιωτικότητας ασχολείται με την ανάπτυξη διαφόρων αλγορίθμων και τεχνικών ανωνυμοποίησης, οι οποίοι αφαιρούν αναγνωριστική πληροφορία από τα δεδομένα που παρέχονται έτσι ώστε να μην μπορεί ο επιτιθέμενος να προσδιορίσει μονοσήμαντα ένα άτομο.

Τόσο οι τεχνικές αυτές ανωνυμοποίησης όσο και οι τεχνικές διασφάλισής της, οι οποίες απευθύνονται κυρίως σε αναλυτές και προγραμματιστές πληροφοριακών συστημάτων, στοχεύουν στην προστασία της προσωπικής ταυτότητας και των προσωπικών δεδομένων του χρήστη.

Συμπερασματικά η ιδιωτικότητα βρίσκεται σε μια συνεχή διαδικασία επανακαθορισμού, καθώς διαφαίνεται ότι αλλάζει ο τρόπος με τον οποίο τα άτομα ιεραρχούν τη σημασία των προσωπικών πληροφοριών. Αυτό δεν

σημαίνει ότι οι χρήστες του διαδικτύου δεν ενδιαφέρονται πια για τον έλεγχο των προσωπικών τους δεδομένων καθώς δείχνουν να καταβάλλουν προσπάθειες για να τις προστατεύσουν. Αλλιώς ειπωμένο, το γεγονός της αλληλοδιείσδυσης δημόσιου-ιδιωτικού δεν συνεπάγεται ούτε την ακύρωση της σημασίας της προστασίας της ιδιωτικής σφαίρας ούτε το ότι δεν υφίσταται πλέον ανάγκη προστασίας της. Είναι σαφές όμως, πως οι Τεχνολογίες Πληροφορικής κάθε χρόνο γίνονται ακόμα πιο έξυπνες και με το σημερινό ρυθμό ανάπτυξης είναι αρκετά δύσκολο να προβλέψει κανείς με ακρίβεια πως θα είναι το τοπίο σε μερικές δεκαετίες. Η ιδιωτικότητα του χρήστη του διαδικτύου απειλείται με αυξανόμενο ρυθμό καθώς χρόνο με το χρόνο ανακύπτουν ακόμη περισσότερες ανησυχίες σχετικά με την προστασία της και την ασφάλειά της. Σύμφωνα με έρευνα της Kaspersky για το 2015 αναμένονται τα εξής:

- Επιθέσεις κατά εικονικών συστημάτων πληρωμών, οι οποίες θα μπορούσαν να επεκταθούν και στη νέα λύση Apple Pay.
- Επιθέσεις εναντίον μηχανημάτων ATM.
- Περιστατικά με κακόβουλο λογισμικό, όπου οι τράπεζες παραβιάζονται μέσω στοχευμένων επιθέσεων.
- Περισσότερα περιστατικά όπου επικίνδυνες ευπάθειες σε παλαιούς πηγαίους κώδικες εκθέτουν τις υποδομές του Internet σε επικίνδυνες επιθέσεις.
- Τυφλές επιθέσεις εναντίον δικτυωμένων εκτυπωτών και άλλων διασυνδεδεμένων συσκευών, που μπορούν να βοηθήσουν έναν εξελιγμένο εισβολέα να κάνει συνεχείς και πλάγιες κινήσεις μέσα σε ένα εταιρικό δίκτυο.
- Κακόβουλο λογισμικό που έχει σχεδιαστεί για λειτουργικό OSX να προωθείται μέσω torrents και «πειρατικών» πακέτων λογισμικών.
- Μια στροφή, όπου οι μεγαλύτεροι και πιο θορυβώδεις παράγοντες ψηφιακών απειλών μοιράζονται σε μικρότερες μονάδες, οι οποίες θα λειτουργούν ανεξάρτητα η μία από την άλλη. Με τη σειρά της, η στροφή αυτή θα οδηγήσει σε μια πιο ευρεία βάση επίθεσης, με περισσότερες διαφοροποιημένες επιθέσεις να προέρχονται από περισσότερες πηγές.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. J.C. Raines, "Attack on Privacy", Valley Forge: Judson Press, 1974
2. S.D. Warren and L.D. Brandeis, "The Right to Privacy", Harvard Law Review, 1890
3. S. Rhys and J. Shao, "Privacy and e-commerce: a consumer- centric perspective", Springer Science, 2007
4. A.F. Westin, The right to Privacy, Antheneum, 1967
5. J.S. Mill, "On liberty", Pelican Books, LondonMason, 1974
6. R.O. Mason, "Four Ethical Issues of the Information Age" MIS Quarterly, 1986 and D. O'Neil, "Analysis of Internet Users' Level ofOnline Privacy Concerns", Social Science Computer Review, 2001
7. H.J. Moor, "Towards a theory of privacy in the information age". Computers and Society, 1997
8. http://www.emc.com/campaign/privacy-index/global.htm (Προσπελάστηκε στις 01.12.2014)
9. http://www.nytimes.com/2014/11/26/world/un-urges-protection-of-privacy-in-digital-era.html?ref=technology&_r=5 (Προσπελάστηκε στις 01.12.2014)
10. http://www.pewinternet.org/2014/12/18/future-of-privacy/ (Προσπελάστηκε στις 25.12.2014)
11. http://www.lifo.gr/now/digital-life/58035 (Προσπελάστηκε στις 7.01.2015)
12. Νόμος 2472/1997, Κεφάλαιο Α, άρθρο 2
13. Μαρία Λέρα, «Μελέτη ασφάλειας πληροφοριών και πληροφοριακών συστημάτων», διπλωματική του Πανεπιστημίου Δυτικής Μακεδονίας, Κοζάνη, 2012
14. https://hrconvention.wordpress.com/2010/07/03/%CE%AC%CF%81%CE%B8%CF%81%CE%BF-8-%CE%B4%CE%B9%CE%BA%CE%B1%CE%AF%CF%89%CE%BC%CE%B1-%CF%83%CE%B5%CE%B2%CE%B1%CF%83%CE%BC%CE%BF%CF%8D-%CF%84%CE%B7%CF%82-%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CE%AE/ (Προσπελάστηκε στις 05.02.2015)
15. Ι. Καράκωστα, «Προστασία της ιδιωτικότητας στην Κοινωνία της Πληροφορίας», Δίκαιο Μέσων Ενημέρωσης και Επικοινωνίας (ΔΙΜΕΕ), 2004
16. Χρ. Μ. Ακριβοπούλου, « Η εφαρμογή της αναλογικότητας στην προστασία των «ευαίσθητων» προσωπικών δεδομένων, σχόλιο στην απόφαση ΕΔΔΑ S & Marper vs. UK της 4ης Δεκεμβρίου 2008», Τεύχος 2/2011 της Ποινικής Δικαιοσύνης, 2011
17. http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:12012E/TXT (Προσπελάστηκε στις 05.02.2015)

18. Χρ. Μ. Ακριβοπούλου, «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, 2011
19. http://europa.eu/legislation_summaries/information_society/data_protection/l14012_el.htm (Προσπελάστηκε στις 05.02.2015)
20. Aparna, "On cookies that don't crumble: will the electronic pivacy directive 2002 make cyberspace safe?", Computer & Law Telecommunications Law Review, 2003
21. Ι. Ιγγλεζάκης, «Το νομικό πλαίσιο του ηλεκτρονικού εμπορίου», Εκδόσεις Σάκκουλα, 2003
22. Δημήτρης Αναστασόπουλος, «Η προστασία της ιδιωτικότητας κατά το αρθρο 8 της ΕΣΔΑ στο ψηφιακό περιβάλλον», ΔΙΜΕΕ, Νομική Βιβλιοθήκη, 2012
23. http://ec.europa.eu/justice/data-protection/minisite/ (Προσπελάστηκε στις 05.02.2015)
24. http://www.adae.gr/i-adae/paroysiasi/ (Προσπελάστηκε στις 05.02.2015)
25. Horniak Virginia "Privacy of Communication-Ethics and Technology", Malardalen University, 2004
26. https://ico.org.uk/ (Προσπελάστηκε στις 05.02.2015)
27. http://www.kathimerini.gr/75988/article/texnologia/diadiktyo/sony-antimetwph-me-to-nomo-gia-th-megalh-lhsteia-sto-psn (Προσπελάστηκε στις 02.11.2014)
28. Solove Daniel J. , "A taxonomy of Privacy", University of Pensylvania, 2006
29. Abdelmounaam Rezgul, Athman Bouuettaya and Mohamed Y. Eltoweissy "Privacy on the web: Facts, Challenges, and Solutions", Virginia Tech, 2003
30. Ι. Βενιέρης και Ε. Νικολούζου, «Τεχνολογίες Διαδικτύου», Εκδόσεις Τζιόλα, 2003
31. http://www.google.gr/maps/about/behind-the-scenes/streetview/privacy/ (Προσπελάστηκε στις 31.12.2014)
32. http://www.naftemporiki.gr/story/626217/google-epta-ekat-dol-gia-parabiasi-idiotikotitas-apo-to-street-view (Προσπελάστηκε στις 31.12.2014)
33. http://www.webcredible.com/blog-reports/blog/google-street-view (Προσπελάστηκε στις 31.12.2014)
34. http://www.lawnet.gr/news/to-dikaioma-sti-li8i-kai-oi-mixanes-anazitisis-sto-diadiktuo-33470.html (Προσπελάστηκε στις 07.02.2015)
35. http://www.wsj.com/articles/tim-cook-says-apple-to-add-security-alerts-for-icloud-users-1409880977 (Προσπελάστηκε στις 07.02.2015)
36. http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/ (Προσπελάστηκε στις 07.02.2015)
37. https://www.trustwave.com/Resources/SpiderLabs-Blog/Look-What-I-Found---Moar-Pony!/ (Προσπελάστηκε στις 07.02.2015)

38. http://en.wikipedia.org/wiki/HTTP_cookie (Προσπελάστηκε στις 03.11.2014)
39. http://fishbowl.pastiche.org/2004/01/19/persistent_login_cookie_best_practice (Προσπελάστηκε στις 03.11.2014)
40. http://windows.microsoft.com/el-gr/windows/cookies-faq#1TC=windows-7 (Προσπελάστηκε στις 03.11.2014)
41. http://www.europarl.europa.eu/portal/el/cookie-policy (Προσπελάστηκε στις 03.11.2014)
42. http://en.wikipedia.org/wiki/Local_shared_object (Προσπελάστηκε στις 03.11.2014)
43. https://www.futureofprivacy.org/wp-content/uploads/2011/07/Flash%20Cookies%20and%20Privacy%20II%20Now%20with%20HTML5%20and%20ETag%20Respawning.pdf (Προσπελάστηκε στις 03.11.2014)
44. http://en.wikipedia.org/wiki/Evercookie (Προσπελάστηκε στις 03.11.2014)
45. http://www.techhive.com/article/206021/The_cookie_that_doesnt_crumble_a_browser_cookie_that_wont_go_away.html (Προσπελάστηκε στις 03.11.2014)
46. http://www.dap-papei.gr/~dapndfk/images/tmimata_arxeia/ode/simeioseis/20_examino/efarmoges_upologistwn_2.pdf (Προσπελάστηκε στις 04.11.2014)
47. J. Aycock, "Computer viruses and malware advances in information security", university of Calgary Canada, 2006
48. http://el.wikipedia.org/wiki/%CE%99%CF%8C%CF%82_%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE (Προσπελάστηκε στις 04.11.2014)
49. F. Cohen, "A Short Course on Computer Viruses. Wiley Professional Computing", Wiley, Canada, 1994
50. Κ. Παπαφράγκος, «Αναπαράσταση και προσομοίωση σύνθετων δικτύων για ανάλυση χαρακτηριστικών ασφαλείας», διπλωματική του Πανεπιστημίου Πατρών, Ιούνιος 2013
51. K.M. Goertzel., "Malware" Information Assurance Tools Online Report, September 2009
52. P. Peterson, "Malware trends: The Attack of Blended Spyware Crime", the Web Security Report, 2006
53. K. Laudon and J Laudon, "Essentials of Management Information Systems", Prentice Hall 2002
54. D. S. Milojicic, V. Kalogeraki, R. Lukose, K. Nagaraja, J. Pruyne, B. Richard, S. Rollins, Z. Xu, "Peer-to-Peer Computing", HP Laboratories 2002
55. J. Zhang, "Social media and distance education", 2010
56. Kaplan & Haenlein, "Users of the world, unite! The challenges and oppurtinities of Social Media. Business Horizons", 2010
57. B. Wellman & Milena Gulia , "Net surfers don't ride alone", University of Toronto, Canada, 1997

58. S. Hofstetter, www.360i.com
59. A. Mayfield, "What is social media", Publish Spannerworks, 2008
60. Boyd & Ellison, "Social Network Sites: Definition, History, and Scholarship", Journal of Computer-Mediated Communication, 2008
61. K. E. Murray & R. Weller , "Social networking goes abroad", International Educator, 2007
62. Rohani & Hock, "On Social Network Web Sites: Definition, Features, Architectures and Analysis Tools", Journal of Advances in Computer Research, 2010
63. M. Stelzner, Social Media Marketing Industry Report, "How Marketers Are Using Social Media to Grow Their Businesses", 2009
64. N.B. Ellison, C. Steinfield and C. Lampe, "The benefits of Facebook 'friends': social capital and college students' use of online social network sites", Journal of Computer-Mediated Communication, 2007
65. C. Mitchell, "Social Networks", Clyde Nuffield College, Oxford, England, 1974
66. D. Boyd, "Friendster and Publicly Artuculated Social Networks", Conference on Human Factors and Computer Systems, Vienna, 2004
67. J. Donath. & D. Boyd, "Public displays of connection", BT Technology Journal, 2004
68. http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf (Προσπελάστηκε στις 26.11.2014)
69. Μ. Δάρα & Α. Φρέσκου, «Ρατσισμός - Προσηλυτισμός στο διαδίκτυο. Αναζήτηση έγκυρων πληροφοριών και κυβερνοαυτοκτονία», Αθήνα: Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (για το πρόγραμμα ΑΡΙΑΔΝΗ), 2011
70. http://en.wikipedia.org/wiki/Cyber_racism (Προσπελάστηκε στις 26.11.2014)
71. Μ. Δάρα, «Αποπλάνηση μέσω διαδικτύου – Grooming», Αθήνα: Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (για το πρόγραμμα ΑΡΙΑΔΝΗ), 2011
72. D. Hudson, "Rewired: A brief and opinionated net history", Indianapolis: IN: Macmillan Technical Publishing, 1997
73. Ελληνικό Κέντρο Ασφαλούς Διαδικτύου : http://www.saferinternet.gr
74. S. Craven, S. Brown and E. Gilchrist, "Sexual grooming of children: Review of literature and theoretical considerations", Journal of Sexual Aggression, 2006
75. Ο. Γιωτάκος και Μ. Τσιλιάκου, «Βιασμός», Εκδόσεις Αρχιπέλαγος 2008
76. http://www.kathimerini.gr/785125/article/oikonomia/epixeirhseis/ta-mesa-koinwnikhs-diktywshs-ergaleio--gia-anazhthsh-ergasias (Προσπελάστηκε στις 26.11.2014)

77. Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) http://www.sch.gr/96-announces/958-840old (Προσπελάστηκε στις 26.11.2014)
78. Χ. Καλλονιάτης, «Ασφάλεια Δεδομένων στην Κοινωνία της Πληροφορίας», Σημειώσεις μαθήματος, Πανεπιστήμιο Αιγαίου
79. I. Pollach, " What's wrong with online privacy policies?" , University of Economics and Business Administration, Austria, 2007
80. Κανονισμός για την Διασφάλιση του Απορρήτου στις Διαδικτακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές, ΦΕΚ 88, 2005
81. L. Sweeney. "k-Anonymity: A Model for Protecting Privacy." International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, 2002
82. Σ. Καρράς, Φ.Β. Πανοπούλου, «Εργαλείο ανωνυμοποίησης για δημοσιεύσεις δεδομένων, διπλωματική του Εθνικού Μετσόβιου Πολυτεχνείου, 2014
83. M. Terrovitis, N.Mamoulis and P. Kalnis, "Local and Global Recoding Methods fo r Anonymizing Set-valued Data", The VLDB Journal, 2010
84. Σ. Αγγέλης, «k^m-Ανωνυμοποίηση Συλλογών Δεδομένων με Συνεχή Γνωρίσματα», διπλωματική του Εθνικού Μετσόβιου Πολυτεχνείου, 2014
85. Kroes Neelie , "The big data revolution", SPEECH/13/261, 2013
86. International Business Machines, "What is Big Data?", 2013, http://www-01.ibm.com/software/data/bigdata/
87. http://www.kathimerini.gr/802098/article/texnologia/diadiktyo/mesw-kinhtwn-to-97-ths-pagkosmias-diakinhshs-dedomenwn-ws-to-2019 (Προσπελάστηκε στις 04.02.2015)
88. Λ. Μήτρου, «Η προστασία της ιδιωτικότητας στην πληροφορική και τις επικοινωνίες: η νομική διάσταση», Εκδόσεις Παπασωτηρίου, 2010
89. http://www.kathimerini.gr/803077/article/texnologia/diadiktyo/hpa-dhmioyrgia-neas-yphresias-gia-tis-apeiles-toy-diadiktyoy (Προσπελάστηκε στις 10.02.2015)
90. http://www.kathimerini.gr/801736/article/texnologia/diadiktyo/ta-likes-toy-facebook-apokryptografoyn-thn-proswpikothta-mas (Προσπελάστηκε στις 10.02.2015)
91. http://medianalysis.net/2014/10/18/facebook-%CE%BA%CE%B1%CE%B9-%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1-%CE%B1%CE%BD%CF%84%CE%AF%CF%81%CF%81%CE%BF%CF%80%CE%B5%CF%82-%CE%B4%CF%85%CE%BD%CE%AC%CE%BC%CE%B5/ (Προσπελάστηκε στις 26.02.2015)