ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η πρόκληση της νόμιμης ροής προσωπικής πληροφορίας στο διαδίκτυο.

Στόγιου Αικατερίνη-Ευαγγελία Α.Μ. 1578

Επιβλέπων καθηγήτρια:ΛαμπρινήΣερεμέτη

Αντίρριο 2017-2018

ΕΥΧΑΡΙΣΤΙΕΣ

Ευχαριστώ την επιβλέπουσα καθηγήτρια κ. Λαμπρινή Σερεμέτη για την πολύτιμη βοήθεια της για το αποτέλεσμα της πτυχιακής μου άσκησης και για τις άμεσες παρεμβάσεις όπου χρειάστηκαν. Επιπλέον θέλω να ευχαριστήσω τον κ. Ασημακόπουλο Γεώργιο για ό,τι γνώσεις απέκτησα πάνω στο δίκαιο αλλά και την νόμιμη χρήση των προσωπικών δεδομένων μέσα από τις παραδόσεις. Τέλος ευχαριστώ όλους όσους με στήριξαν αυτά τα χρόνια στην προσπάθεια αυτή, και κυρίως τους γονείς μου που ήταν πάντα εκεί σε ό,τι χρειαστώ αλλά και τον συμφοιτητή μου Αντώνιο Ταραντίλη για τις χρήσιμες συμβουλές του.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΡΟΛΟΓΟΣ

Με την ραγδαία ανάπτυξη και την ευρεία χρήση των νέων τεχνολογιών του Διαδικτύου, η προοπτική της ιδιωτικής ζωής έχει μεταβληθεί.Με την άνοδο των κοινωνικών δικτύων, των smartphones και της διαδικτυακής διαφήμισης, ένα ευρύ φάσμα εταιρειών και όχι μόνο, άρχισε να παρακολουθεί τους ανθρώπους σε όλες σχεδόν τις πτυχές της ζωής τους. Σήμερα, οι συμπεριφορές, τα κινήματα, οι κοινωνικές σχέσεις, τα συμφέροντα, οι αδυναμίες και οι περισσότερες ιδιωτικές στιγμές δισεκατομμυρίων καταγράφονται συνεχώς, αξιολογούνται και αναλύονται σε πραγματικό χρόνο. Τα προσωπικά δεδομένα απειλούνται στο διαδίκτυο.

Ο όρος online προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων αναφέρεται στην πράξη του ατόμου επιλεκτικής αποκάλυψης (του εαυτού του), σε online περιβάλλον.

Έχει διαπιστωθεί ότι υπάρχουν αρκετοί κίνδυνοι που περιβάλλουν την απόσπαση προσωπικών στοιχείων και πληροφοριών σχετικά με τα κοινωνικά δίκτυα. Οι απειλές αυτές μπορούν να προκληθούν από hackers ή spammers που λαμβάνουν προσωπικές πληροφορίες και στοιχεία των χρηστών. Επειδή τα ζητήματα αυτά απασχολούν τους πολίτες καθημερινά όταν συναλλάσσονται με δημόσιες υπηρεσίες, όταν αγοράζουν αγαθά ή υπηρεσίες, όταν ταξιδεύουν ή όταν περιηγούνται στο διαδίκτυο, η Ευρωπαϊκή ένωση και οι χώρες της θεσπίζουν με νόμους τη διασφάλιση των προσωπικών δεδομένων.

ΣΤΟΧΟΣ

Λαμβάνοντας υπόψη τα παραπάνω στην παρούσα εργασία καταβάλλεται μια προσπάθεια που στόχο έχει να καταγράψει αφενός την έννοια της ιδιωτικότητας και των προσωπικών δεδομένων στο χώρο του διαδικτύου και αφετέρου να αναλύσει την Ευρωπαϊκή και Ελληνική Νομοθεσία, σε θέματα που άπτονται της χρήσης και της ανάκλησης των προσωπικών δεδομένων.

Η εργασία αποτελείται από 3 κεφάλαια.

- Στο πρώτο κεφάλαιο γίνεται μια ιστορική αναδρομή στην ιστορική εξέλιξη του διαδικτύου μέχρι να φτάσει στη σημερινή του κατάσταση.
- Στο δεύτερο κεφάλαιο αναλύονται οι έννοιες προσωπικά δεδομένα και ιδιωτικότητα στο χώρο του διαδικτύου.
- Τέλος, στο τρίτο κεφάλαιο παρουσιάζονται οι νόμοι της Ευρωπαϊκής και της Ελληνικής νομοθεσίας αλλά και διάφορα μέσα που μπορούν να ληφθούν για την προστασία των προσωπικών δεδομένων.

Η εργασία ολοκληρώνεται με τον επίλογο όπου πραγματοποιείται μια σύνοψη των όσων προηγήθηκαν.

ABSTRACT

This thesis is an effort to capture the concept of privacy and personal data in the Internet and to analyze European and Greek Legislation on issues related to the use and revocation of personal data.

The work consists of 3 chapters.

• In the first chapter there is a historical retrospection of the evolution of the Internet until it reaches its present situation.

• The second chapter analyzes the concepts of personal data and privacy on theInternet.

•Finally, the third chapter presents the laws of the European and Greek legislation as well as various means that can be taken for the protection of personal data.

The work is completed with a synopsis of what preceded.

ΚΕΦΑΛΑΙΟ 1
ΤΟ ΔΙΑΔΙΚΤΥΟ

1.1 ΕΙΣΑΓΩΓΗ

Ο Floridi (2009, 2010) υποστήριξε ότι, με την ανάπτυξη της πληροφορίας, βιώνεται η τέταρτη επιστημονική επανάσταση.Το διαδίκτυο διαδραματίζει έναν κρίσιμο ρόλο στη σημερινή τεχνολογία και κοινωνία (Luppicini, 2010).

Σε πενήντα χρόνια (1960-2010) η τεχνολογία εξελίχθηκε γρήγορα, αποτελώντας μια εποχή καινοτομίας, όπου οι ιδέες οδήγησαν στην ανάπτυξη νέων εφαρμογών οι οποίες με τη σειρά τους οδήγησαν στη ζήτηση. Οι νέες απαιτήσεις απέδωσαν περαιτέρω καινοτομία και πολλές νέες εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο, τον παγκόσμιο ιστό, την κοινή χρήση αρχείων, την κοινωνική δικτύωση, τους ισότοπους και το skype (Almagor, 2011).

Για να κατανοηθεί πώς το Διαδίκτυο έγινε αναπόσπαστο κομμάτι της ζωής των ανθρώπων, είναι σημαντικό να εξεταστεί η ιστορία του και οι κυριότερες εξελίξεις που σημειώθηκαν από τη μέτρια βρεφική ηλικία μέχρι τη γιγαντιαία του παρουσία (Almagor, 2011).

1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Η ιστορία του Διαδικτύου ξεκίνησε στις Ηνωμένες Πολιτείες στις αρχές της δεκαετίας του 1960. Αυτή η περίοδος ήταν η περίοδος του Ψυχρού Πολέμου, όπου οι Ηνωμένες Πολιτείες και η Σοβιετική Ένωση ανταγωνίζονταν να επεκτείνουν την επιρροή τους στον κόσμο, βλέποντας ο ένας τον άλλον με μεγάλη προσοχή και υποψία (Almagor, 2011).
Το Διαδίκτυο εμφανίστηκε στις 2 Σεπτεμβρίου του 1969, μέσω της σύνδεσης δύο υπολογιστών, μεταξύ των Πανεπιστημίων UCTA και του Stanford. Αρχικά

ονομάστηκε ARPANET (AdvancedResearchProjectAgency). Το δίκτυοαναπτύχθηκε από το Υπουργείο Εθνικής Άμυνας των Η.Π.Α. ως ένας τρόπος που εξασφάλιζε την επιτυχή σύνδεση των εργαστήριων έρευνας ζωτικής σημασίας σε ολόκληρη τη χώρα (Belch&Belch, 2012).

Ουσιαστικά, η αποστολή της ARPA ήταν να παράγει καινοτόμες ερευνητικές ιδέες, να παράσχει ουσιαστικές τεχνολογικές προσεγγίσεις που ξεπερνούσαν πολύ τις συμβατικές εξελικτικές αναπτυξιακές προσεγγίσεις και να δράσει σε αυτές τις ιδέες αναπτύσσοντας πρότυπα συστήματα (Almagor, 2011).

Η πρώτη δημόσια επίδειξη της νέας αυτής τεχνολογίας για το κοινό πραγματοποιήθηκε από τον Kahn τον Οκτώβριο του 1972, όπου ο τελευταίος οργάνωσε μια μεγάλη και πολύ επιτυχημένη επίδειξη του ARPANET στο Διεθνές Συνέδριο Επικοινωνίας Υπολογιστών. Την ίδια χρονιά εισήχθη και το ηλεκτρονικό ταχυδρομείο (Leineretal., 2009).

Στα μέσα της δεκαετίας του 1980, το Διαδίκτυο άρχισε την εμπορική δραστηριότητα. Το 1984, το Υπουργείο Άμυνας χώρισε το ARPANET σε δύο εξειδικευμένα δίκτυα: το ARPANET που θα συνέχιζε την προηγμένη έρευνα των δραστηριοτήτων του, και το MILNET (για στρατιωτικό δίκτυο) που προοριζόταν για στρατιωτικές χρήσεις όπου χρειαζόταν μεγαλύτερη ασφάλεια. Προκείμενου οι χρήστες να μπορούν να επικοινωνούν μεταξύ των δύο δικτύων, αναπτύχθηκαν διάφορες συνδέσεις (Almagor, 2011).

Ο αριθμός τηςεπισκεψιμότητας το 1989 είχε φτάσει τις 159.000 και το ίδιο έτος ο Άγγλος TimBernersLee, ερευνητής στον Οργανισμό (CERN)EuropeanOrganizationforNuclearResearch, στη Γενεύη, πρότεινε την ιδέα ενός διεθνούς συστήματος πρωτοκόλλων, ονομάζοντας το WorldWide Web (WWW) (Almagor, 2011).

Στα τέλη της δεκαετίας του 1980 και στις αρχές της δεκαετίας του 1990, η δημιουργία της γλώσσας HypertextMarkup (HTML), με τις προδιαγραφές για τον

ομοιόμορφο εντοπισμό πηγών (URLs) επέτρεψε στο Web να εξελιχθεί στο περιβάλλον που είναι γνωστό σήμερα (Tian&Stewart 2008).

Κατά τη διάρκεια της δεκαετίας του 1990 παρατηρήθηκε μια τεράστια επέκταση του Δικτύου. Η προσβασιμότητα του Διαδικτύου, η πολυεπίπεδη εφαρμογή του και ο αποκεντρωμένος χαρακτήρας του ήταν καθοριστικής σημασίας για την ταχεία αυτή ανάπτυξη. Επιχειρήσεις καθώς και προσωπικοί υπολογιστές με διαφορετικά λειτουργικά συστήματα μπορούσαν να ενταχθούν στο παγκόσμιο δίκτυο. Το Διαδίκτυο έγινε παγκόσμιο φαινόμενο, ενώ περισσότερες χώρες και άνθρωποι ενώθηκαν καθώς πρωτοποριακές εφαρμογές επέκτειναν τους ορίζοντες της πλατφόρμας με νέες καινοτομίες (Almagor, 2011).

Πιο συγκεκριμένα, το 1991 ιδρύθηκε η κοινωνία του Διαδικτύου (Internet Society, ISOC) (Su&Lee, 2010.Το 1992, ο αριθμός των οικοδεσποτών του Διαδικτύου ξεπέρασε το 1 εκατομμύριο με σχεδόν 50 ιστοσελίδες (Almagor, 2011).

Το 1993, κυκλοφόρησε ο πρώτος εμπορικός γραφικός περιηγητής browserMosaic και υπήρχαν 623 ιστοχώροι στον κόσμο (Su&Lee, 2010).
Μέχρι το τέλος του 1993 υπήρχαν 2,1 εκατομμύρια οικοδεσπότες. Η εκπληκτική ανάπτυξη και η επιτυχία του Διαδικτύου ήταν αποτέλεσμα της τεχνολογικής δημιουργικότητας, της ευελιξίας και της αποκέντρωσης (Almagor, 2011).

Το 1994, δημιουργήθηκε η πρώτη μηχανή αναζήτησης «Yahoo». Στις 24 Οκτωβρίου 1995, το Ομοσπονδιακό Συμβούλιο Δικτύωσης ψήφισε ομόφωνα ψήφισμα που ορίζει τον όρο Internet(Su&Lee, 2010).

Τα μέσα της δεκαετίας του 1990 ήταν τα έτη κατά τα οποία το Διαδίκτυο καθιερώθηκε ως το επίκεντρο επικοινωνίας, ενημέρωσης και επιχειρηματικότητας. Παράλληλα, πολλοί άνθρωποι άρχισαν να δημιουργούν τις δικές τους προσωπικές ιστοσελίδες Web. Το Διαδίκτυο αυξανόταν έντονα με ταχύ ρυθμό, προσελκύοντας όλο και περισσότερους ανθρώπους που μάθαιναν να το χρησιμοποιούν στην καθημερινότητα τους για: αναζήτηση πληροφοριών, έρευνα, επιχειρήσεις, εμπόριο, διασκέδαση, ταξίδια και ουσιαστικά οποιαδήποτε ανάγκη (Almagor, 2011).

1.3 ΕΞΕΛΙΞΗ ΤΟΥ ΠΑΓΚΟΣΜΙΟΥ ΙΣΤΟΥ: ΑΠΟ ΤΟ WEB 1.0 ΕΩΣ ΤΟ WEB 4.0.

Ο Παγκόσμιος Ιστός (WorldWidWeb) (κοινώς γνωστός ως Web) δεν είναι συνώνυμος με το διαδίκτυο, αλλά είναι το πιο σημαντικό μέρος του διαδικτύου και μπορεί να οριστεί ως «ένα τεχνολογικό κοινωνικό σύστημα όπου αλληλεπιδρούν οι άνθρωποι χρησιμοποιώντας τα τεχνολογικά δίκτυα». Η έννοια του τεχν-κοινωνικού συστήματος αναφέρεται σε ένα σύστημα που ενισχύει την ανθρώπινη γνώση, την επικοινωνία και τη συνεργασία. Η γνώσηείναι η αναγκαία προϋπόθεση για τηλεπικοινωνία και η προϋπόθεση για τη συνεργασία (AghaeiNematbakhsh&Farsani 2012).

Ο Παγκόσμιος Ιστός είναι το μεγαλύτερο μετασχηματιστικό πληροφοριακό κατασκεύασμα και η ιδέα του εισήχθη από τον TimBurners-Lee το 1989. Από την εμφάνιση του Web εισάγονται τέσσερις γενεές του: το Web 1.0 ως ένα Web της γνώσης, το Web 2.0 ως ένα Web της επικοινωνίας, το Web 3.0 ως ένα Web συνεργασίας και το Web 4.0 ως ένα Web της ενσωμάτωσης (Aghaei, Nematbakhsh&Farsani, 2012).

1.3.1 Web 1.0

Η πρώτη γενιά του Διαδικτύου έγινε γνωστή ως Web 1.0. Το Web 1.0 είναι σε μεγάλο βαθμό μια «στατική» πλατφόρμα στην οποία οι χρήστες επισκέπτονται τους ιστότοπους και εξετάζουν τις πληροφορίες, αλλά δεν αλληλεπιδρούν με τον ιστότοπο. Ως εκ τούτου, οι ιστότοποι του Web 1.0 χρησιμοποιούνται κυρίως ως χώροι αποθήκευσης πληροφοριών που περιέχουν πληροφορίες χρήσιμες για τον χρήστη αλλά με τις οποίες ο χρήστης δεν αλληλεπιδρά με κανέναν τρόπο (Vervaart, n.d.). Το Web 1.0 ξεκίνησε ως χώρος πληροφοριών για τις επιχειρήσεις ώστε να μεταδίδουν τις πληροφορίες τους στους ανθρώπους (Aghaei, Nematbakhsh&Farsani, 2012).

1.3.2 Web 2.0

Η ανάπτυξη του κοινωνικού και συλλογικού χαρακτήρα του Web 2.0. έκανε τους χρήστες πιο ενεργούς στα συλλογικά δίκτυα με αποτέλεσμα να διατυπώνεται η άποψη ότι το διαδίκτυο έχει την ικανότητα να προκαλέσει επανάσταση στη δημόσια επικοινωνία. Αυτό συμβαίνει στην περίπτωση του Web 2.0, τα χαρακτηριστικά του οποίου θεωρείται ότι προσφέρουν μεγαλύτερη ευελιξία στην επικοινωνία μέσω διαδικτύου, τόσο σε επίπεδο επικοινωνιακού ύφους όσο και σε επίπεδο τρόπου, χρόνου και τόπου πρόσβασης της επικοινωνίας. Ο Reilly (2005) υποστηρίζει ότι ο Web 2.0 δημιουργεί ένα «σχεδιασμό της συμμετοχής» που διευκολύνει τη συμπαραγωγή της πληροφορίας, την κοινωνική δικτύωση και τη δημιουργία χώρων για την αλληλεπίδραση μεταξύ ατόμων. Αυτό συνιστά μια δυναμική για τη δημιουργία όχι μίας, αλλά πολλαπλών δημοσίων σφαιρών που βασίζονται σε ποικίλα θέματα ή ενδιαφέροντα, οι αλληλεπιδράσεις των οποίων πιστεύεται ότι ενθαρρύνουν μια «πληροφοριακή δημοκρατία» (Jackson&Lilleker, 2009).

Ο Web 2.0 αναφέρεται σε νέες διαδικτυακές υπηρεσίες που έχουν κατασκευαστεί ειδικά για:

1. την ελεύθερη συλλογική δημοσίευση και
2. για τη διαμόρφωση ή συμμετοχή σε μέσα κοινωνικής δικτύωσης στο διαδίκτυο μέσω του περιβάλλοντος που προσφέρεται από το «www».

Οι «ιστότοποι κοινωνικής δικτύωσης» ορίζονται από τις Boyd και Ellison (2007) ως «διαδικτυακές υπηρεσίες που δίνουν τη δυνατότητα στο άτομο να:

- δημιουργήσει ένα δημόσιο ή ημι-δημόσιο προφίλ μέσα σε ένα σύστημα που διέπεται από νομικές δεσμεύσεις.
- να δημιουργήσει μια λίστα με άλλους χρήστες με τους οποίους έχει μια κοινή επαφή

- να δει και να διασταυρώσουν τη λίστα των επαφών τους και αυτές που έχουν δημιουργηθεί από άλλους στα πλαίσια του συστήματος» (Kalnes, 2008).

Μια από τις βασικότερες αρχές φιλοσοφίας του Web 2.0 είναι η συμμετοχή μέσω διαδικτύου ως συμπαραγωγή. Θεωρείται ότι ο Web 2.0 απαιτεί μια θεμελιώδη αλλαγή σκέψης. Ο Web 2.0 αφορά την αλληλεπίδραση με περιεχόμενο του διαδικτύου, προσθήκη σχολίων ή «ανέβασμα» αρχείων. Η εμπειρία του χρήστη δεν είναι πια αποκλειστικό δικαίωμα του κατασκευαστή της ιστοσελίδας, αλλά, χάρη στην αρχιτεκτονική της συμμετοχής κάθε επισκέπτης πλέον μπορεί να παρέχει το χώρο για δημόσια συνεισφορά, να μοιράζεται την κυριότητα με άλλον όσον αφορά την ανάπτυξη του ιστότοπου. Αυτό υποδηλώνει μια αλλαγή στη δομή τις εξουσίας και μετατόπιση του οργανωτικό τρόπο σκέψης προς τα μοντέλα που βασίζονται σε συνεργασία με ίσους όρους παρά στην κυριαρχία της ελίτ (Jackson&Lilleker, 2009).

OTimO' Reilly αναγνωρίζει ως κύρια χαρακτηριστικά της τεχνολογίας του Web 2.0 τη δυνατότητα δημιουργίας δικτύων που συνδέουν άτομα με οργανισμούς μέσα σε μια κοινότητα και όπου οι πληροφορίες κοινοποιούνται, προσαρμόζονται και ανανεώνονται από όλα τα μέλη της κοινότητας που επιλέγουν να συμμετέχουν. Από μια οργανωτική προοπτική, υποδηλώνει τη δημοκρατικοποίηση των πληροφοριών. Με τον Web 1.0 η πληροφορία έγινε διαθέσιμη στο ευρύ κοινό. Ο Web 2.0 αφορά την πιο ανθρώπινη πλευρά διαδραστικότητας στο διαδίκτυο (Brasky, 2006). Βασίζεται σε μια αντίληψη που έχει ως επίκεντρο το χρήστη. Σύμφωνα με τον Abram (2005), πρόκειται για «συζητήσεις, διαπροσωπική δικτύωση και ατομικισμό». Αυτό σημαίνει ότι αυτοί που επιλέγουν να συμμετέχουν μπορούν να μιλάνε με οποιονδήποτε θέλουν και να δημιουργούν ένα δίκτυο βασισμένο σε οποιοδήποτε συνδυασμό κοινών ενδιαφερόντων και ιδανικών, ενώ παρουσιάζονται όπως επιθυμούν σε αυτούς με τους οποίους συναναστρέφονται. Επιπλέον, σημαίνει ότι οι οργανισμοί που επιθυμούν να χρησιμοποιούν εργαλεία του Web 2.0 θα πρέπει να παραιτηθούν από τον έλεγχο του περιεχομένου και της εμπειρίας του χρήστη προκειμένου να αποκομίσουν τα οφέλη της συμμετοχής του χρήστη (Jackson&Lilleker, 2009).

Ο Barsky και ο Purdon (2006) υποστηρίζουν ότι ενώ ο Web 1.0 ωφέλησε τους εμπορικούς οργανισμούς και μετέδωσε πληροφορίες στο ευρύ κοινό, οWeb 2.0

«αφορά σχεδόν αποκλειστικά τους ανθρώπους». Με τη σειρά της, η δημοκρατία της πληροφορίας δεν αφορά μόνο τη διαφάνεια και τη διαθεσιμότητα της πληροφορίας, αλλά επίσης και την κοινή παραγωγή περιεχομένου και κοινοποίησης ιδεών στα πλαίσια μιας ψηφιακής κοινότητας. Οι κοινότητες του Web 2.0 ενθαρρύνουν τη συμμετοχή διευκολύνοντας την «αλληλεπίδραση μιας ομάδας σε ένα χώρο [αρχιτεκτονική της συμμετοχής] όπου τα άτομα συμμετέχουν, κοινωνικοποιούνται και καθορίζουν κοινωνικές νόρμες» (Cho, 2007). Εφαρμόζοντας την έννοια των κοινοτήτων πρακτικής, που ορίζονται ως ομάδες ή δίκτυα και περιορίζονται από πρακτικές και αξίες (Wenger 1999), υποστηρίζεται ότι οι ψηφιακές κοινότητες με επίκεντρο δράσης συγκεκριμένους ιστότοπους, φόρουμ ή κοινωνικά δίκτυα αναπτύσσουν κώδικες συμπεριφοράς που υποδηλώνουν αληθινή συμμετοχή, αποδοχή και ενσωμάτωση μέσα στην κοινότητα. Στις κοινότητες που δημιουργήθηκαν με εργαλεία του Web 2.0, οι κώδικες συμπεριφοράς επικεντρώνονται, συνήθως, στις έννοιες της συνεργασίας, της συζήτησης και της αλληλεπίδρασης καταλήγουν στην κοινή κυριότητα οποιουδήποτε έργου παράγεται από την κοινότητα (Barsky&Cho, 2007). Η αποδοχή σε μια κοινότητα μπορεί να βασίζεται στο βαθμό που τηρούνται ή παραβιάζονται οι κανόνες μιας κοινότητας. Ένας οργανισμός που χρησιμοποιεί ένα blog ή προφίλ κοινωνικού δικτύου αποκλειστικά για τον εαυτό του ή για προώθηση προϊόντος στην καλύτερη περίπτωση αγνοείται από τους χρήστες ή στη χειρότερη τίθεται εκτός ιστότοπου από τους διαχειριστές. Πολλές δημοσιεύσεις υποστηρίζουν ότι η διαδραστικότητα θα έπρεπε να αποτελεί στόχο των οργανισμών με σκοπό τη δημιουργία σχέσεων με τους πελάτες, τους υποστηρικτές και να επικοινωνούν με το ακροατήριό τους επιθυμώντας μιας τέτοια μετατόπιση στη συμπεριφορά και στη φιλοσοφία ενός πολιτικού κόμματος. Οι Ferber, Foltz και Pugliese (2007) εγείρουν το ερώτημα για το αν το διαδίκτυο προσφέρει, γενικότερα, «ευκαιρίες για [δημόσιο] διάλογο που δίνει τροφή για σκέψη και που θα μπορούσε να παρέχει μια κατεύθυνση για τους αντιπροσώπους-νομοθέτες ή ένα πειστικό επιχείρημα που μπορεί να επηρεάσει την κρίση των εντολοδόχων».

Με άλλα λόγια, συμπεραίνεται ότι, θεωρητικά στο διαδίκτυο οι σχέσεις εξουσίας μπορούν να ανατραπούν στα πλαίσια μιας πραγματικά διαδραστικής συμμετοχικής δημοκρατίας πληροφορίας μέσω των εργαλείων του Web 2.0. Ωστόσο, υπάρχουν αντιρρήσεις σ' αυτό το επιχείρημα που αφορούν στο αν είναι ειλικρινής η χρήση των εργαλείων του Web 2.0 από τα κόμματα απέναντι σε όλους τους χρήστες, ακόμα και

στο ίδιο το κόμμα ή αν τα κόμματα θέλουν απλώς να δώσουν την εντύπωση μιας διαλογικής σχέσης με τους ψηφοφόρους (Jackson&Lilleker, 2009).

1.3.3 Web 3.0

Ο JohnMarkoff των NewYorkTimes πρότεινε, το 2006, το Web 3.0 ως η τρίτη γενιά του ιστού. Η βασική ιδέα του Web 3.0 είναι να καθορίσει τα δεδομένα δομής και να τα συνδέσει, ώστε να γίνει πιο αποτελεσματική ανακάλυψη, αυτοματοποίηση, ενσωμάτωση και επαναχρησιμοποίηση σε διάφορες εφαρμογές (Palmer, 2001).Το Web 3.0 προσπαθεί να συνδέσει, να ενσωματώσει και να αναλύσει δεδομένα από διάφορα σύνολα δεδομένων ώστε να αποκτηθεί νέα ροή πληροφοριών. Είναι σε θέση να βελτιώσει τη διαχείριση δεδομένων, να υποστηρίξει την προσβασιμότητα του κινητού διαδικτύου, να προσομοιώσει τη δημιουργικότητα και την καινοτομία, να ενθαρρύνει τον παράγοντα των φαινομένων της παγκοσμιοποίησης, να αυξήσει την ικανοποίηση των χρηστών και να βοηθήσει στην οργάνωση της συνεργασίας στον κοινωνικό ιστό (Aghaei, Nematbakhsh&Farsani, 2012).

1.3.4 Web 4.0

Το Web 4.0 εξακολουθεί να είναι μια ιδέα σε εξέλιξη. Το Web 4.0 είναι επίσης γνωστό ως συμβιωτικός ιστός. Το όνειρο του συμβιωτικού ιστού είναι η αλληλεπίδραση μεταξύ ανθρώπων και μηχανών σε συμβίωση. Θα είναι δυνατή η δημιουργία ισχυρότερων διεπαφών, όπως οι ελεγχόμενες διεπαφές χρησιμοποιώντας το Web 4.0. Με απλά λόγια, τα μηχανήματα θα είναι έξυπνα κατά την ανάγνωση του περιεχομένου του ιστού και θα αντιδρούν με τη μορφή εκτέλεσης και απόφασης για το τι θα εκτελέσουν πρώτα για να φορτώσουν γρήγορα τους ιστότοπους με ανώτερη ποιότητα και απόδοση και να δημιουργήσουν πιο επιβλητικές διεπαφές (Aghaei, Nematbakhsh&Farsani, 2012).

Το Web 4.0 θα είναι ο ιστότοπος ανάγνωσης-εγγραφής-εκτέλεσης-ταυτότητας. Επιτυγχάνει μια κρίσιμη μάζα συμμετοχής σε διαδικτυακά δίκτυα που παρέχουν παγκόσμια διαφάνεια, διακυβέρνηση, διανομή, συμμετοχή, συνεργασία σε βασικές κοινότητες όπως η βιομηχανία, οι πολιτικές, οι κοινωνικές και άλλες κοινότητες. Το Web 4.0 ή το webOS θα είναι ένα ενδιάμεσο λογισμικό στο οποίο θα αρχίσει να λειτουργεί όπως ένα λειτουργικό σύστημα.Το webOS θα είναι παράλληλο με τον ανθρώπινο εγκέφαλο και θα περιλαμβάνει ένα τεράστιο δίκτυο πολύ ευφυών αλληλεπιδράσεων(Aghaei, Nematbakhsh&Farsani, 2012).

Παρόλο που δεν υπάρχει ακριβής ιδέα για το web 4.0 και τις τεχνολογίες του, είναι προφανές ότι ο ιστός κινείται προς τη χρήση της τεχνητής νοημοσύνης για να γίνει ένας έξυπνος ιστός (Aghaei, Nematbakhsh&Farsani, 2012).

1.4 ΙΣΤΟΤΟΠΟΙ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ (SOCIALMEDIA)

Στα τέλη της δεκαετίας του 1990, καθώς το ευρυζωνικό διαδίκτυο έγινε πιο δημοφιλές, άρχισαν να εμφανίζονται ιστότοποι που επιτρέπουν στους χρήστες να δημιουργούν και να ανεβάζουν περιεχόμενο. Ο πρώτος ιστότοπος κοινωνικού δικτύου (SixDegrees.com) εμφανίστηκε το 1997. Από το 2002 και μετά, ξεκίνησε ένας μεγάλος αριθμός κοινωνικών δικτύων. Κάποιοι από αυτούς τους ιστότοπους, όπως ο Friendster, απολάμβαναν μια δημοτικότητα, και στη συνέχεια εξασθένισαν. Άλλοι ανέπτυξαν εξειδικευμένες κοινότητες, όπως για παράδειγμα το MySpace, που απευθύνθηκε σε λάτρεις της εφηβικής μουσικής (Dewing, 2010).

Μέχρι τα τέλη της δεκαετίας του 2000, τα κοινωνικά μέσα είχαν αποκτήσει ευρεία αποδοχή και ορισμένες υπηρεσίες κέρδισαν τεράστιο αριθμό χρηστών. Για παράδειγμα, το Νοέμβριο του 2012, το Facebook ανακοίνωσε ότι είχε 1 δισεκατομμύριο χρήστες σε όλο τον κόσμο. Τον Ιούλιο του 2012, το Twitter είχε περίπου 517 εκατομμύρια χρήστες, εκ των οποίων 10 εκατομμύρια ήταν στον Καναδά (Dewing, 2010).

Ο όρος «κοινωνικά μέσα» αναφέρεται στο ευρύ φάσμα υπηρεσιών μέσω διαδικτύου και κινητής τηλεφωνίας που επιτρέπουν στους χρήστες να συμμετέχουν σε ηλεκτρονικές ανταλλαγές, να συνεισφέρουν στο περιεχόμενο που δημιουργείται από τους χρήστες ή να συμμετέχουν σε διαδικτυακές κοινότητες (Dewing, 2010).

Σε αυτή την ταχεία αύξηση της συμμετοχής των κοινωνικών μέσων ενημέρωσης συνέβαλαν διάφοροι παράγοντες. Αυτοί περιλαμβάνουν: τεχνολογικούς παράγοντες όπως αυξημένη διαθεσιμότητα ευρυζωνικών συνδέσεων, βελτίωση των εργαλείων λογισμικού και ανάπτυξη ισχυρότερων υπολογιστών και κινητών συσκευών, κοινωνικούς παράγοντες, όπως η ταχεία υιοθέτηση των κοινωνικών μέσων από νεότερες ηλικιακές ομάδες, οικονομικούς παράγοντες όπως η αυξανόμενη οικονομική προσιτότητα των ηλεκτρονικών υπολογιστών και του λογισμικού και το αυξανόμενο εμπορικό ενδιαφέρον στις τοποθεσίες κοινωνικών μέσων μαζικής ενημέρωσης (Dewing, 2010)

.

Τα χαρακτηριστικά των μέσων κοινωνικής δικτύωσης είναι:

- Περιλαμβάνουν μεγάλη ποικιλία μορφών περιεχομένου, όπως κείμενο, βίντεο, φωτογραφίες, ήχο. Πολλά μέσα κοινωνικής δικτύωσης κάνουν χρήση αυτών των επιλογών επιτρέποντας περισσότερες από μία εναλλακτικές λύσεις περιεχομένου.
- Επιτρέπουν, μέσω των αλληλεπιδράσεων, στους χρήστες να βλέπουν μία ή περισσότερες πλατφόρμες.

- Διευκολύνουν την αυξημένη ταχύτητα και το εύρος της διάδοσης των πληροφοριών.

- Παρέχουν επικοινωνίες one-to-one, one-to-many και πολλές προς πολλές.

- Επιτρέπουν την πραγματοποίηση επικοινωνίας σε πραγματικό χρόνο η οποία μπορεί να πραγματοποιηθεί μέσω υπολογιστή, tablet και smartphone.

- Δημιουργούν, σε απευθείας σύνδεση, γεγονότα σε πραγματικό χρόνο, επεκτείνοντας τις διαδικτυακές αλληλεπιδράσεις εκτός σύνδεσης ή αυξάνοντας τις ζωντανές εκδηλώσεις στο διαδίκτυο (Vele&Zlateva, n.d).

1.4.1 Διάφορα μέσα κοινωνικής δικτύωσης

Τα είδη υπηρεσιών Internet που συνήθως συνδέονται με κοινωνικά μέσα (μερικές φορές αναφέρονται ως «Web 2.0») περιλαμβάνουν τα εξής:

- Blogs. Ένα blog είναι μια ηλεκτρονική, χρονολογική συλλογή προσωπικών σχολίων και συνδέσμων. Εύκολο στη δημιουργία και τη χρήση από οπουδήποτε με σύνδεση στο Internet. Τα blogs είναι μια μορφή δημοσίευσης στο διαδίκτυο που έχει γίνει ένα καθιερωμένο μέσο επικοινωνίας
- Wikis. Ένα wiki είναι ένας συλλογικός ιστότοπος στον οποίο οποιοσδήποτε συμμετέχων μπορεί να τροποποιήσει οποιαδήποτε σελίδα ή να δημιουργήσει μια νέα σελίδα. Ένα πολύ γνωστό παράδειγμα είναι η Wikipedia, μια δωρεάν ηλεκτρονική εγκυκλοπαίδεια που χρησιμοποιεί την τεχνολογία wiki (Dewing, 2010).
- Κοινωνικός σελιδοδείκτης. Οι ιστότοποι κοινωνικού bookmarking επιτρέπουν στους χρήστες να οργανώνουν και να μοιράζονται συνδέσμους σε ιστότοπους. Παραδείγματα περιλαμβάνουν τα reddit, StumbleUpon και Digg. (Dewing, 2010).
- Τοποθεσίες κοινωνικού δικτύου. Αυτές έχουν οριστεί ως «υπηρεσίες μέσω διαδικτύου που επιτρέπουν στα άτομα να (1) κατασκευάσουν ένα δημόσιο ή ημι-δημόσιο προφίλ εντός ενός οριακού συστήματος, (2) να διατυπώσουν μια λίστα με άλλους χρήστες με τους οποίους μοιράζονται μια σύνδεση και (3) να βλέπουν και να διασχίζουν τη λίστα των συνδέσεών τους και εκείνες που γίνονται από άλλους εντός του συστήματος». Μεταξύ των πιο δημοφιλών είναι το Facebook και το Linkedln (Dewing, 2010).

Το Facebook είναι ένα ιδιαίτερα ανεπτυγμένο κοινωνικό δίκτυο. Πρόκειται για μια ανοιχτή online υπηρεσία κοινωνικής δικτύωσης όπου οι άνθρωποι μπορούν να επικοινωνούν με τους φίλους τους, να δημιουργήσουν νέες σχέσεις και να συγκροτήσουν ομάδες κοινού ενδιαφέροντος (Γεωργίου &Πορίκης, 2011-2012).

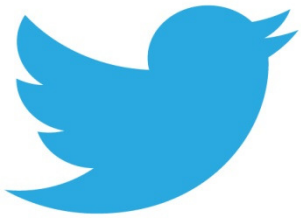
Εικόνα 1.1: Αρχική σελίδαfacebook

Τίτλος Κοινωνικού δικτύου	Facebook
Διεύθυνση ιστότοπου	www.facebook.com
Ελεύθερη εγγραφή μελών	Ναι
Απαιτούμενα στοιχεία για την εγγραφή μελών	Ονοματεπώνυμο, ηλικία, φύλο, ηλεκτρονική διεύθυνση
Στοιχεία που εμφανίζονται στο προφίλ των μελών	Φωτογραφία, ημερομηνία γέννησης, σπουδές, επάγγελμα, ενδιαφέροντα, προσωπική κατάσταση (ελεύθερος/δεσμευμένος κλπ)
Τρόπος διασύνδεσης με άλλους χρήστες	Ελεύθερη / μετά από πρόσκληση / μετά από αίτημα
Υλικό που μπορούν να δημοσιεύσουν οι χρήστες	Κείμενο, Εικόνες, Βίντεο, Σύνδεσμοι
Άλμπουμ φωτογραφιών	Υποστηρίζεται
Αριθμός χρηστών παγκοσμίως	Περίπου 800.000.000
Αριθμός χρηστών πανελλήνια	Περίπου 6.000.000

Πίνακας 1.1: Γενικά χαρακτηριστικά του facebook

• Υπηρεσίες ενημέρωσης κατάστασης. Επίσης γνωστές ως υπηρεσίες microblogging. Οι υπηρεσίες ενημέρωσης κατάστασης, όπως το Twitter, επιτρέπουν στους χρήστες να μοιράζονται σύντομες ενημερώσεις σχετικά με άτομα ή εκδηλώσεις και να βλέπουν τις ενημερώσεις που δημιουργούνται από άλλους (Dewing, 2010).

Από την εμφάνισή του το 2006, ο ιστότοπος του Twitter έχει αναπτυχθεί τόσο που πλέον κατατάσσεται ως ο δέκατος ιστότοπος με τη μεγαλύτερη επισκεψιμότητα παγκοσμίως. Το Twitter είναι πλατφόρμα μικροϊστολογίου. Αυτό σημαίνει ότι πρόκειται για ένα σύστημα κοινοποίησης πληροφοριών όπου οι χρήστες μπορούν είτε να «ακολουθήσουν» άλλους χρήστες που δημοσιεύουν σύντομα μηνύματα ή να «ακολουθούνται» από άλλους. Τον Ιανουάριο του 2010, ο αριθμός των μηνυμάτων που ανταλλάχθηκαν μέσω twitter έφτασε τα 1,2 δισεκατομμύρια, ενώ ανταλλάχθηκαν περισσότερα από 40 εκατομμύρια μηνύματα την ημέρα (Bouillotet.al, 2012).



Εικόνα 1.2: Το σήμα του twitter

• Περιεχόμενο του εικονικού κόσμου. Αυτοί οι ιστότοποι προσφέρουν εικονικά περιβάλλοντα τύπου παιχνιδιών στα οποία οι χρήστες αλληλεπιδρούν. Ένα παράδειγμα είναι ο φανταστικός κόσμος που κατασκευάστηκε στο SecondLife, στον οποίο οι χρήστες δημιουργούν avatars (μια εικονική αναπαράσταση του χρήστη) που αλληλεπιδρούν με άλλους(Dewing, 2010).

• Τοποθεσίες κοινής χρήσης μέσων. Αυτοί οι ιστότοποι επιτρέπουν στους χρήστες να δημοσιεύουν βίντεο ή φωτογραφίες. Δημοφιλή παραδείγματα είναι το YouTube, το Pinterest και το Instagram (Dewing, 2010).

Η επίσημη έναρξη λειτουργίας του YouTube έλαβε χώρα το Δεκέμβριο του 2005 και γρήγορα καθιερώθηκε ως ο «ηγέτης των διαδικτυακών video», όπου οι χρήστες μπορούσαν να δουν και να κοινοποιήσουν εύκολα πρωτότυπα video μέσω ενός προγράμματος περιήγησης (http://www.youtube.com/t/fact_sheet). Χάρη στην

ενσωματωμένη εφαρμογή αναπαραγωγής, τα video που δημοσιεύονται στο YouTubeμπορούν εύκολα να ενσωματωθούν σε διαφορετικό ιστότοπο, π.χ. ενός πολιτικού κόμματος. Έτσι το YouTube μπορεί να αποτελεί έναν απλό τρόπο για την δωρεάν αποθήκευση και αποστολή video. Για το «ανέβασμα» των video και τη δημιουργία «καναλιού» χρειάζεται ένας λογαριασμός χρήστη, ενώ δεν απαιτείται η δημιουργία δημόσιου προσωπικού προφίλ.

Εικόνα 1.3: Το σήμα του youtube

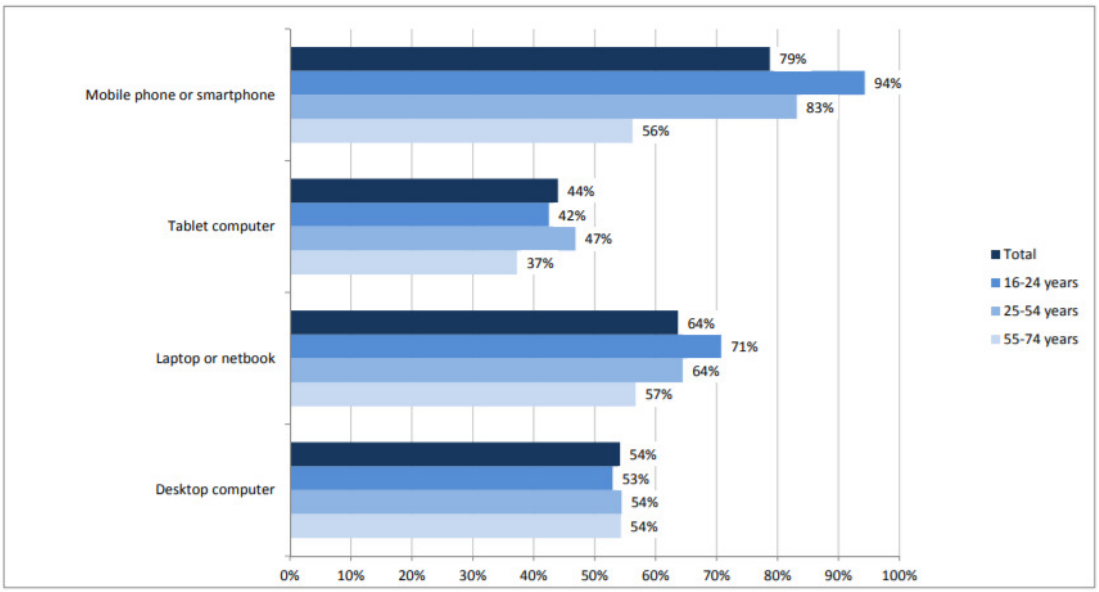
Τίτλος Κοινωνικού δικτύου	Youtube
Διεύθυνση ιστότοπου	www.youtube.com
Ελεύθερη εγγραφή μελών	Ναι, σύνδεση με λογαριασμό gmail
Απαιτούμενα στοιχεία για την εγγραφή μελών	Διεύθυνση ηλεκτρονικού ταχυδρομείου, όνομα χρήστη, τοποθεσία, ημερομηνία γέννησης, φύλλο
Στοιχεία που εμφανίζονται στο προφίλ των μελών	Φωτογραφία, ημερομηνία γέννησης, σπουδές, επάγγελμα, ενδιαφέροντα, κατάσταση
Τρόπος διασύνδεσης με άλλους χρήστες	Ελεύθερη / μετά από πρόσκληση / μετά από αίτημα
Υλικό δημοσίευσης	Κείμενο, εικόνες, βίντεο, σύνδεσμοι
Άλμπουμ φωτογραφιών	Ναι, / όχι
Αριθμός προβολών βίντεο	Περισσότερες από 1 δισεκατομμύριο την εβδομάδα

Πίνακας 1.2: Γενικά χαρακτηριστικά του youtube

1.5 ΣΤΑΤΙΣΤΙΚΑ ΣΤΟΙΧΕΙΑ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΥΡΩΠΗ

Σύμφωνα με στοιχεία που εκδόθηκαν από την Eurostat (Δεκέμβριος, 2016), τη στατιστική υπηρεσία της Ευρωπαϊκής Ένωσης και αποτελούν μέρος των αποτελεσμάτων της έρευνας που διεξήχθη το 2016 σχετικά με τις ΤΠΕ (χρήση τεχνολογιών πληροφοριών και επικοινωνιών) σε νοικοκυριά και ιδιώτες, περισσότερο από το 80% των ατόμων ηλικίας 16 έως 74 ετών στην Ευρωπαϊκή Ένωση (ΕΕ) χρησιμοποίησαν το διαδίκτυο σε πολλές περιπτώσεις, μέσω πολλών διαφορετικών συσκευών. Τα κινητά τηλέφωνα ή τα έξυπνα τηλέφωνα ήταν η συσκευή που χρησιμοποιείται περισσότερο για να «σερφάρουν» οι χρήστες στο Διαδίκτυο, με ποσοστό 79%. Ακολουθούν οι φορητοί υπολογιστές ή τα netbooks (64%), οι σταθεροί υπολογιστές (54%) και τα tablet (44%).

Επιπλέον, κατά τη διάρκεια του εξεταζόμενου έτους, περισσότερο από το 70% των χρηστών του διαδικτύου στην ΕΕ παρείχε κάποιο είδος ηλεκτρονικών προσωπικών πληροφοριών στο διαδίκτυο, πολλοί από τους οποίους χρησιμοποιούσαν διαφορετικές ενέργειες για τον έλεγχο της πρόσβασης σε αυτές τις προσωπικές πληροφορίες. Σχεδόν οι μισοί από αυτούς (46%) δεν επέτρεπαν τη χρήση προσωπικών πληροφοριών για διαφήμιση και το 40% είχε περιορισμένη πρόσβαση στο προφίλ τους ή σε περιεχόμενο ιστότοπων κοινωνικής δικτύωσης. Επιπλέον, το 37% των χρηστών του διαδικτύου διαβάζει τις δηλώσεις πολιτικής προστασίας προσωπικών δεδομένων προτού παράσχουν προσωπικές πληροφορίες και 31% έχουν περιορισμένη πρόσβαση στη γεωγραφική τους θέση.



Διάγραμμα 1.1: Κύριες συσκευές που χρησιμοποιούνται στην ΕΕ για πλοήγηση στο διαδίκτυο, ανά ηλικιακή ομάδα, 2016 (ως % των χρηστών του διαδικτύου τους τελευταίους τρεις μήνες)

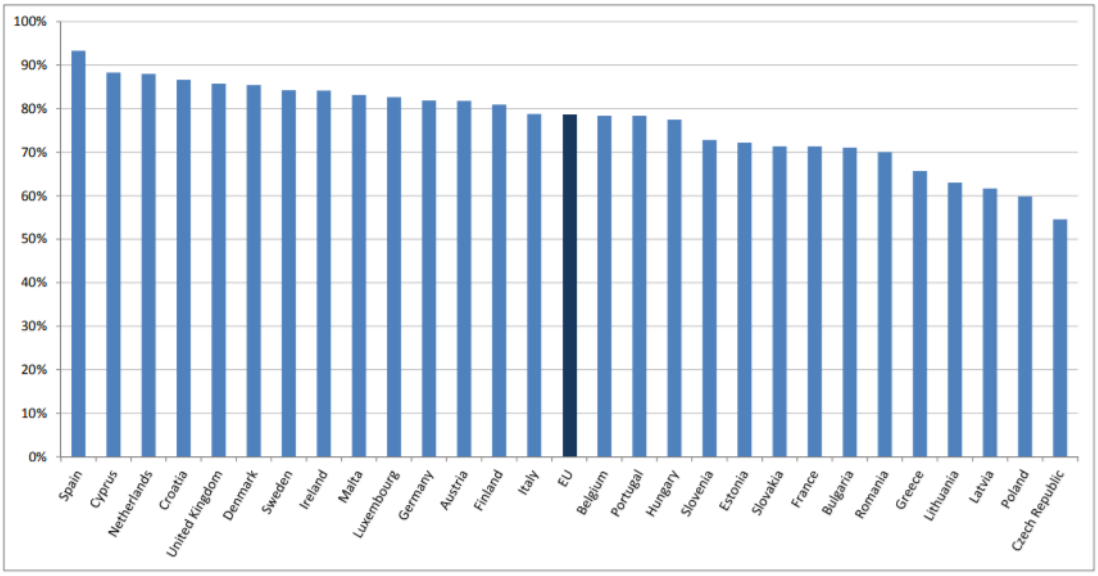
Πηγή: Eurostat, 2016.

Σύμφωνα με την ίδια πηγή, τα υψηλότερα ποσοστά των χρηστών μέσω κινητού τηλεφώνου ή smartphone, σημειώθηκαν στην Ισπανία, την Κύπρο και την Ολλανδία Τα κινητά τηλέφωνα ή τα smartphones ήταν οι συσκευές που χρησιμοποιούνταν περισσότερο το 2016 από χρήστες στο διαδίκτυο σε κάθε κράτος μέλος της ΕΕ, εκτός από την Τσεχία, την Εσθονία, τη Λιθουανία, την Πολωνία και τη Σλοβακία όπου ήταν φορητοί υπολογιστές ή τα netbooks. Το 2016, το μεγαλύτερο ποσοστό των χρηστών του Διαδικτύου που είχαν πρόσβαση στο Διαδίκτυο μέσω κινητού τηλεφώνου ή smartphone, καταγράφηκε στην Ισπανία (93% των χρηστών που χρησιμοποίησαν το διαδίκτυο το τελευταίο τρίμηνο), ακολουθούν η Κύπρος και η Ολλανδία (88%), η Κροατία (87%), το Ηνωμένο Βασίλειο (86%) και η Δανία (85%). Στο αντίθετο άκρο της κλίμακας, το χαμηλότερο ποσοστό καταγράφηκε στην Τσεχική Δημοκρατία (55%), ακολουθούμενη από την Πολωνία (60%), τη Λετονία (62%), τη Λιθουανία (63%) και την Ελλάδα (66%).

Μεταξύ των κρατών μελών, οι φορητοί υπολογιστές ή τα netbook, χρησιμοποιήθηκαν, για να περιηγηθούν στο διαδίκτυο, τουλάχιστον από τα τρία τέταρτα των χρηστών του διαδικτύου στην Ολλανδία (80%), τη Φινλανδία, το Βέλγιο (78%) και τη Δανία (76%). Περισσότερο από τα δύο τρίτα των χρηστών του

διαδικτύου στην Ουγγαρία, το Λουξεμβούργο και τη Ρουμανία (το σύνολο 68%) καθώς και τη Γερμανία (67%). Τέλος, οι υπολογιστές tablet χρησιμοποιήθηκαν για πρόσβαση στο διαδίκτυο, από λιγότερους από τους μισούς χρήστες στο Διαδίκτυο, σε μεγάλη πλειοψηφία των κρατών μελών, με εξαίρεση την Ολλανδία (66%), το Ηνωμένο Βασίλειο (61%), τη Δανία (56%), τη Γερμανία (55%), το Λουξεμβούργο (53%) και τη Φινλανδία (52%).

Σε επίπεδο ΕΕ, τα άτομα ηλικίας 16-24 ετών προτιμούσαν κυρίως την πρόσβαση στο διαδίκτυο μέσω κινητού τηλεφώνου ή smartphone (94%), καθώς και μέσω φορητού υπολογιστή ή netbook (71%), ενώ η χρήση ενός tablet ήταν πιο δημοφιλής μεταξύ των ατόμων ηλικίας 25-54 ετών (47%).

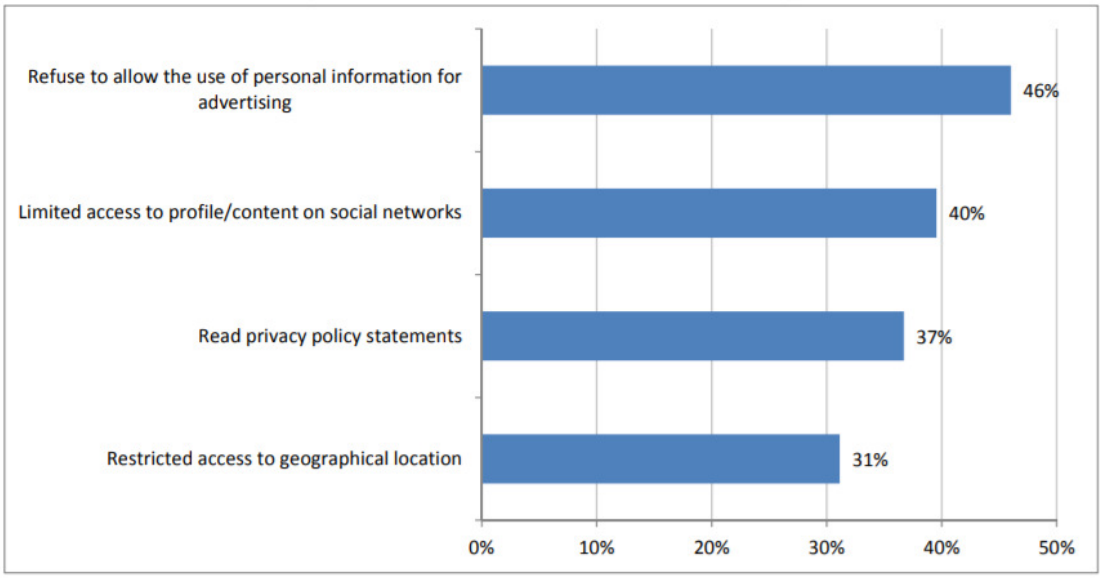


Διάγραμμα 1.2: Οι χρήστες του Διαδικτύου που έχουν πρόσβαση στο διαδίκτυο μέσω κινητού τηλεφώνου ή smartphone στην ΕΕ το 2016 (ως% των χρηστών του διαδικτύου τους τελευταίους τρεις μήνες)

Πηγή: Eurostat, 2016.

Σε ότι αφορά τις διαφορές στους τρόπους διαχείρισης της πρόσβασης σε διαδικτυακές προσωπικές πληροφορίες, μεταξύ των κρατών μελών της ΕΕ, παρατηρούνται στον τρόπο με τον οποίο οι χρήστες του διαδικτύου διαχειρίζονταν την πρόσβαση στις προσωπικές τους πληροφορίες στο διαδίκτυο. Σε δώδεκα κράτη μέλη οι χρήστες αρνήθηκαν να επιτρέψουν τη χρήση προσωπικών πληροφοριών (72% των χρηστών του διαδικτύου), ανάμεσα τους η Φινλανδία (71%), ακολουθούμενη από την

Ολλανδία (65%), τη Δανία (60%) και την Εσθονία (59%). Σε εννέα κράτη μέλη, η πρόσβαση σε προσωπικές πληροφορίες διαχειρίστηκε κατά κύριο λόγο μέσω των πολιτικών απορρήτου, όπως για παράδειγμα μέσω περιορισμένης πρόσβασης σε προφίλ ή σε περιεχόμενο κοινωνικών δικτύων. Μολονότι ο περιορισμός της πρόσβασης της γεωγραφικής θέσης δεν ήταν το πλέον χρησιμοποιούμενο εργαλείο σε οποιοδήποτε κράτος μέλος, περισσότεροι από τους μισούς χρήστες του διαδικτύου το έπραξαν, όπως για παράδειγμα στο Λουξεμβούργο (63%), στη Φινλανδία (58%), στην Αυστρία και στην Ολλανδία (και οι δύο 52%).



Διάγραμμα 1.3: Κύριες δράσεις που αναλήφθηκαν από τους χρήστες του διαδικτύου στην ΕΕ το 2016, για τη διαχείριση της πρόσβασης σε προσωπικές πληροφορίες (ως % των χρηστών του διαδικτύου τους τελευταίους δώδεκα μήνες)

Πηγή: Eurostat, 2016.

Τέλος, η ίδια έρευνα παραθέτει σε δυο πίνακες, οι οποίοι παρουσιάζονται στη συνέχεια, αναλυτικά τα ποσοστά για κάθε χώρα της ΕΕ των κύριων συσκευών που χρησιμοποιούνται από τα άτομα για πλοήγηση στο Internet το 2016 καθώς και τις δράσεις που αναλαμβάνονται από τα άτομα αυτά προκειμένου να προστατεύσουν τα προσωπικά τους δεδομένα.

	Σταθερός υπολογιστής	Φορητός υπολογιστήςήnetbook	Tablet	Κινητό τηλέφωνο ή smartphone
Ευρωπαϊκή Ένωση	**54**	**64**	**44**	**79**
Βέλγιο	53	78	49	78
Βουλγαρία	58	51	19	71
Τσεχική Δημοκρατία	51	66	19	55
Δανία	40	76	56	85
Γερμανία	67	71	55	82
Εσθονία	49	73	32	72
Ιρλανδία	25	67	37	84
Ελλάδα	49	62	31	66
Ισπανία	45	58	42	93
Γαλλία	60	63	46	71
Κροατία	63	66	29	87
Ιταλία	50	31	29	79
Κύπρος	29	69	37	88
Λετονία	54	59	25	62
Λιθουανία	42	69	23	63
Λουξεμβούργο	68	74	53	83
Ουγγαρία	68	64	22	77
Μάλτα	42	69	45	83
Ολλανδία	64	80	66	88
Αυστρία	56	69	35	82
Πολωνία	49	74	21	60
Πορτογαλία	46	73	44	78
Ρουμανία	68	37	26	70
Σλοβενία	57	70	30	73
Σλοβακία	54	73	36	71
Φινλανδία	51	78	52	81
Σουηδία	43	70	49	84
Ηνωμένο Βασίλειο	45	70	61	86
Νορβηγία	33	84	66	89
Πρώην Γιουγκοσλαβική Δημοκρατία της Μακεδονίας	59	54	17	81

Πίνακας 1.3: Κύριες συσκευές που χρησιμοποιούνται από άτομα για πλοήγηση στο Internet, 2016 (ως% των χρηστών του διαδικτύου τους τελευταίους τρεις μήνες)[1]

Πηγή: Eurostat, 2016.

[1]Οι ερωτηθέντες μπορούσαν να απαντήσουν περισσότερες από μία ενέργειες.

	Παρέχονται προσωπικές πληροφορίες	Προστατεύουν τα προσωπικά δεδομένα	Παρέχουν περιορισμένη πρόσβαση στη γεωγραφική θέση	Παρέχουν περιορισμένη πρόσβαση σε προφίλ / περιεχόμενο, στα κοινωνικά δίκτυα	Δεν επιτρέπουν τη χρήση προσωπικών πληροφοριών για διαφήμιση
Ευρωπαϊκή Ένωση	**71**	**37**	**31**	**40**	**46**
Βέλγιο	71	29	34	49	48
Βουλγαρία	50	29	10	20	12
Τσεχική Δημοκρατία	67	45	14	15	25
Δανία	83	44	47	59	60
Γερμανία	80	45	36	41	55
Εσθονία	77	42	44	49	59
Ιρλανδία	76	26	21	32	32
Ελλάδα	83	32	18	28	28
Ισπανία	74	36	40	50	52
Γαλλία	73	22	32	39	50
Κροατία	65	50	37	55	50
Ιταλία	52	33	11	22	31
Κύπρος	61	22	16	34	26
Λετονία	70	49	26	30	31
Λιθουανία	56	37	22	29	33
Λουξεμβούργο	92	43	63	64	72
Ουγγαρία	65	57	27	42	48
Μάλτα	70	44	43	56	46
Ολλανδία	85	41	52	56	65
Αυστρία	80	45	52	53	56
Πολωνία	51	26	15	25	29
Πορτογαλία	49	44	48	57	52
Ρουμανία	31	24	7	15	15
Σλοβενία	59	34	24	32	35
Σλοβακία	74	59	18	29	31
Φινλανδία	80	50	58	58	71
Σουηδία[2]					
Ηνωμένο Βασίλειο	88	43	38	50	54
Νορβηγία	87	42	47	60	56
Πρώην Γιουγκοσλαβική Δημοκρατία της Μακεδονίας	51	33	25	41	37

Πίνακας 1.4: Κύριες δράσεις που αναλήφθηκαν για τη διαχείριση της πρόσβασης σε προσωπικές πληροφορίες στο διαδίκτυο, το έτος 2016 (ως % των χρηστών του διαδικτύου τους τελευταίους δώδεκα μήνες)[3]

[2]Τα δεδομένα δεν είναι διαθέσιμα.

1.6 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΔΙΑΔΙΚΤΥΟΥ

Το Διαδίκτυο έχει καταστεί ένα ουσιαστικό εργαλείο επικοινωνίας τα τελευταία χρόνια, τόσο για τους ανθρώπους όσο και για τις επιχειρήσεις γενικότερα (Moriyama, 1999).

Η ανάπτυξη όλο και πιο εξελιγμένων τεχνολογιών έχει δημιουργήσει ένα δίκτυο με μια πραγματικά παγκόσμια εμβέλεια, και σχετικά χαμηλά εμπόδια εισόδου στην αγορά. Η τεχνολογία του Διαδικτύου το καθιστά εύκολο στα άτομα να επικοινωνούν με σχετική ανωνυμία, γρήγορα και αποτελεσματικά σε διασυνοριακό επίπεδο, σε ένα σχεδόν απεριόριστο ακροατήριο. Η μεγάλη απήχηση του οφείλεται στα οφέλη που προσφέρει. Τα οφέλη αυτά είναι πολλά, ξεκινώντας με τη μοναδική καταλληλότητά του για ανταλλαγή πληροφοριών και ιδεών, η οποία αναγνωρίζεται ως θεμελιώδες ανθρώπινο δικαίωμα (Ki-moon, 2012).Το Διαδίκτυο, με άλλα λόγια, είναι η λεωφόρος πληροφοριών. Περιέχει περισσότερες πληροφορίες από ό,τι ίσως χρειάζεται. Ανοίγοντας μια σελίδα, τα άτομα μπορούν σε απευθείας σύνδεση να ψωνίζουν, να παίξουν παιχνίδια, να συνομιλήσουν, να παρακολουθήσουν ένα μάθημα σε κάποιο Πανεπιστήμιο, να πληρώσουν λογαριασμούς, να επενδύσουν τα χρήματά τους, να παραγγείλουν φαγητό κ.α. Επιπλέον, η ταχύτητα με την οποία συμβαίνουν όλες αυτές οι ενέργειες είναι εξαιρετικά γρήγορη (Su, 2010).

Ως αποτέλεσμα των παραπάνω, όμως, το Διαδίκτυο μειώνει τις κοινωνικές αλληλεπιδράσεις στη ζωή των ανθρώπων. Με το Διαδίκτυο να έχει τόσες πολλές χρήσεις και να προσφέρει πολυάριθμες υπηρεσίες δημιουργεί μια νωθρότητα στον άνθρωπο και τον αποξενώνει από την επαφή με άλλους ανθρώπους. Επιπλέον, υπάρχει πιθανότητα να παραβιαστεί το λογισμικό και να παραβιαστούν τα προσωπικά δεδομένα (Su, 2010).

Ένα άλλο πρόβλημα ή μειονέκτημα του διαδικτύου είναι ότι επιτρέπει την ανωνυμία και έτσι τα άτομα μπορούν να έχουν πρόσβαση σε διαφορετικές ιστοσελίδες, φόρουμ και αίθουσες συνομιλίας που είναι διαθέσιμες. Αυτό βοηθάει κάποια άτομα να εκμεταλλευτούν κατά καιρούς άλλα άτομα εξαπατώντας τα ή κακοποιώντας τα (Su, 2010).

Είναι γεγονός ότι το διαδίκτυο προσφέρει πολλές δυνατότητες και αποτελεί ένα χρήσιμο εργαλείο τόσο για τον άνθρωπο όσο και για την επιχείρηση, η χρήση του οποίου όμως απαιτεί ιδιαίτερο και προσεκτικό χειρισμό.

ΚΕΦΑΛΑΙΟ 2
ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

2.1 ΕΙΣΑΓΩΓΗ

Η έννοια της ιδιωτικότητας, η οποία έχει διαχρονικά απασχολήσει τους κοινωνικούς επιστήμονες, τους φιλόσοφους και τους νομικούς, εντοπίζεται σε νόμους για την προστασία δεδομένων, τοποθετώντας την στο πλαίσιο διαχείρισης προσωπικών πληροφοριών. Η ιδιωτικότητα έχει κατοχυρωθεί ως βασικό πανανθρώπινο δικαίωμα στη Διακήρυξη Ανθρωπίνων Δικαιωμάτων των Ηνωμένων Εθνών, στη Συνθήκη για τα Αστικά και Πολιτικά Δικαιώματα και σε πολλές άλλες εθνικές και διεθνείς συνθήκες. Στις σημερινές δημοκρατικές κοινωνίες, η ανάγκη διασφάλισης της ιδιωτικότητας συνιστά απαραίτητη προϋπόθεση, αλλά με τηναξιοποίηση πληροφοριακών και επικοινωνιακών τεχνολογικών συστημάτων, η ιδιωτικότητα βρίσκεται σε ολοένα αυξανόμενο κίνδυνο (Μαυρωνά, 2012).

2.2 ΟΡΙΣΜΟΣ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Το δικαίωμα στην ιδιωτικότητα είναι ένα αρχαίο δικαίωμα, με ρίζες σε διάφορες θρησκευτικές παραδόσεις-συμπεριλαμβανομένων των εβραϊκών, χριστιανικών και μουσουλμανικών- καθώς και στην αρχαία Ελλάδα και την Κίνα. Ορισμένα είδη προστασίας της ιδιωτικής ζωής υπήρχαν στην Αγγλία ήδη από το 1361. Η προστασία της ιδιωτικής ζωής έχει βρεθεί εξ αρχής ως διεθνές ανθρώπινο δικαίωμα και περιλαμβάνεται στην Οικουμενική Διακήρυξη των Ανθρωπίνων Δικαιωμάτων (UDHR), καθώς και στο Διεθνές Σύμφωνο για τα ατομικά και πολιτικά δικαιώματα (ICCPR) (Puddephatt, Mendel, Wanger, Hawtin&Torres, 2012).

Ταυτόχρονα, αποδείχθηκε δύσκολο να επιτευχθεί συναίνεση σχετικά με το συγκεκριμένο περιεχόμενο αυτού του δικαιώματος. Είναι σαφές ότι έχει στο βασικό της πυρήνα κάποια έννοια του δικαιώματος να είναι ελεύθερη από εξωτερική εισβολή, αλλά πέρα από αυτό διάφοροι συγγραφείς έχουν καταλήξει σε διαφορετικούς ορισμούς. Έτσι, η έκθεση της κυβέρνησης του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας για την προστασία της ιδιωτικής ζωής, γνωστή ως έκθεση Calcutt, δήλωσε ότι οι συγγραφείς δεν μπορούσαν να βρουν έναν «εξ'ολοκλήρου ικανοποιητικό ορισμό» (Puddephatt, Mendel, Wanger, Hawtin&Torres, 2012).

Οι Αμερικανοί δικαστές S. Warren και L. Brandeis, ωστόσο, το 1890, προσδιόρισαν την ιδιωτικότητα ως *«...το δικαίωμα των πολιτών* σε *μία ανενόχλητη ιδιωτική ζωή»* (Μαυρωνά, 2012). Το Συνταγματικό Δικαστήριο της Νότιας Αφρικής ορίζει την ιδιωτικότητα ως το «δικαίωμα ενός ατόμου να ζήσει τη ζωή του ως αυτός θέλει», ενώ, το Ανώτατο Δικαστήριο του Καναδά ως «τη στενή σφαίρα της προσωπικής αυτονομίας μέσα στην οποία γίνονται εγγενώς ιδιωτικές επιλογές»(Puddephatt, Mendel, Wanger, Hawtin&Torres, 2012).

Στη συνέχεια, άλλοι σύγχρονοι ερευνητές όπως οι Bünnig και Cap (2009) περιέγραψαν την ιδιωτικότητα ως την προστασία των προσωπικών πληροφοριών, από καταχρήσεις και κακόβουλες οντότητες, επιτρέποντας, παράλληλα, σε ορισμένα εξουσιοδοτημένα πρόσωπα να έχουν πρόσβαση στα προσωπικά δεδομένα, καθιστώντας τα ορατά σε αυτά. Τέλος, οι Taherietal. (2010) υποστήριξαν ότι το απόρρητο είναι ιδιαίτερα σημαντικό σε ένα ευρύ φάσμα εφαρμογών που επιδιώκουν να προστατεύσουν τις πληροφορίες θέσης του χρήστη, κρύβοντας μερικές λεπτομέρειες από τους άλλους (Aldhafferiet.al., 2013).

2.3 Η ΕΝΝΟΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σύμφωνα με το δίκαιο της Ευρωπαϊκής Ένωσηςαλλά και με το δίκαιο του ΣΤΕ, ο όρος «προσωπικά δεδομένα», υποδηλώνει οποιαδήποτε πληροφορία που αναφέρεται σε φυσικό πρόσωπο, του οποίου η ταυτότητα είναι γνωστή, ή μπορεί να εξακριβωθεί,δηλαδή κάθε πληροφορία σχετικά με φυσικό πρόσωπο του οποίου η ταυτότητα είναι φανερή ή μπορεί να εξακριβωθεί με την απόκτηση πρόσθετων πληροφοριών.

Με άλλα λόγια τα προσωπικά δεδομένα αφορούν οποιεσδήποτε προσωπικές πληροφορίες σχετικά με την ιδιωτική ζωή του προσώπου, καθώς και πληροφορίες που αναφέρονται στην επαγγελματική ή τη δημόσια ζωή του και μπορούν να χρησιμοποιηθούν για την άμεση ή έμμεση αναγνώρισή του (EuropeanCommission). Τα προσωπικά δεδομένα ορίζονται στο νόμο, δηλαδή, ως δεδομένα που μπορούν να συνδεθούν με ένα φυσικό πρόσωπο και παραδείγματα αυτών περιλαμβάνουν την ημερομηνία γέννησης, τη σεξουαλική προτίμηση, τη θρησκεία, αλλά και τη διεύθυνση IP του υπολογιστή ή τα δεδομένα που σχετίζονται με αυτές τις πληροφορίες (VandenHoven, Blaauw, Pieters, &Warnier, 2014).

Ορισμένες κατηγορίες προσωπικών δεδομένων, που αναφέρονται στον πυρήνα της ιδιωτικής ζωής, χαρακτηρίζονται από το Νόμο ως ευαίσθητα και απολαύουν μεγαλύτερης προστασίας. Τα ευαίσθητα δεδομένα αναφέρονται αποκλειστικά σε: φυλετική ή εθνοτική προέλευση, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, υγεία και κοινωνική πρόνοια, ερωτική ζωή, ποινικές διώξεις και καταδίκες, συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).

2.4 ΗΘΙΚΟΙ ΛΟΓΟΙ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Οι ηθικοί λόγοι για την προστασία των προσωπικών δεδομένων και για τον άμεσο ή έμμεσο έλεγχο της πρόσβασης στα δεδομένα αυτά από άλλους μπορούν να διακριθούν στους εξής (VandenHoven, Blaauw, Pieters, &Warnier, 2014):

- Πρόληψη της βλάβης: Η απεριόριστη πρόσβαση τρίτων στους κωδικούς πρόσβασης, στα χαρακτηριστικά τους και στον εντοπισμό τους μπορεί να χρησιμοποιηθεί για να βλάψει το υποκείμενο των δεδομένων με διάφορους τρόπους.
- Ενημερωτική ανισότητα: Τα δεδομένα προσωπικού χαρακτήρα έχουν καταστεί εμπορεύματα. Τα άτομα συνήθως δεν βρίσκονται σε καλή θέση να διαπραγματεύονται συμβάσεις σχετικά με τη χρήση των δεδομένων τους και δεν έχουν τα μέσα να ελέγχουν εάν οι εταίροι συμμορφώνονται με τους όρους της σύμβασης. Οι νόμοι, η κανονιστική ρύθμιση και η διακυβέρνηση για την προστασία των δεδομένων στοχεύουν στη δημιουργία δίκαιων συνθηκών για τη σύνταξη συμβάσεων σχετικά με τη διαβίβαση και την ανταλλαγή προσωπικών δεδομένων και την παροχή των υποκειμένων των δεδομένων με ελέγχους και ισορροπίες, εγγυήσεις για αποκατάσταση.
- Αδικαιολόγητη πληροφόρηση και διακρίσεις: Οι προσωπικές πληροφορίες που παρέχονται σε μια σφαίρα ή στο πλαίσιο (για παράδειγμα, η υγειονομική περίθαλψη) μπορεί να αλλάξουν τη σημασία τους όταν χρησιμοποιούνται σε μια άλλη σφαίρα ή στο πλαίσιο (όπως οι εμπορικές συναλλαγές) και μπορεί να οδηγήσουν σε διακρίσεις και μειονεκτήματα για το άτομο.
- Παραβίαση της ηθικής αυτονομίας: Η έλλειψη προστασίας της ιδιωτικής ζωής μπορεί να εκθέσει άτομα σε εξωτερικές δυνάμεις που επηρεάζουν τις επιλογές τους.

Οι παραπάνω λόγοι παρέχουν όλα τα καλά ηθικά αίτια για τον περιορισμό και τον περιορισμό της πρόσβασης σε προσωπικά δεδομένα και την παροχή στους πολίτες του ελέγχου των δεδομένων τους.

2.5 ΔΙΑΔΙΚΤΥΟ, ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Με την ραγδαία ανάπτυξη και την ευρεία χρήση των νέων τεχνολογιών του Διαδικτύου, η προοπτική της ιδιωτικής ζωής έχει μεταβληθεί. Ο όρος online προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων αναφέρεται στην πράξη του ατόμου επιλεκτικής αποκάλυψης (του εαυτού του), σε online περιβάλλον. Η προστασία των προσωπικών δεδομένων σε online περιβάλλον ορίζεται, συνήθως, ως η ανησυχία των χρηστών του Διαδικτύου σχετικά με (1) τον έλεγχό τους για τη συλλογή των πληροφοριών κατά τη διάρκεια της διαδικτυακής δραστηριότητας, και (2) τον έλεγχο της χρήσης των πληροφοριών που συλλέχθηκαν. Κατά συνέπεια, το ηλεκτρονικό απόρρητο καλύπτει τις ανησυχίες των χρηστών σχετικά με: (α) τον τύπο και την ποιότητα των πληροφοριών που μια συγκεκριμένη ιστοσελίδα θα εισπράξει γι'αυτούς, (β) πόσο έλεγχο έχουν οι χρήστες των συλλεγόμενων πληροφοριών και (γ) την ευαισθητοποίηση των χρηστών των πρακτικών προστασίας της ιδιωτικής ζωής. Αυτή η διαδικασία ελέγχου της ιδιωτικής ζωής επηρεάζεται από πολλούς παράγοντες (MekovecandVrek, 2011).

Οι Sheehan και Hoy (2000) ήταν μεταξύ των πρώτων που ερεύνησαν τις ανησυχίες χρηστών του διαδικτύου για την προστασία της ιδιωτικής ζωής. Οι συγγραφείς προσδιόρισαν τρεις παράγοντες που επηρεάζουν τους χρήστες:

1. τον έλεγχο για τη συλλογή πληροφοριών και τη χρήση των πληροφοριών,
2. τη βραχυπρόθεσμη συναλλαγή, η οποία αναφέρεται σε θέματα συναλλαγματικών συναλλαγών, που αφορούν την ανησυχία, σχετικά, με το είδος των πληροφοριών που ανταλλάσσονται για ένα συγκεκριμένο όφελος, και
3. την εγκαθίδρυση σχέσης που ασχολείται με θέματα σχετικά με την ύπαρξη των σχέσεων μεταξύ ενός πελάτη και ενός δικτυακού τόπου.

Οι online δραστηριότητες των χρηστών του Διαδικτύου περιλαμβάνουν διάφορους τύπους δραστηριοτήτων, π.χ. επικοινωνιακή, εμπορικές και πληροφοριακές online δραστηριότητες. Κατά συνέπεια, η απόφαση σχετικά με την προσωπική δημοσιοποίηση πληροφοριών στις online συναλλαγές επηρεάζεται από πολλούς

παράγοντες, π.χ. την αντίληψη της προστασίας της ιδιωτικής ζωής, τις πιθανές ζημίες, τις σωματικές ανάγκες ή τα αντιληπτά πλεονεκτήματα σε ένα συγκεκριμένο είδος της online συναλλαγής (MekovecandVrek, 2011).

Μια σωστή κατανόηση όλων αυτών των ανησυχιών της ιδιωτικής ζωής, είναι ζωτικής σημασίας για τη σωστή χρήση του διαδικτύου από όλους. Επιπλέον, ο εντοπισμός και η συστηματοποίηση των παραγόντων που επηρεάζουν τις ανησυχίες για την προστασία της ιδιωτικής ζωής των χρηστών του διαδικτύου, επιτρέπει την λεπτομερή ανάλυση της αλληλεξάρτησης τους. Με βάση τα αποτελέσματα των αναλύσεων αυτών, οι εταιρείες που προσφέρουν υπηρεσίες ή προϊόντα στο διαδίκτυο, μπορούν να βελτιώσουν ή να τροποποιήσουν τις προσφορές τους. Τέλος, δημόσιοι και ιδιωτικοί φορείς που χαράσσουν πολιτική μπορούν να κατανοήσουν σημαντικούς παράγοντες που διαμορφώνουν την συμπεριφορά του online καταναλωτή (MekovecandVrek, 2011).

Επιπλέον, σύμφωνα με την Bandyopadhyay (2012) δύο σημαντικοί παράγοντες που έχουν εντοπιστεί στη βιβλιογραφία ως κύρια επιρροή για την προστασία της ιδιωτικότητας σε online συνδέσεις, είναι: (1) ο ευάλωτος χαρακτήρας των καταναλωτών, με την μη εξουσιοδοτημένη συλλογή και κατάχρηση των προσωπικών πληροφοριών και (2) η ικανότητα των καταναλωτών να ελέγχουν τον τρόπο με τον οποίο οι προσωπικές πληροφορίες συλλέγονται και χρησιμοποιούνται. Οι χρήστες περιγράφονται ως ευάλωτοι μπροστά στον αντιληπτό δυνητικό κίνδυνο αποκάλυψης προσωπικών πληροφοριών τους. Η αποκάλυψη των προσωπικών πληροφοριών θα μπορούσε να προκληθεί από πολλούς παράγοντες, όπως η τυχαία αποκάλυψη, η μη εξουσιοδοτημένη πρόσβαση, η εισβολή σε δίκτυα, κ.λπ.. Οι πιθανές αρνητικές συνέπειες για τους χρήστες περιλαμβάνουν κλοπή ταυτότητας (Saunders και Zucker, 1999), ανεπιθύμητα προφίλ τους (Budnitz, 1998), και στοχευμένα ανεπιθύμητα διαφημιστικά μηνύματα στο διαδίκτυο (δηλαδή «spam» στα e- mails). Αυτοί οι παράγοντες συμβάλλουν στο να αισθάνονται οι χρήστες όλο και πιο ευάλωτοι μπροστά στον κίνδυνο της κατάχρησης των προσωπικών τους δεδομένων (Bandyopadhyay, 2012).

Η ικανότητα ελέγχου είναι ο βαθμός στον οποίο οι χρήστες πιστεύουν ότι μπορούν να αποτρέψουν τις προσωπικές πληροφορίες από την κοινοποίηση τους στο διαδίκτυο. Οι χρήστες τείνουν να πιστεύουν ότι η δημοσιοποίηση πληροφοριών είναι λιγότερο επεμβατική για την προστασία της ιδιωτικής ζωής τους, και λιγότερο πιθανό να οδηγήσει σε αρνητικές συνέπειες, όταν μπορούν να ελέγχουν πότε και πώς οι πληροφορίες αυτές κοινοποιούνται και πως αυτές μπορούν να χρησιμοποιηθούν στο μέλλον. Ως εκ τούτου, οι ανησυχίες για την προστασία της ιδιωτικής ζωής των χρηστών είναι πιθανόν να μειωθούν, όταν οι χρήστες θα είναι ικανοί να ελέγχουν τη συλλογή πληροφοριών και τη διάδοση τους (Bandyopadhyay, 2012).

Υπάρχει τέλος, μια πιθανή σχέση μεταξύ της αντιληπτής ικανότητας να ελέγχουν οι χρήστες τη συλλογή προσωπικών πληροφοριών και τη χρήση τους και τις αντιληπτής ευπάθειας που οδηγεί σε κατάχρηση πληροφοριών. Αν οι χρήστες νιώθουν ότι μπορούν πραγματικά να ελέγχουν τον τρόπο που συλλέγονται και χρησιμοποιούνται οι ιδιωτικές πληροφορίες από ιστοσελίδες, θα αισθάνονται λιγότερο ευάλωτοι στις ενδεχόμενες αρνητικές εκβάσεις των πληροφοριών αυτών και στην πιθανή κατάχρηση τους (Bandyopadhyay, 2012).

2.6 ΚΟΙΝΩΝΙΚΑ ΔΙΚΤΥΑ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Οι κοινωνικοί χρήστες του δικτύου μπορούν να μοιράζονται τις διαφορετικές πτυχές των προσωπικών πληροφοριών με τους άλλους. Ωστόσο, αυτές οι λεπτομέρειες μπορεί να χρησιμοποιηθούν καταχρηστικά από τους φίλους. Οι GrossandAcquisti (2005) σε μια μελέτη, αναφορικά με τις ανησυχίες της ιδιωτικής ζωής των χρηστών του Facebook, διαπίστωσαν ότι το 91% των χρηστών αποστέλλουν φωτογραφίες τους, το 88% δημοσιοποιούντην ημερομηνία γέννησής τους, το 40 % δείχνουν τον αριθμό του τηλεφώνου τους και τέλος, το 51% γράφουν τη διεύθυνσή τους.

Η ανταλλαγή πληροφοριών προσωπικού χαρακτήρα μπορεί να οδηγήσει σε κακή χρήση των δεδομένων, είτε εκ προθέσεως είτε όχι. Για παράδειγμα, σε μερικούς ανθρώπους που μοιράζονται στοιχεία όπως τα παραπάνω, μπορούν οι hackers να κάνουν κατάχρηση

αυτών των λεπτομερειών για να εκβιάσουν τους χρήστες (Rosenblum 2007).

Σε μια μελέτη από τους Williamsetal. (2009) διαπιστώθηκε ότι οι ηλικιωμένοι χρήστες είναι πιο προσεκτικοί, σχετικά με την απόσπαση πληροφοριών, που αφορούν προσωπικά στοιχεία, όπως η ημερομηνία γέννησης, λίστα φίλων και πληροφορίες για το σχολείο από τους νεότερους χρήστες. Ομοίως, οι Zukowski και Brown (2007) διαπίστωσαν ότι οι παλαιότεροι χρήστες του Διαδικτύου ανησυχούν περισσότερο για το απόρρητο των προσωπικών πληροφοριών από τους νεότερους χρήστες. Μερικοί από τους νεότερους χρήστες δημοσιεύουν τις δικές τους πληροφορίες, χωρίς τη γνώση των κινδύνων που μπορεί να προκύψουν από την κακή χρήση των δεδομένων αυτών. Το ηλεκτρονικό περιβάλλον μπορεί να αποβεί επικίνδυνο για τους χρήστες, ανεξάρτητα από την ηλικία, εξαιτίας της πιθανής διαρροής προσωπικών στοιχείων πληροφοριών.

Ο George (2006) ανέφερε την περίπτωση στις ΗΠΑ, όπου αθλητές κολεγίου, των οποίων εικόνες αναρτήθηκαν στο διαδίκτυο, αποτέλεσαν αντικείμενο κατάχρησης από μια ιστοσελίδα, η οποία δημοσιεύει ιστορίες για σκάνδαλα στον τομέα του αθλητισμού.

Δεδομένου ότι οι χρήστες του Διαδικτύου αντιπροσωπεύουν μια σειρά διαφορετικών πολιτισμών και ηλικιών, οι επιλογές απορρήτου θα πρέπει να είναι σαφείς, απλές και εύκολες στη χρήση. Οι χρήστες πρέπει να έχουν τη δυνατότητα να ελέγχουν τις επιλογές της ιδιωτικής τους ζωής, ανά πάσα στιγμή. Αυτές οι επιλογές ιδιωτικότητας επιτρέπουν στους χρήστες να αποδεχθούν ή να απορρίψουν τη διάδοση των πληροφοριών αυτών σε άλλους (Aldhafferiet.al., 2013).

2.6.1 Κίνδυνοι κοινωνικών δικτύων

Σύμφωνα με τα παραπάνω διαπιστώνεται ότι υπάρχουν αρκετοί κίνδυνοι που περιβάλλουν την απόσπαση προσωπικών στοιχείων και πληροφοριών σχετικά με τα κοινωνικά δίκτυα. Οι απειλές αυτές μπορούν να προκληθούν από hackers ή spammers που λαμβάνουν προσωπικές πληροφορίες και στοιχεία των χρηστών.

Η κλοπή ταυτότητας είναι ένα από τους μεγαλύτερους κινδύνους που αντιμετωπίζουν οι χρήστες (Williamsetal. 2009). Η πρόσβαση σε ευαίσθητες πληροφορίες μπορεί επίσης να οδηγήσει σε κινδύνους τρομοκρατικών ενεργειών, χρηματοοικονομικούς κίνδυνους, και κινδύνους που αφορούν σωματικό η σεξουαλικό εκφοβισμό (Gharibi&Shaabi 2012).

Η δεύτερη παραβίαση της ιδιωτικής ζωής μπορεί να προκληθεί από τους φίλους του χρήστη, ο οποίος μπορεί να μοιραστεί προσωπικές πληροφορίες και στοιχεία του χρήστη με τους άλλους. Φίλοι που έχουν πρόσβαση στα προσωπικά στοιχεία του χρήστη, μπορούν να αντιγράψουν και να δημοσιεύσουν τις πληροφορίες αυτές.

Τέλος, η τρίτη παράβαση οφείλεται σε spammers. Όταν οι spammers δουν λίστα των φίλων του χρήστη, μπορούν να δουν τις προσωπικές πληροφορίες άλλων χρηστών, στέλνοντάς τους ένα αίτημα για νέο φίλο, κάνοντας πλαστοπροσωπία έναν από τους φίλους του / της, χρησιμοποιώντας το όνομα του φίλου ή εικόνα (Aldhafferiet.al., 2013).

Με τα κοινωνικά δίκτυα να συνεχίζουν να προσθέτουν εκατομμύρια χρήστες στη βάση τους, οι spammers εκμεταλλεύονται τη δημοτικότητα αυτών των δικτύων για να σχεδιάσουν νέες τεχνικές ανεπιθύμητης αλληλογραφίας εβδομάδα με την εβδομάδα. Δεδομένου ότι σχεδόν όλες αυτές οι υπηρεσίες επιτρέπουν στους χρήστες να στέλνουν μηνύματα μεταξύ τους δωρεάν, παρέχουν ένα εύκολο σημείο εισόδου για τους αποστολείς ανεπιθύμητων μηνυμάτων (Wüest, 2010).

Τρία από τα πιο δημοφιλή χαρακτηριστικά του Facebook, είναι, η δυνατότητα ο χρήστης να προσθέτει φίλους, να ενημερώνει την κατάστασή του και να εκτελεί

διαφορές εφαρμογές όπως παιχνίδια και κουίζ. Ένας «φίλος» του χρήστη είναι οποιοδήποτε άτομο στο δίκτυο του Facebook, στον οποίο επιτρέπετε να βλέπει διάφορα επίπεδα προσωπικών πληροφοριών, όπως εργασία, ημερομηνία γέννησης, φωτογραφίες, συμμετοχή σε ομάδες, σχόλια και τη λίστα των υπολοίπων Φίλων. Αυτό σημαίνει ότι άτομα που δεν γνωρίζονται καθόλου μεταξύ τους, μπορούν να δουν πληροφορίες και δεδομένα άλλων ατόμων (Dinerman, 2011).

ΚΕΦΑΛΑΙΟ 3
Η ΕΥΡΩΠΑΪΚΗ ΚΑΙ Η ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

3.1 ΕΙΣΑΓΩΓΗ

Στη σημερινή εποχή, η ανταλλαγή πληροφοριών σε παγκόσμιο επίπεδο είναι πλέον μια εύκολη και γρήγορη διαδικασία. Η παραπάνω απότομη και γρήγορη αύξηση της ροής των εξελίξεων σε όλη την υφήλιο αποτελεί μεγάλο ζήτημα, σχετικά με το δικαίωμα του ανθρώπου στη μεταχείριση των προσωπικών του στοιχείων με αξιοπιστία. Θέματα που αφορούν την προάσπιση της ιδιωτικότητας, σε συνδυασμό με την εξάπλωση του διαδικτύου σε παγκόσμια κλίμακα, προβληματίζουν τους ανθρώπους συνεχώς, σε περιπτώσεις που προβαίνουν σε διαδικτυακές αγορές, πραγματοποιούν συναλλαγές με δημόσιες υπηρεσίες, κάνουν ταξίδια ή απλά «σερφάρουν» στο διαδίκτυο. Έτσι, η προάσπιση των προσωπικών στοιχείων αποτελεί καίριο ζήτημα, που κατοχυρώνεται με νόμους στην Ευρωπαϊκή Ένωση, αλλά και στην Ελλάδα (EuropeanCommission, 2011).

Εν συνεχεία, καταγράφονται με χρονολογική σειρά οι νόμοι, που σχετίζονται με τα προσωπικά στοιχεία.

3.2 ΝΟΜΟΘΕΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

3.2.1 Ευρωπαϊκή νομοθεσία

Σύμφωνα με την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου και το άρθρο 8 παρ. 1 του 1950, η προάσπιση της προσωπικών δεδομένων γίνεται αποδεκτή ως δικαίωμα. Συγκεκριμένα επισημαίνεται: *Κάθε άτομο έχει το δικαίωμα να απολαμβάνει*

σεβασμού στην προσωπική και οικογενειακή του ζωή, τοσπίτι του, αλλά και την αλληλογραφία του (Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου).

Ακολούθως, το Συμβούλιο της Ευρώπης το 1981, με τη Σύμβαση 108 σχετικά με τη προάσπιση των δικαιωμάτων των ατόμων λόγω της αυτόματης επεξεργασίας των προσωπικών στοιχείων, δημιουργεί την πρώτη δεσμευτική ενέργεια, που κατοχυρώνεται νομικά και έχει ισχύ σε παγκόσμιο επίπεδο και που εισήχθη στον τομέα της προάσπισης της ιδιωτικότητας. Βασικός στόχος της πράξης αυτής είναι να προστατεύει το σεβασμό των δικαιωμάτων και των βασικών ελευθεριών των ανθρώπων, και κυρίως του δικαιώματος τους στην ιδιωτικότητα, απέναντι στην αυτόματη διαμόρφωση και τροποποίηση των στοιχείων που αφορούν την ιδιωτική ζωή (Milt, 2018). Πιο ειδικά επισημαίνει: Τα στοιχεία που αφορούν την προσωπική ζωή φανερώνουν τις φυλετικές καταβολές, τις πολιτικές ιδεολογίες και τις θρησκευτικές πεποιθήσεις. *Τέτοια είναι και οι πληροφορίες για την ιδιωτική ζωή, την υγεία ή την σεξουαλική ζωή, οι οποίες σε περίπτωση που το εσωτερικό δίκαιο δεν περιλαμβάνει τις απαραίτητες εγγυήσεις, δεν μπορούν να υποστούν αυτοματοποιημένη επεξεργασία. Η παραπάνω απόφαση έχει ισχύ για δεδομένα που αφορούν τα προσωπικά στοιχεία και έχουν σχέση με ποινικές καταδίκες* (Λιμνιώτης, 2013).

Η Σύμβαση 108 του Συμβουλίου της Ευρώπης, αποτελεί καθοριστικό παράγοντα για 43 χώρες στην Ευρώπη, αλλά και το μοναδικό δεσμευτικό έγγραφο σε νομικό επίπεδο, που έχει τη δυνατότητα να εφαρμοστεί σε όλο τον κόσμο. Κάθε χώρα που εφαρμόζει την απαραίτητη νομοθεσία και αποσκοπεί στην προάσπιση των προσωπικών πληροφοριών είναι δυνατό να αποτελέσει συμβαλλόμενο μέρος της παραπάνω σύμβασης(EuropeanCommission, 2011).

Στη σύμβαση διακρίνονται κάποιες απαραίτητες αρχές, οι οποίες γίνονται αποδεκτές από το σύνολο των κρατών, αλλά και πρότυπα, τα οποία είναι δεσμευτικά υπό το πρίσμα των νομικού πλαισίου. Τα τεχνολογικά ουδέτερα τμήματα του νόμου προφυλάσσουν τον άνθρωπο από έλλειψη σεβασμού στην προσωπική του ζωή, προερχόμενη είτε από δημόσιους είτε από ιδιωτικούς παράγοντες. Η σύμβαση διαθέτει νομική προστασία για τηνμεταφορά προσωπικών στοιχείων ανάμεσα σε κράτη που έχουν δεχθεί την εγκυρότητα της, αλλά και μια πλατφόρμα που προβλέπει

τη πολυδιάστατη και επί ίσοις όροις σύμπραξη ανάμεσα στις χώρες που είναι μέρος της (EuropeanCommission, 2011).

Το 1995 η Ευρωπαϊκή Ένωση ανακοίνωσε απόφαση που είχε ως σκοπό την προάσπιση των βασικών δικαιωμάτων και ελευθεριών του ατόμου και κυρίως του δικαιώματος στην προάσπιση των προσωπικών στοιχείων, αλλά και της απερίσπαστης κυκλοφορίας των προσωπικών δεδομένων[4]. Την παραπάνω απόφαση για την προάσπιση της ιδιωτικότητας ακολούθησαν και άλλες νομοθετικές αρχές. Μία από αυτές είναι η απόφαση για την προάσπιση των ιδιωτικών δεδομένων στις ηλεκτρονικές επικοινωνίες (EuropeanCommission, 2011).

Πιο ειδικά, ο Οδηγός 95/46, προβλέπει ότι η επεξεργασία προσωπικών πληροφοριών είναι σύμφωνη με το νόμο σε περίπτωση που:

α) το άτομο, το οποίο αφορούν τα στοιχεία έχει δώσει την απόλυτη συναίνεση του ή
β) είναι αναγκαία για την εφαρμογή της σύμβασης κατά την οποία το άτομο το οποίο αφορά είναι συμβαλλόμενο μέρος ή πρόκειται για την λήψη προσυμβατικών μέτρων που έχουν εφαρμοστεί κατόπιν αιτήσεως του ή
γ) είναι σημαντική για την εφαρμογή, σε περίπτωση που ο νόμος το υπαγορεύει από τον αρμόδιο της επεξεργασίας
δ) είναι θεμιτή για τη προστασία σημαντικού συμφέροντος του ατόμου στο οποίο ανήκουν οι πληροφορίες ή
ε) είναι αναγκαία για την εκτέλεση έργου δημοσίου συμφέροντος ή έργου που περιλαμβάνεται στην άσκηση δημοσίας εξουσίας, την οποία ασκεί ο αρμόδιος της επεξεργασίας ή ένας τρίτος, ο οποίος αποτελεί το άτομο στο οποίο γίνεται η ανακοίνωση των στοιχείων ή
στ) είναι θεμιτή για την επικράτηση του εννόμου συμφέροντος στο οποίο αποβλέπει ο αρμόδιος της επεξεργασίας ή οι άλλοι αρμόδιοι στους οποίους γνωστοποιούνται τα στοιχεία, με την προϋπόθεση ότι δεν έχει προτεραιότητα το συμφέρον ή τα ανθρώπινα δικαιώματα και οι ελευθερίες του άτομου στο οποίο ανήκουν τα στοιχεία

[4]Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αναγνωρίζεται ρητά από το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ καθώς και από τη συνθήκη της Λισαβόνας. Η συνθήκη, στο άρθρο 16, παρέχει τη νομική βάση για θέσπιση κανόνων σχετικά με την προστασία των δεδομένων για όλες τις δραστηριότητες που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της ΕΕ (EuropeanCommission, 2011).

που είναι απαραίτητο να προστατευτούν με βάση το άρθρο 1 παράγραφο 1 της συγκεκριμένης οδηγίας.

3.2.2 Ελληνική νομοθεσία, Νόμος 2472/1997

Όλες οι χώρες πορεύονται σύμφωνα με την προηγούμενη οδηγία. Η Ελλάδα θεσμοθετεί το Νόμο 2472/1997 «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Το περιεχόμενο του παραπάνω νόμου αφορά την καθιέρωση των όρων για την επεξεργασία πληροφοριών που σχετίζονται με προσωπικά δεδομένα για την προάσπιση των δικαιωμάτων και των θεμελιωδών ελευθεριών των ανθρώπων και πρωτίστως της ιδιωτικής ζωής (Νόμος 2472/1997).

Σύμφωνα με το νόμο τα προσωπικά στοιχεία αφορούν το σύνολο των πληροφοριών *κάθε, δηλαδή, στοιχείο(άμεσο ή έμμεσο) που αφορά φυσικό πρόσωπο και προσδιορίζει το άτομο από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη*. Συγκεκριμένα, ως προσωπικά στοιχεία νοούνται το όνομα, η ταχυδρομική και ηλεκτρονική διεύθυνση, το τηλέφωνο, οι ενασχολήσεις, η κοσμοθεωρία του κάθε ατόμου κ.α. (Νόμος 2472/1997).

Κατά το Άρθρο 5 του Νόμου, η διαδικασία διαμόρφωσης προσωπικών δεδομένων ενός ατόμου είναι εφικτή μόνο σε περίπτωση που ο ίδιος(υποκείμενο των δεδομένων) έχει συναινέσει (κατηγορηματικά, με σαφήνεια). Διαφοροποιήσεις από τον αρχικό κανόνα παρατηρούνται όταν:

- η επεξεργασία κρίνεται απαραίτητη για την εφαρμογή σύμβασης,
- την επεξεργασία υποχρεώνει ο νόμος(ο αρμόδιος επεξεργασίας υποχρεούται για αυτή σύμφωνα με το νόμο),
- η επεξεργασία είναι απαραίτητη για τη προστασία κρίσιμων συμφερόντων του ατόμου
- η επεξεργασία κρίνεται απαραίτητη για την υλοποίηση έργου δημοσίου συμφέροντος,

- η επεξεργασία είναι σε κάθε περίπτωση απαραίτητη για την εξυπηρέτηση του έννομου συμφέροντος του αρμόδιου της επεξεργασίας ή άλλου προσώπου, στον οποίο γνωστοποιούνται τα στοιχεία(Νόμος 2472/1997).

Ο νόμος προβλέπει, επίσης, την ύπαρξη μιας ακόμη ομάδας προσωπικών στοιχείων, που περιλαμβάνει σημαντικές προσωπικές πληροφορίες, αλλά και στοιχεία που έχουν μεγάλη ανάγκη να προστατευτούν. Στα παραπάνω στοιχεία περιλαμβάνονται: οι φυλετικές ή εθνικές καταβολές, οι πολιτικές πεποιθήσεις, τα θρησκευτικά πιστεύω ή φιλοσοφικές καταβολές, η ανάμειξη σε συνδικαλιστική οργάνωση, η υγεία, η κοινωνική φροντίδα, οι ποινικές διώξεις ή καταδίκες (Νόμος 2472/1997).

Το άρθρο 7 του Νόμου συνάδει με την Ευρωπαϊκή Οδηγία 95/46, η οποία προβλέπει ότι δεν επιτρέπεται η συγκέντρωση και επεξεργασία προσωπικών δεδομένων. Μοναδική εξαίρεση αποτελεί η περίπτωση που παρέχεται η συναίνεση της Αρχής Προστασίας Προσωπικών Δεδομένων[5], αν πληρείται μία από το σύνολο των προϋποθέσεων:

α) Το άτομο παραχώρησε εγγράφως τη συναίνεση του, με εξαίρεση την περίπτωση που η συναίνεση του έχει πραγματοποιηθεί με τρόπο που έρχεται σε αντίθεση με το νόμο ή την κρατούσα ηθική αντίληψη ή νόμος προβλέπει ότι η συναίνεση δεν ακυρώνει την απαγόρευση.
β) Η επεξεργασία είναι απαραίτητη για τη προάσπιση κρίσιμου συμφέροντος για το άτομο ή συμφέροντος που κατοχυρώνεται από το νόμο κάποιου άλλου προσώπου, σε περίπτωση που το άτομο αδυνατεί λόγω φυσικών ή νομικών παραγόντων να δώσει την έγκριση του.
γ) Η επεξεργασία περιλαμβάνει πληροφορίες που το ίδιο το άτομο φέρει στην δημοσιότητα ή κρίνονται απαραίτητες για την αναγνώριση, εκτέλεση ή υπεράσπιση δικαιώματος μπροστά στο δικαστήριο ή πειθαρχικό όργανο.
δ) Η επεξεργασία σχετίζεται με ζητήματα υγείας και εφαρμόζεται από άτομο που το επάγγελμα του αφορά την παροχή υπηρεσιών υγείας και είναι υποχρεωμένο να είναι

[5]Στο άρθρο 15 (Κεφάλαιο Δ), ο νομός ορίζει ότι συνιστάται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Αρχή), με αποστολή την εποπτεία της εφαρμογής του παρόντος νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά (Νόμος 2472/1997).

αξιόπιστο ή να τηρεί παρόμοιους κώδικες δεοντολογίας, με την προϋπόθεση ότι η επεξεργασία κρίνεται αναγκαία για την ιατρική πρόληψη, διάγνωση, φροντίδα ή τη διαχείριση υπηρεσιών υγείας.

ε) Η επεξεργασία εφαρμόζεται από Δημόσια Αρχή και είναι υποχρεωτική είτε αα) για τη διασφάλιση της ασφάλειας των πολιτών μιας χώρας είτε ββ) για την διευκόλυνση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και σχετίζεται με τη διαλεύκανση εγκλημάτων, ποινικές καταδίκες ή ενέργειες ασφαλείας είτε γγ) για την διασφάλιση της δημόσιας υγείας είτε δδ) για την εφαρμογή δημόσιου ελέγχου για θέματα φορολογικού περιεχομένου ή κοινωνικών παροχών .

στ) Η επεξεργασία γίνεται για την επίτευξη ερευνητικών ή επιστημονικών στόχων και με την προϋπόθεση ότι υπάρχει απόκρυψη ονόματος και εφαρμόζονται όλες οι κατάλληλες ενέργειες για την προάσπιση των δικαιωμάτων των ατόμων στα οποία αναφέρονται.

ζ) Η επεξεργασία περιλαμβάνει πληροφορίες για δημόσια πρόσωπα, αν αυτά είναι φορείς δημοσίου λειτουργήματος ή τη ρύθμιση συμφερόντων άλλων ατόμων, και συμβαίνει μόνο σε περίπτωση άσκησης του δημοσιογραφικού επαγγέλματος. Η συγκεκριμένη άδεια δίνεται μόνο αν η επεξεργασία κρίνεται τελείως απαραίτητη για να έχει κανείς τη δυνατότητα να πληροφορείται σε θέματα που αφορούν το δημόσιο τομέα, αλλά και για να είναι δυνατή η καλλιτεχνική δημιουργία, αν δεν καταπατάται με κάποιον τρόπο το δικαίωμα προάσπισης της ιδιωτικής και οικογενειακής ζωής (Νόμος 2472/1997).

Με βάση τη Συνταγματική αναθεώρηση του 2001, προβλέπεται η θέσπιση ενός καινούργιου άρθρου(9^{A}) στο Σύνταγμα, το οποίο προσβλέπει στην προάσπιση των προσωπικών στοιχείων. Με το παραπάνω άρθρο καλύπτεται η ανάγκη προφύλαξης από το σχηματισμό προσωπικών στοιχείων και συλλήβδην από τους κινδύνους που ελλοχεύει η περιήγηση στο διαδίκτυο σχετικά με το απόρρητο προσωπικών δεδομένων. Η παραπάνω προσπάθεια αποτελεί τη συνταγματική επικύρωση και ολοκλήρωση των ενεργειών, τις οποίες είχε πραγματοποιήσει η έννομη τάξη της χώρας, αφού υπέγραψε τη σχετική σύμβαση του Συμβουλίου της Ευρώπης το 1981, με την προσαρμογή της προς τη σχετική Κοινοτική Οδηγία 95/46 ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και κυρίως με την θέσπιση του νόμου 2472/1997, με τον οποίο συγκροτήθηκε η ανεξάρτητη διοικητική αρχή για την προάσπιση από την διαδικασία διαμόρφωσης των προσωπικών στοιχείων. Στα

παραπάνω προστίθεται ο ρυθμιστικός χαρακτήρας του άρθρου 9 παρ. 1 εδαφ. β' Σ, αλλά και του άρθρου 5 παρ.1 Σ. Τα θεμελιώδη δικαιώματα της ενημέρωσης και της πρόσβασης σε δεδομένα που μεταφέρονται ηλεκτρονικά είναι απαραίτητο να συμβαδίζουν με το δικαίωμα της προάσπισης των προσωπικών στοιχείων όλων των ανθρώπων, αλλά και με την βεβαίωση της αρμόδιας ανεξάρτητης αρχής (Κούης, 2008).

3.3 ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ

3.3.1 Ευρωπαϊκή νομοθεσία

Το Ευρωπαϊκό Κοινοβούλιο ανακοίνωσε στις 15 Δεκεμβρίου του 1997 την Οδηγία 97/66/ΕΚ, σχετικά με την επεξεργασία των προσωπικών δεδομένων και τη προάσπιση της ιδιωτικότητας στον τηλεπικοινωνιακό χώρο. Η παραπάνω οδηγία απέβλεπε στο συγχρονισμό των κανονισμών των χωρώνμελών, που κρίνονται απαραίτητες για την κατοχύρωση της προάσπισης των ανθρωπίνων δικαιωμάτων και ελευθεριών στον ίδιο βαθμό, κυρίως το δικαίωμα στην ιδιωτικότητα, σε σχέση με την καταγραφή προσωπικών στοιχείων στον τηλεπικοινωνιακό τομέα, αλλά και στην μεταφορά των στοιχείων αυτών και των τηλεπικοινωνιακών εξοπλισμών και υπηρεσιών στην Κοινότητα χωρίς περιορισμούς. Οι κανονισμοί αυτής της οδηγίας λειτούργησαν συμπληρωματικά και κατέστησαν πιο εξειδικευμένους τους κανονισμούς της οδηγίας 95/46/ΕΚ για τις επιδιώξεις που καταγράφονται στην παράγραφο. Επιπροσθέτως, εξασφαλίζουν τη διαφύλαξη των εννόμων συμφερόντων των μελών, τα οποία είναι νομικά πρόσωπα (Οδηγία 97/66/ΕΚ).

Με βάση την Οδηγία στο άρθρο 2 ορίζονται οι παρακάτω έννοιες:

α) Ως Συνδρομητής ορίζεται κάθε φυσικό ή νομικό πρόσωπο, το οποίο έχει κάνει γραπτή συμφωνία με οργανισμό που έχει διαθέσιμους στην αγορά τηλεπικοινωνιακούς οργανισμούς, οι οποίοι εξασφαλίζουν τις υπηρεσίες αυτές,

β) Ως Χρήστης ορίζεται κάθε φυσικό πρόσωπο που κάνει χρήση της διαθέσιμης στην αγορά τηλεπικοινωνιακής υπηρεσίας για προσωπικούς ή επαγγελματικούς λόγους, ο οποίος βέβαια δεν είναι αναγκαστικά μέλος του συγκεκριμένου οργανισμού.
γ) Ως Δημόσιο τηλεπικοινωνιακό δίκτυο ορίζονται τα μέσα μετάδοσης και, όπου είναι απαραίτητο, ο εξοπλισμός μεταφοράς και τα άλλα μέσα που καθιστούν εφικτή την μεταβίβαση σημάτων ανάμεσα σε συγκεκριμένα τερματικά σημεία χρησιμοποιώντας καλώδιο, ραδιοκύματα, οπτικά ή άλλα ηλεκτρομαγνητικά μέσα, των οποίων η χρήση γίνεται, συνολικά ή μερικώς, για να δίνονται στην αγορά τηλεπικοινωνιακές υπηρεσίες.
δ) Ως τηλεπικοινωνιακές υπηρεσίες ορίζονται οι οργανισμοί, οι οποίοι παρέχονται συνολικά ή μερικά με τη μεταφορά και επιπλέον μετάβαση σημάτων σε τηλεπικοινωνιακά δίκτυα, με εξαίρεση τις ραδιοφωνικές και τηλεοπτικές εκπομπές (Οδηγία 97/66/ΕΚ).

Επιπλέον, το άρθρο 5, διατυπώνει το Απόρρητο των επικοινωνιών. Λαμβάνοντας υπόψη το άρθρο, οι χώρες μέλη εξασφαλίζουν, με νομοθεσία σε εθνικό επίπεδο, το απόρρητο των επικοινωνιών που πραγματοποιούνται με τη χρήση του δημόσιου τηλεπικοινωνιακού δικτύου και των διαθέσιμων στην αγορά τηλεπικοινωνιακών οργανισμών. Συγκεκριμένα, δεν επιτρέπουν την παρακολούθηση, ή παράνομη ηχογράφηση, αποθήκευση ή κάποια άλλη παρακολούθηση των επικοινωνιών από άτομα εκτός των χρηστών χωρίς τη σύμφωνη γνώμη των ατόμων με τα οποία σχετίζονται, με εξαίρεση την ύπαρξη της απαραίτητης νόμιμης άδειας, κατά το άρθρο 14 παράγραφος 1 (Οδηγία 97/66/ΕΚ).

Ακολούθως, το Ευρωπαϊκό Κοινοβούλιο δημοσίευσε στις 12 Ιουλίου του 2002 την Οδηγία 2002/58/ΕΚ, η οποία αφορά την επεξεργασία των προσωπικών στοιχείων και την προάσπιση της ιδιωτικότητας αναφορικά με τις ηλεκτρονικές επικοινωνίες (πληροφορίες για την προάσπιση της ιδιωτικότητας στις ηλεκτρονικές επικοινωνίες), με σκοπό η οδηγία 97/66/ΕΚ να εναρμονιστεί στις συνθήκες που επικρατούν στις αγορές και στις τεχνολογίες των υπηρεσιών ηλεκτρονικών επικοινωνιών, να προσφέρει στο ίδιο βαθμό τη προάσπιση των προσωπικών στοιχείων και της ιδιωτικότητας σε κάθε άτομο που κάνει χρήση των υπηρεσιών επικοινωνιών που απευθύνονται στο κοινό, χωρίς να σχετίζεται με τις τεχνολογίες που εφαρμόζονται (Οδηγία 2002/58/ΕΚ).

Με βάση, λοιπόν, τα παραπάνω η βασική λειτουργία και σκοπός της Οδηγίας 2002/58/ΕΚ, ήταν να καθορίζει την προσαρμογή των εθνικών κανονισμών που είναι απαραίτητες για να προστατεύσουν σε ίδιο βαθμό τα ανθρώπινα δικαιώματα και ελευθερίες, και κυρίως του δικαιώματος στην προστασία των προσωπικών δεδομένων και την εχεμύθεια, σε σχέση με την επεξεργασία προσωπικών στοιχείων στον χώρο των επικοινωνιών μέσω διαδικτύου. Επίσης, σκοπός της οδηγίας είναι η παροχή ασφάλειας στημεταφορά των προσωπικών πληροφοριών και των εξοπλισμών, χωρίς περιορισμούς, αλλά και υπηρεσιών διαδικτυακών επικοινωνιών στην Κοινότητα (Οδηγία 2002/58/ΕΚ).

Η οδηγία, στο άρθρο 2, συμπληρώνει με τους παρακάτω ορισμούς τους ήδη υπάρχοντες ορισμούς του ίδιου άρθρου στην Οδηγία 97/66/ΕΚ:
α) Ως δεδομένα θέσης ορίζονται τα στοιχεία που τίθενται σε επεξεργασία σε διαδικτυακή επικοινωνία ή από υπηρεσία διαδικτυακών επικοινωνιών και που δείχνουν τη τοποθεσία του τερματικού εξοπλισμού σε γεωγραφικό επίπεδο του ατόμου που χρησιμοποιεί μια υπηρεσία ηλεκτρονικών επικοινωνιών που προσφέρεται στην αγορά.
β) Ως παραβίαση προσωπικών δεδομένων ορίζεται η καταστρατήγηση της ασφάλειας που επιφέρει ζημιά, είτε κατά τύχη είτε με άνομα μέσα, απώλεια, διαστρέβλωση, δημοσιοποίηση ή πρόσβαση σε προσωπικά στοιχεία που στάλθηκαν χωρίς τη συγκατάθεση του ατόμου, το οποίο αφορούν, αποθηκεύτηκαν ή έγιναν αντικείμενο επεξεργασίας, σε συγκερασμό με την προσφορά ηλεκτρονικής υπηρεσίας επικοινωνιών στην Κοινότητα, η οποία παρέχεται στην αγορά (Οδηγία 2002/58/ΕΚ).

Το άρθρο 4 έχει σχέση με την ασφάλεια της επεξεργασίας τονίζοντας ότι τα μέτρα που εφαρμόζονται:

- κατοχυρώνουν ότι τα προσωπικά στοιχεία είναι προσβάσιμα για χρήση μόνο από εξουσιοδοτημένα άτομα, σύμφωνα με τις νομοθετικές διατάξεις και κατόπιν έγκρισης από τις αρχές,

- προστατεύουν τα στοιχεία, που έχουν συλλεχθεί ή μεταφερθεί είτε κατά τύχη είτε μετά από άνομη καταστροφή ή φθορά, αλλά και από επεξεργασία, πρόσβαση ή αποθήκευση που δεν έχει λάβει έγκριση ή δεν συμβαδίζει με το νόμο και,
- κατοχυρώνουν την τήρηση πολιτικής ασφάλειας αναφορικά με την επεξεργασία προσωπικών δεδομένων (Οδηγία 2002/58/ΕΚ).

Στην παράγραφο 3 του ίδιου άρθρου αναφέρεται ότι αν σημειωθεί η καταστρατήγηση προσωπικών στοιχείων, ο ενδιαφερόμενος πάροχος διαθέσιμης στην αγορά υπηρεσίας ηλεκτρονικών επικοινωνιών κάνει αμέσως γνωστή την καταπάτηση της ιδιωτικότητας στις υπεύθυνες αρχές. Σε περίπτωση που η καταπάτηση των ανθρωπίνων δικαιωμάτων είναι πιθανό να έχει συνέπειες στα προσωπικά στοιχεία ενός χρήστη ή ενός ατόμου και στην προσωπική του ζωή, ο πάροχος κάνει γνωστή, επιπλέον, την καταπάτηση αυτή στον ενδιαφερόμενο χρήστη ή άτομο, χωρίς να αργήσει την ενημέρωση αν δεν υπάρχει σοβαρή δικαιολογία (Οδηγία 2002/58/ΕΚ).

Εν κατακλείδι, το άρθρο 5 αναφέρει ότι οι χώρες μέλη φροντίζουν ώστε να είναι εφικτή η συλλογή δεδομένων ή η δυνατότητα πρόσβασης σε ήδη καταχωρημένα στοιχεία στον τερματικό εξοπλισμό χρήστη, μόνο σε περίπτωση που ο συγκεκριμένος χρήστης έχει συναινέσει, λαμβάνοντας υπόψη συγκεκριμένες και αναλυτικές πληροφορίες σχετικά με την οδηγία 95/46/ΕΚ, προκειμένου να γίνει η επεξεργασία. Το παραπάνω δεν αποτελεί εμπόδιο για αποθήκευση ή πρόσβαση που αφορά τον τεχνικό τομέα, βασικός στόχος της οποίας έγκειται στη διεξαγωγή της μεταφοράς μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι σε μεγάλο βαθμό απαραίτητη για να έχει τη δυνατότητα ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει απαιτήσει ο χρήστης να διαθέτει αυτή την υπηρεσία (Οδηγία 2002/58/ΕΚ).

Η Οδηγία 2002/58/ΕΚ υπέστη μεταβολές με την Οδηγία 2009/136/ΕΚ. Οι αλλαγές είχαν σκοπό την προσαρμογή των νομοθετημάτων στα πρόσφατα τεχνολογικά και οικονομικά τεκταινόμενα που έλαβαν χώρα κατά τη διάρκεια των λίγων ετών που μεσολάβησαν ανάμεσα στις δύο Οδηγίες.

Μια από τις μεταβολές που συγκαταλέγονται στην διορθωτική Οδηγία 2009/136/ΕΚ, είναι η αλλαγή του άρθρου 5(3) της βασικής Οδηγίας 2002/58/ΕΚ που σχετίζεται με τα Cookies[6]. Κατά το άρθρο 5 της Οδηγίας 2009/136/ΕΚ οι ιστοσελίδες που εφαρμόζουν τα cookies είναι απαραίτητο να εξασφαλίζουν από πριν τη συναίνεση των χρηστών, εφόσον πρώτα τους πληροφορήσουν αναφορικά με το πώς θα εφαρμοστούν τα cookies (Τροποποίηση Οδηγίας 2002/58/ΕΚ-16/12/2013).

Λαμβάνοντας υπόψη την παραπάνω τροποποιητική Οδηγία, δεν είναι αναγκαία η συναίνεση για τη συλλογή δεδομένων σε τεχνικό επίπεδο ή για την πρόσβαση, απώτερος στόχος της οποίας είναι η διεξαγωγή της μεταφοράς μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή που είναι σε κάθε περίπτωση απαραίτητη για να έχει τη δυνατότητα ο πάροχος υπηρεσίας της κοινωνίας της πληροφορίας την οποία έχει απαιτήσει ο συνδρομητής ή ο χρήστης να διαθέτει αυτή την υπηρεσία (Τροποποίηση Οδηγίας 2002/58/ΕΚ-16/12/2013).

3.3.2 Ελληνική νομοθεσία

Το περιεχόμενο της Οδηγίας 97/66/ΕΚ ενσωματώθηκε στην νόμιμη τάξη της χώρας με τον Ν. 2774/99 για την προάσπιση προσωπικών στοιχείων στον χώρο των τηλεπικοινωνιακών. Οι ρυθμίσεις αυτές συμπληρώνουν και εξειδικεύουν τους κανόνες του Ν. 2472/97 για την προάσπιση του πολίτη από την επεξεργασία στοιχείων ιδιωτικής ζωής.

[6]Τα cookies είναι μικρά αρχεία κειμένου που αποθηκεύονται στους ηλεκτρονικούς υπολογιστές των χρηστών κατά τις επισκέψεις τους στις διάφορες ιστοσελίδες στο διαδίκτυο, με σκοπό να παρέχουν στην ιστοσελίδα τη δυνατότητα αναγνώρισης του χρήστη σε μεταγενέστερες επισκέψεις του στην ίδια ιστοσελίδα.
Πιο συγκεκριμένα, παρέχουν εξατομικευμένες υπηρεσίες όπως, για παράδειγμα, οι χρήστες να μπορούν να επιλέξουν τη γλώσσα με την οποία προτιμούν να εμφανίζεται μια ιστοσελίδα και η προτίμηση αυτή να αποθηκεύεται ώστε να μη χρειάζεται να επιλέξουν εκ νέου τη γλώσσα κατά την επόμενη επίσκεψη τους στην ίδια ιστοσελίδα. Επίσης, χρησιμοποιούνται στο γνωστό «shoppingcart» όπου ο χρήστης μπορεί να αποθηκεύσει διάφορα προϊόντα τα οποία σκοπεύει να αγοράσει και να επανέλθει σε μεταγενέστερο χρόνο για να τα αγοράσει.
Εκτός όμως από τις πιο πάνω χρήσεις τα cookies μπορούν να χρησιμοποιηθούν και για την παρακολούθηση των κινήσεων των χρηστών στο διαδίκτυο ώστε να διαμορφώνεται το προφίλ των προτιμήσεων τους με σκοπό να τους παρουσιάζονται διαφημίσεις που πιθανό να βρουν δελεαστικές (Τροποποίηση Οδηγίας 2002/58/ΕΚ-16/12/2013).

Η προσθήκη, βέβαια της καινούργιας Οδηγίας 2002/58/ΕΚ υποχρέωσε την ελληνική νομοθεσία να προσαρμόσει εκ νέου το αντίστοιχο νομικό πλαίσιο. Επειδή άλλαξε το σύνολο των κανονισμών του Ν. 2774/1999, ο καινούργιος Νόμος 3471/06, για να μην υπάρξει ασάφεια και αποπροσανατολισμός, παρουσιάζεται σαν καινούργιο νομοθετικό διάταγμα, και όχι ως μια αλλαγή του υπάρχοντος Ν. 2774/1999, του οποίου το περιεχόμενο ακυρώθηκε. Ο νόμος αποβλέπει στην προάσπιση της ιδιωτικότητας και των προσωπικών στοιχείων στον τομέα των ηλεκτρονικών επικοινωνιών, αλλά και του απορρήτου των επικοινωνιών (Νόμος 3471/2006).

Ακολούθως, και μετά από τη καινούργια διορθωτική οδηγία του Ευρωπαϊκού Κοινοβουλίου του 2009, ο Νόμος 3471/06 υπέστη μεταβολές με τον Ν. 4070/12 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις».

Με βάση «τα Προσωπικά στοιχεία στον χώρο των ηλεκτρονικών επικοινωνιών» ο Νόμος 3471/06 με το άρθρο 4 προβλέπει ότι:

- Κάθε εφαρμογή των ηλεκτρονικών υπηρεσιών επικοινωνιών που εξυπηρετείται με τη βοήθεια δημοσίου δικτύου επικοινωνιών, αλλά και των σχετικών δεδομένων κίνησης και θέσης[7], τίθεται υπό την προστασία του απόρρητου των επικοινωνιών. Η ακύρωση αυτού είναι δυνατή μόνο υπό τις προϋποθέσεις και ενέργειες που ορίζονται στο άρθρο 19 του Συντάγματος.
- Δεν επιτρέπεται η παρακολούθηση, υποκλοπή, αποθήκευση ή επίβλεψη των ηλεκτρονικών επικοινωνιών και των σχετικών στοιχείων κίνησης και θέσης.
- Είναι δυνατή η καταχώριση συνομιλιών και των σχετικών πληροφοριών κίνησης μόνο σε περίπτωση άσκησης έννομης επαγγελματικής πράξης.

[7] Ως δεδομένα κίνησης ορίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, η μορφοποίηση, η δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία (Νόμος 3471/2006).
Ως δεδομένα θέσης ορίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών (Νόμος 3471/2006).

- Η συλλογή δεδομένων ή η δυνατότητα πρόσβασης στον τερματικό εξοπλισμό χρήστη είναι εφικτή μόνο αν ο άμεσα ενδιαφερόμενος έχει δώσει τη συναίνεση του μετά από λεπτομερειακή και αναλυτική πληροφόρηση(όπως υπέστη μεταβολές στο Ν. 4070/2012) (παράδειγμα: cookies) (Λιμνιώτης, 2013).

Σε ότι σχετίζεται με τα «Δικαιώματα χρηστών - Μη ζητηθείσα επικοινωνία», το άρθρο 11 του νόμου προβλέπει ότι:

- Η εφαρμογή επικοινωνιών με κάθε μέσο ηλεκτρονικής επικοινωνίας, οι οποίες δεν απαιτήθηκαν, χωρίς να παρεμβαίνει ο άνθρωπος, για την επίτευξη άμεσης εμπορικής προώθησης αντικειμένων ή υπηρεσιών και με στόχο τη διαφήμιση, είναι δυνατή μόνο αν ο χρήστης δώσει τη συγκατάθεση του από πριν κατηγορηματικά.
- Απαγορεύεται να πραγματοποιούνται κλήσεις για τους παραπάνω λόγους, σε περίπτωση που ο χρήστης έχει επισημάνει προς το φορέα της διαθέσιμης στην αγορά υπηρεσίας ότι δεν θέλει να λαμβάνει τέτοιου είδους κλήσεις (όπως υπέστη μεταβολές στο Ν. 3917/2011).
- Τα δεδομένα του ηλεκτρονικού ταχυδρομείου που ελήφθησαν με νόμιμο τρόπο, προκειμένου να είναι εφικτή η πώληση αντικείμενων ή υπηρεσιών ή εκτέλεση κάποιας άλλης συναλλαγής, δύνανται να αξιοποιούνται για την άμεση προώθηση παραπλήσιων αγαθών ή υπηρεσιών του παρόχου, ακόμα και χωρίς την παραπάνω συναίνεση (opt-out), υπό τον όρο ότι καθίσταται εφικτό να εναντιώνεται εύκολα και χωρίς οικονομική επιβάρυνση, για μελλοντική χρήση.
- Απαγορεύεται από οποιανδήποτε επιχείρηση να αποστέλλει διαφημιστικό μήνυμα μέσω ηλεκτρονικού ταχυδρομείου χωρίς να έχει δώσει τη συγκατάθεση του ο άμεσα ενδιαφερόμενος. Μοναδική περίπτωση κατά την οποία δεν ισχύει ο παραπάνω κανόνας είναι να έχει σημειωθεί κάποια συναλλαγή με την επιχείρηση (Λιμνιώτης, 2013).

Όσον αφορά τις «Ηλεκτρονικές επικοινωνίες - Ασφάλεια επεξεργασίας» ο ισχύων Νόμος στο άρθρο 12 (όπως άλλαξε στο Ν. 4070/2012) προβλέπει ότι:

1. Ο φορέας των τηλεπικοινωνιών έχει υποχρέωση να εφαρμόζει τις απαραίτητες ενέργειες για την ασφάλεια, προκειμένου να κατοχυρώνει τουλάχιστον τα παρακάτω:
   - Πρόσβαση σε ιδιωτικά στοιχεία δίνεται μόνο σε εξουσιοδοτημένα άτομα, που έχουν λάβει έγκριση για την έννομη χρήση των δεδομένων

• Προστασία στοιχείων, προσωπικού χαρακτήρα (από απώλεια ή πρόκληση φθορών και αλλοιώσεων)

• Τήρηση τακτικής ασφάλειας

2. Αν παρατηρηθεί η καταπάτηση προσωπικών στοιχείων, ο φορέας ενημερώνει την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

3. Σε περίπτωση που η καταπάτηση είναι πιθανό να έχει δυσάρεστες συνέπειες στο χρήστη ή σε άλλο πρόσωπο, ο πάροχος καθιστά ενήμερο όποιον αφορά η παραβίαση

4. Να τηρείται αρχείο συμβάντων καταπάτησης (με λεπτομερειακή καταγραφή αυτών) (Λιμνιώτης, 2013).

3.4 Ο ΝΕΟΣ ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Δεν υπάρχει αμφιβολία πως η θέσπιση του καινοτόμου νόμου της Οδηγίας 95/46 ΕΚ «για την προάσπιση των φυσικών προσώπων απέναντι στην επεξεργασίας ιδιωτικών στοιχείων και την διακίνηση τους, χωρίς περιορισμούς» επρόκειτο για ένα θεμέλιο λίθο από το 1995, ώστε να υπάρξει σύμπνοια ανάμεσα στις ευρωπαϊκές χώρες αναφορικά με το διαδίκτυο (Κανελλάκη, 2016).

Η Οδηγία 95/46/ΕΚ απέβλεπε στη μεγαλύτερη δυνατή προάσπιση των θεμελιωδών δικαιωμάτων του ατόμου στο διαδίκτυο, ανάλογα με τις συνθήκες κάθε περιόδου και παρείχε την απαιτούμενη ελευθερία για την εξασφάλιση μιας ακόμα αποτελεσματικότερης προάσπισης των στοιχείων ακόμα και σε περίπτωση που αυτό σήμαινε την καθολική εφαρμογή της. Ωστόσο, παρά το αξιόλογο περιεχόμενο και τις αρχές τις οποίες εισήγαγε η Οδηγία αυτή, θεωρήθηκε αναγκαίο να μεταβληθεί και να προσαρμοστεί σε ένα ευρύτερο Κανονισμό, που αποσκοπεί στη συμπόρευση με την εξέλιξη της τεχνολογίας, που παρατηρείται το τελευταίο χρονικό διάστημα, αλλά και στη παροχή επιπρόσθετων νομοσχεδίων και εννοιών, γεγονός που κρίθηκε απαραίτητο προκειμένου να αντιμετωπιστεί καλύτερα η σημερινή κατάσταση (Κανελλάκη, 2016).

Στις 25 Ιανουαρίου 2012, λοιπόν, η Επιτροπή ανακοίνωσε ένα γενικό νομοθετικό σχέδιο, για να αλλάξει το νομοθετικό πλαίσιο της ΕΕ αναφορικά με την προάσπιση των ιδιωτικών στοιχείων. Η νέα τροποποίηση αποβλέπει στην προάσπιση των προσωπικών στοιχείων στο σύνολο της ΕΕ, ενδυναμώνοντας την άσκηση ελέγχου των ατόμων που κάνουν χρήση διαδικτύου πάνω στις πληροφορίες που τους ενδιαφέρουν και μειώνοντας τη δαπάνη για τις επιχειρήσεις. Η ανάπτυξη της τεχνολογίας και ο διεθνισμός έχουν αλλάξει άρδην το πώς γίνεται η αποθήκευση, πρόσβαση και εφαρμογή των στοιχείων. Επιπροσθέτως, οι 28 χώρες μέλη έχουν τηρήσει τα νομοθετήματα του 1995 με διαφορετική προσέγγιση. Ένας ενιαίος νόμος θα σταματήσει τη παρούσα διάσπαση και τις διοικητικές δαπάνες αναφορικά με το κόστος. Αυτό θα βοηθήσει στην ενδυνάμωση της εμπιστοσύνης του αγοραστικού κοινού στις ηλεκτρονικές υπηρεσίες και θα αποτελέσει εφαλτήριο για την πρόοδο, την εργασία και την πρωτοπορία στην Ευρώπη. Τον Δεκέμβριο του 2015, το Κοινοβούλιο (σε επίπεδο επιτροπής) και το Συμβούλιο (σε πρεσβευτικό επίπεδο) προχώρησαν σε συμφωνία αναφορικά με τις καινούργιες αρχές προάσπισης της ιδιωτικότητας μετά από τρία χρόνια διαρκών διαβουλεύσεων. Οι καινούργιοι κανόνες ανακοινώθηκαν τον Απρίλιο του 2016 και θα εφαρμοστούν από τον Μάιο του 2018:

- κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προάσπιση των ατόμων από την επεξεργασία των ιδιωτικών στοιχείων, για την ανεμπόδιστη μετακίνηση των στοιχείων αυτών και την ακύρωση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)·
- οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προάσπιση των ατόμων από την επεξεργασία προσωπικών στοιχείων από υπευθύνους φορείς για την επίτευξη της πρόληψης, επέκτασης, εντοπισμού ή δίωξης ποινικών αδικημάτων ή της εφαρμογής ποινικών κυρώσεων και για την ανεμπόδιστη μετακίνηση των στοιχείων αυτών και την ακύρωση της οδηγίας-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (Milt, 2018).

Η ουσιώδης αυτή αλλαγή αποσκοπούσε στην ενδυνάμωση της αποτελεσματικότητας της προάσπισης των δεδομένων των ατόμων των οποίων τα προσωπικά στοιχεία υποβάλλονται σε επεξεργασία. Επιπλέον, είχε ως σκοπό να τροποποιήσει και πρωτίστως να ενδυναμώσει τις επιχειρηματικές δυνατότητες που αφορούν την ψηφιακή ενιαία αγορά, ωστόσο ταυτόχρονα απέβλεπε στη δημιουργία μιας ορατής

ελάττωσης των διοικητικών δαπανών. Έτσι, η τροποποίηση αυτή αφορούσε δύο νομοθετικές πράξεις: τη γενική αρχή προάσπισης των ιδιωτικών στοιχείων, που πήρε τη θέση της Οδηγίας 95/46.ΕΚ, και της Οδηγίας προάσπισης των στοιχείων σχετικά με την εφαρμογή του νόμου που πήρε τη θέση της οδηγίας-πλαισίου του 2008 για την προάσπιση της ιδιωτικότητας (Κανελλάκη, 2018).

3.4.1 Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου

Η καινούργια αρχή που τέθηκε σε εφαρμογή στις 25 Μαΐου του 2018 περιλαμβάνει τα δικαιώματα του ατόμου, το οποίο αφορούν τα δεδομένα, δηλαδή εκείνου του οποίου τα προσωπικά στοιχεία υπόκειντο σε επεξεργασία. Τα παραπάνω δικαιώματα, που είναι πιο διευρυμένα δίνουν στους χρήστες αποτελεσματικότερο έλεγχο για τα προσωπικά τους στοιχεία, όπως:

- την ανάγκη παραχώρησης ρητής συναίνεσης του χρήστη για την επεξεργασία των προσωπικών του στοιχείων
- την πρόσβαση με άμεσο και εύκολο τρόπο του χρήστη στα προσωπικά του στοιχεία
- τη δυνατότητα τροπολογίας , σβήσιμου και «λήθης»
- τη δυνατότητα να εναντιωθεί στη χρήση των προσωπικών στοιχείων για τη «συγκρότηση προφίλ»
- το δυνατότητα μεταφοράς των πληροφοριών από πάροχο σε πάροχο.

Όσον αφορά τη παραπάνω νομοθεσία, μία από τις δραστικές μεταβολές που θεσμοθετούνται είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) προκειμένου να είναι εφικτή η εμπορική επικοινωνία, λαμβάνοντας υπόψη τη σπουδαιότητα της συναίνεσης του ατόμου που λαμβάνει το μήνυμα. Ακόμα, καθιερώνεται η υποχρέωση των αρμόδιων που είναι υπεύθυνοι για την επεξεργασία δεδομένων να δίνουν πληροφορίες αληθινές και επαληθεύσιμες στα άτομα, με τα οποία σχετίζονται τα δεδομένα αναφορικά με την επεξεργασία των στοιχείων τους.

Στο νέο νομικό πλαίσιο περιγράφονται με κάθε λεπτομέρεια οι ευρύτερες ευθύνες που φέρουν οι αρμόδιοι για την επεξεργασία και όσοι εκτελούν την επεξεργασία των προσωπικών στοιχείων κατόπιν απαίτησης των πρώτων. Και οι δύο υποχρεούνται να τηρούν τα σωστά μέτρα ασφαλείας λαμβάνοντας υπόψη τον κίνδυνο τον οποίο κρύβουν οι ενέργειες της επεξεργασίας πληροφοριών τις οποίες πραγματοποιούν.

Οι αρμόδιοι για την επεξεργασία, κάποιες φορές, είναι απαραίτητο να γνωστοποιούν τα περιστατικά καταπάτησης προσωπικών στοιχείων μέσα σε 72 ώρες από την εμφάνιση τους και την απώλεια δεδομένων προσωπικού χαρακτήρα στους αρμόδιους φορείς και στα άτομα, τα οποία αφορούν τα στοιχεία, σε περίπτωση που κρίνεται απαραίτητο, εξαιτίας του περιεχομένου των στοιχείων που χάθηκαν.

Επιπροσθέτως, σχετικά με τις επιχειρήσεις και τους δημόσιους φορείς που αναλαμβάνουν την επεξεργασία δεδομένων που κρύβουν κινδύνους είναι απαραίτητο να έχουν τοποθετήσει αρμόδιο προάσπισης δεδομένων.

Για τα άτομα που είναι υπεύθυνα για την επεξεργασία ή για εκείνους που αναλαμβάνουν την επεξεργασία δεδομένων και που καταστρατηγούν τους νόμους για την προάσπιση των δεδομένων ακολουθούν βαρύτατες ποινές.

Στους αρμόδιους επεξεργασίας στοιχείων είναι δυνατό να οριστεί ποινή καταβολής χρηματικού ποσού, ικανού να φτάσει τα 20 εκατ. € ή το 4% από το σύνολο των εσόδων που έλαβαν από την εργασία τους σε ένα χρόνο.
Προκειμένου να οριστεί η διοικητική ποινή καταβολής χρηματικού ποσού, αλλά και το μέγεθος του ποσού που θα επιβληθεί για κάθε ξεχωριστό περιστατικό, προσμετρούνται και οι παρακάτω παράγοντες:

- ο χαρακτήρας, το μέγεθος και η διάρκεια της παράβασης, προσμετρώντας το χαρακτήρα, το μέγεθος ή το σκοπό της επεξεργασίας, αλλά και το σύνολο των ατόμων, τα οποία αφορούν τα δεδομένα και που έβλαψε η παράβαση και το μέγεθος ζημίας που προκλήθηκε σ' αυτούς,
- ο δόλος ή η αμέλεια που οδήγησε στην καταστρατήγηση,

- κάθε είδους πράξεις, τις οποίες έκανε ο αρμόδιος επεξεργασίας ή αυτός που ανέλαβε την επεξεργασία για να ελαττώσει τη βλάβη που προκλήθηκε στα άτομα, τα οποία αφορούν τα δεδομένα
- το μέγεθος της ευθύνης που φέρει ο αρμόδιος επεξεργασίας ή το άτομο που πραγματοποιεί την επεξεργασία, συνεκτιμώντας τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν,
- πιθανή πρωτύτερη καταστρατήγηση από τον αρμόδιο επεξεργασίας ή το άτομο που έχει αναλάβει την επεξεργασία
- το κατά πόσο υπήρξε σύμπραξη με τον φορέα ελέγχου για την διόρθωση της ζημιάς που προκάλεσε η καταστρατήγηση και την μείωση των τυχών αρνητικών συνεπειών της,
- οι κατηγορίες προσωπικών στοιχείων που θίγει η καταπάτηση,
- με ποιο μέσο η εποπτική αρχή ενημερώθηκε την παράβαση, και πιο συγκεκριμένα εάν και σε πιο βαθμό ο αρμόδιος επεξεργασίας ή αυτός που διέπραξε την επεξεργασία ανακοίνωσε την παράβαση,
- αν δόθηκε η εντολή προηγουμένως για εφαρμογή των μέτρων που προβλέπονται κατά του αρμόδιου επεξεργασίας ή του ατόμου που εκτέλεσε την επεξεργασία αναφορικά με το ίδιο αντικείμενο ή συνετισμός με τα προβλεπόμενα μέτρα,
- η εφαρμογή κωδίκων δεοντολογίας ή συστημάτων πιστοποίησης, που έχουν λάβει έγκριση σύμφωνα και
- οποιοσδήποτε άλλος παράγοντας επιβαρυντικός ή όχι που απορρέει από τις συνθήκες της εκάστοτε περίπτωσης, όπως τα οικονομικά κέρδη που συγκεντρώθηκαν ή βλαβών που αποφεύχθηκαν, άμεσα ή έμμεσα, από την παράβαση.

Εν κατακλείδι, ο κανονισμός δίνει στα άτομα, τα οποία αφορούν τα δεδομένα τη δυνατότητα να προβούν σε καταγγελία στην αρμόδια αρχή, όπου αναγνωρίζει το δικαίωμά τους να καταφύγουν στη δικαιοσύνη και να διεκδικήσουν δικαστική αποζημίωση. Με αυτόν τον τρόπο οι επιχειρήσεις έχουν δεχτεί αγωγές από άτομα των οποίων σημειώθηκε απώλεια των προσωπικών τους στοιχείων.

3.4.2 Ανάκληση της συγκατάθεσης για χρήση προσωπικών δεδομένων και δικαίωμα απαγόρευσης της επεξεργασίας τους

Ο παραπάνω κανονισμός καθιστά σαφείς τις ενέργειες που προβλέπονται αν κάποιο άτομο είχε δώσει τη συναίνεση του σε επιχείρηση ή φορέα να κάνει χρήση των προσωπικών του στοιχείων και στο εξής δεν θέλει να γίνεται εφαρμογή αυτών. Συγκεκριμένα, είναι εφικτό το πρόσωπο, οποιαδήποτε στιγμή, να έρθει σε επαφή με τον αρμόδιο επεξεργασίας των στοιχείων(το άτομο ή τον φορέα που διαχειρίζεται τα προσωπικά στοιχεία) και να αναιρέσει την παραπάνω συγκατάθεση. Η επιχείρηση ή ο φορέας, όταν συμβεί αυτό, δεν έχει τη δυνατότητα να κάνει χρήση προσωπικών στοιχείων.

Επιπροσθέτως, ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει ηλεκτρονική υπηρεσία ακύρωσης της συναίνεσης, η οποία μπορεί να συμβεί οποιαδήποτε στιγμή, μέσω ενός συστήματος παραπλήσιου με το σύστημα με το οποίο έγινε η δήλωση της συναίνεσης. Συγκεκριμένα, σε περίπτωση που η δήλωση της συναίνεσης του συνδρομητή ή χρήστη έχει υποβληθεί μέσω ιστοσελίδας, η ακύρωση της συναίνεσης είναι απαραίτητο να μπορεί να εφαρμοστεί μέσω της ίδιας ιστοσελίδας. Η ακύρωση της συναίνεσης είναι θεμιτό να συμβαίνει πάντα χωρίς να απαιτείται από τον συνδρομητή ή χρήστη η κατάθεση και άλλων προσωπικών στοιχείων εκτός αυτών που έχουν ήδη καταχωρηθεί και είναι γνωστά στον αρμόδιο επεξεργασίας (π.χ. γνωστοποίηση δεδομένων ταυτότητας, όταν κατά την έκφραση της συναίνεσης είχε ζητηθεί μόνο η διεύθυνση ηλεκτρονικού ταχυδρομείου). Ο αρμόδιος επεξεργασίας πρέπει να κατοχυρώνει ότι η ακύρωση της συναίνεσης δεν είναι εφικτό να τεθεί υπό αμφισβήτηση ως πράξη που πηγάζει από τον συγκεκριμένο συνδρομητή ή χρήστη. Για την επίτευξη του στόχου αυτού, ο υπεύθυνος επεξεργασίας έχει τη δυνατότητα να συγκεντρώνει αποθηκευμένο στο αρχείο του το σύνολο των δηλώσεων ακύρωσης της συναίνεσης(Οδηγία 2/2011).

Παρ' όλα αυτά, σε περίπτωση που ένας πάροχος προβαίνει σε επεξεργασία προσωπικών στοιχείων για την εξυπηρέτηση των δικών του νόμιμων σκοπιμοτήτων ή του δημόσιου συμφέροντος ή για μια επίσημη αρχή, δεν έχει τη δυνατότητα ακύρωσης της επεξεργασίας τους ο συνδρομητής. Σε κάποιες καταστάσεις, είναι

πιθανό το δημόσιο συμφέρον να έχει προτεραιότητα και να δοθεί στην επιχείρηση ή τον φορέα το δικαίωμα να εξακολουθεί να κάνει χρήση των προσωπικών του στοιχείων. Αυτό θα ήταν δυνατό να γίνει στην επιστημονική έρευνα και συλλογή στατιστικών δεδομένων από δημόσια αρχή για τις ανάγκες των αρμοδιοτήτων της.

Οι συνδρομητές είναι αναγκαίο να έχουν πάντα επίγνωση των εξελίξεων, αναφορικά με τη δυνατότητα που έχουν να μην επιτρέπουν τη χρήση των προσωπικών τους στοιχείων από τη πρώτη στιγμή, κατά την οποία ο πάροχος θα έρθει σε επαφή με αυτούς.

3.5 ΙΔΙΩΤΙΚΕΣ ΠΡΩΤΟΒΟΥΛΙΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

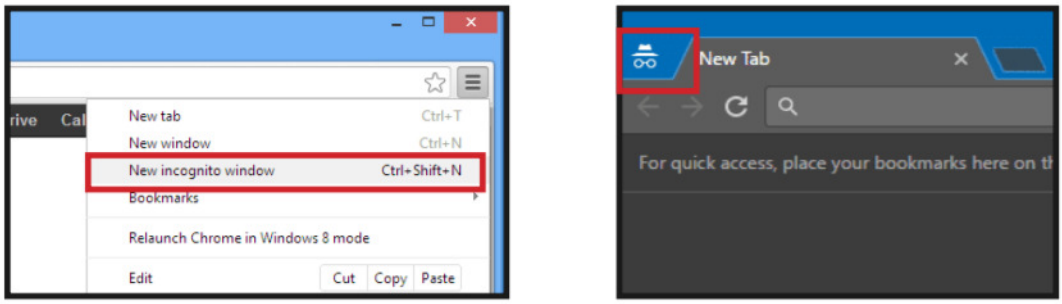
Εκτός του ισχύοντος νομοθετικού πλαισίου, οι χρήστες έχουν τη δυνατότητα να προασπίσουν τα προσωπικά τους δεδομένα και την ανωνυμία τους μέσω κατάλληλων λογισμικών, όπως είναι: η ανώνυμη περιήγηση,τα BrowserExtensions το VPN, και το OnionRouting.

3.5.1 Ανώνυμη περιήγηση

Η ιδιωτική περιήγηση αποτελεί μια παραπάνω δυνατότητα που διαθέτει κάθε πρόγραμμα πλοήγησης. Με αυτόν τον τρόποο χρήστης περιηγείται στο διαδίκτυο αλλά το ιστορικό, οι κωδικοί πρόσβασης, τacookies και άλλα στοιχεία που έχει καταγράψει σε φόρμες δεν αποθηκεύονται. Συγκεκριμένα όσων αφορά τα cookies, αυτά καταχωρούνται κατά την διάρκεια της πλοήγησης του χρήστη, όμως όταν σταματήσει την ιδιωτική πλοήγηση διαγράφονται αυτόματα (αντιθέτως στην κανονική πλοήγηση αυτά αποθηκεύονται) («Ιδιωτική Περιήγηση για υπολογιστές και κινητά», χ.χ.)

Προκειμένου να γίνει εφικτή η ανώνυμη πλοήγηση στο GoogleChrome (είτε σε λειτουργικό σύστημα Windows, είτε σε Mac, είτε σε Android, είτε σε iOS) ο χρήστης

είναι απαραίτητο να επιλέξει τις τρεις τελίτσες που είναι τοποθετημένες πάνω δεξιά στο GoogleChrome πρόγραμμα για να αποκτήσει πρόσβαση στο μενού και να διαλέξει NewIncognitoWindow σύμφωνα με την εικόνα που ακολουθεί. Με το άνοιγμα της ανώνυμης πλοήγησης το άτομο θα αντικρύσει ένα σκούρο γκρι παράθυρο με το γνωστό ανθρωπάκι που φοράει γυαλιά και καπέλο πάνω αριστερά και που θα του γνωστοποιεί ότι η ανώνυμη περιήγηση είναι ενεργοποιημένη. («Ιδιωτική Περιήγηση για υπολογιστές και κινητά», χ.χ.)



Εικόνα 3.1: Ανώνυμη περιήγηση

Πηγή: «Ιδιωτική Περιήγηση για υπολογιστές και κινητά».

Τα πλεονεκτήματα της ιδιωτικής περιήγησης είναι ότι:

1) Καθιστά εφικτή την πλοήγηση χωρίς την αποθήκευση του ιστορικού σε περίπτωση που το άτομο το επιθυμεί.
2) Δεν προβάλλονται στοχευμένες διαφημίσεις από ιστοσελίδες που ο χρήστης έχει παλιότερα επισκεφτεί, κατά την διάρκεια ιδιωτικής πλοήγησης.
3) Δεν αποθηκεύονται δεδομένα όπως username, passwords και άλλα ιδιωτικά δεδομένα που έχει προσθέσει το άτομο σε φόρμες με αποτέλεσμα να είναι πιο ασφαλή τα ιδιωτικά δεδομένα («Ιδιωτική Περιήγηση για υπολογιστές και κινητά»)

Τα μειονεκτήματα είναι:
1) Η εσφαλμένη εντύπωση ότι ο χρήστης έχει τη ευχέρεια να κάνει όποιες ενέργειες επιθυμεί χωρίς να έχουν τη δυνατότητα να τον εντοπίσουν.
2) Σε περίπτωση που το παιδί κάνει εφαρμογή της ανώνυμης περιήγησης δεν θα έχουν τη δυνατότητα οι γονείς να ασκούν έλεγχο στις ιστοσελίδες στις οποίες περιηγήθηκε κατά την πρόσβαση του στο διαδικτύου(«Ιδιωτική Περιήγηση για υπολογιστές και κινητά»)

3.5.2 BrowserExtensions

Ταbrowserextensionsείναιπρογράμματα τα οποία επεκτείνουν τις δυνατότητες ενός browser.Κάθε πρόγραμμα περιήγησης έχει το δικό του ‘κατάστημα’ όπου σου δίνεται η δυνατότητα να διαλέξεις το extensionsπου επιθυμείς. Συγκεκριμένα τα extensionsχωρίζονται σε κάποιες κατηγόριες ανάλογα τη λειτουργία τους και άλλοτε είναι δωρεάν και άλλοτε όχι.

Κάποιες από τις κατηγορίες που υπάρχουν και που θα ασχοληθούμε με την συγκεκριμένη εργασία είναι τα extensionsασφάλειας, προσβασιμότητας και προσωπικών δεδομένων. Τα πιο διαδεδομένα extensionsαφορούν την απόκρυψη διαφημίσεων και την παρακολούθηση κινήσεων του χρήστη. Ας δούμε κάποια από τα extensionsπου χρησιμοποιούνται από τους περισσότερους χρήστες.

AdBlock

Θεωρείται το δημοφιλέστερο extensionμε πάνω από 60 εκατομμύρια χρήστεςκαι είναι συμβατό με όλους τους browser. Η εγκατάσταση του είναι δωρεάν και έχει ως στόχο την αποφυγή διαφημίσεων κατά τη πλοήγηση ενός χρήστη. Αυτό έχει ως αποτέλεσμα οι σελίδες να φορτώνουν πιο γρήγορα και η πλοήγηση μας να γίνεται πιο ευχάριστη και αποτελεσματική.

DuckDuckGo

Το duckduckgo είναι μία μηχανή αναζήτησης η οποία δεσμεύεται ότι δεν αποθηκεύει προσωπικά δεδομένα και αναζητήσεις του χρήστη. Επιπλέονμε την εγκατάσταση του συγκεκριμένου extensionεξασφαλίζουμε περιήγηση χωρίς διαφημίσεις.

PrivacyBadger

Toprivacybadgerπροστατεύειτον χρήστη από scriptsπου τον ακολουθούν σε όλα τα ανοιχτά παράθυρα του browser. Με αυτό τον τρόπο εμποδίζει τους ιστότοπους να παρακολουθούν οποιαδήποτε κίνηση στο διαδίκτυο.

3.5.3VirtualPrivateNetwork

Το VirtualPrivateNetwork πρόκειται για ένα εικονικό, ιδιωτικό δίκτυο. Συγκεκριμένα, πρόκειται για ένα δίκτυο με τις ιδιότητες του LAN («τοπικές» διευθύνσεις IP, δυνατότητα FileSharing, δημιουργία τοπικών servers, Internet ConnectionSharing)

στο οποίο μπορούν να συνδεθούν, με κρυπτογραφημένη σύνδεση υψηλής ασφάλειας, υπολογιστές από ολόκληρο τον κόσμο.

Ο διαρκής αγώνας τον χρηστών για προστασία των προσωπικών τους δεδομένων έχει οδηγήσει στην ραγδαία αύξηση εταιρειών που παρέχουν VPNυπηρεσίες. Γενικότερα η εγγραφή ενός χρήστη σε VPNκοστίζει αλλά υπάρχουν εταιρείες που για να δελεάσουν τους χρήστες προσφέρουν δωρεάν τις λειτουργίες τους είτε για μικρό χρονικό διάστημα (freetrialλίγων μηνών), είτε για μικρό όγκο δεδομένων (συνήθως 500MBτον μήνα).

Μολονότι το VPN φαντάζει απλό, ουσιαστικά παρέχει ποικίλες λειτουργίες, όπως:

- Πρόσβαση σε συγκεκριμένα site (με βάση τη χώρα). Υπηρεσίες όπως το Pandora, το Netflix και το Hulu, αλλά και κάποια βίντεο του youtube απευθύνονται μόνο σε περιοχές εντός των ΗΠΑ. Η σύνδεση με τη χρήση VPN συμβάλλει στην αντιμετώπιση του παραπάνω περιορισμού.

- Παράκαμψη Τοπικής Λογοκρισίας. Σε περίπτωση που ένας χρήστης έχει μπλοκάρει την περιήγηση στο Facebook ή το YouTube, αν συνδεθεί με ένα VPN έχει τη δυνατότητα να περιηγηθεί όπου επιθυμεί, χωρίς περιορισμούς.

- Ασφαλής περιήγηση στο δίκτυο της εργασίας εξ' αποστάσεως. Άτομα που ταξιδεύουν συνεχώς για επαγγελματικούς λόγους, δύνανται να χρησιμοποιήσουν VPN, τοποθετημένο στην επιχείρηση για να μπορούν να περιηγηθούν σε κάθε τοπικό πόρο (π.χ. shares στον εταιρικό server).

- Ασφαλής περιήγηση στο οικιακό δίκτυο εξ' αποστάσεως. Αν εγκατασταθεί ένα VPN στο σπίτι, ο χρήστης έχει τη δυνατότητα πρόσβασης από κάθε μέρος σε υπηρεσίες όπως το RemoteDesktop, τα τοπικά shares, αλλά μπορεί και να ασχολείται με παιχνίδια με τη χρήση διαδικτύου σαν να πρόκειται για το ίδιο τοπικό δίκτυο LAN.

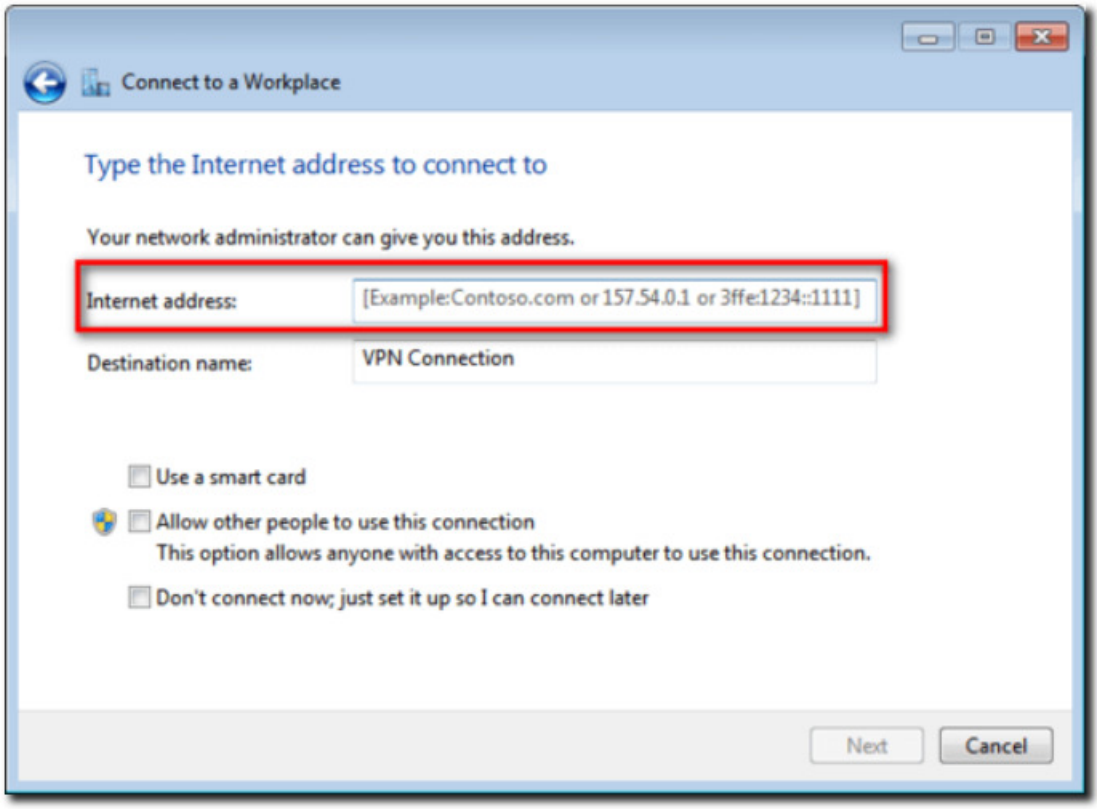
- Απόκρυψη των ενεργειών ενός χρήστη από το τοπικό δίκτυο ή τον ISP. Σε περίπτωση που το άτομο κάνει χρήση μιας ελεύθερης σύνδεσης WiFi (δημόσια ή σε

περίπτωση που δεν είναι κλειδωμένη), σε κάθε ιστοσελίδα που έχει πρόσβαση και που δεν είναι HTTPS, το σύνολο των ενεργειών του είναι ευδιάκριτο σε όποιον θέλει να έχει πρόσβαση σε αυτές. Ωστόσο, αν χρησιμοποιεί ένα VPN, το μόνο που θα είναι εμφανές είναι η ασφαλής περιήγηση με το VPN, και κάθε άλλο στοιχείο θα είναι προστατευμένο στο VPN.

- Κατέβασμα Αρχείων. Αρκετοί χρήστες προτιμούν VPN για να κατεβάσουν αρχεία μέσω BitTorrent – υπηρεσία κατάλληλη και για νόμιμα αρχεία, σε περίπτωση που ένας συγκεκριμένος ISP περιορίζει σκοπίμως την κίνηση μέσω BitTorrent. Το παραπάνω παρατηρείται και για κάθε άλλη δέσμευση που έχει ο ISP σε συγκεκριμένη μορφή μεταφοράς στοιχείων– εκτός των περιπτώσεων που ο ISP έχει θέσει περιορισμούς γενικά στο VPN (Κυρίτσης, 2013).

Οι πάροχοιVPNέχουν κάνει πλέον την διαδικασία προσθήκης ενός χρήστη στο δίκτυο τους αυτοματοποιημένη. Ειδικά με την εμφάνιση των Windows 10 δημιουργήθηκαν εφαρμογέςπου κάνουν την διαδικασία της παραμετροποίησης να διαρκεί μερικά δευτερόλεπτα. Σε περίπτωση όμως που ο χρήστης επιθυμεί να έχει τον απόλυτο έλεγχο στις ρυθμίσεις του VPNμπορεί μετά την εγγραφή του στην σελίδα του πάροχουνα προσθέσει χειροκίνητα τα στοιχεία που του δόθηκαν όπως βλέπουμε παρακάτω.

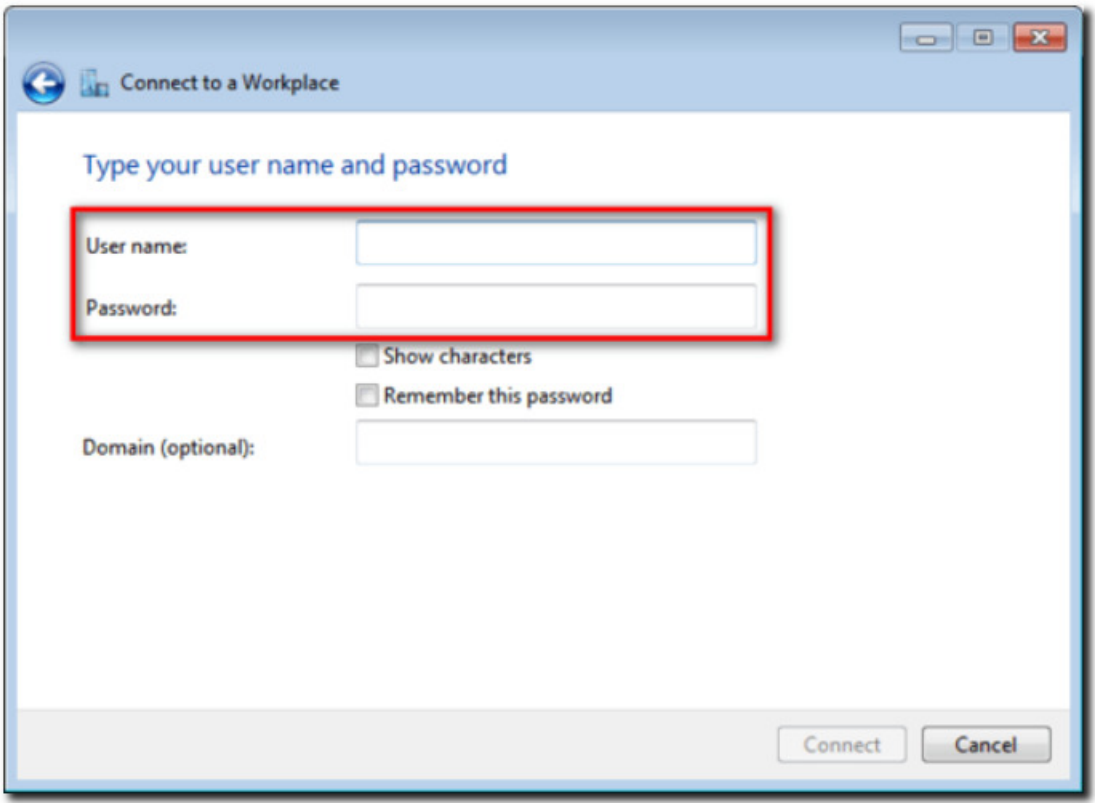
Δεν απαιτούνται εξειδικευμένες τεχνικές γνώσεις για να έχει πρόσβαση ένας υπολογιστής με Windows σε VPN. Στην ουσία, χρειάζεται το άτομο να μεταβεί στο StartMenu, να βάλει VPN στην αναζήτηση και να επιλέξει "Setup a virtualprivatenetwork (VPN) connection". Ο παρακάτω οδηγός θα βοηθήσει το άτομο στο να τοποθετήσει τη διεύθυνση και τα δεδομένα σύνδεσης της υπηρεσίας VPN που επιθυμεί να κάνει χρήση(Κυρίτσης, 2013).



Εικόνα 3.2 (α): Σύνδεση VPN

Πηγή: Κυρίτσης, 2013.

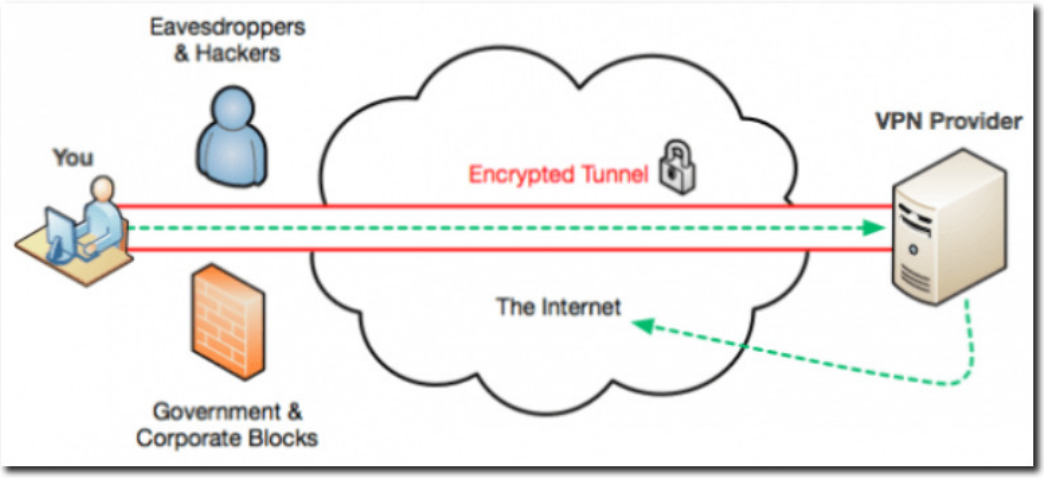
Η υπηρεσία θα έχει παραχωρήσει επιπλέον ένα username και password. Εν συνεχεία ο χρήστης δύναται να συνδεθεί ή να αποσυνδεθεί από το VPN κάνοντας χρήση της εικόνας του δικτύου στη μπάρα εργασιών (το ίδιο σύμβολο από το οποίο διαλέγουμε το δίκτυο Wi-Fi μέσω του οποίου θέλουμε να περιηγηθούμε).



Εικόνα 3.2 (β): Σύνδεση VPN

Πηγή: Κυρίτσης, 2013.

Η λειτουργία των VPN μπορεί να παρομοιαστεί ως μια κωδικοποιημένη σήραγγα που συνδέει την συσκευή μας με τονserver της εταιρείας και από εκεί με τον παγκόσμιο ιστό. Όσο κινούμαστε μέσα στην σήραγγα κρύβουμε τα προσωπικά μας δεδομένα από τους διαχειριστές των Server, από τους εξωτερικούς χρήστες αλλά ακόμα και από τον πάροχο του δικτύου μας.



Εικόνα 3.3: Χρήση του Vpn

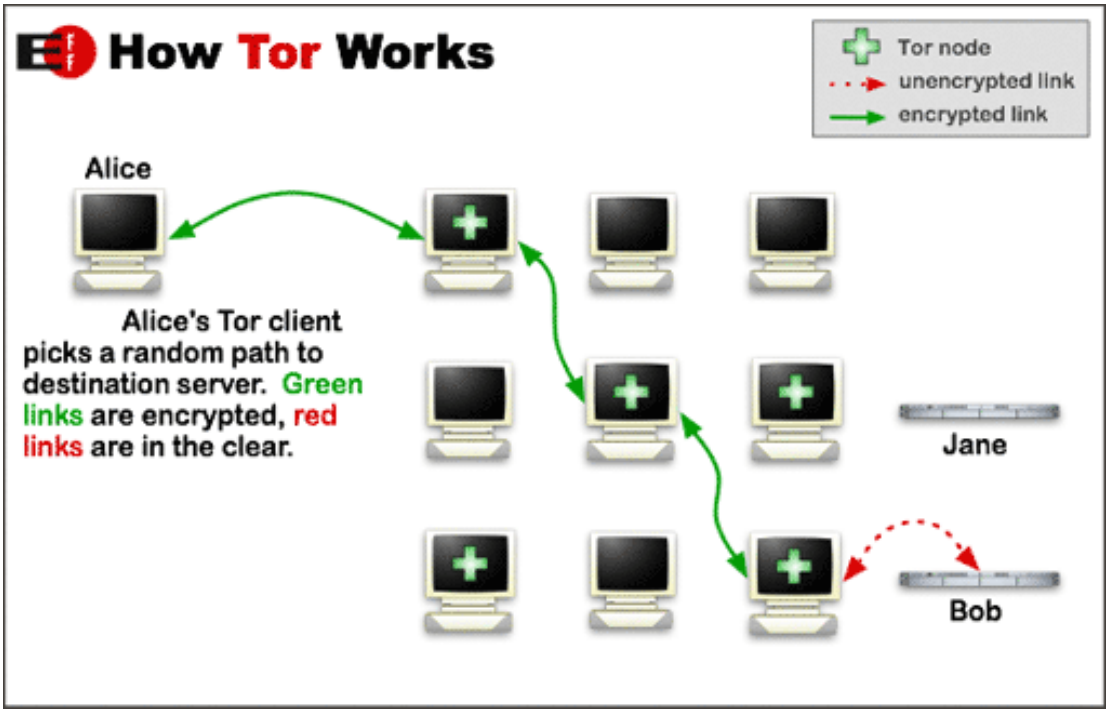
Πηγή: Κυρίτσης, 2013.

Ως αρνητικά στοιχεία της λειτουργίας των VPNμπορούμε να θεωρήσουμε το κόστος τους (συνήθως 5 με 10 ευρώ τον μήνα) και το ότι δημιουργούν την ψευδαίσθηση της απόλυτης ανωνυμίας. Δεν πρέπει να ξεχνάμε πως αποκρύπτουμε τας προσωπικά μας δεδομένα από τους εξωτερικούς κινδύνους αλλά όχι και από την εταιρεία που μας παρέχει την σήραγγα. Είναι αυτονόητο πως όταν κάνουμε εγγραφή για VPN υπηρεσίες διαβάζουμε αναλυτικά τους όρους και τις προϋποθέσεις της εταιρείας.

3.5.4 Onionrouting

Η τεχνική δρομολόγησης onionrouting χρησιμοποιείται για την ανώνυμη επικοινωνία μέσω ενός δικτύου υπολογιστών. Σε έναδίκτυο με onionrouters το πακέτο της πληροφορίας ξεκινά με πολλά επίπεδα κρυπτογράφησης (από εκεί προκύπτει και το όνομα του δικτύου).Κάθε κόμβος που λαμβάνει το πακέτο αποκρυπτογραφεί ένα επίπεδο το οποίο του αποκαλύπτει τον επόμενο προορισμό του πακέτου μέσα στο δίκτυο. Η διαδικασία επαναλαμβάνεται μέχρι το πακέτο να φτάσει στο τελικό κόμβο όπου πλέον χωρίς άλλο επίπεδο κρυπτογράφησης το πακέτο προωθείται στον τελικό προορισμό. Η διαδρομή που θα ακολουθήσει το πακέτο δεδομένων είναι τυχαία και αλλάζει διαρκώς.

Με αυτή την διαδικασία εξασφαλίζεται πως οι ενδιάμεσοι κόμβοι δεν γνωρίζουν τίποτα για την συνολική διαδρομή του πακέτου παρά μόνο τον αμέσως επόμενο προορισμό.Το πιο διαδεδομένο δωρεάν δίκτυο που αποτελείται αποκλειστικά από εθελοντικούς onionrouterseίναι το Tortou οποίου η χρήση τα τελευταία χρόνια έχει αυξηθεί κατακόρυφα. Η πλήρης ονομασία του είναι TheOnionRouterκαι δημιουργήθηκε πριν κάποια χρόνια για τις ανάγκες του ναυτικού των ΗΠΑ.



Εικόνα 3.4: ΗλειτουργίατουTor

Πηγή: Electronic Frontier Foundation (EFF)

Στόχος του Tor είναι να αποκρύπτει τις ταυτότητες των χρηστών του και την δραστηριότητά τους στο δίκτυο, αποτρέποντας την παρακολούθηση και την ανάλυση της κίνησης και διαχωρίζοντας τον εντοπισμό από την δρομολόγηση. Αυτή η ανωνυμία επεκτείνεται στην φιλοξενία ανθεκτικού στην λογοκρισία περιεχομένου μέσω των ανώνυμων κρυμμένων υπηρεσιών του Tor. Επιπλέον, διατηρώντας κάποιους από τους κόμβουςεισόδου (γεφυρωμένους κόμβους) μυστικούς, οι χρήστες αποφεύγουν την διαδικτυακή λογοκρισία η οποία στηρίζεται στο μπλοκάρισμα των δημόσιων κόμβων του Tor («TorFlow: Πώς δουλεύουν οι κόμβοι τουTor;», 2016).

Η διαδικτυακή διεύθυνση του αποστολέα και του παραλήπτη δεν είναι αμφότερες σε μορφή αρχικού κειμένου (cleartext) σε κάθε πέρασμα κατά μήκος της διαδρομής προς έναν κόμβο, ο οποίος δεν είναι εξόδου (ή ενδιάμεσος), ούτε κομμάτια της πληροφορίας είναι σε μορφή μη κρυπτογραφημένου κειμένου, έτσι ώστε οποιοσδήποτε ωτακουστής σε οποιοδήποτε σημείο κατά μήκος του καναλιού επικοινωνίας δεν μπορεί άμεσα να τυποποιήσει και τα δύο άκρα. Επιπλέον, στον

παραλήπτη φαίνεται ότι ο τελευταίος κόμβος Tor(κόμβος εξόδου) είναι ο δημιουργός της επικοινωνίας («TorFlow: Πώς δουλεύουν οι κόμβοι τουTor;», 2016).

Βέβαια ανοίγοντας έναν Torbrowser δε σημαίνει ότι κάποιος είναι απολύτως ανώνυμος, γι'αυτό ο κάθε χρήστης πρέπει να είναι πολύ προσεκτικός και να προβαίνει σε συγκεκριμένες ενέργειες κατά τη χρήση του λογισμικού αυτού. Για παράδειγμα αν δημιουργήσει κάποιος ιδιώτης σε κάποια υπηρεσία έναν λογαριασμό μέσω του Tor δεν πρέπει να χρησιμοποιήσει αυτούςτους λογαριασμούς έξω από το δίκτυο του Tor. Επίσης, δεν πρέπει να δημοσιεύονται προσωπικά στοιχεία μέσω του Tor, δεν πρέπει να στέλνονται κρυπτογραφημένα δεδομένα, δεν πρέπει να συνδέεται ο χρήστης στον ίδιο διακομιστή με και χωρίς Tor ταυτόχρονα, πρέπει να διαγράφονται τα cookies και τέλος καλό είναι να μην χρησιμοποιείται το Tor με Windows («9 συμβουλές για σωστή χρήση του Tor», 2016).

Υπάρχουν κάποιες ιστοσελίδες οι οποίες αγνοούν τα αιτήματα των χρηστών που έρχονται μέσω Tor, ενώ αντίθετα υπάρχουν σελίδες οι οποίες είναι προσβάσιμες αποκλειστικά μέσω του δικτύου. Πρέπει επίσης να αναφέρουμε πως παρόλοπου ο Torπροστατεύει τα προσωπικά δεδομένα του χρήστη, δεν αποκρύπτει και το γεγονός ότι ο χρήστης τον χρησιμοποιεί για την περιήγηση του στο διαδίκτυο.

ΕΠΙΛΟΓΟΣ

Σε μια εποχή γρήγορων τεχνολογικών εξελίξεων, τα ζητήματα που σχετίζονται με τον έλεγχο και τη χρήση των προσωπικών δεδομένων βρίσκονται στο επίκεντρο. Τα προσωπικά δεδομένα συχνά αναφέρονται ως «το νέο νόμισμα του ψηφιακού κόσμου» Επιπλέον, η διάκριση μεταξύ δημόσιων και προσωπικών δεδομένων είναι συχνά θολή.

Ένα μεγάλο μέρος της ζωής τους, τα άτομα τα διαθέτουν στο διαδίκτυο και στις ηλεκτρονικές δραστηριότητες - από ψώνια μέχρι ψυχαγωγία, αναζήτηση πληροφοριών και συλλογή – οι οποίες έχουν δημιουργήσει έναν πρωτοφανή αριθμό δεδομένων. Αλλά τα δεδομένα αυτά φέρουν κινδύνους. Με την εξόρυξη τους και μετέπειτα επεξεργασία τους αποκαλύπτουν οικεία στοιχεία σχετικά με το εισόδημα, τη φυλή, την εθνότητα, τη θρησκεία και άλλες προσωπικές πληροφορίες των ανθρώπων.

Επομένως, η προστασία της ιδιωτικής ζωής, είναι επί του παρόντος, ένα θέμα ευρέως διαδεδομένου κοινωνικού ενδιαφέροντος και συζήτησης, καθώς οι ψηφιακές τεχνολογίες παράγουν και εμπορεύονται προσωπικά δεδομένα σε μια άνευ προηγουμένου κλίμακα.

Ο έλεγχος των προσωπικών δεδομένων είναι το δικαίωμα των ατόμων να καθορίζουν ποιες πληροφορίες συλλέγονται, να καθορίζουν ποιες πληροφορίες διατίθενται σε τρίτους και έχουν πρόσβαση στα δεδομένα τους.

Ωστόσο, η δημόσια πολιτική που διέπει την προστασία των δεδομένων ακολούθησε μια ενδιαφέρουσα πορεία τα τελευταία χρόνια, ξεκινώντας από το να είναι ένα εξειδικευμένο ρυθμιστικό θέμα σε ένα κύριο μέλημα των πολιτικών ιθυνόντων, των ατόμων και των επιχειρήσεων.

Το Ευρωπαϊκό Κοινοβούλιο εξέδωσε στις 15 Δεκεμβρίου του 1997 την Οδηγία 97/66/ΕΚ, περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα. Οι χώρες της Ευρώπης, ανάμεσα

τους και η χώρα μας, προκειμένου να εναρμονιστούν με την ευρωπαϊκή πολιτική και τα νέα δεδομένα στον κυβερνοχώρο υιοθέτησαν μια σειρά από νόμους, οι οποίοι ανανεώνονται και συμπληρώνονται στο πέρασμα του χρόνου με σκοπό την προστασία των πολιτών στο διαδίκτυο και την ηθελημένη παραχώρηση των προσωπικών δεδομένων τους.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Α. ΕΛΛΗΝΙΚΗ

«Ιδιωτική Περιήγηση για υπολογιστές και κινητά». Διαθέσιμο στο https://saferinternet4kids.gr/wp-content/uploads/2018/05/privatewindow.pdf

9 συμβουλές για σωστή χρήση του Tor. (2016). Διαθέσιμο στο https://privacy.ellak.gr/2017/02/20/9-simvoules-gia-sosti-chrisi-tou-tor/

BelchG.andBelchM., (2012), *Διαφήμιση και Προώθηση*, Αθήνα: Τζιόλα.

EuropeanCommission, (2011).Ημέρα Προστασίας Δεδομένων: εγγύηση του δικαιώματος των πολιτών στην ιδιωτικότητα.Διαθέσιμο στοhttp://europa.eu/rapid/press-release_IP-11-102_el.htm

Milt, K. (2018). Προστασία των δεδομένων προσωπικού χαρακτήρα. ΕυρωπαικόΚοινοβούλιο.Διαθέσιμοhttp://www.europarl.europa.eu/atyourservice/el/displayFtu.html?ftuId=FTU_4.2.8.html

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. Διαθέσιμο στο http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/NEWSMAIN/PUBLICATIONS/ENTYPO_GENERAL_FINAL_LOW_PAGES_0.PDF

Γεωργίου, Γ. &Πορίκης. Ν. (2011-2012). Κοινωνικά δίκτυα: Ο ρόλος τους στην οικονομική και κοινωνική ζωή.

Ευρωπαϊκή Ένωση. (2018). Προστασία των δεδομένων και της ιδιωτικής ζωής στο διαδίκτυο.Διαθέσιμο στο https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_el.htm

Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου. (1950). Διαθέσιμο στο https://www.lawspot.gr/nomikes-plirofories/nomothesia/esda/arthro-8-eyropaiki-symvasi-dikaiomaton-toy-anthropoy-dikaioma

Κανελλάκη, Μ. (2016). Ο νέος γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων – Τα πλαίσια ασάφειας και οι προβληματισμοί πάνω στις νέες διατάξεις. Νομική Σχολή, Ευρωπαϊκό Πανεπιστήμιο Κύπρου. Διαθέσιμο στο http://webcache.googleusercontent.com/search?q=cache:lx1J3AtdCjMJ:entha.euc.ac.cy/index.php/entha/article/download/45/40+&cd=1&hl=en&ct=clnk&gl=gr

Κανονισμός(ΕΕ)2016/679.Διαθέσιμοστο https://www.cyberinsurancequote.gr/insurance/nomothesia/

Κουής, Ι.Π. (2008). Η συνταγματική Αναθεώρηση του 2001. Εθνικό Καποδιστριακό ΠανεπιστήμιοΑθηνών.Διαθέσιμοστοhttp://www.greeklaws.com/pubs/uploads/2628.pdf

Κυρίτσης, Αγγ. (2013). Τι είναι το VPN – VirtualPrivateNetwork – και γιατί μπορεί να χρειάζεστε ένα. Διαθέσιμο στο https://www.pcsteps.gr/1376-vpn-technology-explained/

Λιμνιώτης, Κ. (2013). Τα προσωπικά μας δεδομένα: δικαιώματα και υποχρεώσεις. Διαθέσιμο στο http://blogs.sch.gr/webinarspe1920/files/2013/09/2013-10-09_10_Webinar_Limniotis_Prosopika-Dedomena.pdf

Μαυρωνά, Ελ. (2012). Μελέτη Προστασίας Ιδιωτικότητας. Εθνική Σχολή Δημόσιας Διοίκησης. Διαθέσιμο στο http://www.esdy.edu.gr/files/013_ELKE/e-Master/P2%20MELETH%20IDIWTIKOTHTAS.pdf

Νόμος2472/1997.Διαθέσιμοhttp://www.dpa.gr/portal/page?_pageid=33,19052&_dad=portal&_schema=PORTAL

Νόμος3471/2006.Διαθέσιμο http://webcache.googleusercontent.com/search?q=cache:xG5zCIhpUpMJ:www.greekecommerce.gr/gr/file-download/nomos_3471_2006+&cd=1&hl=en&ct=clnk&gl=gr

Οδηγία2/2011. Διαθέσιμοhttp://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL

Οδηγία2002/58/ΕΚ.Διαθέσιμο https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_el.pdf

Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου. Διαθέσιμο στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:el:HTML

Οδηγία 97/66/ΕΚ.Διαθέσιμο http://www.3lykeiolamias.gr/sites/default/files/files/pdf/odhgia_97-66.pdf

ΤροποποίησηΟδηγίας2002/58/ΕΚ-16/12/2013.Διαθέσιμοhttp://www.dpa.gr/pls/portal/docs/PAGE/APDPX/THEMATIKES_ENOTITES/ODHGIA%202002_58_EK%20_3.PDF

https://duckduckgo.com/

https://getadblock.com/

https://medium.com/searchencrypt/the-best-browser-extensions-for-privacy-f611d8bc90a6

https://el.wikipedia.org/wiki/%CE%95%CE%B9%CE%BA%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%B9%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C_%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF

Β. ΞΕΝΟΓΛΩΣΣΗ

Aghaei, S., Nematbakhsh, A.M. &Farsani, K.H. (2012).Evolution of the World Wide Web: from Web 1.0 to Web 4.0. *International Journal of Web & Semantic Technology*, Vol.3 (No.1), p.p. 1-10. Διαθέσιμο στο http://www.ftsm.ukm.my/ss/Book/EVOLUTION%20OF%20WWW.pdf

Aldhafferi, N. Watson, C. &Sajeev, M.S.A. (2013).Personal information privacy settings of online social networks and their suitability for mobile internet devices.*International Journal of Security, Privacy and Trust Management*, Vol. 2 (No 2), p.p. 1-17. Διαθέσιμο στο https://arxiv.org/ftp/arxiv/papers/1305/1305.2770.pdf

Almagor, C.R. (2011). Internet History.*International Journal of Technoethics*, Vol 2 (No 2), p.p.45-64.Διαθέσιμοστοhttp://www.hull.ac.uk/rca/docs/articles/internet-history.pdf

Bandyopadhyay, S. (2012). Consumers' online privacy concerns: causes and effects. *Innovative Marketing*, Vol. 8 (No 3), p.p.32-39.Διαθέσιμοστοhttp://businessperspectives.org/journals_free/im/2012/im_en_2012_03_Bandyopadhyay.pdf

Bouillot, F., Ienco, D., Matwin, St., Poncelet, P. & Roche, M. (2012).*Presidential Election 2012: How French politicians tweet?*.

Dewing, M. (2010). Social Media: An introduction. Library of Parliament, Vol. 1.

Dinerman, B. (2011).Social networking and security risks.GFI White Paper.

European Commision.Διαθέσιμοστοhttp://ec.europa.eu/justice/data-protection/files/eujls08b-1002_-_protection_of_personnal_data_a4_en.pdf

Eurostat.(2016). Internet use by individuals.Διαθέσιμοστοhttps://ec.europa.eu/eurostat/documents/2995521/7771139/9-20122016-BP-EN.pdf/f023d81a-dce2-4959-93e3-8cc7082b6edd

Green A., (2007), *How can multimedia marketing techniques support Customer*

Relationship Management (CRM) for Small and Medium sized Enterprises (SME)?

Jackson, A. N. &Lilleker, G. D. (2009). Building an Architecture of Participation? Political Parties and Web 2.0 in Britain.*Journal of Information Technology & Politics*, Vol. 6 (No 3-4), p.p. 232-250.

Ki-moon, B. (2012). The use of the internet for terrorist purposes.Διαθέσιμοστοhttps://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Leiner, et al. (2009).A Brief History of the Internet.*ACM SIGCOMM Computer Communication Review*, Vol. 39 (No 5), p.p. 22-31.Διαθέσιμο στο http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf

Mekovec, R. &Vrcek, N. (2011).Factors That Influence Internet Users' Privacy Perception.*Proceedings of the ITI 2011 33rd Int. Conf. on Information Technology Interfaces*, p.p.227-232.Διαθέσιμοστοhttps://bib.irb.hr/datoteka/518331.ITI-07-02-208.pdf

Moriyama, K. (1999). Essay: Advantages of using the Internet for Vacationing. Διαθέσιμο στο https://www.cc.gatech.edu/projects/calton+morimori/home/english/EFL4300-991128-01f.pdf

Puddephatt, An., Mendel, T., Wanger, B., Hawtin, D. & Torres, N. (2012).Global Survey on Internet privacy and freedom of Expression.Unesco.Διαθέσιμοστοhttp://unesdoc.unesco.org/images/0021/002182/218273e.pdf

Su, G.G. & Lee, J. (2010). Is the Creation of Internet Beneficial to Humanity?.Διαθέσιμοστοhttp://web.cs.ucdavis.edu/~rogaway/classes/188/fall10/p4.pdf

Su, G.G. (2010). Is the Creation of Internet Beneficial to Humanity? Διαθέσιμο στο http://web.cs.ucdavis.edu/~rogaway/classes/188/fall10/p4.pdf

Sudhakar K., Guru Prasath R. S., Ashok Kumar V., *Modern Marketing Practice*, IOSR Journal of Business and Management (IOSR-JBM) e-ISSN : 2278-487X, p-ISSN : 2319-7668, PP 34-37.

Tian, Y. & Stewart, C. (2008).History of E-Commerce.IGIGlobal.Διαθέσιμοστοhttp://www.irma-international.org/viewtitle/9447/

Van den Hoven, J., Blaauw, M., Pieters, W. &Warnier, M. (2014).Privacy and Information Technology.Stanford Encyclopedia of Philosophy.Διαθέσιμοστοhttps://plato.stanford.edu/entries/it-privacy/#PerDat

Velet, D. &Zlateva, P. (n.d).Use of Social Media in Natural Disaster Management.Διαθέσιμοστοhttp://www.ipedr.com/vol39/009-ICITE2012-B00019.pdf

Vervaart, P. (n.d.). Role of Social Media And The Internet In Education. *The Journal of the International Federation of Clinical Chemistry and Laboratory Medicine*, Vol. 23, (No 2), p.p.1-4.Διαθέσιμοστοhttp://www.ifcc.org/media/199318/01_Vervaart.pdf

Wüest, C. (2010). The Risks of Social Networking.Διαθέσιμοστοhttps://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf