ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΔΙΚΤΥΑ ΔΗΜΟΣΙΑΣ ΧΡΗΣΗΣ & ΔΙΑΣΥΝΔΕΣΗ ΔΙΚΤΥΩΝ

Η ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

ΜΕΝΤΑΚΗΣ ΔΗΜΗΤΡΙΟΣ

Α.Μ: 235955

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

- OSINT: Open Source Intelligence Techniquies
- API: Application Programming Interface
- ToS: Terms of Service
- NRLB: National Labor Relations Board
- FCRA: Fair Credit Reporting Act
- ECPA: Electronic Communications Privacy Act
- COPPA: Children's Online Privacy Protection Act
- NSA: National Security Agency
- SIGINT: Signal Intelligence
- ΕΕ: Ευρωπαϊκή Ένωση
- VPN: Virtual Private Networks
- TOR: The Onion Router
- FBI: Federal Bureau of Investigation
- CEO: Chief Executive Officer

Κεφαλαιο 1: Εισαγωγη

1.1 Διαδίκτυο και Μέσα Κοινωνικής Δικτύωσης

Η εξάπλωση της νέας γενιάς του Παγκόσμιου Ιστού ή αλλιώς World Wide Web ή Web 2.0, βασίζεται στην μεγάλη δυνατότητα των χρηστών να μοιράζονται πληροφορίες και να συνεργάζονται online, χωρίς να έχουν απαραίτητα άρτια τεχνική κατάρτιση και γνώσεις πάνω σε θέματα υπολογιστών και δικτύων. Ως εκ τούτου, το Web 2.0, συντέλεσε στην μετατροπή των χρηστών, παλιών και νέων, από παθητικούς αναγνώστες και θεατές σε άμεσα συνεισφέροντας. Οι χρήστες έχουν πλέον την δυνατότητα να δημιουργούν, να διανέμουν, να ανταλλάσσουν πληροφορίες και απόψεις και να αλληλοεπιδρούν με άλλους χρήστες σε online κοινότητες. Όλα αυτά τα μέσα επικοινωνίας, οι εικονικοί διαδικτυακοί χώροι, που έχουν ως βασική παροχή υπηρεσίας την δημοσίευση και ανταλλαγή περιεχομένου και έχουν στην διάθεση τους οι χρήστες αναφέρονται με τον όρο Μέσα Κοινωνικής Δικτύωσης ή αλλιώς Social Media. Μέσα σε αυτές τις κοινότητες χρηστών, οι χρήστες δημιουργούν τις προσωπικές τους ψηφιακές ταυτότητες, αποκαλύπτοντας πτυχές της προσωπικής τους ζωής.

Τα Μέσα Κοινωνικής Δικτύωσης, θα μπορούσαν να κατηγοριοποιηθούν σύμφωνα με την κύρια προς προσφορά υπηρεσία στην οποία βασίζονται στις παρακάτω ενότητες:

1. Βασισμένα στην Κοινωνική Δικτύωση και Ενημέρωση
    - Κοινωνικά Δίκτυα (Facebook, Google+ MySpace, LinkedIn)
    - Προσωπικά Ιστολόγια (Blogger, WordPress)
    - Μικρά Ιστολόγια ή αλλιώς Microblogging (Twitter, Tumblr)
    - Ιστολόγια που προσφέρουν την δυνατότητα συνεργατικής επεξεργασίας ή αλλιώς Wikis (Wikipedia, Wikinews)

2. Βασισμένα σε περιεχόμενο
    - Φωτογραφίες και εικόνες (Instagram, Imgur, Flickr, DevianArt, Photobucket)
    - Βίντεο (YouTube, Dailymotion, Vimeo, Netflix)
    - Μουσική (Spotify, Napster, Soundcloud)
    - Παρουσιάσεις και αρχεία κειμένων (SlideShare, Scribd)
3. Βασισμένες σε συγκεκριμένη λειτουργία
    - Ζωντανή μετάδοση (Skype, Ustream, Twitch.tv)
    - Συλλογή σελιδοδεικτών (Delicious, Diigo)
    - Διοργανώσεις και συμβάντα (Eventful)
    - Τοποθεσίες (Foursquare)
4. Βασισμένα στα ενδιαφέροντα
    - Ειδήσεις (Digg)
    - Κριτικές (IMDb, Flixter, GoodReads, Yelp)
    - Αγορές (Blippy, Etsy)

Σύμφωνα με τον αριθμό ενεργών χρηστών, οι πιο δημοφιλείς ιστότοποι κοινωνικής δικτύωσης σήμερα είναι οι εξής:

- ❖ Facebook
- ❖ Twitter
- ❖ Google+
- ❖ Youtube

Και ακολουθούν, Blogger, LinkedIn, Instagram, Flickr οι οποίοι συγκεντρώνουν καθημερινά εκατομμύρια παλιούς αλλά και νέους χρήστες. Οι χρήστες συμμετέχουν σε αυτά για μία πληθώρα λόγων όπως δικτύωση για επαγγελματικούς σκοπούς, διασκέδαση και επικοινωνία με άλλους με κάθε είδους περιεχόμενο.

1.2 Συλλογή Πληροφορίας

Η εξάπλωση και δημοφιλία των Μέσων Κοινωνικής Δικτύωσης, έχει οδηγήσει σε έρευνες και μελέτες οι οποίες παρατηρώντας την καθημερινή χρήση τους, αποδεικνύουν την έντονη τάση της μεταφοράς της καθημερινής συμπεριφοράς online. Λίγα χρόνια μετά την παρθενική λειτουργία του Facebook, οι άνθρωποι για πρώτη φορά στην ιστορία, έδωσαν αβίαστα χωρίς ενδοιασμούς προσωπικά στοιχεία online ενώ μέχρι πρότινος το μεγαλύτερο ποσοστό χρησιμοποιούσε ψευδώνυμά και όχι αληθινά ονόματα.

Ένα αντιπροσωπευτικό παράδειγμα αποτελούν οι απανταχού μαθητές που ολοένα και περισσότερο μοιράζονται τις προσωπικές τους ζωές online καθημερινά έχοντας λίγη έως καθόλου ανησυχία για το ποιο άτομο, ίδρυμα, επιχείρηση ή οργάνωση μπορεί να έχει πρόσβαση στα προσωπικά τους δεδομένα. Με την νέα τεχνολογία και εξάπλωση των μέσων, τίθενται ερωτήματα για την ηθική χρήση τους και οι λεπτές γραμμές που διαχωρίζουν τί είναι ιδιωτικό και τί όχι γίνονται ολοένα και πιο δυσδιάκριτες.

Συνδυάζοντας την ροή διαθέσιμης online πληροφορίας των χρηστών με την δυνατότητα επεξεργασίας μεγάλου όγκου δεδομένων και πληροφορίας χρησιμοποιώντας ευρέως γνωστές OSINT, η δημιουργία προτύπων συμπεριφοράς και χρήσης για έναν χρήστη ή μία ομάδα χρηστών είναι πιο εφικτή από ποτέ. Τα πρότυπα συμπεριφοράς, μπορούν να χρησιμοποιηθούν για την δημιουργία προφίλ προσωπικότητας, για πρόβλεψη συμπεριφοράς, για έλεγχο καταλληλόλητας για συγκεκριμένη θέση εργασίας, για στοχευμένη διαφήμιση και άλλα.

Επιπρόσθετα η εισαγωγή της Διεπαφής Προγραμματισμού Εφαρμογών ή αλλιώς API κάνει την προσκόμιση της πληροφορίας αυτοματοποιημένη και ακόμα πιο εύκολη. Για παράδειγμα το Facebook ήταν το πρώτο μέσο κοινωνικής δικτύωσης που δημιούργησε το δικό του API για δημιουργία third-party εφαρμογών τον Μάιο του 2007. Εφαρμογές φτιαγμένες να χρησιμοποιούν το εν λόγω API αποτελούν σοβαρό κίνδυνο στην ιδιωτικότητα των χρηστών καθώς μπορούν να αντλούν εύκολα σημαντικές πληροφορίες.

Το σημαντικότερο σημείο κλειδί που θα πρέπει να αναφερθεί στο σημείο αυτό, είναι ότι τα δεδομένα αυτά είναι προσβάσιμα από τον οποιονδήποτε και για την μελέτη τους και εξαγωγή προτύπων συμπεριφοράς δεν απαιτείται η συγκατάθεση του

εκάστοτε χρήστη. Τόσο το Facebook όσο και τα υπόλοιπα Μέσα Κοινωνικής Δικτύωσης, ενημερώνουν τους χρήστες κατά την δημιουργία λογαριασμού στην υπηρεσία με τους Όρους Χρήσης ToS και την πολιτική απορρήτου ή Privacy Policy για την συλλογή και διαχείριση των προσωπικών τους δεδομένων ώστε να είναι δυνατή η αποφυγή πιθανών ποινικών διώξεων. Όπως είναι λογικό, ελάχιστοι διαβάζουν τους όρους αυτούς, είτε γιατί το διάβασμα τους είναι ιδιαίτερα χρονοβόρο, είτε γιατί αγνοούν την ύπαρξή τους, είτε γιατί δεν ενδιαφέρονται. Η εν λόγω συλλογή και επεξεργασία προσωπικών δεδομένων μπορεί να πραγματοποιείται, όπως οι τα περισσότερα μέσα δηλώ- νουν, για αθώους σκοπούς όπως για παράδειγμα την προσφορά καλύτερων υπηρεσιών στον χρήστη, βασισμένες στα ενδιαφέροντα και την προσωπικότητα του ώστε να βελτιώνεται η εμπειρία χρήσης ή αλλιώς το User Experience.

Παρόλο αυτά, η δυνατότητα διεξαγωγής αυτοματοποιημένης ψυχομετρικής εκτίμησης και η χρήση, αποκάλυψη και επεξεργασία προσωπικών δεδομένων θέτει την ιδιωτικότητα των χρηστών σε κίνδυνο και η θεσμοθέτηση των ψηφιακών δικαιωμάτων ή Digital Rights κρίνεται απαραίτητη για την προστασία των χρηστών και των δεδομένων τους.

Το βασικό ερώτημα που τίθεται είναι πως ορίζονται τελικά η ιδιωτικότητα και τα ψηφιακά δικαιώματα;

1.3 Ιδιωτικότητα(Privacy)

Η ιδιωτικότητα ορίζεται ως το σύνολο της πληροφορίας που ένα άτομο κρίνει σημαντική, προσωπική και μη προσβάσιμη από άλλους. Η προσωπική πληροφορία περιέχει το όνομα ενός ατόμου, την φυσική του διεύθυνση, το e-mail του, το online ψευδώνυμο ή username, το τηλέφωνο και γενικότερα οποιαδήποτε άλλη πληροφορία με την οποία το άτομο μπορεί να αναγνωριστεί και να στοχοποιηθεί. Ο όρος ιδιωτικότητα περιλαμβάνει επίσης την δυνατότητα του ατόμου να διαχειρίζεται ο ίδιος την περαιτέρω διάδοση της προσωπικής του πληροφορίας. Η δυνατότητα αυτή, η αυτονομία δηλαδή του ατόμου στην διαχείριση, τον διαμοιρασμό και την μετέπειτα χρήσης της προσωπικής πληροφορίας είναι κρίσιμη για το δικαίωμα του ατόμου στην ψηφιακή ιδιωτικότητα.

Αναφερόμενοι στον ορισμό και την σημασία της ιδιωτικότητας είναι σημαντικό στο σημείο αυτό να θέσουμε μία κρίσιμη θεώρηση: Την πρόθεση να παραμείνει ιδιωτική η δια μοίρας μένη πληροφορία. Όπως είναι προφανές, ένα άτομο που χρησιμοποιεί κάποιο μέσο κοινωνικής δικτύωσης όπως το Facebook, μοιράζεται προσωπικές πληροφορίες με άλλους και επομένως δεν μπορεί να υποθέσει ότι η πληροφορία είναι ιδιωτική. Ωστόσο, όταν ένα άτομο θέτει περιορισμούς στις ρυθμίσεις του εκάστοτε μέσου με σκοπό την επίτευξη ιδιωτικότητας και την απόκρυψη πληροφορίας από άλλους, τότε έχει την προσδοκία ότι η πληροφορία αυτή θα παραμείνει ιδιωτική.

Η εκ βάθους κατανόηση και σημασία της ιδιωτικότητας όπως αυτή σχετίζεται με τα Μέσα Κοινωνικής Δικτύωσης απαιτεί τον ορισμό της πρόθεσης κοινοποίησης προσωπικής πληροφορίας και την κατανόηση του πώς αυτή μπορεί να διαμοιράζεται. Ο μεγαλύτερος, αν όχι όλος, όγκος πληροφορίας σε ένα online μέσο, είναι πληροφορία που ο ίδιος ο χρήστης επιλέγει οικειοθελώς να μοιραστεί. Ακόμη κι αν η πρόθεση του χρήστη είναι να μοιραστεί την πληροφορία με μια συγκεκριμένη ομάδα άλλων χρηστών, στην ουσία η πληροφορία αυτή είναι διαθέσιμη σε τον υπόλοιπο κόσμο.

Άλλο ένα σημαντικό θέμα προς συζήτηση είναι το πώς αυτή η πληροφορία μπορεί να χρησιμοποιηθεί ενάντια σε κάποιον χρήστη. Όπως αναφέρθηκε παραπάνω, η αναζήτηση πληροφορίας για κάποιον χρήστη σε ένα οποιοδήποτε Μέσο Κοινωνικής Δικτύωσης από τον οποιονδήποτε δεν θεωρείται παράνομη εφόσον η πληροφορία βρίσκεται σε κοινή δημόσια θεά. Πληροφορίες όπως αρνητικά σχόλια, φωτογραφισμένες κακές συνήθειες και πολλά άλλα μπορούν να χρησιμοποιηθούν εναντίον κάποιου ατόμου, όπως για παράδειγμα, την αποθάρρυνση ενός εργοδότη για μια θέση εργασίας. Περισσότερα για το θέμα αυτό στο Κεφάλαιο 2.

Τόσο το Facebook, όσο και τα περισσότερα κοινωνικά δίκτυα, παρέχουν την πολιτική απορρήτου ή αλλιώς Privacy Policy ή Privacy Statement για να ενημερώσουν τους χρήστες για τα όρια της προστασίας που προσφέρει η υπηρεσία στην διαμοιρασμένη πληροφορία όπως επίσης και για το πώς μπορεί να χρησιμοποιήσει η ίδια η υπηρεσία τις διαμοιρασμένες πληροφορίες. Θεωρείται σαν ένα είδους συμβολαίου που επισυνάπτεται μεταξύ των επισκεπτών της ιστοσελίδας και της εταιρείας που πρέπει να τηρείται από τις δύο πλευρές. Ωστόσο οι εν λόγω πολιτικές ιδιωτικότητας δεν αποσαφηνίζουν ποιος μπορεί να έχει πρόσβαση στις

πληροφορίες αυτές παρά μόνο την δράση των διαχειριστών της υπηρεσίας. Το κύριο σημείο στο οποίο εστιάζουν οι πολιτικές ιδιωτικότητας είναι στο τί πληροφορία θα διαμοιράζεται με τρίτους (ιδιωτικούς ή κρατικούς οργανισμούς, επιχειρήσεις κ.ο.κ).

Όπως αναφέρεται παραπάνω, είναι άγνωστο αν οι χρήστες αν γνωρίζουν ή πόσο μάλλον αν διαβάζουν την πολιτική απορρήτου του εκάστοτε μέσου κοινωνικής δικτύωσης που χρησιμοποιούν. Το Facebook συγκεκριμένα αναφέρει ότι θα κάνει ό,τι είναι δυνατό για να προστατέψει την οποιαδήποτε πληροφορία μοιράζεται στην υπηρεσία αλλά τονίζει ότι δεν μπορεί να εγγυηθεί πως η πληροφορία του χρήστη δεν θα είναι προσβάσιμη από μη εξουσιοδοτημένα άτομα, οργανισμούς και επιχειρήσεις.

Σε συνδυασμό με την παραπάνω δήλωση, τα Μέσα Κοινωνικής Δικτύωσης αποσαφηνίζουν επίσης το ποιος είναι υπεύθυνος για την πληροφορία που διαμοιράζεται στην υπηρεσία τους. Το Facebook όπως και τα άλλα μέσα, προσφέρουν συμβουλές σε χρήστες και γονείς για το πώς μπορούν να προστατέψουν τις πληροφορίες που διαμοιράζονται στην υπηρεσία. Παρέχονται εργαλεία και ρυθμίσεις για την ρύθμιση της δημοσιότητας της πληροφορίας, που μπορούν να χρησιμοποιηθούν για να αποκλείσουν άλλους από την πρόσβαση της.

Ωστόσο αξίζει να σημειωθεί ότι οι προεπιλεγμένες ρυθμίσεις απορρήτου για το Facebook επιτρέπουν σε όλα τα μέλη του δικτύου ενός χρήστη να μπορούν να δουν όλη την πληροφορία που υπάρχει διαθέσιμη εκτός από τα προσωπικά του μηνύματα. Στα περισσότερα μέσα, συμπεριλαμβανομένου και του Facebook, με τις κατάλληλες ρυθμίσεις απορρήτου, ο χρήστης μπορεί να περιορίσει σημαντικά το ποσοστό της πληροφορίας που είναι διαθέσιμο και προς ποιους χρήστες. Δυστυχώς το μεγαλύτερο ποσοστό των χρηστών αγνοεί την ύπαρξη των ρυθμίσεων αυτών και την σημασία τους. Μια πρόσφατη έρευνα που έγινε σε χρήστες, συγκεκριμένα του Facebook, ηλικίας 15-25 χρονών στις ΗΠΑ , έδειξαν πως το 90% αυτών δεν διαβάζουν τους ορούς αποδοχής για την προστασία ιδιωτικότητας ενώ το 60% αγνοεί το συγκεκριμένο θέμα.

Υπάρχουν τρείς κύριοι λογικοί τρόποι με τους οποίους μπορεί να προστατευτεί σήμερα η ιδιωτικότητα των χρηστών στο διαδίκτυο:

I. Να μην ζητείται από τους ιστότοπους και τα μέσα να παρέχουν οι χρήστες ιδιωτικές πληροφορίες.

II. Η πηγή από την οποία προέρχονται τα ιδιωτικά δεδομένα να είναι κρυμμένη, επομένως να διατηρείται η ανωνυμία των χρηστών.

III. Οι πολιτικές ιδιωτικότητας των ιστοτόπων που υπόσχονται την υπεύθυνη και ορθή διαχείριση των ιδιωτικών δεδομένων.

1.4 Μέσα Κοινωνικής Δικτύωσης

Τα Μέσα Κοινωνικής Δικτύωσης προσφέρουν την δυνατότητα στους χρήστες να επικοινωνούν και να αλληλοεπιδρούν μεταξύ τους. Για την εγγραφή στην οποιαδήποτε υπηρεσία, απαιτείται το προσωπικό e-mail, ένα όνομα χρήστη το οποίο μπορεί να είναι είτε το αληθινό είτε κάποιο ψευδώνυμο και άλλες προσωπικές πληροφορίες όπως τον αριθμό τηλεφώνου ή την διεύθυνση κατοικίας. Το πιο σημαντικό κομμάτι της διαδικασίας εγγραφής είναι ο προσωπικός κωδικός. Ο προσωπικός κωδικός δημιουργεί ένα ψευδές και εσφαλμένο αίσθημα ασφάλειας και την εντύπωση ότι η πληροφορία είναι και θα είναι ιδιωτική.

Δημιουργώντας το προσωπικό του προφίλ, ο χρήστης έχει την δυνατότητα να μοιραστεί την πόλη διαμονής, το σχολείο ή/και το ίδρυμα στο οποίο φοίτησε/φοιτά ή τον οργανισμό ή επιχείρηση που εργαζόταν/εργάζεται, το γούστο του σε μουσική και ταινίες, ακόμη και την προσωπική του ερωτική κατάσταση.

Το οποιοδήποτε προφίλ μπορεί να φαίνεται αληθινό και έγκυρο, ο χρήστης ωστόσο, έχοντας έλεγχο σε όλη την πληροφορία την οποία μοιράζεται, μπορεί να παρουσιάζει τον ιδανικό του εαυτό (το πώς δηλαδή θα ήθελε να είναι) ή κάποια άλλη προσωπικότητα persona) και οι σκοποί μπορεί να ποικίλουν. Ο χρήστης μπορεί να θέλει να προωθήσει συγκεκριμένες ιδέες, απόψεις ή και προϊόντα, ή να θέλει να φαίνεται ελκυστικός κ.ο.κ. Ενδεικτικά αναφέρουμε ότι δεν είναι λίγοι οι χρήστες που δημιουργούν προσεκτικά και υπομονετικά ψεύτικες online προσωπικότητες με κάποιον απώτερο κακόβουλο σκοπό. Η πληροφορία που διαμοιράζεται στην υπηρεσία ο χρήστης είναι αυτή που θεωρεί σημαντική και κατάλληλη. Κι ενώ κάποιοι χρησιμοποιούν μέσα κοινωνικής δικτύωσης για την επικοινωνία, κάποιοι τα χρησιμοποιούν για προσωπική έκφραση, αληθινή ή όχι.

ΚΕΦΑΛΑΙΟ 2: ΔΕΟΝΤΟΛΟΓΙΑ (ETHICAL IMPLICATIONS)

Όπως αναφέρθηκε και στο Κεφάλαιο 1.2, υπάρχουν πολλές και διάφοροι μέθοδοι για την συλλογή και επεξεργασία πληροφορίας με σκοπό την δημιουργία προφίλ προσωπικότητας και συμπεριφοράς. Για παράδειγμα, η μεθοδολογία Panopticon επιτρέπει την αυτόματη ταξινόμηση των χρηστών σε προκαθορισμένες κατηγορίες, βάσει του περιεχομένου που έχουν εισάγει στα Μέσα Κοινωνικής Δικτύωσης, ακόμη και χωρίς την συγκατάθεση τους. Αυτό οδηγεί στην έκθεση προσωπικών πληροφοριών κατά τρόπο αυτοματοποιημένο. Η εφαρμογή τέτοιων μεθόδων χωρίς την συγκατάθεση των χρηστών, αποτελεί τρόπο ανήθικο και δημιουργεί πολλά ηθικά και νομικά ζητήματα. Η παραβίαση της ιδιωτικότητας για δημιουργία προφίλ προσωπικότητας εγείρει πολλές απειλές και η αυτοματοποιημένη δημιουργία των προφίλ για την ενίσχυση νομικών μηχανισμών, αποτελεί ένα ισχυρό μέσο στα κατάλληλα χέρια.

2.1 Μελέτη Περίπτωσης: Φοιτητές Ιδρύματος

Καθώς η χρήση των Μέσων Κοινωνικής Δικτύωσης από φοιτητές γίνεται ολοένα και μεγαλύτερη, εμφανίζονται στο προσκήνιο ηθικά ζητήματα σε υποθέσεις που δημιουργούνται ανάμεσα σε φοιτητές και καθηγητές. Το συγκεκριμένο θέμα εγείρει πολλές ερωτήσεις για την φοιτητική μέριμνα που πρέπει να απαντηθούν προκειμένου να μελετηθεί η επίδραση των μέσων στην φοιτητική και ακαδημαϊκή κοινότητα.

Βασισμένοι στους ειδικούς σε θέματα φοιτητικής μέριμνας για το πώς οι φοιτητές χρησιμοποιούν τα Μέσα Κοινωνικής Δικτύωσης, οι Εθνικοί Επαγγελματικοί Οργανισμοί μπορούν να παίξουν παραγοντικό ρόλο στην καθιέρωση ηθικών

προτύπων που θα μπορούσαν να καθορίσουν συμπεριφορές και δράσεις καθηγητών ανώτατης εκπαίδευσης.

Σύμφωνα με την Association of Student Judicial Affairs, τα ηθικά πρότυπα καθιερώνονται για να διατηρήσουν και να ενδυναμώσουν το ηθικό κλίμα, και να προωθήσουν την ακαδημαϊκή ακεραιότητα των ιδρυμάτων που εκπροσωπούν. Ως ένα ακόμη παράδειγμα, σύμφωνα με την American College Personnel Association, τα ηθικά πρότυπα που καθιερώνει βοηθούν τους ειδικούς φοιτητικής μέριμνας στην ρύθμιση της συμπεριφοράς τους, ευαισθητοποιώντας τους σε πιθανά ηθικά προβλήματα και προσφέροντας πρότυπα χρήσιμα σε καθημερινή βάση. Η τελευταία, αναφέρεται επίσης στη ηθική ευθύνη των επαγγελματιών πάνω στο θέμα των δικαιωμάτων ιδιωτικότητας και τους παρακινεί να είναι γνώστες και ενημερωμένοι για τους τρέχοντες νόμους και κανονισμούς για τον τρόπο που διαμοιράζονται οι πληροφορίες και τα αρχεία των φοιτητών.

Οι ειδικοί σε θέματα φοιτητικής μέριμνας, καλούνται επίσης να αποτελούν πρότυπα και να δημιουργούν σχέσεις με φοιτητές που προωθούν την εξέλιξη και γνώση. Αυτό επιτυγχάνεται με την μοντελοποίηση της ηθικής συμπεριφοράς. Οι εν λόγω ειδικοί, χρησιμοποιώντας τα Μέσα Κοινωνικής Δικτύωσης, μπορούν να διακρίνουν πως να δημιουργήσουν ένα κατάλληλο πρότυπο συμπεριφοράς. Εκτός αυτού, οι ειδικοί που χρησιμοποιούν τα μέσα, είναι λιγότερο πιθανό να θέσουν πολιτικές που παραβαίνουν φοιτητικά δικαιώματα.

Η συμπεριφορά των απανταχού φοιτητών δεν έχει αλλάξει δραματικά τα τελευταία χρόνια. Ακόμα διασκεδάζουν, πίνουν και πειραματίζονται ποικιλοτρόπως. Ωστόσο, οι ασχολίες και καθημερινές συνήθειες των φοιτητών, εντοπίζονται εύκολα στα Μέσα Κοινωνικής Δικτύωσης.

Αυτό που έχει αλλάξει είναι η δυνατότητα των διαχειριστών και καθηγητών να βλέπουν αυτές τις συμπεριφορές. Αυτομάτως, η πρόκληση που δημιουργείται για τους καθηγητές είναι η ενασχόληση τους με τα μέσα χωρίς όμως να υπερβαίνουν τα όρια της εξουσίας τους.

Υπάρχουν πολλά σχετικά παραδείγματα κατηγορίας φοιτητών για κατανάλωση αλκοόλ με βάση εικόνες που οι ίδιοι οι φοιτητές ανέβασαν στα Μέσα Κοινωνικής Δικτύωσης. Αν ο/οι φοιτητής/ές δεν έχει ρυθμίσει κατάλληλα τις ρυθμίσεις ιδιωτικότητας περιεχομένου, οι πληροφορίες αυτές είναι διαθέσιμες προς

όλους στο δίκτυο, συμπεριλαμβανομένων καθηγητών, ειδικών φοιτητικής μέριμνας ακόμη και αστυνομικών του ιδρύματος. Οι φοιτητές έχουν την εσφαλμένη πεποίθηση ότι οι καθηγητές ή οι διαχειριστές δεν παρακολουθούν τις πληροφορίες που διαμοιράζονται στα μέσα. Τα ερωτήματα που εγείρονται εδώ είναι τα εξής:

- ✓ Αν καθηγητές και διαχειριστές θα πρέπει να παρακολουθούν τις καθημερινές ασχολίες των φοιτητών τους.
- ✓ Αν η κατάσταση θα ήταν διαφορετική αν οι φοιτητές γνώριζαν ότι οι διαχειριστές θα έβλεπαν τις φωτογραφίες τους και θα τους τιμωρούσαν. Αν δηλαδή το ίδρυμα είχε δηλώσει ξεκάθαρα ότι παρακολουθεί τις online δραστηριότητες των φοιτητών σε καθημερινή βάση.
- ✓ Τί θα μπορούσαν να κάνουν οι ειδικοί φοιτητικής μέριμνας για να αποφύγουν μία τέτοια κατάσταση καθώς επίσης αν θα μπορούσαν να κάνουν ανοιχτές συζητήσεις σχετικά με το τι πληροφορίες οι φοιτητές διαμοιράζονται στα μέσα εφόσον γνωρίζουν για την καθημερινή παρακολούθηση.
- ✓ Ποια η ευθύνη των ειδικών για την επιμόρφωση των φοιτητών σχετικά με το περιεχόμενο των πληροφοριών που μπορούν να διαμοιράζονται online.

Ως ένα ακόμα αξιοσημείωτο παράδειγμα, έχουν παρατηρηθεί αιτήσεις αλλαγής συγκατοίκου από φοιτητές, που πριν καν φτάσουν στην Πανεπιστημιούπολη, είχαν εξετάσει τα προφίλ των συγκατοίκων τους στα μέσα, και είχαν καταλήξει στο ότι δεν θα ταίριαζαν στην συγκατοίκηση.

Όπως αναφέρθηκε και παραπάνω, για να επιτελούν καταλληλότερα το έργο τους, οι ειδικοί φοιτητικής μέριμνας, θα πρέπει να έχουν επίγνωση της τρέχουσας τεχνολογίας και εμπειρία με τα Μέσα Κοινωνικής Δικτύωσης. Για να προσφέρουν την μέγιστη δυνατή υποστήριξη, οι ειδικοί θα πρέπει επίσης να κατανοούν εις βάθος τις επιπτώσεις των μέσων στα ιδρύματα ανώτατης εκπαίδευσης. Κατανοώντας τα όρια τους σαν ειδικοί του ιδρύματος, την τρέχουσα πολιτική, παρακολουθώντας την συμπεριφορά των φοιτητών και αλληλοεπιδρώντας με αυτούς μέσω των μέσων, αυξάνεται η ικανότητά τους να προσφέρουν ικανή και ισχυρή υποστήριξη στους φοιτητές, κι αυτό ανεξάρτητα από το προσωπικό τους ενδιαφέρον για χρήση των Μέσων Κοινωνικής Δικτύωσης.

Στο σημείο αυτό πρέπει να αποσαφηνιστεί πλήρως ο ρόλος των ιδρυμάτων στην λειτουργία των ειδικών φοιτητικής μέριμνας. Είναι ιδιαίτερα σημαντικό να

καθοριστεί από τα ιδρύματα το πότε ένας ειδικός λειτουργεί ως πράκτορας του ιδρύματος και πότε ως ένα ακόμα άτομο που χρησιμοποιεί το Μέσο Κοινωνικής Δικτύωσης. Υπάρχουν τέσσερα σημεία που πρέπει να ληφθούν υπόψιν σχετικά με τον καθορισμό του ρόλου ενός ειδικού-πράκτορα του ιδρύματος και των Μέσων:

- Τι μπορεί να εξετάσει ο πράκτορας του ιδρύματος.
- Πότε θα πρέπει να αναφέρει επίσημα πληροφορίες που βρήκε σε κάποιο μέσο.
- Ο τύπος τις πληροφορίας που θα πρέπει να αναφέρεται επίσημα.
- Πότε δεν αναφέρει κάτι και γιατί.

Η αποσαφήνιση του πότε ένας ειδικός θεωρείται πράκτορας του ιδρύματος, θα δώσει την δυνατότητα στον ειδικό να χρησιμοποιεί καλύτερα τα Μέσα Κοινωνικής Δικτύωσης και να πληροφορεί τους φοιτητές κατάλληλα σχετικά με την χρήση αυτών.

2.2 Μελέτη Περίπτωσης: Εργαζόμενοι

Τα πράγματα δεν είναι πολύ διαφορετικά στο τομέα αυτό, αλλά είναι σίγουρα πιο αυστηρά καθώς η διαρροή σημαντικών πληροφοριών για την εταιρεία μπορεί να προκαλέσει τεράστια οικονομική ζημία και να την άσκηση ποινικών διώξεων. Στην σύγχρονη εποχή στόχος του κάθε εργοδότη είναι να έχει όσο των δυνατών καλύτερους εργαζομένους, οι οποίοι θα είναι αφοσιωμένοι και αποτελεσματικοί στη δουλεία τους. Παρόλο αυτά αρκετοί εργαζόμενοι εκθέτουν τα προσωπικά τους δεδομένα στα Μέσα Κοινωνικής Δικτύωσης χωρίς να σκεφτούν τις επιπτώσεις που θα μπορεί να έχει μια τέτοια ενέργεια για τη δουλεία τους. Όπως είναι αναμενόμενο, οι εργοδότες τους ελέγχουν συνεχώς τα μέσα των εργαζομένων τους για να διασφαλίσουν την ποιότητα των εργαζομένων τους.

Αρκετές εταιρείες διατηρούν συγκεκριμένες πολιτικές χρήσης που επιτρέπουν τον έλεγχο των δημοσιεύσεων των εργαζομένων τους ακόμα και αν οι εργαζόμενοι τους έχουν "κλειδωμένους" τους λογαριασμούς τους. Δηλαδή ρυθμισμένους για την μέγιστη δυνατή ιδιωτικότητα. Επιπρόσθετα, είναι συχνό φαινόμενο οι εταιρείες να έχουν και επιμέρους πολιτικές για τα Μέσα Κοινωνικής Δικτύωσης που περιορίζουν

τους εργαζόμενους να δημοσιεύουν οτιδήποτε. Χαρακτηριστικό παράδειγμα αποτελεί η ιστοσελίδα Compliance Building, η οποία παρέχει μια βάση δεδομένων για όλες τις επιχειρήσεις που αναγράφει τις πολιτικές αρκετών εταιρειών σχετικά με τα Μέσα Κοινωνικής Δικτύωσης. Παρόλο αυτά, σε ορισμένα κράτη έχουν ψηφιστεί νόμοι που απαγορεύουν στους εργοδότες των εταιρειών να ελέγχουν τους εργαζόμενους τους στα Μέσα. Ωστόσο, αν αποδειχθεί πως κάποια δραστηριότητα των υπαλλήλων λειτουργεί ή θα λειτουργήσει σε βάρος της εταιρείας, τότε οι εργοδότες μπορούν να εισάγουν την απόλυση των υπαλλήλων τους.

Είναι λογικό, όπως και με την περίπτωση των φοιτητών, να υπάρχουν νόμοι που να προστατεύουν τους εργαζόμενους σε ειδικές περιπτώσεις, όπως την απόλυσή τους με βάση στοιχεία που βρέθηκαν παραβιάζοντας την ιδιωτικότητα τους στα Μέσα Κοινωνικής Δικτύωσης.

Υπάρχουν ειδικοί νόμοι που απαγορεύουν στους εργοδότες να πειθαρχούν υπαλλήλους όταν κάνουν διακρίσεις, ανάλογα με το τί έχουν δημοσιεύσει, την ηλικία τους, τη φυλή τους, τη θρησκεία, την εθνική καταγωγή και το φύλο τους. Αν ο εργαζόμενος αισθανθεί πως έχει πέσει θύμα διακρίσεων με πρόφαση την οποιαδήποτε δημοσίευση ή κάτι από τα παραπάνω, σε κάποιο κοινωνικό δίκτυο, μπορεί να συμβουλευτεί δικηγόρο και το εργατικό δίκαιο ώστε να δικαιωθεί.

Το Εθνικό Συμβούλιο Εργασιακών Σχέσεων (NLRB) έχει εκδώσει αποφάσεις που αφορούν ζητήματα σχετικά με τις πολιτικές αρχές εργοδότη-υπαλλήλου στα Μέσα Κοινωνικής Δικτύωσης. Πιο συγκεκριμένα, οι γενικοί κανόνες που ισχύουν για τους εργαζόμενους με αναφορά τις δημοσιεύσεις τους στα Μέσα, βασισμένοι στο επίσημο Your Business: Make your social media policy clear είναι οι παρακάτω:

- Ενημέρωση των εργαζομένων πως τα Μέσα Κοινωνικής Δικτύωσης αποτελούν μέρος της εταιρείας και εκτός υπηρεσίας ενέργειες μπορεί να οδηγήσουν σε απόρριψη.
- Απαγόρευση της διανομής των εμπιστευτικών ή αποκλειστικών επιχειρηματικών πληροφοριών μέσω αναρτήσεων ή online συνομιλιών.
- Απαγορεύεται η δυσφήμηση και η απάτη εις βάρος της εταιρίας που εργάζονται.
- Απαγορεύεται η παρενόχληση και διακρίσεις εις βάρος συναδέλφων είτε με μηνύματα είτε με δημοσιεύσεις οποιουδήποτε είδους.

- Απαγόρευση της παράνομης συμπεριφοράς, όπως η παραβίαση εμπορικού σήματος ή παράνομη προσέγγιση μέσω μηνυμάτων πελατών με στόχο το προσωπικό όφελος βασιζόμενοι στο όνομα της εταιρείας.
- Απαγόρευση αναφορών προς τους πελάτες. Για παράδειγμα μια δημοσίευση που θα αναφέρει κάτι θετικό για κάποιον πελάτη ή κάτι αρνητικό.
- Απαιτείται συμμόρφωση και να είναι συνεπείς στις πολιτικές χρήσης των Μέσων Κοινωνικής Δικτύωσης με βάση τους κανόνες της εταιρείας.
- Ενημέρωση των εργαζομένων ότι δεν έχουν καμία προσδοκία της ιδιωτικής ζωής σε κάθε έγγραφο ή ανακοίνωση που δημιουργείται, που αποστέλλεται ή λαμβάνεται με τη χρήση εξοπλισμού ή τεχνολογίας της εταιρείας.
- Απαγόρευση της απόσπασης φωτογραφιών ή βίντεο από εταιρικές εκδηλώσεις, δραστηριότητες ή εγκαταστάσεις.

Δεν είναι λίγα παραδείγματα, σύμφωνα με τα οποία τα Μέσα Κοινωνικής Δικτύωσης έχουν εμποδίσει την κατοχύρωση θέσης εργασίας. Οι εργοδότες προκειμένου να προσλάβουν κάποιον ικανό υπάλληλο, λαμβάνουν υπόψιν όλες τις πληροφορίες που μπορούν να συγκεντρώσουν για τον πιθανό υποψήφιο και ιδιαίτερη έμφαση δίνεται στις πληροφορίες όπου βρίσκονται προσβάσιμες στα Μέσα. Αυτό δημιουργεί την ανάγκη να γνωρίζουν οι υποψήφιοι εργαζόμενοι τις εκτεθειμένες στο δημόσιο κοινό πληροφορίες τους και αν μπορούν να βλάψουν την γνώμη που θα σχηματίσει ο μελλοντικός εργοδότης. Εικόνες ή βίντεο με ακατάλληλο περιεχόμενο καθώς επίσης και δημοσιεύσεις με υβριστικό περιεχόμενο ή ανάρμοστα σχόλια είναι πολύ πιθανό να αποτρέψουν την πρόσληψη ή προαγωγή του υποψηφίου και ακόμα χειρότερα, να οδηγήσουν στην απόλυσή του.

Χαρακτηριστικό παράδειγμα, έναν πρώην υπάλληλος της Microsoft, ο οποίος μετά την παραίτησή του από την εταιρεία, δήλωσε δημόσια σε ένα από τα πιο γνωστά online forum, το Reddit, ότι η Microsoft ήταν η χειρότερη εταιρεία που είχε δουλέψει ποτέ. Δεν είναι λίγοι αυτοί που μετά από κάποια παραίτηση ή απόλυση, κακολογούν τις εταιρείες τους στα Μέσα με αποτέλεσμα και να διώκονται ποινικά αλλά και να καθιστούν την μελλοντική εύρεση εργασίας από δύσκολη έως αδύνατη.

Ένας νόμος που όχι μόνο ρυθμίζει τις πιστωτικές εκθέσεις, αλλά ορίζει και τα εθνικά πρότυπα για τον έλεγχο των εργαζομένων σχετικά με το προφίλ

προσωπικότητας και συμπεριφοράς που έχει διαμορφωθεί με βάση τα Μέσα Κοινωνικής Δικτύωσης είναι η FCRA. Θέτει όρια στις πληροφορίες που μπορούν να έχουν πρόσβαση οι εργοδότες από τους ελέγχους του ιστορικού των υποψηφίων και πώς μπορούν να τις χρησιμοποιήσουν. Ωστόσο, η FCRA ισχύει μόνο για τους εργοδότες που χρησιμοποιούν οι εταιρείες ελέγχου από τρίτους. Οι πληροφορίες που ένας εργοδότης συγκεντρώνει ανεξάρτητα, μεταξύ άλλων και από την άτυπη αναζήτηση στο Διαδίκτυο, δεν καλύπτεται από την FCRA.

ΚΕΦΑΛΑΙΟ 3: ΒΑΣΙΚΑ ΔΙΚΑΙΩΜΑΤΑ ΤΟΥ ΑΤΟΜΟΥ

3.1 Ποια πραγματικά είναι τα βασικά δικαιώματα

Αρχικά αξίζει θα γίνει μια εισαγωγή στα βασικά δικαιώματα του ατόμου στα οποία εν συνεχεία θα εμβαθύνουμε. Πιο συγκεκριμένα,

1. Ο χρήστης έχει το δικαίωμα να ενημερώνεται για κάθε επεξεργασία των δεδομένων του.

Οι διαχειριστές των δεδομένων, οφείλουν να ενημερώνουν το χρήστη όποτε συγκεντρώνουν δεδομένα προσωπικού χαρακτήρα που τον αφορούν, εκτός και αν έχει ενημερωθεί για αυτά στο παρελθόν. Ο χρήστης έχει το δικαίωμα να ενημερώνεται για την ταυτότητα του ελεγκτή, τους σκοπούς της επεξεργασίας και οποιαδήποτε περαιτέρω πληροφορία, όπως για τους παραλήπτες των δεδομένων και τα προσωπικά του δικαιώματα. Έχει το δικαίωμα να λάβει τα δεδομένα αυτά ακόμα κι αν λήφθηκαν άμεσα ή έμμεσα από τρίτους. Παρεκκλίσεις επιτρέπονται στην τελευταία περίπτωση, εφόσον παροχή των πληροφοριών αποδεικνύεται αδύνατη ή εξαιρετικά δύσκολη, ή εάν απαιτείται από το νόμο.

2. Ο χρήστης έχει το δικαίωμα πρόσβασης στην συλλογή δεδομένων για το πρόσωπό του.

Ο χρήστης έχει το δικαίωμα να προσεγγίσει οποιονδήποτε διαχειριστή δεδομένων για να μάθει αν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, για να παραλάβει ένα αντίγραφο των δεδομένων σε κατανοητή μορφή και να του δοθεί κάθε διαθέσιμη πληροφορία σχετικά με τις πηγές του. Εάν τα δεδομένα προσωπικού χαρακτήρα είναι ανακριβή, ή εάν έχουν αποτελέσει αντικείμενο παράνομης επεξεργασίας, έχει το δικαίωμα να ζητήσει τη διόρθωση, το κλείδωμα ή τη διαγραφή των δεδομένων. Σε τέτοιες περιπτώσεις, το υποκείμενο των δεδομένων, μπορεί επίσης να απαιτήσει από τον διαχειριστή της επεξεργασίας να ειδοποιήσει τυχόν τρίτους που είχαν προηγουμένως πρόσβαση στα ανακριβή στοιχεία, εκτός αν αυτό είναι αδύνατο. Μια

λογική αμοιβή για την παροχή πρόσβασης μπορεί να χρεωθεί σε ορισμένες περιπτώσεις.

3. Ο χρήστης έχει πρόσβαση στην λογική με την οποία λαμβάνονται αυτοματοποιημένες αποφάσεις.

Οι αποφάσεις, που επηρεάζουν σημαντικά τον χρήστη, όπως η απόφαση για τη χορήγηση δανείου ή την έκδοση ασφάλειας, μπορεί να λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας των δεδομένων. Ως εκ τούτου, ο διαχειριστής της επεξεργασίας δεδομένων, οφείλει να λάβει κατάλληλα μέτρα διασφάλισης, όπως να παρέχει στον χρήστη τη δυνατότητα να γνωρίσει το σκεπτικό πίσω από το οποίο συλλέγονται τα δεδομένα ή ακόμα να αμφισβητήσει αποφάσεις που βασίζονται σε ανακριβή δεδομένα.

3.2 Ψηφιακά Δικαιώματα

Υπάρχουν, επί του παρόντος, λίγοι νόμοι που μπορεί να ερμηνευθούν υπέρ της προστασίας της πληροφορίας που δίνεται στα Μέσα Κοινωνικής Δικτύωσης. Οι περισσότεροι νόμοι για την προστασία της ιδιωτικότητας στις Ηνωμένες Πολιτείες, προστατεύουν συγκεκριμένους τύπους πληροφορίας, όπως τα ιατρικά ή τα οικονομικά αρχεία. Μερικοί νόμοι που προστατεύουν το απόρρητο της πληροφορίας, δεν ισχύουν για το καθημερινό surfing/browsing στο Διαδίκτυο ή με τις πληροφορίες που αποκαλύπτονται από τον χρήστη, όπως για παράδειγμα ένα κουίζ για την υγεία που παρέχει πληροφορίες στις φαρμακευτικές εταιρείες.

Η Πράξη Προστασίας Προσωπικών Δεδομένων Ηλεκτρονικών Επικοινωνιών (ECPA) ψηφίστηκε το 1986, πριν το Διαδίκτυο να γίνει το βασικότερο μέσο επικοινωνίας. Εάν οι πληροφορίες είναι αποθηκευμένες σε ένα διακομιστή, όπως οι πληροφορίες σε όλα τα Μέσα Κοινωνικής Δικτύωσης, ο νόμος αυτός καθιστά εύκολο για τις υπηρεσίες επιβολής του νόμου ή την κυβέρνηση, να έχει πρόσβαση μέσω κλήτευσης. Ένας μεγάλος αριθμός από βιομηχανίες και οργανώσεις υπεράσπισης, πιέζουν για την ενημέρωση του νόμου αυτού. Η προτεινόμενη ενημέρωση, θα ενισχύσει τις προϋποθέσεις που απαιτούνται για την κυβερνητική πρόσβαση στα δεδομένα που είναι αποθηκευμένα σε ένα διακομιστή απαιτώντας ένταλμα έρευνας. Πληροφορίες για την τοποθεσία δεν είναι ισχυρά προστατευόμενες από την ECPA.

Ο Νόμος Ηλεκτρονικού Απόρρητου για την προστασία των παιδιών (COPPA), απαιτεί ότι οι ιστοσελίδες και υπηρεσίες που απευθύνονται σε παιδιά κάτω των 13 ετών, πρέπει να περιορίζουν τη συλλογή δεδομένων και τη χρήση με συγκεκριμένους τρόπους. Υπάρχουν επίσης περιορισμοί σχετικά με τις πληροφορίες που μπορούν να αποσταλούν σε διαφημιστές. Ορισμένα κοινωνικά δίκτυα, επομένως, δεν επιτρέπουν χρήστες κάτω των 13 ετών.

Ο Νόμος προστασίας δεδομένων στο διαδίκτυο της Καλιφόρνια (California Online Privacy Act), απαιτεί από οποιαδήποτε ιστοσελίδα που συλλέγει προσωπικά αναγνωρίσιμες πληροφορίες σχετικά με τους καταναλωτές της πολιτείας, να δημοσιεύει μια πολιτική προστασίας online προσωπικών δεδομένων. Αυτή η πολιτική προστασίας της ιδιωτικότητας, πρέπει να περιγράφει ποιες κατηγορίες πληροφοριών συλλέγονται, ποιες οι κατηγορίες τρίτων που τους επιτρέπεται πρόσβαση σε αυτές τις πληροφορίες, πώς ο ιδιοκτήτης της ιστοσελίδας/υπηρεσίας θα ενημερώνει τους χρήστες σχετικά με τις αλλαγές στην πολιτική και την ημερομηνία έναρξης ισχύος αυτής. Ιστοσελίδες χωρίς πολιτική απορρήτου, έχουν προθεσμία 30 ημερών από την κοινοποίηση του νόμου για να συμμορφωθούν.

Αρκετές πολιτείες έχουν θεσπίσει νομοθεσία για την προστασία των εργαζομένων ή των αιτούντων εργασίας από τους εργοδότες, που τους υποχρεώνουν να δίνουν ένα όνομα χρήστη ή τον κωδικό πρόσβασης για ένα λογαριασμό σε κάποιο Μέσο Κοινωνικής Δικτύωσης. Για μια τρέχουσα λίστα των νόμων του κράτους και την εν αναμονή της νομοθεσίας, διαβάστε την ολοκληρωμένη συζήτηση Littler Ινστιτούτο Πολιτικής στο χώρο εργασίας της ιστορίας και το υπόβαθρο της νομοθεσίας για την προστασία κωδικού πρόσβασης των κοινωνικών μέσων μαζικής ενημέρωσης.

3.3 Εξαιρέσεις και Περιορισμοί

Το δικαίωμα στην ιδιωτικότητα μπορεί μερικές φορές να συγκρούεται με την ελευθερία της έκφρασης και, ειδικότερα, την ελευθερία του τύπου και των μέσων ενημέρωσης. Είναι, επομένως, στην διάθεση των κρατών-μελών να προβλέψουν εξαιρέσεις στη νομοθεσία περί προστασίας των δεδομένων, προκειμένου να επιτευχθεί ισορροπία μεταξύ αυτών των διαφορετικών αλλά εξίσου θεμελιωδών δικαιωμάτων.

Το εθνικό δίκαιο μπορεί να επιτρέψει άλλες εξαιρέσεις από τις διατάξεις της οδηγίας. Αυτές περιλαμβάνουν την υποχρέωση να ενημερώνεται ο χρήστης των δεδομένων, τη δημοσιοποίηση των πράξεων επεξεργασίας δεδομένων, την υποχρέωση να σέβονται τις βασικές αρχές της ορθής πρακτικής διαχείρισης δεδομένων. Τέτοιες εξαιρέσεις επιτρέπονται εφόσον, μεταξύ άλλων, είναι απαραίτητο για λόγους εθνικής ασφάλειας, άμυνας, ανίχνευση του εγκλήματος, επιβολή του ποινικού δικαίου, ή για την προστασία των χρηστών ή τα δικαιώματα και την ελευθερία των άλλων. Επιπλέον, παρέκκλιση από το δικαίωμα πρόσβασης στα δεδομένα μπορεί να χορηγείται για την επεξεργασία των δεδομένων για επιστημονικούς ή στατιστικούς σκοπούς.

3.4 Παραβίαση Δικαιωμάτων

Σε περίπτωση που θεωρήσει κάποιος ότι τα δικαιώματα του έχουν παραβιαστεί, το πρώτο βήμα είναι να επικοινωνήσει με το άτομο ή την υπηρεσία που φαίνεται να είναι η πηγή της παραβίασης με σκοπό να μάθει ποιος είναι ο διαχειριστής της επεξεργασίας δεδομένων. Στην περίπτωση που η προσπάθεια αυτή δεν φέρει κάποιο ικανοποιητικό αποτέλεσμα, μπορεί να επικοινωνήσει με την εθνική αρχή προστασίας δεδομένων. Σύμφωνα με την Ευρωπαϊκή Οδηγία, κάθε κράτος θα πρέπει να παρέχει μία ή περισσότερες δημόσιες αρχές για την εξασφάλιση της ορθής εφαρμογής της νομοθεσίας για την προστασία δεδομένων. Η αρχή αυτή, που αναφέρεται ως εποπτική αρχή, είναι αρμόδια να ακούσει τις καταγγελίες που υποβάλλονται από κάθε πρόσωπο ή επιχείρηση. Με την σειρά της, πρέπει να διερευνήσει την καταγγελία και ενδέχεται να μπορεί να απαγορεύσει προσωρινά την επεξεργασία των προσωπικών δεδομένων. Εάν διαπιστωθεί παραβίαση της νομοθεσίας για την προστασία δεδομένων, τότε μπορεί, μεταξύ άλλων, να διατάξει τη διαγραφή ή την καταστροφή των δεδομένων και/ή να απαγορεύσει την περαιτέρω επεξεργασία.

Για να επικοινωνήσει με την εποπτική αρχή, ο χρήστης θα πρέπει (κατά προτίμηση εγγράφως) να περιγράψει το πρόβλημα και να υποβάλει επαρκείς πληροφορίες, ώστε το πρόβλημα να είναι καλά ορισμένο. Σε ορισμένα κράτη-μέλη, η εποπτική αρχή έχει τυποποιημένα έντυπα που μπορεί να συμπληρώσει για να κάνει μια καταγγελία. Εάν αυτό είναι διαθέσιμο, τότε θα πρέπει να χρησιμοποιήσει τα

έτοιμα έντυπα, επειδή θα επιταχύνει τη διεκπεραίωση της υπόθεσής και θα λάβει μια απάντηση πιο γρήγορα. Σε ορισμένα κράτη-μέλη οι καταγγελίες μπορούν να υποβληθούν και μέσω e-mail.

Αν το αποτέλεσμα δεν είναι ικανοποιητικό, μπορεί να χρειαστεί να το δικαστήριο. Σε τέτοια περίπτωση είναι φρόνιμο να ζητήσει νομική συμβουλή. Το δικαστήριο μπορεί επίσης να είναι απαραίτητο, εάν έχει υποστεί ζημιές εξαιτίας της παραβίασης των δικαιωμάτων. Μπορεί να δικαιούται αποζημίωση.

Κάθε πρόσωπο ή επιχείρηση μπορεί να υποβάλει καταγγελία στην Επιτροπή σχετικά με μια υποτιθέμενη παραβίαση του νόμου δικαίου από το κράτος-μέλος. Η Ευρωπαϊκή Επιτροπή είναι υπεύθυνη για τη διασφάλιση ότι το δίκαιο εφαρμόζεται σωστά στα κράτη-μέλη. Εάν είναι απαραίτητο, η Επιτροπή υπενθυμίζει στα κράτη μέλη τις ευθύνες τους για την εφαρμογή της κοινοτικής νομοθεσίας έγκαιρα και σωστά. Σε ορισμένες περιπτώσεις, εάν ένα κράτος-μέλος αδυνατεί να εκπληρώσει τις υποχρεώσεις αυτές, η Επιτροπή μπορεί να χρειαστεί να προσφύγει στο Ευρωπαϊκό δικαστήριο, το οποίο αποφασίζει κατά πόσον ή όχι το κράτος-μέλος έχει παραβιάσει το κοινοτικό δίκαιο.

Δεν θα πρέπει να αποδείξει ότι επηρεάστηκε άμεσα από την παράβαση που επικαλείται. Ωστόσο, διαφορές μεταξύ ιδιωτών δεν μπορούν να διευθετηθούν από την Επιτροπή υπό αυτό το πλαίσιο. Αεν θα χρεωθεί για την υποβολή καταγγελίας και δεν χρειάζεται να ζητήσει τη συνδρομή δικηγόρου. Είναι σημαντικό να συμπεριλάβει σχετικές πληροφορίες και έγγραφα τεκμηρίωσης (π.χ. σχετικούς εθνικούς κανόνες) στην καταγγελία.

3.4.1 Παραδείγματα Παραβίασης

1.Ένας πάροχος τηλεπικοινωνιακών υπηρεσιών έδωσε πληροφορίες σχετικά με το τηλέφωνο ή το e-mail λογαριασμό σας σε άλλη εταιρεία. Ως αποτέλεσμα, μπορείτε να λάβετε αυτόκλητες κλήσεις ή μηνύματα ηλεκτρονικού ταχυδρομείου. Τι συμβαίνει στην περίπτωση αυτή·

==========

Εάν προσωπικά δεδομένα συλλέγονται αποκλειστικά για λόγους χρέωσης και δεν έχετε συναινέσει στην περαιτέρω μεταφορά των δεδομένων σας, τότε έχετε το δικαίωμα να αντιταχθείτε στη μεταφορά των δεδομένων σας σε τρίτους. Το πρώτο

βήμα θα πρέπει να είναι να επικοινωνήσετε με τον πάροχο, δηλώνοντας με σαφήνεια την καταγγελία σας. Εάν δεν λάβετε ικανοποιητική απάντηση, τότε θα πρέπει να επικοινωνήσετε με την εθνική εποπτική αρχή.

2. Δεν μπορείτε να πάρετε δάνειο, λόγω ανακριβών στοιχείων στο αρχείο της τράπεζας. Κάνατε μια αίτηση πρόσβασης στην τράπεζά σας, ώστε να μάθετε ποια στοιχεία έχουν καταγραφεί στην βάση δεδομένων της τράπεζας σχετικά με το πιστωτικό ιστορικό σας. Ωστόσο, η τράπεζα απέτυχε να ανταποκριθεί στο αίτημα πρόσβασης σας. Κάνατε αρκετά τηλεφωνήματα στην τράπεζα σχετικά με το αίτημα αυτό, αλλά μάταια. Τι μπορείτε να κάνετε·

==========

Η οδηγία αναφέρει ότι έχετε το δικαίωμα να αποκτήσετε πρόσβαση χωρίς υπερβολική καθυστέρηση σε όλα τα προσωπικά δεδομένα που διατηρούνται για εσάς. Εάν τα δεδομένα είναι ανακριβή, έχετε το δικαίωμα να προβείτε σε διόρθωσή τους. Ως εκ τούτου, εάν δεν λάβετε απάντηση από την τράπεζα μέσα σε ένα εύλογο χρονικό διάστημα, μπορείτε να παραπονεθείτε άμεσα στην εθνική εποπτική αρχή. Σύμφωνα με την οδηγία, η εθνική εποπτική αρχή πρέπει να διερευνήσει την καταγγελία και να ενημερώσει τον καταγγέλλοντα σχετικά με την έκβαση.

ΚΕΦΑΛΑΙΟ 4: ΑΡΝΗΤΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΚΑΙ ΑΝΑΔΥΟΜΕΝΕΣ ΑΠΕΙΛΕΣ

4.1 Προφίλ Προσωπικότητας

Παρά το γεγονός ότι τα Μέσα Κοινωνικής Δικτύωσης προσφέρουν μία πληθώρα εργαλείων για τον έλεγχο και την ρύθμιση της ιδιωτικότητας, οι χρήστες σπάνια γνωρίζουν την ύπαρξη αυτών των ρυθμίσεων και ακόμα πιο σπάνια τις θέτουν κατάλληλα για την μέγιστη δυνατή ιδιωτικότητα. Όπως αναφέρθηκε και παραπάνω, οι προεπιλεγμένες ρυθμίσεις, σχεδόν σε όλα τα μέσα όπως το Facebook, επιτρέπουν σε τρίτους να έχουν πρόσβαση σε όλη την διαθέσιμη πληροφορία. Η παραγωγή περιεχομένου στα Μέσα Κοινωνικής Δικτύωσης, παράγει με την σειρά της ροές πληροφορίας. Τα Μέσα, ενσωματώνουν την μετάβαση στην διαπροσωπική και αμοιβαία επικοινωνία και προσφέρουν την δυνατότητα για συνάθροιση της πληροφορίας. Οι χρήστες όντας αντικείμενα της επικοινωνίας, καθιστούν της πληροφορίες τους διαθέσιμες σε άλλους, και μετατρέπονται έτσι σε αντικείμενα πληροφορίας και ως εκ τούτου αντικείμενα παρακολούθησης. Η παρατήρηση της συμπεριφοράς και των χαρακτηριστικών των ατόμων, που έχουν την τάση να μεταφέρουν την καθημερινή συμπεριφορά τους online, μέσω της εξόρυξης μεγάλων ποσοτήτων δεδομένων, παραβιάζει θεμελιώδη δικαιώματα.

Αυτό έχει ως αποτέλεσμα την ανάπτυξη ειδικών εργαλείων που σε συνδυασμό με OSINT, καθιστούν εφικτή την δημιουργία ενός προφίλ προσωπικότητας και την πρόβλεψη συμπεριφοράς για κάποιον χρήστη ή μία ομάδα χρηστών. Είναι δυνατή η συλλογή και καταγραφή μεγάλου όγκου πληροφορίας, η οποία με επεξεργασία τις περισσότερες φορές κατά τρόπο αυτοματοποιημένο και με αναγνώριση προ- τύπων, οδηγεί στην εύκολη πρόβλεψη συμπεριφοράς, γεγονός το οποίο παραβαίνει το δικαίωμα για την προστασία της ιδιωτικότητας και εγκυμονεί κινδύνους. Ένας τέτοιος κίνδυνος είναι αυτός της διάκρισης με βάση πολιτικές πεποιθήσεις που μπορεί

να οδηγήσει στην αποτυχία κατοχύρωσης κάποιας θέσης εργασίας. Επιπρόσθετα, μια σημαντική απειλή για το δικαίωμα στην ιδιωτικότητα πηγάζει από το γεγονός ότι το προφίλ μπορεί να ελεγχθεί από τους λεγόμενους «ισχυρούς» και έτσι μπορεί να δημιουργήσει ευαίσθητες πληροφορίες από φαινομενικά ασήμαντα και όχι μονό, δεδομένα. Με κατάλληλη έρευνα, από τα δεδομένα του χρήστη, είναι δυνατό να εξαχθούν πληροφορίες που σχετίζονται με την προσωπικότητά του, ειδικά όταν αναφέρεται σε πολιτική ή/και θρησκευτική τοποθέτηση. Μολονότι, ο χρήστης έχει την δυνατότητα να διατηρεί ιδιωτικό προφίλ, τα σχόλιά του μπορεί να συλλέγονται διάφορες άλλες πηγές όπως σχόλια σε τοποθετήσεις φίλων. Ως εκ τούτου, είναι δυνατό να δημιουργηθεί ένα εικονικό προφίλ προσωπικότητας για τον κάθε χρήστη αποκλειστικά με βάση τις δραστηριότητες του στα κοινωνικά δίκτυα που ενδέχεται να μην απέχει πολύ από την πραγματικότητα.

Οι χρήστες εθελοντικά, συνειδητά ή ασυνείδητα, αποκαλύπτουν προσωπικά δεδομένα σε ένα ευρύ κοινό. Όπως αναφέρθηκε και παραπάνω, μία σημαντική παρατήρηση είναι ότι δεν απαιτείται απευθείας πρόσβαση στα δεδομένα των Μέσων Κοινωνικής Δικτύωσης ενός χρήστη κι αυτό γιατί μπορεί να είναι προσβάσιμα έμμεσα ψάχνοντας αυτοματοποιημένα το εκάστοτε μέσο είτε μέσω άλλων χρηστών με τους οποίους ο χρήστης επικοινωνεί ή επικοινώνησε. Η έμμεση συλλογή πληροφορίας είναι ιδιαίτερα σημαντική για την περίπτωση που ο χρήστης έχει θέσει σωστά τις ρυθμίσεις ιδιωτικότητας που του προσφέρει το μέσο. Κατά συνέπεια, ο οποιοσδήποτε είναι σε θέση να συλλέξει τέτοιες πληροφορίες και να τις επεξεργαστεί. Οι OSINT τεχνικές, όσο πιο αξιόπιστα δεδομένα έχουν στην είσοδό τους, τόσο πιο ακριβής, αξιόπιστη και παρεμβαίνουσα θα είναι η ανάλυση.

Για τον λόγο αυτό, τα παρακάτω σημαντικά σημεία πρέπει να ληφθούν υπόψιν εφόσον η ποιότητα των αποτελεσμάτων της παρακολούθησης είναι ανάλογη της ποιότητας της συλλογής δεδομένων:

- Αποκάλυψη της τοποθεσίας δεδομένων: Απαιτείται να υπάρχει γνώση της τοποθεσίας από όπου συγκεντρώθηκαν τα δεδομένα.
- Προ-επεξεργασία πηγών: Η προ-επεξεργασία χρήσιμων και σχετικών πηγών είναι ιδιαίτερα σημαντική για να αποφεύγεται η συλλογή άχρηστων ή παλιών δεδομένων.

- Καθορισμός αποτελεσμάτων: Μετά τα συμπεράσματα για το πρόσωπο της έρευνας, είναι χρήσιμη η περαιτέρω επεξεργασία των αποτελεσμάτων, με σκοπό να συγκεντρωθεί μεγαλύτερη ανάλυση στις παραμέτρους του προσώπου. Τα δεδομένα υπόκεινται σε μία διαδικασία μετεκπαίδευσης (meta-training) διότι είναι πιθανό να προκύψουν μυστικές συνδέσεις ή συσχετίσεις ανάμεσα στις παραμέτρους των δεδομένων.

4.1.1 Μελέτη Περίπτωσης Youtube

Οι παραπάνω τεχνικές και μέθοδοι δεν περιορίζονται μόνο σε Μέσα Κοινωνικής Δικτύωσης όπως το Facebook ή το Twitter. Εξίσου σημαντικό αποτελεί το κανάλι του χρήστη στο YouTube. Παρά το γεγονός ότι προσφέρει πολλές ρυθμίσεις για την προστασία της ιδιωτικότητας, οι χρήστες θα πρέπει να γνωρίζουν τις γενικές αρχές του συγκεκριμένου μέσου. Φαίνεται ότι η πλειοψηφία των χρηστών επιλέγουν να γνωστοποιήσουν τα προσωπικά τους δεδομένα σε όσο το δυνατόν περισσότερους χρήστες, αν και κατά μέσο όρο οι χρήστες δεν έχουν σαφή ιδέα για την πραγματική εμβέλεια των πληροφοριών που αποκαλύπτουν ή τείνουν να υποτιμούν το εύρος του κοινού. Χάνουν επομένως τον έλεγχο των δεδομένων τους και αγνοούν την επεξεργασία τους, καθώς γίνονται εύκολα ανιχνεύσιμα και ανάλογα με το είδος των δημοσιεύσεων μπορούν να αποτελέσουν σημείο ενδιαφέροντος για κάποιους τρίτους. Το συνονθύλευμα της πληροφορίας αυτής, παρέχει ένα ισχυρό εργαλείο για την δημιουργία ενός τελικού προφίλ του κάθε χρήστη. Επιπρόσθετα, είναι αρκετά εύκολο να προσδιορισθεί ένα συγκεκριμένο πρόσωπο, ακόμη και αν τα βασικά χαρακτηριστικά του (όνομα, οργανισμός, διεύθυνση, κλπ) έχουν αφαιρεθεί ή αποκρυφθεί, με βάση μόνο το ιστορικό του στο κάθε κοινωνικό μέσο. Επομένως, ακόμα και το YouTube, μπορεί να χρησιμοποιηθεί για αυτό το σκοπό.

Για παράδειγμα μπορεί να χρησιμοποιηθεί για ανίχνευση πολιτικών πεποιθήσεων και για εντοπισμό πιθανών απειλών. Συμπεράσματα για τις πολιτικές πεποιθήσεις των χρηστών παίρνονται με χρήση τεχνικών μηχανικής μάθησης (machine learning) για την κατηγοριοποίησης των δεδομένων των χρηστών. Οι αλγόριθμοι μηχανικής μάθησης, “μαθαίνουν” από τα παραδείγματα κειμένων που λαμβάνουν στην είσοδο και κατασκευάζουν μοντέλα που είναι σε θέση να προσδιορίσουν την ετικέτα που χαρακτηρίζει τα κείμενα αυτά. Η ανάθεση ετικετών

απαιτεί την βοήθεια ενός ειδικού, ο οποίος μπορεί να διαχωρίσει και να αιτιολογήσει τις κατηγορίες στις οποίες εντάσσεται κάθε κείμενο.

4.2 Προγνωστική Γενική Εικόνα και Πρόβλεψη

Το περιεχόμενο και η ροή πληροφορίας, μπορούν να χρησιμοποιηθούν για σκοπούς που κυμαίνονται από την δημιουργία προφίλ για στοχευμένη διαφήμιση (με βάση την ανάλυση των online χαρακτηριστικών και συμπεριφορά χρηστών), για την δημιουργία προφίλ προσωπικότητας και την πρόβλεψη συμπεριφοράς. Η ανάλυση των πληροφοριών των χρηστών, μπορεί να αποδειχθεί χρήσιμη για την εξατομίκευση, διαχείριση προφίλ ή ανίχνευση κακόβουλων ή ακόμα και για αποκλίνουσες από την συμπεριφορά του χρήστη. Μελετώντας τις ανεβασμένες πληροφορίες του χρήστη, είναι δυνατό να εξαχθούν πληροφορίες που σχετίζονται με το περιεχόμενο, ειδικά όταν σχετίζεται με τομείς όπως η πολιτική τοποθέτηση ή η προδιάθεση του χρήστη σε σχέση με την επιβολή του νόμου και των αρχών.

Τα δεδομένα που προκύπτουν από την παρακολούθηση και την επεξεργασία δεδομένων, μπορούν να οδηγήσουν σε κινδύνους εγγενείς σε κάθε είδους δημιουργίας προφίλ. Με τον όρο δημιουργία προφίλ, εννοούμε μεθόδους που περιλαμβάνουν την εξόρυξη δεδομένων και την αυτοματοποιημένη ταξινόμηση, που είναι πιθανό να κατηγοριοποιήσει τα άτομα σε συγκεκριμένες κατηγορίες κυρίως για την λήψη αποφάσεων που τα αφορούν ή επηρεάζουν.

Ο αντίστοιχος ορισμός που υιοθετήθηκε από το Συμβούλιο της Ευρωπαϊκής Σύστασης (Council of Europe Recommendation), επικεντρώνεται στην δημιουργία ή/και την χρήση των προφίλ για την αξιολόγηση, ανάλυση ή την πρόβλεψη των προσωπικών πτυχών όπως η απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προ- τιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, την τοποθεσία ή τις κινήσεις.

Η προβλεψιμότητα των επιμέρους χαρακτηριστικών και της συμπεριφοράς, εγείρει ηθικά και νομικά ζητήματα. Η δημιουργία προφίλ, καταλήγει σε να αντιμετωπίζει το άτομο σαν να ανήκει σε μια συγκεκριμένη κατηγορία, η οποία με τη σειρά της δείχνει τα χαρακτηριστικά του, και ως εκ τούτου η κατηγορία γίνεται πιο σημαντική από το άτομο το ίδιο. Η προβλεπτική εξόρυξη δεδομένων και δημιουργία προφίλ (όπως για παράδειγμα η στοχοποίηση κάποιου ως δυνητική απειλή) οδηγεί σε

ταξινομήσεις που ενδέχεται να έχουν σημαντικές συνέπειες για την ευημερία και την ελευθερία του ατόμου και άλλων συμφερόντων και δικαιωμάτων του. Σε ένα μικρό-κοινωνικό επίπεδο, η εξόρυξη δεδομένων του περιεχομένου των Μέσων Κοινωνικής Δικτύωσης, μπορεί να οδηγήσει σε διακρίσεις και προκαταλήψεις εναντίον προσώπων και ομάδων.

Όπως αναφέρθηκε παραπάνω, ένας ορατός κίνδυνος που θα πρέπει να ληφθεί υπόψη, είναι η δυνατότητα για διακρίσεις στο χώρο εργασίας. Τα online προφίλ στα Μέσα Κοινωνικής Δικτύωσης, τα blogs, τα tweets και η απευθείας σύνδεση σε φόρουμ, ελέγχονται όλο και περισσότερο από εργοδότες που ψάχνουν για πληροφορίες που μπορούν να παράσχουν στοιχεία σχετικά με τους εργαζόμενους και τους μελλοντικούς υποψήφιους. Λαμβάνοντας υπόψιν την εκθετικά αυξανόμενη συμμετοχή σε διαδικτυακούς ιστότοπους κοινωνικής δικτύωσης και σε μέσα μαζικής ενημέρωσης, δεν είναι έκπληξη το γεγονός ότι οι εργοδότες ψάχνουν για πληροφορίες σχετικά με τους αιτούντες που δεν μπορούν να γνωρίσουν με διαφορετικό τρόπο. Μια ευρύτερη και ενδεχομένως λιγότερο λογοκριμένη ή πιο ειλικρινής ροή πληροφοριών είναι εύκολα προσβάσιμη στο Διαδίκτυο. Η διαφάνεια και η ανταλλαγή των πληροφοριών που κυριαρχεί στο Διαδίκτυο και τα Μέσα Κοινωνικής Δικτύωσης, χαρακτηρίζει έναν πληθυσμό που δεν διαχωρίζει με σαφήνεια δημόσια και ιδιωτική πληροφορία. Οι πιο προσωπικές και ιδιωτικές πληροφορίες, έχουν γίνει εύκολα προσβάσιμες, ιδιαίτερα κοινόχρηστες και μεταβιβάσιμες, μεταφέροντας το βάρος της παρακολούθησης και του ελέγχου σε αυτές. Οι παραπάνω μέθοδοι, δίνουν την δυνατότητα στον εκάστοτε εργοδότη να συλλέγει συγκεντρωτικές πληροφορίες, οι οποίες χαρακτηρίζουν την συμπεριφορά του χρήστη και την αλληλεπίδρασή του με άλλους, με σκοπό την παραγωγή σχετικών προτύπων/προφίλ και την πρόβλεψη μελλοντικής συμπεριφοράς.

4.3 Καταναλωτικό Προφίλ

Οι online διαφημίσεις είναι μια βασική πηγή εισοδήματος για ένα ευρύ φάσμα υπηρεσιών και αποτελεί σημαντικό παράγοντα στην ανάπτυξη και επέκταση της οικονομίας του Διαδικτύου. Οι εταιρείες κοινωνικής δικτύωσης που παρέχουν δωρεάν διαδικτυακές υπηρεσίες στους χρήστες τους, αποτελούν εταιρείες ηλεκτρονικού εμπορίου. Είναι γνωστή εξάλλου η έκφραση: «Όταν κάτι είναι δωρεάν,

εσύ είσαι το προϊόν.» Ωστόσο, η συγκεκριμένη πρακτική των "προσωπικών" διαφημίσεων, εγείρει ανησυχίες για την προστασία των δεδομένων και την ιδιωτική ζωή. Βασικές τεχνολογίας του διαδικτύου επιτρέπουν στους παρόχους διαφημιστικών δικτύων την παρακολούθηση των χρηστών σε διάφορους δικτυακούς τόπους. Οι πληροφορίες που συγκεντρώνονται σχετικά με τη surfing συμπεριφορά και συνήθειες των χρηστών, αναλύονται ώστε να οικοδομήσει ένα εκτεταμένο προφίλ για τα συμφέροντα υπηρεσιών. Αυτά τα χαρακτηριστικά μπορούν να χρησιμοποιηθούν για να παρέχουν στους χρήστες προσαρμοσμένες ειδικά για αυτούς διαφημίσεις. Η δια δραστική διαφήμιση στα μέσα μαζικής ενημέρωσης, αναφέρεται σε ένα ευρύ φάσμα μεθόδων που αποσκοπούν στη δημιουργία πιο σχετικών διαφημίσεων.

Υπάρχουν διάφορα επιχειρηματικά μοντέλα, τα οποία μπορούν να ακολουθήσουν οι υπηρεσίες κοινωνικής δικτύωσης. Συνήθως ακολουθούν την άμεση εμπορική προώθηση. Ωστόσο, η εμπορική προώθηση που γίνεται με χρήση των προσωπικών δεδομένων, θα πρέπει να είναι σύμφωνη με τις διατάξεις της οδηγίας για την προστασία των δεδομένων και της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Οι μέθοδοι δημιουργίας σχετικών διαφημίσεων είναι οι εξής:

- Η εμπορική προώθηση που γίνεται με βάση τις ανάγκες και τα ενδιαφέροντα των αντικειμένων (contextual marketing) προσαρμόζεται στο περιεχόμενο που βλέπει ή στο οποίο έχει πρόσβαση ο χρήστης.
- Η τμηματοποιημένη εμπορική προώθηση (segmented marketing) αφορά την προώθηση διαφημίσεων προς στοχοθετημένες ομάδες χρηστών. Ένας χρήστης ανήκει σε μια ομάδα ανάλογα με τις πληροφορίες, που έχει καταχωρήσει άμεσα στην υπηρεσία της κοινωνικής δικτύωσης.
- Η εμπορική προώθηση βάσει συμπεριφοράς (behavioral marketing) επιλέγει τις διαφημίσεις βάσει τις παρατήρησης και της δυναμικής ανάλυσης της δραστηριότητας των χρηστών. Οι τεχνικές αυτές ενδέχεται να συμμορφώνονται σε διάφορες νομικές απαιτήσεις ανάλογα με τις ισχύουσες νομικές βάσεις και τα χαρακτηριστικά των τεχνικών, που εφαρμόζονται. Η ομάδα εργασίας συνιστά την αποφυγή χρησιμοποίησης των ευ- αισθητών προσωπικών δεδομένων ως μοντέλα διαφήμισης βάσει συμπεριφοράς, εκτός εάν πληρούνται όλες οι νόμιμες απαιτήσεις.

Η διαφήμιση βάσει συμπεριφοράς, είναι η διαφήμιση που βασίζεται στην παρατήρηση της συμπεριφοράς των ατόμων στην πάροδο του χρόνου. Επιδιώκει να μελετήσει τα χαρακτηριστικά αυτής της συμπεριφοράς με τις ενέργειές τους (επανειλημμένες επιτόπιες επισκέψεις, αλληλεπιδράσεις, λέξεις-κλειδιά, παραγωγή περιεχομένου online, κ.λπ.), με σκοπό την ανάπτυξη συγκεκριμένου προφίλ και την παροχή προσαρμοσμένων διαφημίσεων στους χρήστες, για να εξυπηρετούν τα δικά τους συμφέροντα. Σε αντίθεση με τις άλλες κατηγορίες διαφημίσεων που στηρίζονται στην επεξεργασία στιγμιότυπων των δεδομένων που αναζητούν οι χρήστες και τις κινήσεις τους, η εν λόγω διαφήμιση παρέχει στους διαφημιστές μια πολύ συγκεκριμένη και λεπτομερή εικόνα στους διαφημιστές για την online ζωή του χρήστη όπως τις ιστοσελίδες που επισκέφτηκε, για πόσο διάστημα κ.ο.κ

Η διαφήμιση βάσει συμπεριφοράς περιλαμβάνει τους εξής βασικούς ρόλους:

- Πάροχοι διαφημιστικών δικτύων (ad network providers). Οι πιο σημαντικοί διανομείς των διαφημίσεων βάσει συμπεριφοράς διότι συνδέουν εκδότες με διαφημιστές.
- Διαφημιστές που θέλουν να προωθήσουν ένα προϊόν ή μια υπηρεσία σε ένα συγκεκριμένο κοινό.
- Εκδότες που είναι ιδιοκτήτες ιστοτόπων και χαίρουν οικονομικής ενίσχυσης πουλώντας χώρο στις σελίδες τους για προβολή διαφημίσεων.

Η διανομή των διαφημίσεων μέσω διαφημιστικών δικτύων λειτουργεί ως εξής: Ο εκδότης δεσμεύει κενό χώρο στην ιστοσελίδα της υπηρεσίας του για να εμφανιστεί μια διαφήμιση και αφήνει το υπόλοιπο της διαδικασίας σε έναν ή περισσότερους παρόχους διαφημιστικών δικτύων. Οι πάροχοι διαφημιστικών δικτύων είναι υπεύθυνοι για τη διανομή διαφημίσεων στους εκδότες με τη μέγιστη δυνατή επίδραση, ελέγχοντας την τεχνολογία στόχευσης (tracking/targeting technology) και των σχετικών βάσεων δεδομένων. Όσο μεγαλύτερο είναι το διαφημιστικό δίκτυο, τόσο περισσότερους πόρους διαθέτει για την παρακολούθηση των χρηστών και της συμπεριφοράς τους. Ο διαφημιζόμενος συνήθως αλληλοεπιδρά με ένα ή περισσότερα δίκτυα διαφημίσεων και δεν γνωρίζει απαραιτήτως την ταυτότητα όλων των εκδοτών που διανέμουν τις διαφημίσεις του. Εκτός αυτού, ένας εκ- δότης μπορεί να έχει συμβάσεις με διαφορετικά διαφημιστικά δίκτυα, διατηρώντας διαφορετικές θέσεις στην ιστοσελίδα του για διάφορα διαφημιστικά δίκτυα.

4.3.1 Υπηρεσίες Εντοπισμού

Οι περισσότερες τεχνολογίες παρακολούθησης και διαφήμισης που χρησιμοποιούνται για την παροχή διαφήμισης βάσει συμπεριφοράς, χρησιμοποιούν κάποια μορφή επεξεργασίας στην πλευρά του χρήστη. Χρησιμοποιούν πληροφορίες από το πρόγραμμα περιήγησης του χρήστη και του υπολογιστή ή του κινητού του. Ειδικότερα, η κύρια τεχνολογία ανίχνευσης η οποία χρησιμοποιείται για την παρακολούθηση των χρηστών στο Διαδίκτυο, βασίζεται σε 'cookies παρακολούθησης. Τα Cookies αποτελούν το μέσο για την παρακολούθηση της περιήγησης του χρήστη κατά τη διάρκεια μιας εκτεταμένης χρονικής περιόδου και θεωρητικά σε διάφορους ιστότοπους.

Ενδεικτικά λειτουργούν ως εξής: Κατά κανόνα, ο πάροχος του δικτύου διαφημίσεων, τοποθετεί ένα cookie παρακολούθησης στον υπολογιστή ή κινητό του χρήστη, όταν για πρώτη φορά επισκεφτεί μια ιστοσελίδα που περιέχει μια διαφήμιση του δικτύου του. Το cookie είναι ένα μικρό αλφαριθμητικό κειμένου που αποθηκεύονται και αργότερα μπορεί να ανακτηθεί, στον υπολογιστή του χρήστη από τον ίδιο τον πάροχο δικτύου. Στο πλαίσιο της διαφήμισης βάσει συμπεριφοράς, το cookie επιτρέπει στον πάροχο διαφημιστικού δικτύου να αναγνωρίζει έναν επισκέπτη που επιστρέφει σε αυτό τον ιστότοπο ή επισκέπτεται οποιαδήποτε άλλη ιστοσελίδα εταίρα του δικτύου διαφήμισης. Τέτοιες επαναλαμβανόμενες επισκέψεις επιτρέπουν στον πάροχο διαφημιστικού δικτύου να χτίσει ένα προφίλ του επισκέπτη που θα χρησιμοποιηθεί για την παροχή εξατομικευμένων διαφημίσεων. Επειδή τα cookies παρακολούθησης τοποθετούνται από τρίτους που δεν σχετίζονται άμεσα με τον εκδότη της ιστοσελίδας, αναφέρονται συχνά ως 'cookies τρίτων (third-party cookies). Τα cookies είναι συνδεδεμένα με έναν συγκεκριμένο ιστότοπο. Μπορούν να διαβαστούν και να τροποποιηθούν μόνο από το ίδιο domain κα όχι από κάποιον άλλο ιστότοπο διαφορετικού domain. Η διάρκεια ζωής τους ποικίλει. Μπορεί ή δεν μπορεί να παραταθεί με περισσότερες επισκέψεις στον ίδιο ιστότοπο. Ωστόσο, μια ειδική κατηγορία που ονομάζεται "persistent cookies", είτε έχουν ιδιαίτερα μελλοντική ημερομηνία λήξης ή μπορούν μόνο να διαγραφούν χειροκίνητα.

Οι περισσότεροι φυλλομετρητές διαδικτύου (browsers) προσφέρουν την δυνατότητα αποκλεισμού cookies τρίτων και υποστηρίζουν επίσης την δυνατότητα ιδιωτικής περιήγησης που καταστρέφει αυτόματα τα cookies όταν ο χρήστης κλείσει τον φυλλομετρητή.

Όπως τονίστηκε παραπάνω, ένα ενιαίο δίκτυο διαφημίσεων μπορεί συνήθως να παρακολουθεί μόνο ένα μέρος της συμπεριφοράς της περιήγησης του χρήστη στο διαδίκτυο, επειδή η δυνατότητα εντοπισμού του είναι περιορισμένη στο σύνολο των εκδοτών που συνδέονται σε αυτό. Ωστόσο, μια άλλη προσέγγιση δοκιμάστηκε με την οποία ο πάροχος του δικτύου διαφημίσεων σύνηψε συνεργασία με έναν πάροχο διαδικτυακών υπηρεσιών (Internet Service Provider (ISP)), προκειμένου να παρακολουθεί το περιεχόμενο της περιήγησης του χρήστη και να εισάγει τα cookies παρακολούθησης σε όλη την μη κρυπτογραφημένη κυκλοφορία στο διαδίκτυο. Η εφαρμογή αυτής της τεχνολογίας εγείρει σοβαρά νομικά ζητήματα πέρα από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από το σκοπό για τον οποίο χρησιμοποιούνται τα δεδομένα αυτά.

4.3.2 Μελέτη Περίπτωσης: Facebook

Το Facebook συνεχίζει να προσθέσει νέες λειτουργίες και εξελίξεις σε σταθερή βάση. Δεδομένου ότι η δημιουργία λογαριασμού είναι δωρεάν, το Facebook πρέπει να αποκτήσει έσοδα με τρόπους, όπως η διαφήμιση. Οι εταιρείες μπορούν να χρησιμοποιήσουν τις δυνατότητες του Facebook ώστε να προσεγγίσουν το κοινό τους με διαφορετικούς τρόπους. Τα Μέσα Κοινωνικής Δικτύωσης, έχουν αλλάξει τον τρόπο με τον οποίο υπάρχει πρόσβαση στους καταναλωτές από τους διαφημιστές, και αυτό αλλάξει την online διαφήμιση.

Υπάρχει μία πληθώρα τρόπων με τους οποίους μπορεί να χρησιμοποιηθεί το Facebook και οι διαφορετικές επιλογές επιτρέπουν την δημιουργικότητα και τον πειραματισμό στον χώρο της διαφήμισης. Οι διαφημιστές έχουν στην διάθεσή τους, όπως και οι χρήστες, τις προσωπικές τους σελίδες, τα γκρουπ, τα μηνύματα, τις εφαρμογές (Platform Applications) κ.ο.κ. Σύμφωνα με τα δημοσιευμένα στατιστικά του Facebook για το 2009, περισσότερο από το 70% των χρηστών χρησιμοποιούν τις εφαρμογές σε μηνιαία βάση. Είναι σημαντικό να αναφερθεί, ότι η εφαρμογές αυτές είναι προαιρετικές γεγονός που σημαίνει ότι οι χρήστες οι ίδιοι ψάχνουν περισσότερα ενδιαφέροντα μέσω της υπηρεσίας και όχι μόνο την επικοινωνία με φίλους. Η εταιρεία Zynga, που χρησιμοποιεί το Facebook για να προσφέρει στους χρήστες μέσω των εφαρμογών του παιχνίδια όπως online poker, Farm Ville συγκεντρώνοντας εκατομμύρια χρήστες το μήνα, αναφέρει ότι ξοδεύει εκατομμύρια σε διαφημίσεις στο Facebook. Έρευνες και μελέτες έχουν δείξει ότι το 43% των online αγορών προέκυψαν από διαφημίσεις στο Facebook. Η στατιστική αυτή δείχνει το πόση

μεγάλη επίδραση και δύναμη μπορεί να έχει ο διαφημιστής για να φτάσει και να επηρεάσει το καταναλωτικό κοινό.

Το Facebook αποτελεί μία αποδοτική πλατφόρμα marketing διότι η δικτύωση και η επικοινωνία υπάρχουν ως βασικές λειτουργίες. Αυτό επιτρέπει στις εταιρείες να έχουν κέρδος απλά και μόνο με το να υπάρχουν συνδεδεμένες. Εκτός αυτού το Facebook επιτρέπει την πλήρη παραμετροποίηση των διαφημίσεων από τους διαφημιστές. Για την παραδοσιακή διαφήμιση σε κενούς χώρους ιστοτόπων, οι διαφημίσεις στο Facebook είναι ευκολότερο να δημιουργηθούν και να παραμετροποιηθούν και αγγίζουν ένα ευρύτερο κοινό. Δίνει την δυνατότητα στους διαφημιστές να επιλέγουν ακριβώς την περιοχή που θα παρουσιάζεται η διαφήμιση, ως εκ τούτου δεν υπάρχει σπατάλη πόρων για χρήστες έξω από την προβλεπόμενη ομάδα αγοραστών.

Οι προσωπικές πληροφορίες που δημοσιεύονται από τους χρήστες διαδραματίζουν καθοριστικό ρόλο στο έργο των διαφημιστών. Μέσω της ανάλυσης και πρόβλεψης συμπεριφοράς και ορισμένων άλλων κριτηρίων, όπως για παράδειγμα την τοποθεσία, οι καταναλωτές κατηγοριοποιούνται σε ομάδες (clusters) που αποτελούν το αντικείμενο της στοχευμένης διαφήμισης. Το Facebook μάλιστα, φημίζεται για την ευστοχία του στον τομέα τέτοιου είδους δράσεων, καθώς το ποσοστό επιτυχίας του αγγίζει το 89% , εν αντιθέσει με άλλες παρόμοιες διαδικτυακές καμπάνιες που αγγίζουν το 38%. Μάλιστα, διαθέτει και δικό του εργαλείο δημιουργίας τέτοιου είδους διαφημίσεων (Facebook for Business), το οποίο μπορεί να χρησιμοποιηθεί από οποιαδήποτε επιχείρηση ή φορέα ανεξαρτήτως του μεγέθους του. Το εργαλείο αυτό είναι πολύ απλό στη χρήση και λειτουργεί ως εξής :

i. Αρχικά ο χρήστης καλείται να παρουσιάσει ορισμένα στοιχεία της επιχείρησης/φορέα, όπως για παράδειγμα την τοποθεσία του καταστήματος που διαθέτει , και το είδος της επιχείρησης του.

ii. Στην συνέχεια, ρυθμίζονται ορισμένοι παράμετροι, σύμφωνα πάντα με τις επιθυμίες του χρήστη. Αυτές αφορούν αρχικά τη γεωγραφική θέση στην οποία είναι επιθυμητή η εμπορική δραστηριότητα, στη συνέχεια κάποια δημογραφικά χαρακτηριστικά, μερικά από τα οποία είναι η ηλικία, το γένος και το επίπεδο μόρφωσης. Τέλος, προσδιορίζονται τα ενδιαφέροντα και η συμπεριφορά του αγοραστικού κοινού στο οποίο απευθύνεται το εκάστοτε προϊόν.

Εφόσον ελεγχθούν τα παραπάνω στοιχεία και επαληθεύονται για κάποιο χρήστη του Facebook που ταιριάζει στο προφίλ του στοχοποιημένου κοινού (για παράδειγμα η τοποθεσία ελέγχεται μέσω της IR διεύθυνσης και των τοποθεσιών που έχει προσάψει το εκάστοτε άτομο στο ιδιωτικό του προφίλ), η διαφήμιση προβάλλεται με διάφορους τρόπους. Ο πρώτος και πιο διαδεδομένος τρόπος είναι να παρουσιάζεται στην αρχική σελίδα (News Feed) του χρήστη, ανάμεσα στις δημοσιεύσεις σελίδων ή προφίλ με τα οποία σχετίζεται το πρόσωπο στο οποίο απευθύνεται. Μία άλλη μορφή προβολής προϊόντων ή υπηρεσιών είναι στο δεξί μέρος της ιστοσελίδας, στο πεδίο με τις πρόσφατες δραστηριότητες των "φίλων" του προσώπου αυτού. Είναι γεγονός ότι οι διαφημίσεις αυτές είναι φτιαγμένες κατάλληλα ώστε να μην επηρεάζουν αρνητικά την εμπειρία του χρήστη στον ιστότοπο.

Πρόσφατα, στο συγκεκριμένο μέσο κοινωνικής δικτύωσης προστέθηκαν μέθοδοι διευκόλυνσης αναζητήσεων, όπως για παράδειγμα τα hashtags(#). Τα hashtags(#) ομαδοποιούν τα δεδομένα που δημοσιοποιούνται, σύμφωνα με ένα ψευδώνυμο που παραθέτετέ μετά από τη δίεση που τα χαρακτηρίζει. Ως εκ τούτου, ο εκάστοτε χρήστης μπορεί να αναζητεί δεδομένα που σχετίζονται άμεσα με αυτά. Συχνό φαινόμενο όμως είναι και η δημοσιοποίηση προσωπικών δεδομένων με την (εσφαλμένη) χρήση τους. Αυτό δεν αποτελεί τυχαίο γεγονός, αφού τα hashtags(#) αποτελούν μία από τις βασικότερες πηγές δεδομένων για τις δραστηριότητες των χρηστών. Ιστοσελίδες όπως το Twitter τα χρησιμοποιούσαν προκειμένου να εφαρμόσουν στοχευμένη διαφήμιση. Το Facebook και άλλα μέσα κοινωνικής δικτύωσης, παρατηρώντας την επιτυχία τους τα εφάρμοσαν και στις δικές τους υπηρεσίες.

Τα παραπάνω εγείρουν ανησυχίες για το κατά πόσο προσβάσιμη είναι η ιδιωτική πληροφορία. Μολονότι οι χρήστες ανεβάζουν οικειοθελώς προσωπικές πληροφορίες, ενδέχεται να αγνοούν το γεγονός ότι οι πληροφορίες αυτές μοιράζονται με τρίτους. Μεγάλες μελέτες και έρευνες αποδεικνύουν ότι όταν οι χρήστες αποδέχονται τους όρους χρήσης (Terms and Conditions) όταν δημιουργούν λογαριασμό σε μία υπηρεσία ή προσθέτουν μία εφαρμογή στην πλατφόρμα του Facebook, τείνουν να μην διαβάζουν το σημείο που αναφέρεται στην παράδοση ή/και πώληση των προσωπικών δεδομένων τους σε τρίτους φορείς χωρίς την ενημέρωση του χρήστη.

Το Facebook εγγυάται ότι η πληροφορίες που μεταβιβάζονται σε τρίτους, μεταβιβάζονται ανώνυμα. Εγγυάται δηλαδή ότι οι διαφημιστές δεν αποκτούν προσωπικές, ατομικές πληροφορίες οι οποίες θα μπορούσαν να χρησιμοποιηθούν για την ανίχνευση και τον προσδιορισμό του χρήστη, αλλά μόνο γενικού περιεχομένου δημογραφικές πληροφορίες.

Παρά το γεγονός ότι το Facebook βελτιώνει την επικοινωνία με τους χρήστες του μέσω ανακοινώσεων τέτοιου είδους, δεν θέτει με σαφήνεια και διαφάνεια τι είδους πληροφορίες διαμοιράζει και σε ποιους. Ως εκ τούτου, δεν μπορεί κανείς να εγγυηθεί ότι το Facebook διατηρεί όλες τις προσωπικές πληροφορίες ιδιωτικές.

4.4 Μέσα Κοινωνικής Δικτύωσης και Παρακολούθηση Πολιτών

Μέσα Κοινωνικής Δικτύωσης και online υπηρεσίες με εισερχόμενη ροή πληροφορίας χρηστών, έχουν καταστήσει έναν εντυπωσιακό όγκο δεδομένων διαθέσιμα στην κυβέρνηση. Οι κυβερνήσεις προσπαθούν να χρησιμοποιήσουν αυτό το χρυσωρυχείο πληροφορίας για να εξάγουν απεριόριστες, προηγουμένως άγνωστες και δυνητικά χρήσιμες πληροφορίες και να ανακαλύψουν ή να συμπεράνουν μέχρι πρότινος άγνωστα γεγονότα, μοτίβα και συσχετίσεις. Η εξόρυξη δεδομένων από τα Μέσα Κοινωνικής Δικτύωσης, έχει σοβαρές συνέπειες στο πλαίσιο της κυβερνητικής παρακολούθησης. Η ανάπτυξη της τεχνολογίας σε συνδυασμό με την εθελοντική έκθεση απεριόριστης πληροφορίας στο ευρύ κοινό, συνεισφέρουν στην παραδοσιακή κυβερνητική παρακολούθηση εφόσον η κυβέρνηση είναι σε θέση να ‘ενώσει τις τελείες’ συνδυάζοντας τις πληροφορίες και να δημιουργήσει μαζικά προφίλ χρηστών για αναγνώριση προτύπων. Τα άτομα κατατάσσονται σε κατηγορίες και αντιστοιχίζονται πρότυπα συμπεριφορών και χαρακτηριστικών.

Εδώ είναι σημαντικό να αναφερθεί η εξέλιξη της επιστήμης Big Data, που αυξάνει κατά πολύ την ανακάλυψη γνώσης. Αυτό που καθιστά την εν λόγω επιστήμη σχετική και σημαντική για την κυβερνητική παρακολούθηση, δεν είναι ο όγκος των δεδομένων αλλά η ακριβής πιθανότητα να συγκεντρώσουν και να συσχετίσουν διακριτά, κρυφά και μεγάλου όγκου σετ δεδομένων. Αεν υπάρχει αμφιβολία ότι οι κυβερνήσεις κάνουν εκτεταμένη χρήση της επιστήμης για σκοπούς παρακολούθησης. Ενδεικτικά αναφέρουμε ως παράδειγμα το σύστημα παρακολούθησης της

Αμερικανικής Κυβέρνησης με κωδική ονομασία PRISM που συλλέγει δεδομένα για την Υπηρεσία Εθνικής Ασφάλειας (NSA) και αναλύει τηλεπικοινωνίες εκτός συνόρων που συγκεντρώνονται από μία πληθώρα διαφορετικών πηγών, συμπεριλαμβανομένων και των Μέσων Κοινωνικής Δικτύωσης.

Η παρατήρηση της συμπεριφοράς και των χαρακτηριστικών των ατόμων μέσω της εξόρυξης μεγάλων ποσοτήτων δεδομένων, μπορεί να παραβιάζει τα θεμελιώδη δικαιώματα, πόσο μάλλον η συσχέτιση μεταξύ καθημερινών δραστηριοτήτων και πολιτικών πεποιθήσεων, μεταξύ χαρακτηριστικών και πρότυπων και η αντίστοιχη για την κατάταξη των ατόμων. Ο κίνδυνος να στιγματίσουν ομάδες ή πρόσωπα είναι ιδιαίτερα υψηλός. Μελέτες έχουν αποδείξει πως η εκτεταμένη συλλογή και συγκέντρωση προσωπικών πληροφοριών, συντελούν στην αύξηση της κοινωνικής αδικίας δημιουργώντας ακόμα περισσότερες διακρίσεις κατά των πολιτικών ή εθνοτικών μειονοτήτων ή των παραδοσιακά μειονεκτούντων ομάδων.

Η συλλογή και επεξεργασία δεδομένων σχετικά με τις πολιτικές πεποιθήσεις, θεωρείται από το νόμο ιδιαίτερα ευαίσθητη κατάσταση. Πολλές διεθνείς και εθνικές νομικές διατάξεις απαγορεύουν ρητά την επεξεργασία των προσωπικών δεδομένων που αποκαλύπτουν πολιτικές απόψεις. Παρέκκλιση από την απαγόρευση επεξεργασίας ευαίσθητων δεδομένων, επιτρέπεται αν και εφόσον γίνεται υπό νόμο που αποσαφηνίζει τους συγκεκριμένους σκοπούς και υποστηρίζει κατάλληλες εγγυήσεις. Οι παρεκκλίσεις αυτές πρέπει να βασίζονται στο δημόσιο συμφέρον ή τη ρητή, ενημερωμένη και γραπτή συγκατάθεση του ενδιαφερομένου.

Πολλοί οργανισμοί πιστοποιούν τη νομιμότητα της συλλογής και ανάλυσης πληροφοριών που έχει αποκτηθεί με μεθόδους εξόρυξης δεδομένων, τονίζοντας το γεγονός ότι τα δεδομένα αυτά έχουν δημοσιευτεί από το ενδιαφερόμενο άτομο. Ουσιαστικά αναφέρονται στην περίπτωση που οι άνθρωποι παράγουν περιεχόμενο ή κάποιο σχόλιο σχετικό με το περιεχόμενο άλλων χρηστών σε κοινωνικά δίκτυα ή άλλα μέσα που χρησιμοποιούν με την πραγματική τους ταυτότητα, με στόχο την έκφραση της γνώμης τους δημοσίως.

Η επιχειρηματολογία αυτή αντικατοπτρίζει την επικρατούσα θεωρία και νομολογία στις Η.Π.Α, όπου δεν υπάρχει "εύλογη προσδοκία ιδιωτικής ζωής", αν τα δεδομένα αποκαλύπτονται οικειοθελώς σε άλλους και χρησιμοποιείται για να δικαιολογήσει μεγάλης κλίμακας εξόρυξη δεδομένων, ακόμη και χωρίς τη

διασφάλιση συμμόρφωσης με διαδικαστικές εγγυήσεις και απαιτήσεις όπως άδεια ένταλμα κ.α.

Ενδεικτικά, ειδικά το λεγόμενο πρότυπο που βασίζεται στην εξόρυξη δεδομένων για πρότυπα, όταν η κυβέρνηση αναπτύσσει ένα υποθετικό μοντέλο σχετικά με τις δραστηριότητες και τα χαρακτηριστικά των ατόμων ή τους δείκτες της εγκληματικής τους συμπεριφοράς, εγείρει σοβαρές ανησυχίες. Οι κίνδυνοι από την κακή χρήση και τα σφάλματα που προκύπτουν από τη συσσώρευση και την εξόρυξη δεδομένων μεγάλης ποσότητας δεδομένων και την δημοσίευση των αποτελεσμάτων για άλλους σκοπούς είναι επίσης υψηλοί και προ- φανείς.

4.4.1 Παγκόσμια Παρακολούθηση – The Fourteen Eyes

Η συμφωνία UKUSA (UKSUA Agreement), είναι μία συμφωνία στα σήματα πληροφοριών (SIGINT) μεταξύ των χωρών: Ηνωμένο Βασίλειο, Ηνωμένες Πολιτείες Αμερικής, Αυστραλία, Καναδά και Νέα Ζηλανδία. Η συμφωνία ορίζει συν-εργασιακή συλλογή, ανάλυση και διαμοιρασμό πληροφοριών. Οι ανωτέρω χώρες-μέλη είναι επίσης γνωστές και ως Five Eyes (FVEY) και στοχεύουν στην συγκέντρωση και ανάλυση πληροφοριών από διαφορετικά μέρη του κόσμου. Παρά το γεγονός ότι οι χώρες-μέλη του FVEY έχουν συμφωνήσει να μην κατασκοπεύουν η μία την άλλη, πρόσφατα έγγραφα δημοσιευμένα από τον πληροφοριοδότη Edward Snowden, αποδεικνύουν ότι κάποιες χώρες-μέλη κατασκοπεύουν η μία τους πολίτες της άλλης και διαμοιράζονται πληροφορίες με σκοπό την παράκαμψη της εγχώριας νομοθεσίας που απαγορεύει στην παρακολούθηση των πολιτών. **(chief executive officer)**

Η συνεργασία αυτή, γίνεται και με άλλες χώρες για τον διαμοιρασμό πληροφοριών, σχηματίζοντας έτσι άλλες δύο ομάδες:

A. Nine Eyes Countries

   a. Δανία
   b. Γαλλία
   c. Ολλανδία
   d. Νορβηγία

B. Fourteen Eyes Countries

   a. Βέλγιο

   b. Γερμανία

   c. Ιταλία

   d. Ισπανία

   e. Σουηδία

Η κάθε μία από τις παραπάνω χώρες μπορεί να κατασκοπεύει τους πολίτες της άλλης.

ΚΕΦΑΛΑΙΟ 5: ΠΟΛΙΤΙΚΗ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

5.1 Βασική πολιτική

Με την όλο και μεγαλύτερη εξοικείωση του ατόμου με το Διαδίκτυο και τα Μέσα Κοινωνικής Δικτύωσης, αρχίζει πλέον να είναι κοινό μυστικό στην εποχή της παγκοσμιοποίησης, ότι είναι δύσκολο και σε κάποιες περιπτώσεις αδύνατο να κρατήσει κάποιος απόρρητα προσωπικά του δεδομένα. Είναι γνωστή σε όλους η έκφραση Ό,τι συμβαίνει στο Διαδίκτυο, μένει στο Διαδίκτυο (What happens on the Internet, stays on the Internet).

Ο χρήστης θα πρέπει να είναι ενήμερος για την τρέχουσα τεχνολογία και νομοθεσία και να γνωρίζει ότι τα στοιχεία που παραθέτει online συγκεντρώνονται και υπόκεινται επεξεργασία. Κάθε φορά που κάνει μια αγορά μέσω Διαδικτύου, κάθε φορά που στέλνει μια φωτογραφία, κάθε φορά που μοιράζεται μία πληροφορία, θα πρέπει να γνωρίζει ότι ενδεχομένως τα στοιχεία αυτά δεν θα παραμείνουν απόρρητα. Τουναντίον, δεδομένα τέτοιου είδους μπορούν μεταγενέστερα να χρησιμοποιηθούν για διάφορους σκοπούς ή/και να μοιράσουν με τρίτες υπηρεσίες, οργανισμούς ή επιχειρήσεις.

Η εξέλιξη της τεχνολογίας ηλεκτρονικών υπολογιστών παράλληλα με τις νέες τεχνολογίες του Διαδικτύου και των δικτύων, επιτρέπει τον ευκολότερο διαμοιρασμό των προσωπικών δεδομένων, ακόμη και εκτός συνόρων. Ως αποτέλεσμα, δεδομένα που αφορούν πολίτες μίας χώρας-μέλους της ΕΕ, μερικές φορές επεξεργάζονται σε άλλη χώρα-μέλος της ΕΕ. Ως εκ τούτου, καθώς προσωπικά δεδομένα συγκεντρώνονται και επεξεργάζονται συχνά, είναι απαραίτητη η θέσπιση κανονισμών για τις μεταφορές δεδομένων.

Υπό αυτό το πλαίσιο, εθνικοί νόμοι που αφορούν στην προστασία δεδομένων απαιτούν υγιείς πρακτικές και πολιτικές διαχείρισης δεδομένων από την πλευρά των όσων εκτελούν επεξεργασία δεδομένων. Οι εν λόγω πολιτικές περιλαμβάνουν την υποχρέωση να διαχειρίζονται τα δεδομένα με ασφάλεια και να χρησιμοποιούν προσωπικά δεδομένα παρά μόνο για σαφείς και νόμιμους σκοπούς. Οι εθνικοί νόμοι κατοχυρώνουν επίσης μια σειρά δικαιωμάτων για τα άτομα, όπως το δικαίωμα να ενημερωθούν σε περίπτωση επεξεργασίας προσωπικών δεδομένων και για τους λόγους αυτής και τέλος το δικαίωμα να έχουν πρόσβαση σε όλα τα δεδομένα αν χρειαστεί, το δικαίωμα να απαιτήσουν την τροποποίηση ή διαγραφή αυτών.

Παρά το γεγονός ότι οι εθνικοί νόμοι για την προστασία δεδομένων στοχεύουν στην κατοχύρωση των ίδιων δικαιωμάτων, υπήρξαν μερικές διαφορές, οι οποίες θα μπορούσαν να αναπτύξουν πιθανά εμπόδια στην ελεύθερη ροή πληροφορίας και να εισάγουν επιπρόσθετο φορτίο στους χρηματοοικονομικούς τελεστές και στους πολίτες. Ενδεικτικά, μερικές από αυτές ήταν:

- Η αναγκαιότητα εγγραφής ή εξουσιοδότησης για την επεξεργασία δεδομένα υπό την επίβλεψη των αρμόδιων αρχών σε μερικές χώρες-μέλη της Ευρωπαϊκής Ένωσης.
- Η ανάγκη συμμόρφωσης με διαφορετικά πρότυπα και η πιθανότητα περιορισμού μεταφοράς δεδομένων σε άλλες χώρες-μέλη. Επιπρόσθετα, κάποιες χώρες-μέλη δεν είχαν νόμους για την προστασία των δεδομένων.

Για τους παραπάνω λόγους, υπήρχε η ανάγκη για καθιέρωση προτύπων σε Ευρωπαϊκό επίπεδο με την μορφή Ευρωπαϊκών οδηγιών.

5.2 Η Ευρωπαϊκή Οδηγία 95/46/EC: Προστασία Δεδομένων

Για την αποφυγή των εμποδίων στην ελεύθερη ροή πληροφορίας χωρίς τον υποβιβασμό της προστασίας των προσωπικών δεδομένων, η Ευρωπαϊκή Οδηγία 95/46/EC ορίσθηκε για να εναρμονίσει τις εθνικές διατάξεις. Ως αποτέλεσμα, τα προσωπικά δεδομένα όλων των πολιτών θα έχουν ανάλογη προστασία σε όλες τις χώρες-μέλη της Ευρωπαϊκής Ένωσης.

Η εν λόγω Ευρωπαϊκή Οδηγία ισχύει για οποιοδήποτε εγχείρημα ή σύνολο εγχειρημάτων πάνω σε προσωπικά δεδομένα, δηλαδή σε οποιοδήποτε είδος

επεξεργασίας προσωπικών δεδομένων όπως για παράδειγμα την συλλογή τους, την αποθήκευσή τους, την αποκάλυψή τους σε τρίτους κ.ο.κ. Η οδηγία ισχύει και για δεδομένα τα οποία υπόκειται οποιοδήποτε είδος επεξεργασίας κατά τρόπο αυτοματοποιημένο, όπως για παράδειγμα μία βάση δεδομένων πελατών.

Ωστόσο, η Οδηγία για την προστασία δεδομένων, δεν ισχύει για επεξεργασία δεδομένων που γίνεται για καθαρά προσωπικό σκοπό ή για οικιακές δραστηριότητες, όπως ένα ηλεκτρονικό προσωπικό ημερολόγιο. Επιπρόσθετα δεν ισχύει σε θέματα που αφορούν σε δημόσια ασφάλεια, άμυνα ή επιβολή ποινικού δικαίου. Τα θέματα αυτά βρίσκονται εκτός της αρμοδιότητας της Ευρωπαϊκής Οδηγίας και παραμένουν εθνικά προνόμια. Η Εθνική νομοθεσία παρέχει την προστασία του ατόμου σε αυτά τα θέματα.

Μολονότι οι κανόνες της Ευρωπαϊκής Ένωσης για την προστασία των προσωπικών δεδομένων είναι από τους αυστηρότερους στον κόσμο, η ραγδαία αλλαγή και εξέλιξη της τεχνολογίας και της καθημερινής ζωής βάση της προηγούμενης, δημιουργεί την άμεση ανάγκη για επανεξέταση και ενδεχομένως αναθεώρηση αυτών. Η νέα στρατηγική για την προστασία των δεδομένων έχει ως σκοπό να διασφαλίσει, ότι όλοι οι χρήστες θα γνωρίζουν τον τρόπο με τον οποίο χρησιμοποιούνται οι πληροφορίες που εμπιστεύονται σε εταιρείες είτε δημόσιες είτε ιδιωτικές, δημόσιες αρχές και ιστοσελίδες κοινωνικής δικτύωσης. Παροχής Διαδικτυακών Υπηρεσιών, Μηχανές Αναζήτησης και γενικότερα όσες υπηρεσίες έχουν στην διάθεση τους προσωπικά δεδομένα, θα υποχρεούνται να αποκαλύπτουν ποιος συλλέγει τα δεδομένα αυτά και για ποιο σκοπό.

Η νέα στρατηγική εισάγει για πρώτη φορά την έννοια του δικαιώματος διαγραφής από τη μνήμη (Right to be forgotten), δηλαδή το δικαίωμα του καθενός να απαιτεί την πλήρη διαγραφή των δεδομένων του αμέσως μετά την εξυπηρέτηση του αρχικού σκοπού αποστολής τους. Ωστόσο σήμερα, μόνον οι εταιρείες τηλεπικοινωνιών οφείλουν να ενημερώνουν παράνομη πρόσβαση στα προσωπικά τους στοιχεία.

Η νέα αυτή στρατηγική, θα επεκτείνει την υποχρέωση αυτή και σε άλλους κλάδους, όπως για παράδειγμα στον χρηματοπιστωτικό τομέα. Οι εταιρείες θα μπορούν να στέλνουν προσωπικά στοιχεία εκτός Ευρωπαϊκής Ένωσης μόνον εφόσον ο αποδέκτης των στοιχείων αυτών βρίσκεται σε χώρα, που διαθέτει ανάλογο επίπεδο

προστασίας δεδομένων. Θα προστατεύονται επίσης και τα προσωπικά στοιχεία, που κατέχουν η αστυνομία και οι δικαστικές αρχές. Οι εθνικές αρχές προστασίας δεδομένων θα ενισχυθούν και θα πρέπει να συνεργάζονται πιο στενά μεταξύ τους για την αποφυγή τυχόν καταχρήσεων.

Στοχεύει επίσης στην διαμόρφωση μιας κοινής προσέγγισης σε όλες τις χώρες τις Ευρωπαϊκής Ένωσης. Δεδομένου ότι οι σημερινοί κανόνες δεν εφαρμόζονται με τον ίδιο τρόπο από όλες τις χώρες, δεν είναι σαφές κάθε φορά ποιος νόμος ισχύει και σε ποια περίπτωση. Αυτό μπορεί να αποβεί εμπόδιο για την ανάπτυξη επιχειρηματικής δραστηριότητας. Με την αναθεώρηση της νομοθεσίας, οι πολυεθνικές εταιρείες θα πρέπει να συμμορφώνονται με ένα ενιαίο σύνολο κανόνων.

5.3 Ευρωπαϊκή Οδηγία 97/66/EC: Ιδιωτικότητα στις Τηλεπικοινωνίες

Ως ξεχωριστή οδηγία, η Οδηγία 97/66/EC, ασχολείται αποκλειστικά με την προστασία της ιδιωτικότητας στις τηλεπικοινωνίες. Η οδηγία ορίζει ότι όλα τα κράτη-μέλη της Ευρωπαϊκής Ένωσης πρέπει να εγγυούνται το απόρρητο της επικοινωνίας μέσα από εθνικούς κανονισμούς. Αυτό σημαίνει ότι οποιουδήποτε είδους υποκλοπή, αποθήκευση ή άλλου είδους διακοπή και παρακολούθηση επικοινωνίας μή-εξουσιοδοτημένη είναι παράνομη. Επιπρόσθετα, σε περιπτώσεις που προσφέρεται η αναγνώριση καλούντο αριθμού, οι χρήστες θα πρέπει να έχουν την δυνατότητα να ζητήσουν να μην αποκαλύπτεται ο προσωπικός τους αριθμός και ταυτότητα όταν πραγματοποιούν κλήσεις. Αντιστρόφως, όσοι έχουν ζητήσει αναγνώριση καλούντο, θα πρέπει να έχουν την δυνατότητα να απορρίψουν εισερχόμενες κλήσεις από χρήστες που έχουν αποκρύψει τον προσωπικό τους αριθμό. Η Οδηγία αποσαφηνίζει επίσης ότι όπου τυπώνονται ή υπάρχουν κατάλογοι τηλεπικοινωνιών, όπως για παράδειγμα τηλεφωνικοί κατάλογοι, ο χρήστης έχει το δικαίωμα να ζητήσει να μην βρίσκεται στην λίστα, χωρίς κάποιο κόστος.

5.4 Κανόνες για τους Διαχειριστές Δεδομένων

Διαχειριστές δεδομένων, είναι οι άνθρωποι ή το σώμα, που καθορίζει τον σκοπό και τα μέσα της επεξεργασίας δεδομένων, τόσο στον δημόσιο όσο και στον

ιδιωτικό τομέα. Για παράδειγμα, ένας γιατρός είναι συνήθως ο διαχειριστής των δεδομένων των ασθενών του, μία εταιρεία είναι ο διαχειριστής των δεδομένων των υπαλλήλων της, ένα Μέσο Κοινωνικής Δικτύωσης είναι ο διαχειριστής των δεδομένων των χρηστών του κ.ο.κ.

Οι διαχειριστές δεδομένων πρέπει να πληρούν ορισμένες βασικές αρχές. Οι αρχές αυτές, όχι μόνο στοχεύουν στην προστασία του ατόμου αλλά αποτελούν μία δήλωση καλής επιχειρηματικής πολιτικής που συνεισφέρει στην αξιόπιστη και αποδοτική επεξεργασία δεδομένων. Ο κάθε διαχειριστής δεδομένων, πρέπει να υπόκειται στους κανόνες επεξεργασίας δεδομένων της χώρας-μέλους της Ευρωπαϊκής Ένωσης, και αυτό ισχύει ακόμα και αν τα προς επεξεργασία δεδομένα ανήκουν σε άτομο άλλης χώρας-μέλους. Οι κανόνες είναι οι παρακάτω:

a. Τα δεδομένα πρέπει να επεξεργάζονται δίκαια και νόμιμα.

    - Η συλλογή δεδομένων πρέπει να γίνεται για σαφείς και νόμιμους σκοπούς και να χρησιμοποιείται αναλόγως.
    - Τα δεδομένα πρέπει να είναι σχετικά και όχι υπερβολικά σε σχέση με τον σκοπό για τον οποίο γίνεται η συλλογή τους.

b. Τα δεδομένα πρέπει να είναι ακριβή, και όπου χρειάζεται, πρέπει να είναι ενημερωμένα.

    - Οι διαχειριστές δεδομένων, πρέπει να παρέχουν εύλογα μέτρα με σκοπό να μπορούν οι χρήστες να διορθώσουν, διαγράψουν ή να φράξουν εσφαλμένα δεδομένα για τους ίδιους.
    - Δεδομένα που προσδιορίζουν και πιστοποιούν άτομα, δεν θα πρέπει να διατηρείται για παραπάνω από το αναγκαίο χρονικό διάστημα.
    - Η οδηγία καθιστά σαφές ότι κάθε κράτος-μέλος θα πρέπει να παρέχει μία ή περισσότερες εποπτικές αρχές υπεύθυνες για τον έλεγχο της εφαρμογής της οδηγίας. Μία βασική ευθύνη της εποπτικής αρχής είναι να διατηρεί ένα ενημερωμένο δημόσιο μητρώο έτσι ώστε το ευρύ κοινό να έχει πρόσβαση σε όλα τα ονόματα όλων των διαχειριστών δεδομένων καθώς και το είδος της επεξεργασίας που επιτελούν.
    - Όλοι οι διαχειριστές δεδομένων πρέπει να ενημερώνουν την εποπτική αρχή όταν επεξεργάζονται δεδομένα. Τα κράτη-μέλη μπορούν να προβούν στην

απλούστευση ή απαλλαγή από ορισμένα είδη επεξεργασίας δεδομένων που δεν παρουσιάζουν ιδιαίτερους κινδύνους. Αυτό μπορεί να χορηγηθεί όταν, σε συμφωνία με την εθνική νομοθεσία, ένας ανεξάρτητος αξιωματικός επικεφαλής της προστασίας δεδομένων έχει διοριστεί από τον διαχειριστή. Τα κράτη μέλη μπορούν να απαιτήσουν προκαταρκτικό έλεγχο από την εποπτική αρχή πριν από επεξεργασία δεδομένων που ενέχει κινδύνους. Τα είδη της επεξεργασίας δεδομένων που περιλαμβάνουν ρίσκο και κινδύνους, καθορίζονται από τα κράτη-μέλη.

5.5 Μεταφορές Δεδομένων στο Διαδίκτυο

Θα ήταν μάλλον παράλογο και χωρίς νομική αιτιολόγηση, να εξαιρεθεί ένα τόσο σημαντικό μέσο μεταφοράς δεδομένων όπως το Διαδίκτυο από το πεδίο εφαρμογής της οδηγίας για την προστασία των δεδομένων. Τουναντίον, ο τεράστιος όγκος και η πολλαπλή φύση των προσωπικών δεδομένων που μεταδίδονται μέσω του Διαδικτύου σε όλο τον κόσμο, συμπεριλαμβανομένων των χωρών χωρίς επαρκή προστασία, απαιτεί ιδιαίτερη προσοχή και έμφαση. Ως εκ τούτου, η οδηγία για την προστασία των δεδομένων, είναι τεχνολογικά ουδέτερη.

Αυτό σημαίνει πως οι διατάξεις της, ισχύουν ανεξάρτητα από το τεχνολογικό μέσο που χρησιμοποιείται για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, η οδηγία εφαρμόζεται για την ‘αόρατη’ συλλογή δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο (Λόγου χάρη τα «cookies» που χρησιμοποιούνται για να παρακολουθούν τις συνήθειες surfing του χρήστη). Από την άλλη πλευρά, θα μπορούσε να υποστηριχθεί πως εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται με τρόπο «ορατό», ο χρήστης έχει δώσει τη συγκατάθεσή του για τη μεταφορά αυτή, φυσικά υπό την προϋπόθεση ότι έχει ενημερωθεί σωστά σχετικά με τους κινδύνους που εμπλέκονται.

5.6 Αρχές για τους Παρόχους Διαφημιστικών Δικτύων

Όπως αναφέρθηκε και παραπάνω, η Οδηγία 95/46/ΕC, το άρθρο 6 αυτής, θέτει συγκεκριμένες αρχές οι οποίες πρέπει να πληρούνται από τους διαχειριστές δεδομένων. Συγκεκριμένα, το εργατικό σώμα του άρθρου 29, τονίζει ότι θα πρέπει να

είναι ενήμεροι για την συλλογή προσωπικών προφίλ για την δημιουργία διαφημίσεων βάσει συμπεριφοράς αλλά και ότι θα μπορούν να χρησιμοποιηθούν και για άλλους σκοπούς όχι μόνο για διαφημίσεις. Θα μπορούσαν για παράδειγμα να χρησιμοποιηθούν για την δημιουργία νέων υπηρεσιών άγνωστης φύσεως.

Ωστόσο, πρέπει να υπάρχει συμμόρφωση με βάση το άρθρο 6(1)(b) το οποίο θέτει την αρχή του περιορισμού του σκοπού. Η αρχή αυτή απαγορεύει την επεξεργασία προσωπικών δεδομένων που δεν είναι συμβατή με τους σκοπούς που νομιμοποίησαν την αρχική συλλογή. Αυτό σημαίνει ότι ασύμβατες και δευτερεύουσες χρήσεις των αποθηκευμένων δεδομένων για δημιουργία διαφημίσεων βάσει συμπεριφοράς, θα έρχονται σε αντιδιαστολή με το άρθρο 6 της Ευρωπαϊκής Οδηγίας 95/46/EC. Για παράδειγμα, εάν τα δίκτυα διαφημίσεων αποτελούν μέρος ενός ομίλου εταιριών που παρέχουν πολλαπλές υπηρεσίες, κατ' αρχήν, το δίκτυο διαφήμισης δεν μπορεί να χρησιμοποιήσει τα δεδομένα που συλλέγονται για διαφήμιση βάσει συμπεριφοράς για τέτοιες άλλες υπηρεσίες, εκτός εάν μπορεί να αποδειχθεί ότι οι σκοποί είναι συμβατοί. Για τους ίδιους λόγους, τα δίκτυα διαφημίσεων δεν μπορούν να εμπλουτίσουν τις πληροφορίες που συλλέγουν για τους σκοπούς του διαφήμισης με βάσει την συμπεριφορά με άλλες επιπρόσθετες πληροφορίες.

Αν οι πάροχοι δικτύων διαφημίσεων θελήσουν να χρησιμοποιήσουν τις συλλεγμένες πληροφορίες για διαφημίσεις βάσει συμπεριφοράς για δευτερεύοντες και ασύμβατους σκοπούς, για παράδειγμα ανάμεσα σε υπηρεσίες, θα χρειαστούν επιπρόσθετη νομική κάλυψη σύμφωνα με το ΄Άρθρο 7 της Ευρωπαϊκής Οδηγίας 95/46/EC. Ως εκ τούτου, θα πρέπει να πληροφορήσουν τους χρήστες και στις περισσότερες περιπτώσεις να ζητήσουν την συγκατάθεσή τους σύμφωνα με το άρθρο 7(a).

Ως εκ τούτου, η ομάδα εργασίας του άρθρου 29 καλεί τους παρόχους δικτύου διαφημίσεων να εφαρμόσουν πολιτικές που να διασφαλίζουν ότι οι πληροφορίες που συλλέγονται κάθε φορά που διαβάζεται ένα cookie, αμέσως διαγράφεται ή ανωνυμοποιείται εφόσον δεν είναι αναγκαία η διατήρησή του. Κάθε υπεύθυνος επεξεργασίας δεδομένων πρέπει να είναι σε θέση να δικαιολογήσει την ανάγκη για μια δεδομένη περίοδο διατήρησης.

5.7 Προσωπικά Δεδομένα και Ευαίσθητα Δεδομένα

Τα προσωπικά δεδομένα μπορούν να υποστούν επεξεργασία όπως την συλλογή και την περαιτέρω χρήση αν:

- Ο χρήστης έχει απερίφραστα δώσει την συγκατάθεσή του, για παράδειγμα αν έχει συμφωνήσει αφότου έχει ενημερωθεί πλήρως.
- Η επεξεργασία δεδομένων είναι απαραίτητη για την απόδοση ενός συμβολαίου που περιλαμβάνει τον χρήστη ή στην περίπτωση που απαιτείται για την δημιουργία ενός συμβολαίου από τον χρήστη. Για παράδειγμα η επεξεργασία δεδομένων για την δημιουργία λογαριασμών ή για έναν υποψήφιο για μια θέση εργασίας ή για ένα δάνειο.

5.7.1 Η επεξεργασία απαιτείται για νομική υποχρέωση

- Η επεξεργασία δεδομένων είναι απαραίτητη για την προστασία κάποιου στοιχείου που είναι κρίσιμο για την ζωή του χρήστη. Για παράδειγμα, σε περίπτωση αυτοκινητιστικού ατυχήματος που ο χρήστης έχει χάσει τις αισθήσεις του, οι τραυματιοφορείς μπορούν να προβούν σε εξετάσεις αίματος του ασθενούς αν κρίνεται απαραίτητο για να σωθεί η ζωή του.
- Η επεξεργασία είναι απαραίτητη για την εκτέλεση καθηκόντων δημόσιων συμφερόντων ή καθήκοντα επίσημων αρχών όπως για παράδειγμα την κυβέρνηση, τους φορείς πρακτικής αρχής κ.α
- Η επεξεργασία δεδομένων μπορεί να συμβεί οποτεδήποτε ο διαχειριστής ή κάποιος τρίτος οργανισμός/σώμα έχει νόμιμο ενδιαφέρον. Ωστόσο, το ενδιαφέρον αυτό δεν πρέπει να παρακάμπτει τα ενδιαφέροντα ή τα βασικά δικαιώματα του χρήστη, και ειδικά το δικαίωμα στην ιδιωτικότητα. Η διάταξη αυτή καθιερώνει την ανάγκη για την επίτευξη μιας λογικής ισορροπίας, μεταξύ των επιχειρηματικών συμφερόντων των διαχειριστών δεδομένων και την ιδιωτικότητα των χρηστών. Η ισορροπία αυτή αξιολογείται σε πρώτο βαθμό από τους διαχειριστές επεξεργασίας δεδομένων υπό την εποπτεία των αρχών προστασίας των δεδομένων, όμως, αν και εφόσον απαιτείται, τα δικαστήρια έχουν την τελική απόφαση.

Πολύ αυστηροί κανόνες ισχύουν για την επεξεργασία ευαίσθητων δεδομένων. Τα δεδομένα που αφορούν τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα,

τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις, την υγεία των δεδομένων ή σεξουαλικής προτίμησης, θεωρούνται ευαίσθητα δεδομένα. Τέτοιου είδους δεδομένα, δεν μπορούν να υποβληθούν σε επεξεργασία. Η παρέκκλιση αυτού, είναι ανεκτή μόνο κάτω από πολύ συγκεκριμένες συνθήκες. Οι συνθήκες αυτές περιλαμβάνουν τη ρητή συγκατάθεση του υποκειμένου των δεδομένων για την επεξεργασία ευαίσθητων δεδομένων, την επεξεργασία των δεδομένων με εντολή από το εργατικό δίκαιο, όπου μπορεί να είναι αδύνατο για το χρήστη των δεδομένων να συναινέσει (όπως στο προηγούμενο παράδειγμα με την εξέταση αίματος για το θύμα του τροχαίου ατυχήματος), η επεξεργασία των δεδομένων που έχει ανακοινωθεί δημοσίως από το χρήστη ή την επεξεργασία των δεδομένων σχετικά με τα μέλη συνδικάτων, πολιτικών κομμάτων ή εκκλησιών. Τα κράτη-μέλη μπορούν να προβλέπουν πρόσθετες εξαιρέσεις για σημαντικούς λόγους δημοσίου συμφέροντος.

ΚΕΦΑΛΑΙΟ 6: ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Πέρα από τις νομοθετικές αρχές οι οποίες προστατεύουν (ή και όχι) τα δικαιώματα του πολίτη στην ιδιωτικότητα, ο καθένας μπορεί με χρήση κατάλληλων εργαλείων και μεθόδων να προστατέψει όσο το δυνατόν περισσότερο την ιδιωτικότητα του στο Διαδίκτυο και να αγγίξει την ανωνυμία (Θεωρώντας ότι η απόλυτη και συνεχής ανωνυμία στο διαδίκτυο είναι αδύνατη).

6.1 Κρυπτογράφηση

Είναι συχνή η παρατήρηση του όρου κρυπτογράφηση (Encryption) στον χώρο του Διαδικτύου σε συνδυασμό με τους όρους της προστασίας της ιδιωτικότητας και της πληροφορίας. Η κρυπτογράφηση αναφέρεται στην μετατροπή δεδομένων οποιουδήποτε τύπου σε μη-κατανοητή μορφή (cipher text)και αποτελεί τον πιο ασφαλή τρόπο αποθήκευσης και διαμοιρασμού πληροφορίας. Για την πρόσβαση σε κρυπτογραφημένα δεδομένα, δηλαδή για την αποκρυπτογράφηση, θα πρέπει να υπάρχει πρόσβαση στο μυστικό κλειδί-κωδικό που είναι απαραίτητο για την αποκρυπτογράφηση. Για να γίνει κατανοητή η σημασία της επιστήμης της κρυπτογραφίας και της κρυπτογράφησης, ακολουθεί δύο απλά παραδείγματα:

- Ας υποθέσουμε ότι κάποιος έχει μεγάλο όγκο προσωπικών δεδομένων όπως για παράδειγμα μηνύματα, φωτογραφίες και οικονομικά έγγραφα στο προσωπικό του λάπτοπ ή κινητό. Αν έχανε μία από αυτές τις συσκευές, όλη αυτή η ευαίσθητη και ιδιωτική πληροφορία θα ήταν προσβάσιμη από τον οποιονδήποτε το είχε στην κατοχή του.
- Ας υποθέσουμε ότι κάποιος κάνει διάφορες συναλλαγές οικονομικής φύσεως στο Διαδίκτυο όπως για παράδειγμα τραπεζικές συναλλαγές. Αν κάποιος κακόβουλος χρήστης παρακολουθεί τις δραστηριότητες του, μπορεί να υποκλέψει εύκολα όλες τις πληροφορίες, συμπεριλαμβανομένων των οικονομικών στοιχείων όπως τον τραπεζικό αριθμό και τον αριθμό της πιστωτικής/χρεωστικής κάρτας.

Στο σημείο αυτό έγκειται η σημασία της κρυπτογράφησης: Μη-εξουσιοδοτημένα πρόσωπα δεν μπορούν να έχουν πρόσβαση στις ιδιωτικές πληροφορίες. Όταν η πληροφορία δεν είναι κρυπτογραφημένη (καλείται plain text), μπορεί να την διαβάσει και επομένως να αποκτήσει ο καθένας. Όταν όμως η πληροφορία είναι κρυπτογραφημένη (cipher text), μόνο όποιος κατέχει το κλειδί αποκρυπτογράφησης μπορεί να έχει πρόσβαση. Μια καλή αναλογία του κλειδιού αποκρυπτογράφησης μπορεί να γίνει με το κλειδί της εξωτερικής πόρτας του σπιτιού. Για την προστασία λοιπόν της πληροφορίας, αρκεί η προστασία του κλειδιού αποκρυπτογράφησης.

Σε γενικές γραμμές η κρυπτογράφηση δουλεύει για δύο βασικές κατηγορίες: Για την σταθερή πληροφορία,data at rest , όπως στον σταθερό υπολογιστή ή το λάπτοπ και για την πληροφορία σε κίνηση, data in motion, όπως την πληροφορία σε online συναλλαγές.

6.1.1 Σταθερή Πληροφορία

Ο βασικός σκοπός την κρυπτογράφησης σε σταθερή πληροφορία είναι η προστασία αυτής σε περίπτωση που το μέσο χαθεί ή κλαπεί. Πριν κάποια χρόνια αυτό δεν ήταν ιδιαίτερο πρόβλημα καθώς οι φορητοί υπολογιστές δεν υπήρχαν και οι σταθεροί ήταν μεγάλου όγκου. Ωστόσο σήμερα, με τα λάπτοπ και ιδιαίτερα τις κινητές συσκευές που εκτελούν χρέη φορητού υπολογιστή και περιέχουν μεγάλο όγκο ευαίσθητων πληροφοριών, η ανάγκη για κρυπτογράφηση είναι υπαρκτή και σημαντική. Επιπρόσθετα, πολλά άλλα μέσα μετακίνησης πληροφορίας όπως οι εξωτερικοί σκληροί δίσκοι και τα USB παρουσιάζουν την ίδια ανάγκη.

Μια συχνή τεχνική κρυπτογράφησης υπολογιστών και λοιπών φορητών μέσων ονομάζεται Πλήρης Κρυπτογράφηση Δίσκου (Full Disk Encryption) και εργαλεία για την ενεργοποίησή της παρέχονται ενσωματωμένα σε όλα τα σύγχρονα λειτουργικά συστήματα.

6.1.2 Πληροφορία σε Κίνηση

Όπως και στο παράδειγμα με τις online συναλλαγές, η πληροφορία που μεταφέρεται μέσω Διαδικτύου χρειάζεται μηχανισμούς κρυπτογράφησης για να διασφαλίζεται η ιδιωτικότητα των δεδομένων. Αν η πληροφορία δεν είναι κρυπτογραφημένη, είναι εύκολα προσβάσιμη από μη-εξουσιοδοτημένους χρήστες.

Για τον λόγο αυτό πρέπει να διασφαλίζεται η κρυπτογράφηση ευαίσθητων online πληροφοριών όπως τραπεζικές συναλλαγές και e-mail.

Η πιο συχνή κρυπτογράφηση online είναι η κρυπτογράφηση της επικοινωνίας ανάμεσα στο προσωπικό τερματικό του χρήστη και στο απομακρυσμένο τερματικό του διακοσμητή με τον οποίο επικοινωνεί, στηρίζεται στο βασικό πρωτόκολλο επικοινωνίας HTTP (Hypper Text Transfer Protocol) και ονομάζεται HTTPS. Το Transport Layer Security (TLS) και το Secure Socket Layer (SSL) (το S στο HTTPS), διασφαλίζει ότι κάποιος κακόβουλος χρήστης στο μέσο της επικοινωνίας δεν μπορεί να διαβάσει τα δεδομένα που μεταφέρονται. Μια άλλη σημαντική μέθοδος κρυπτογράφησης είναι η κρυπτογράφηση δημοσίου κλειδιού, βασισμένη στον αλγόριθμό των Diffie-Hellman, πάνω στην οποία βασίζονται πολλές σύγχρονες τεχνολογίες όπως η τεχνολογία PGP (Pretty Good Privacy). Το PGP συνδυάζοντας την κρυπτογράφηση δημοσίου κλειδιού και άλλες μεθόδους κρυπτογράφησης, προσφέρει τον καλύτερο τρόπο υπογραφής, κρυπτογράφησης και αποκρυπτογράφησης κειμένου και e-mail.

6.2 Σωστή Εφαρμογή της Κρυπτογράφησης

Ανεξάρτητα από το είδος της κρυπτογράφησης υπάρχουν κάποια βασικά βήματα τα οποία διασφαλίζουν την σωστή εφαρμογή της:

- Η κρυπτογράφηση είναι όσο δυνατή είναι το κλειδί. Αν κάποιος μαντέψει ή αποκτήσει το κλειδί μπορεί να αποκτήσει πρόσβαση στα δεδομένα. Το κλειδί πρέπει να προστατεύεται.
- Αν η επιλογή για κλειδί είναι μία φράση ή ένας κωδικός, θα πρέπει να είναι αρκετά με- γάλος και να πληροί τους βασικούς κανόνες ασφαλείας των κωδικών πρόσβασης. Επιπρόσθετα, δεν θα πρέπει να ξεχαστεί ή χαθεί για ευνόητους λόγους.
- Η κρυπτογράφηση είναι όσο ασφαλής είναι και ο προσωπικός υπολογιστής. Αν κάποιος κακόβουλος χρήστης αποκτήσει πρόσβαση στον υπολογιστή ενδέχεται να βρει τρόπους να αποφύγει τους μηχανισμούς κρυπτογράφησης.
- Αν υπάρχουν διαθέσιμές πολλές και διαφορετικές μέθοδοι κρυπτογράφησης, πρέπει η επιλογή να είναι η ισχυρότερη από αυτές.

6.3 Εικονικά Ιδιωτικά Δίκτυα

Εκτός από το πρωτόκολλο HTTPS, για την προστασία της επικοινωνίας και την ενίσχυση της ανωνυμίας στο Διαδίκτυο, υπάρχουν τα Εικονικά Ιδιωτικά Δίκτυα ή VPN. Ορίζεται ως και αποτελεί ένα δίκτυο που χρησιμοποιεί κατά κύριο λόγο δημόσια τηλεπικοινωνιακή υποδομή, όπως το Διαδίκτυο, και δίνει τη δυνατότητα σε απομακρυσμένους χρήστες ή φορείς να έχουν πρόσβαση στο κεντρικό δίκτυο υπό διαφορετική διεύθυνση. Ένα VPN συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση με κωδικό και όνομα χρήστη, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους. Μπορεί να δημιουργείται για τη λειτουργικότητα του δικτύου που βρίσκεται σε οποιοδήποτε δίκτυο, όπως η κοινή χρήση των δεδομένων και η πρόσβαση σε πόρους δικτύου, εκτυπωτές, βάσεις δεδομένων, ιστοσελίδες, κλπ. Ένας χρήστης VPN αντιμετωπίζει συνήθως το κεντρικό δίκτυο με τρόπο που είναι ταυτόσημος με το να συνδέεται άμεσα με το κεντρικό δίκτυο. Οι δύο βασικοί λόγοι χρήσης VPN είναι για την διατήρηση ανωνυμίας και προστασίας ιδιωτικότητας και για την αποφυγή γεωγραφικών περιορισμών.

Για παράδειγμα, μερικά από τα βίντεο στο YouTube δεν είναι προσβάσιμα από Ελληνικές διευθύνσεις και η Κίνα (The Great Firewall of China) απαγορεύει την πρόσβαση σε μερικά κοινωνικά δίκτυα όπως το Facebook.

6.4 Δρομολόγηση Κρεμμυδιού

Η δρομολόγηση κρεμμυδιού ή αλλιώς Onion Routing είναι μία τεχνική για ανώνυμη επικοινωνία σε ένα υπολογιστικό δίκτυο. Ονομάζεται έτσι επειδή σε ένα δίκτυο που υιοθετεί αυτή την δρομολόγηση, τα μηνύματα/πακέτα της επικοινωνίας ενθυλακώνονται μέσα σε στρώματα κρυπτογράφησης, σε αναλογία με τα στρώματα ενός κρεμμυδιού. Η κρυπτογραφημένη πληροφορία μεταφέρεται μέσα από μία σειρά κόμβων που καλούνται δρομολογητές κρεμμυδιού (onion routers), κάθε ένας από τους οποίους αφαιρεί ένα στρώμα κρυπτογράφησης για να αποκαλυφθεί ο επόμενος κόμβος προορισμού του πακέτου έως ότου φτάσει στον τελικό κόμβο προορισμού. Για όσους βρίσκονται στο μέσο της επικοινωνίας και βλέπουν το πακέτο, εκτός του ότι δεν μπορούν να δουν το περιεχόμενο, δεν μπορούν να δουν και τον αποστολέα παρά μόνο την τοποθεσία του επόμενου κόμβου. Το TOR network αποτελεί ίσως την

πιο ισχυρή μορφή ανωνυμίας στο διαδίκτυο σήμερα, καλύτερη και από τα Εικονικά Ιδιωτικά Δίκτυα.

6.4.1 Facebook και TOR

Το 2014, το Facebook προσέθεσε μια νέα τεχνολογία στην υπηρεσία του ώστε να δίνει την δυνατότητα στους χρήστες του να έχουν πρόσβαση μέσω του δικτύου TOR. Η σημασία εγγυάται στο ότι οι χρήστες μπορούν να έχουν πρόσβαση στους λογαριασμούς τους χωρίς να χάνουν την προστασία και τους κρυπτογραφικούς μηχανισμούς του TOR. Προσφέρεται απευθείας επικοινωνία μεταξύ του φυλλομετρητή και του Facebook κέντρου δεδομένων. Ωστόσο δεν είναι λίγοι εκείνοι που έσπευσαν να εκφράσουν την ειρωνεία πίσω από την τεχνολογία αυτή. «Η λιγότερο ανώνυμη ιστοσελίδα του κόσμου, προχώρησε στην σύνδεση με το πιο ανώνυμο δίκτυο» όπως δήλωσε και ο Andy Greenberg στο online περιοδικό Wired. Παρόλο αυτά, με την κίνηση αυτή, το Facebook, έδειξε αφοσίωση στην ασφαλή πλοήγηση στο Διαδίκτυο και έδωσε την δυνατότητα σε χώρες όπως η Κίνα, η Συρία, η Βόρεια Κορέα, η Αίγυπτος και άλλες, να έχουν πρόσβαση στη υπηρεσία του καθώς οι εν λόγω χώρες απαγορεύουν την χρήση του Facebook από τους πολίτες τους.

6.4.2 TOR και Dark Web

Το Dark Web είναι ένα μικρότερο μέρος του Deep Web, χρησιμοποιεί την δημόσια υποδομή του Διαδικτύου, αλλά για την πρόσβαση σε υπηρεσίες αυτού απαιτείται η χρήση ειδικού λογισμικού ή/και εξοπλισμού. Το δίκτυο TOR είναι μέλος του Dark Web οπότε και χρησιμοποιείται για την πρόσβαση στο τελευταίο.

Όπως είναι λογικό και επόμενο, εφόσον το δίκτυο TOR προσφέρει την καλύτερη δυνατή μέθοδο για ανωνυμία στο Διαδίκτυο, δεν χρησιμοποιείται μόνο από χρήστες που θέλουν να προστατέψουν την ανωνυμία τους online για τους λόγους που αναφέρθηκαν παραπάνω, αλλά και από κακόβουλους χρήστες που καταπιάνονται με εγκληματικές δραστηριότητες όπως ναρκωτικά, κλοπές, παιδική πορνογραφία, πώληση όπλων και άλλα. Το TOR να χρησιμοποιείται από ανθρώπους σε όλο τον κόσμο, ειδικά σε χώρες με ισχυρούς νόμους λογοκρισίας για να αποκτούν πρόσβαση σε απαγορευμένους ιστότοπους όπως το Facebook. Ωστόσο έρευνες έχουν δείξει ότι η πλειοψηφία του υλικού στο δίκτυό του είναι παράνομη όχι μόνο σε χώρες με ισχυρά λογοκριτικούς νόμους αλλά και σε χώρες με περισσότερο φιλελεύθερες νομοθεσίες.

Οι δημιουργοί και οι προγραμματιστές πίσω από το δίκτυο TOR, θα πρέπει να ενθαρρύνουν την κοινότητα των μελών του στην δημιουργία μιας ασφαλούς και νόμιμης εμπειρίας πλοήγησης. Ο σκοπός δημιουργίας του ήταν η ασφάλεια και η ανωνυμία, όχι οι εγκληματικές ενέργειες. Μειώνοντας τις εγκληματικές ενέργειες, θα αποκτήσει και περισσότερους νόμιμους χρήστες.

6.5 Κρυπτογράφηση, TOR, VPN και FBI

Με το TOR και τα VPN να συγκεντρώνουν έναν μεγάλο αριθμό από κακόβουλους χρήστες, οι κυβερνητικές υπηρεσίες της Αμερικής όπως το FBI και διαφόρων άλλων χωρών, κάνουν δημόσιες δηλώσεις και κινήσεις κατά των χρηστών τους.

6.5.1 APPLE VS FBI

Χαρακτηριστικό παράδειγμα, αποτελεί η διαμάχη ανάμεσα στην Apple και το FBI. Ένας δικαστής από την Καλιφόρνια έδωσε εντολή η Apple να ξεκλειδώσει την iPhone συσκευή που χρησιμοποιούσε ένας από τους τρομοκράτες του Σαν Μπερναντίνο. Ίσως η δημόσια ασφάλεια και οι σύγχρονες μέθοδοι ψηφιακής ασφάλειας είναι αναγκασμένοι να συγκρούονται, ωστόσο ο κίνδυνος, όπως πάντα σε τέτοιες συγκρούσεις είναι ότι και οι δύο πλευρές μπορεί να καταλήξουν ζημιωμένες.

Εν συντομία, το FBI ήθελε να παρακάμψει το σύστημα ασφαλείας της συσκευής του τρομοκράτη γιατί δεν γνώριζε τον προσωπικό του κωδικό. Η Apple έδωσε τα διαθέσιμα δεδομένα από το εφεδρικό τους σύστημα, αλλά δεν ήταν καθόλου πρόσφατα σε σχέση με την τρομοκρατική επίθεση και επομένως άχρηστα για την υπόθεση. Το FBI ήθελε λοιπόν να αποκτήσει πρόσβαση στα κρυπτογραφημένα δεδομένα της συσκευής τα οποία θα μπορούσαν να συνεισφέρουν στην έρευνα και ενδεχομένως στον εμποδισμό άλλων τρομοκρατικών ενεργειών.

Για διάφορους τεχνικούς μηχανισμούς που δεν θα αναφερθούν εδώ γιατί είναι εκτός του πεδίου της εργασίας, το FBI δεν μπορούσε να αποκτήσει πρόσβαση στα δεδομένα της συσκευής οπότε ζήτησε από την Apple να κατασκευάσει μία προσαρμοσμένη έκδοση του λειτουργικού της η οποία θα παρακάμπτει τους κρυπτογραφικούς μηχανισμούς ασφαλείας της συσκευής. Σε δημόσια ανακοίνωσή του, ο CEO της Apple Tim Cook, αρνήθηκε να λάβει μέρος σε κάτι τέτοιο και

τόνισε πως η εταιρεία θα ασκούσε έφεση. Τόνισε επίσης πως η αμερικανική κυβέρνηση, ζήτησε κάτι που δεν έχουν και ούτε θα μπορούσαν να φτιάξουν κάτι το οποίο θα έδινε την δυνατότητα της παράκαμψης των κρυπτογραφικών μηχανισμών σε όλες τις συσκευές τους. Αυτό που ήθελε στην ουσία το FBI, γιατί όπως αποδείχθηκε υπήρχαν διάφοροι μέθοδοι με τους οποίους θα μπορούσε να αποκτήσει τα δεδομένα, ήταν ένα κλειδί που θα ανοίγει όλες τις συσκευές της εταιρείας και αυτό πηγάζει από τον φόβο των οργάνων επιβολής του νόμου και των υπηρεσιών εθνικής ασφάλειας ότι οι τρομοκράτες και οι εγκληματίες κινούνται στην αφάνεια. Ωστόσο ο CEO της Apple, έχει ακράδαντο επιχείρημα ότι οι "κερκόπορτες" στα λογισμικά και λειτουργικά δημιουργούν περισσότερα προβλήματα από όσα επιλύουν. Η εισαγωγή τρυπών ασφαλείας που τρίτοι φορείς όπως αστυνομικοί και λοιπά όργανα του νόμου μπορούν να χρησιμοποιήσουν εν ανάγκη, μπορούν να χρησιμοποιηθούν επίσης από hackers, κατασκόπους και άλλους εγκληματίες. Μπορεί τα έθνη να εξουσιοδοτούν "κερκόπορτες", αλλά πάντα θα υπάρχουν κρυπτογραφήσεις σχεδιασμένες από άλλους (ενδεχομένως κακόβουλους) έξω από την δικαιοδοσία και την τεχνολογική κατάρτισή τους. Το αποτέλεσμα θα ήταν προϊόντα με ασθενέστερη ασφάλεια για τους νομοταγείς καταναλωτές που θα αφήνουν τις εταιρίες των Η.Π.Α λιγότερο ανταγωνιστικές και ασφαλείς.

Κεφαλαιο 7: Επιλογος

7.1 Συμπεράσματα

Οι λόγοι που δίνουν αρνητική χροιά στην χρήση των Μέσων Κοινωνικής Δικτύωσης είναι αρκετοί. Η διάχυτη και συνεχής ανταλλαγή πληροφοριών, στις οποίες πολλές φορές συγκαταλέγονται προσωπικά δεδομένα, εντείνουν το αίσθημα του φόβου ως προς την προστασία της ιδιωτικότητας και των προσωπικών δεδομένων των χρηστών. Ως άμεσο επακόλουθο, η ιδιωτικότητα μπορεί εύκολα να πληγεί καθώς οι δημοσιεύσεις των χρηστών ανανεώνονται κάθε δευτερόλεπτο αναφέροντας την καθημερινή τους και όχι μόνο ρουτίνα.

Εγείρονται πολλά ερωτήματα για το είδος της ζωής που θα διάγει κάποιος στο μέλλον. Για παράδειγμα:

- Ποια θα είναι τα όρια της ιδιωτικής ζωής·
- Θα μπορεί κάποιος να απολαμβάνει την ησυχία στην προσωπική του ζωή·
- Τα προσωπικά στοιχεία θα είναι γνωστά από όλους·
- Θα υπάρχει ψηφιακή ταυτότητα σε μια παγκόσμια πολιτεία·
- Θα ελέγχονται όλοι από κάποιον·
- Θα καταργηθούν τελικά οι ιστοσελίδες κοινωνικής δικτύωσης·

Ένας από τους ειδικούς, και συγκεκριμένα ο ιδρυτής του διαδικτύου εξέφρασε φόβους ότι κάποια ιστοσελίδα κοινωνικής δικτύωσης (εννοώντας το Facebook) θα μπορούσε να γίνει τόσο μεγάλη, ώστε να αποτελέσει μονοπώλιο, τείνοντας να περιορίσει την καινοτομία. Αναφέρθηκε στην ιστοσελίδα αυτή γιατί σύντομα θα ξεπεράσει τον αριθμό των 700 εκατομμυρίων χρηστών. Η απουσία της ιδιωτικής ζωής θα οδηγήσει σε χειραγώγηση πολιτών και σε μια ζωή με πολλούς περιορισμούς, αφού όλοι όσοι επιθυμούν, εταιρείες ή κράτος, θα διαθέτουν υπέρογκα ποσά πληροφοριών. Στην ουσία ο φόβος έγκειται στο γεγονός ότι οι συνδεδεμένοι χρήστες θα βρίσκονται παγιδευμένοι σε πολυεθνικές εταιρείες λόγω των υπηρεσιών που

προσφέρουν και ως εκ τούτου η ιδιωτικότητά τους θα είναι πλέον δημόσια. Με αυτόν τον τρόποι οι πολίτες θα ελέγχονται και η ιδιωτική σφαίρα θα χαθεί ή θα συρρικνωθεί. Οι μελλοντικοί πολίτες ενδέχεται να χάσουν την δυνατότητα ανάπτυξης της προσωπικότητάς τους, και να αποκτήσουν μια μορφή συμπεριφοράς "αποδεκτή" από κάποιους, γεγονός το οποίο θέτει τις μελλοντικές κοινωνίες σε κρίση.

Κάποιοι πάλι ανησυχούν για την νέα γενιά. Είναι η γενιά των Social Media, η οποία έχει γαλουχηθεί στις νέες τεχνολογίες. Η γενιά αυτή θεωρεί το Διαδίκτυο αναπόσπαστο μέρος της ζωής του και ενδέχεται να μην ενοχλείται από τον περιορισμό της ιδιωτικής ζωής. Το ερώτημα είναι εάν η γενιά αυτή απλά το αποδέχεται ή μήπως δεν διαθέτει την κατάλληλη κριτική σκέψη για να αντιδράσει και το απορρίψει. Καλώς ή κακώς, υπάρχει και η αντίληψη πως εάν κάποιος δεν ακολουθήσει το ρεύμα της εποχής του, θα χαρακτηρίζεται από τον κοινωνικό του περίγυρο ως "εκτός εποχής".

Οι συνδεδεμένες συσκευές έχουν ξεκινήσει την πορεία τους από τις επιχειρήσεις και τις βιομηχανίες στη μαζική αγορά. Με τις νέες τεχνολογίες να κυριαρχούν τα τελευταία χρόνια καθώς και τη συνεχή άνοδο του Internet of Things, η αξία της πληροφορίας αυξάνεται διαρκώς και ταυτόχρονα η ζήτηση και η απόκτησή της. Σημείο ενδιαφέροντος αποτελεί το γεγονός ότι οι προσωπικές προτιμήσεις και οι συνήθειες του καθενός μπορούν να γίνουν ευκαιρία κέρδους. Με τα ατομικά δεδομένα να διακινούνται και να αποθηκεύονται σε πολλαπλές συσκευές συνδεδεμένες μεταξύ τους, όπως κινητές συσκευές, wearables (υπολογιστές - αξεσουάρ) και sensors (αισθητήρες), η πληροφορία γίνεται ακόμη πιο ευάλωτη σε πιθανές υποκλοπές και παραβιάσεις. Πλέον θα παρατηρούμε συνεχώς περισσότερους αισθητήρες και ενεργοποιητές (actuators) στα αντικείμενα που χρησιμοποιούμε καθημερινά, από οικιακές συσκευές μέχρι και υποδομές των πόλεων. Αναμένεται να παρατηρήσουμε μαζική αύξηση των δεδομένων που παράγονται. Ήδη, εκατομμύρια γεγονότα γεννούν τεράστιο αριθμό πληροφοριών κάθε δευτερόλεπτο, που είναι έτοιμες να υποστούν επεξεργασία, να αναλυθούν και να διαμοιραστούν μεταξύ συσκευών και ανθρώπων.

Σύμφωνα με τον Moor (1997) επειδή είναι σχεδόν αδύνατον να ελεγχθεί το σύνολο των πληροφοριών ενός ατόμου, στην 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 μία σύνθεση από τη μία πλευρά της δυνατότητας ελέγχου της προσωπικής πληροφορίας και από την άλλη της περιορισμένης πρόσβασης σε αυτήν από άλλους.

7.2 Η Θέση της Ελλάδας&&&

Όπως αναφέρθηκε παραπάνω, κάθε κράτος-μέλος της Ευρωπαϊκής Ένωσης, υπόκεινται στους νόμους και οδηγίες της. Η Ελλάδα, σαν μέλος, υιοθετεί το ίδιο νομοθετικό πλαίσιο και πολιτική. Ωστόσο, ο Ελληνικός Κόμβος Ασφαλούς Δικτύου (ENISA102) προτείνει στους φορείς την λήψη μιας σειράς δράσεων και στους χρήστες κάποια μέτρα προστασίας.

(α)Προτείνει την ανάληψη δράσης από τους αρμόδιους φορείς, 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 νομοθεσιών, που ισχύουν, ειδικότερα σε ό,τι 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: 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.
- Συμβουλές για ασφαλή χρήση των ιστοσελίδων κοινωνικής δικτύωσης.

(β) Παραθέτει χρήσιμες συμβουλές στους χρήστες, για να απολαμβάνουν την ηλεκτρονική δικτύωση με μεγαλύτερη ασφάλεια, αποφεύγοντας τους κινδύνους:

- Δεν θα πρέπει να δίνεται σε κανέναν ο κωδικός πρόσβασης, που αφορά το εικονικό προφίλ ενός χρήστη. Όποιος αποκτά πρόσβαση στο προφίλ ενός χρήστη, μπορεί να διαχειριστεί πλήρως τα δεδομένα, που εμφανίζονται σε αυτό.
- Πριν εγγραφεί κάποιος σε μια ιστοσελίδα κοινωνικής δικτύωσης , να αναζητά τη δήλωση περί απορρήτου και να κατανοεί πλήρως με ποιον τρόπο θα χρησιμοποιούν- από την ιστοσελίδα τα προσωπικά του δεδομένα.
- Μην ανεβάζει στο προφίλ του φωτογραφίες όπου φαίνεται καθαρά η τοποθεσία στην οποία βρίσκεται, ειδικότερα αν πρόκειται για το σπίτι του, το σχολείο ή μέρη που συχνάζει. Έτσι θα μειώσει τις πιθανότητες εντοπισμού του στον φυσικό κόσμο. Αν δεχθεί ένα προσβλητικό ή ανεπιθύμητο μήνυμα, να χρησιμοποιήσει την ενσωματωμένη μέθοδο καταγγελιών της ιστοσελίδας κοινωνικής δικτύωσης που χρησιμοποιεί. Συνήθως αναφέρεται με τη λέξη «report».
- Να έχει πάντα υπόψη του ότι οι πληροφορίες που δημοσιεύει στις ιστοσελίδες κοινωνικής δικτύωσης είναι δημόσια προσπελάσιμες, επομένως, καλό θα ήταν να μη δημοσιεύει στοιχεία και φωτογραφίες που θα τον έφερναν σε δύσκολη θέση. Ακόμα και όταν διαγράψει το προφίλ του πολλές πληροφορίες δεν αφαιρούνται και ενδέχεται επίσης να τις συναντήσει και σε άλλη τοποθεσία του διαδικτύου.
- Να γνωρίζει ότι από τη στιγμή που προσθέτει στη λίστα των φίλων του κάποιο άτομο, αυτό το άτομο αποκτά πρόσβαση στα προσωπικά δεδομένα, που εμφανίζονται στο προφίλ του, μεταξύ των οποίων οι φωτογραφίες και τα στοιχεία επικοινωνίας του.
- Από τη στιγμή που δημιουργεί το εικονικό του προφίλ, θα πρέπει μέσα από το μενού των ρυθμίσεων για τη διαχείριση των προσωπικών δεδομένων (συνηθέστερα θα το βρει κάποιος στα αγγλικά ως privacy settings) και να αλλάξει τις προεπιλεγμένες ρυθμίσεις.
- Να επιλέξει αν οι επισκέπτες του προφίλ του μπορούν να δουν αν είναι online ή όχι.

- Να καθορίσει ποιοι θα μπορούν να βλέπουν το εικονικό του προφίλ ή συγκεκριμένα στοιχεία που περιλαμβάνονται σε αυτό (ημερομηνία γέννησης, φωτογραφία, κ.ά.).
- Να απαγορεύσει την πρόσβαση συγκεκριμένων ατόμων στο προφίλ του.
- Να ρυθμίσει από ποιους χρήστες μπορεί να λαμβάνει προσωπικά μηνύματα και σχόλια.
- Να ρυθμίσει αν θα εμφανίζεται το προφίλ του στα αποτελέσματα αναζήτησης μέσω της ιστοσελίδας, καθώς και τη μορφή, που θα έχει (αν θα φαίνεται η φωτογραφία, τα στοιχεία επικοινωνίας, κ.ά.).

7.3 Point of View

Φαινομενικά η τρέχουσα νομοθεσία, οι διατάξεις, οι οδηγίες της Ευρωπαϊκής Ένωσης και όχι μόνο, προστατεύουν το χρήστη. Ωστόσο μπορεί να γίνει εύκολα παράκαμψη λόγω της ραγδαίας αύξησης της τεχνολογίας που δημιουργεί ασάφειες τις οποίες εκμεταλλεύονται εύκολα μεγάλες υπηρεσίες και δίκτυα έχοντας στην διάθεση τους μεγάλο αριθμό δικηγόρων και νομικών συμβούλων. Ως εκ τούτου, είναι στο χέρι του χρήστη να ενημερώνεται για τους κινδύνους της δημοσίευσης των προσωπικών του δεδομένων και να χρησιμοποιεί τα Μέσα Κοινωνικής Δικτύωσης με ωριμότητα και σύνεση. Επιπρόσθετα, με χρήστη των κατάλληλων εργαλείων, όπως τα Εικονικά Ιδιωτικά Δίκτυα και τις μεθόδους κρυπτογράφησης, έχει την δυνατότητα να καθιστά το έργο των τρίτων, δηλαδή τον εντοπισμό και τον προσδιορισμό των χαρακτηριστικών του, ιδιαίτερα δύσκολο.

Δυστυχώς, καμία από τις παραπάνω μεθόδους δεν εγγυάται την ανωνυμία στο Διαδίκτυο καθώς υπάρχουν πολλές περισσότερες μέθοδοι και έρευνες που σχετίζονται με τον εντοπισμό χρηστών και την συλλογή και επεξεργασία των πληροφοριών αυτών, γεγονός που καθιστά το θέμα ιδιαίτερα κρίσιμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Γκρίτζαλης Στέφανος, Λαμπρινουδάκης Κ., Κάτσικας Σωκράτης, Μήτρου Λίλιαν, «Προστασία της ιδιωτικότητας και τεχνολογίες πληροφορικής και επικοινωνιών», εκδόσεις Παπασωτηρίου, 2010

[2] Παπακωνσταντίνου Ευάγγελος, Α.Τσακαλίδης, «Δίκαιο Πληροφορικής», εκδόσεις Σάκκουλα , 2010

[3] Γκρίτζαλης Στέφανος, Γκρίτζαλης Α. Δημήτρης, Κάτσικας Σωκράτης, ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, «ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝΤΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΠΙΧΕΙΡΕΙΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ», εκδόσεις Παπασωτηρίου, Νοέμβριος, 2004

[4] Λιούπα Άννα, «Προστασία προσωπικών δεδομένων στα κοινωνικά δίκτυα», 2011

[5] Gritzalis Dimitris, Kandias Miltiadis, Stavrou Vasilis, Mitrou Lilian, «History of Information: The case of Privacy and Security in Social Media», 2014

[6] Carolyn Miller, Lee Rainie, Kristen Purcell, Amy Mitchell and Tom Rosenstiel, «How people get local news and information in different communities», September 26, 2012

[7] Christopher F. Spinelli, «Social Media: No 'Friend' of Personal Privacy», January 1, 2010

[8] Pierre-Luc Dusseault, M.P. Chair, «PRIVACY AND SOCIAL MEDIA IN THE AGE OF BIG DATA», APRIL, 2013

[9] Jan Dhont, Bert Theeuwes, «Guide of Social Media Privacy», 2013

[10] Eric L. Barnum, « PRIVACY, SOCIAL MEDIA AND THE AMERICAN WORK PLACE: EMPLOYMENT LITIGATION WILL NEVER BE THES AME», 2014

[11] Avner Levin, Mary Foster, Bettina West, Mary Jo Nicholson, Tony Hernandez, Wendy Cukier, Emily Ho, Sarah Lasch and Aubrey Podolsky, «The Next Digital Divide: Online Social Network Privacy », March, 2008

[12] Katherine K. Roberts, «Privacy and Perceptions: How Facebook Advertising Affects its Users», 2010

[13] Ralph Gross, Alessandro Acquisti, «Information Revelation and Privacy in Online Social Networks (The Facebook case)», 2005

URLs:

1. Social Media Privacy Risks
2. How Much Privacy We Still Have on Social Network?
3. Social Media Privacy
4. What the Apple vs. FBI Debacle Taught Us
5. Privacy and Online Behavioral Advertising
6. Marketing using Social Media and Privacy Issues