



**ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΙΓΑΙΟΥ**

**ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ
ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μελέτη κακόβουλων χρηστών κοινωνικών δικτύων

**ΟΝΟΜΑ ΦΟΙΤΗΤΗ
ΜΠΑΛΑΝΤΑΣ ΑΛΕΞΑΝΔΡΟΣ**

**ΟΝΟΜΑ ΕΠΙΒΛΕΠΟΝΤΑ ΚΑΘΗΓΗΤΗ
ΚΑΠΟΡΗΣ ΑΛΕΞΙΟΣ**

**ΑΘΗΝΑ
ΜΑΙΟΣ, 2021**

ΠΕΡΙΛΗΨΗ

Τα μέσα κοινωνικής δικτύωσης έχουν μια συνεχώς αυξανόμενη παρουσία στη ζωή των νέων. Οι έρευνες δείχνουν ότι περισσότεροι από τους μισούς νέους τείνουν να συνδέονται σε κάποια ιστοσελίδα κοινωνικής δικτύωσης περισσότερες από μία φορές την ημέρα ενώ ένας στους 5 συνδέεται περισσότερες από 10 φορές την ημέρα. Αυτοί οι ιστότοποι προσομοιάζουν ένα κοινωνικό περιβάλλον μέσα από το οποίο οι χρήστες μπορούν να συναντηθούν, να κοινωνικοποιηθούν και να αποκτήσουν πρόσβαση σε πληροφορίες.

Παρά τα όποια θετικά σημεία των μέσων κοινωνικής δικτύωσης, η χρήση τους έχει συνδεθεί με ανεπιθύμητες επιπλοκές. Οι νέοι κυρίως, οι οποίοι συνδέονται στα μέσα κοινωνικής δικτύωσης με τα ελλιπή επίπεδα κοινωνικής και συναισθηματικής τους ανάπτυξης, είναι ιδιαίτερα ευάλωτοι στην πίεση των συνομηλίκων, ενώ έχουν περιορισμένη ικανότητα αυτορρύθμισης. Επομένως, τα οφέλη των διαδικτυακών αλληλεπιδράσεων συμβαδίζουν επίσης με έκθεση σε πιθανούς κινδύνους για την ασφάλεια από τη χρήση των κοινωνικών μέσων, συμπεριλαμβανομένων του διαδικτυακού εκφοβισμού, της διαδικτυακής παρενόχλησης και της παραβίασης του απορρήτου.

Ο εκφοβισμός στον κυβερνοχώρο έχει λάβει τα τελευταία χρόνια σημαντική προσοχή από τα ΜΜΕ ενώ απασχολεί έντονα το κομμάτι της νομοθετικής τους ρύθμισης. Ορίζεται ως η επιθετική και εσκεμμένη πράξη ή συμπεριφορά που λαμβάνει χώρα από μια ομάδα ή ένα άτομο, με χρήση ηλεκτρονικών μορφών, επανειλημμένα εναντίον ενός παραλήπτη που δεν είναι σε θέση να υπερασπιστεί τον εαυτό του. Ο εκφοβισμός στον κυβερνοχώρο παρέχει στους εκφοβιστές μέσα επέκτασης του παραδοσιακού εκφοβισμού σε ένα ευρύτερο περιβάλλον όπου οι ενέργειες τους έχουν άμεσα, ευρύτερα και μόνιμα αποτελέσματα. Λόγω της αυξημένης πιθανότητας εξάπλωσης της κακοποίησης και λόγω της δυνατότητας διατήρησης υψηλότερων επιπέδων ανωνυμίας από ό, τι στον παραδοσιακό εκφοβισμό, η ένταση του διαδικτυακού εκφοβισμού θεωρείται μεγαλύτερη από εκείνη του παραδοσιακού εκφοβισμού.

Λέξεις κλειδιά: Διαδίκτυο, Εκφοβισμός στο κυβερνοχώρο, Παραδοσιακός εκφοβισμός, Κοινωνικά Δίκτυα, Ιδιωτικότητα

Abstract

Social media has an ever-increasing presence in the lives of young people. Surveys show that more than half of young people tend to link to a social networking site more than once a day while one in 5 logs in more than 10 times a day. These sites simulate a social environment through which users can meet, socialize, and access information.

Despite the positive aspects of social media, their use has been linked to unwanted complications. Young people in particular, who are linked to social media through their lack of social and emotional development, are particularly vulnerable to peer pressure and have a limited ability to self-regulate. Therefore, the benefits of online interactions also go hand in hand with exposure to potential security risks from the use of social media, including cyberbullying and breaches of privacy.

Cyberbullying has received considerable media attention in recent years and is a major part of its legislation arrangement. It is defined as the aggressive and deliberate act or behavior that takes place by a group or individual, using electronic forms, repeatedly against a recipient who is unable to defend himself. Cyberbullying provides intimidators with the means to extend traditional bullying to a wider environment where their actions have immediate, broader and lasting effects. Due to the increased likelihood of the spread of abuse and the ability to maintain higher levels of anonymity than in traditional bullying, the intensity of cyberbullying is considered greater than that of traditional bullying.

Keywords: Internet, Cyberbullying, Traditional Bullying, Social Networking, Privacy

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Καπόρη Αλέξη, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την καθοδήγηση του, τις υποδείξεις του, τη συνεχή του υποστήριξη και το αμείωτο ενδιαφέρον που έδειξε από την αρχή μέχρι το τέλος.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου και τη σύζυγό μου για όλη τη στήριξη και την κατανόησή τους, καθ' όλη τη διάρκεια των σπουδών μου.

1 Πρόλογος

Η παρούσα εργασία εκπονήθηκε κατά το ακαδημαϊκό έτος 2020-21 στα πλαίσια του μεταπτυχιακού προγράμματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων. Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του καθηγητή Καπώρη Αλέξιου.

Αντικείμενο της εργασίας αποτελεί η συστηματική βιβλιογραφική επισκόπηση του προφίλ των κακόβουλων χρηστών κοινωνικών δικτύων καθώς και των θυμάτων τους.

Περιεχόμενα

1 5

➤ 7

1.1. 8

1.2. 15

1.3. 20

1.4. 26

1.5. 30

1.5.1. 30

1.5.2. 32

1.5.3. 36

1.5.4. 39

➤ 44

2.1 45

2.2 49

2.3 51

2.4 55

2.5 64

➤ 68

3.1. 69

3.2. 74

3.3. 76

➤ 79

➤ 82

➤ ΚΕΦΑΛΑΙΟ 1. Διαδίκτυο

Στο παρόν κεφάλαιο εξετάζεται η ιστορική εξέλιξη του διαδικτύου, η σημερινή του μορφή καθώς και οι αναμενόμενες εξελίξεις στο άμεσο μέλλον. Επίσης επιχειρείται μία σκιαγράφηση των κοινωνικών δικτύων και το πως αυτά έχουν επηρεάσει το σύγχρονο τρόπο ζωής, ιδιαίτερα στον δυτικό κόσμο. Τέλος εξετάζεται η διεθνής και εγχώρια νομοθεσία αναφορικά με τα ζητήματα παραβίασης της ιδιωτικότητας.

1.1. Ιστορικά στοιχεία

Η ιστορία του Διαδικτύου ξεκινάει στις Ηνωμένες Πολιτείες στις αρχές της δεκαετίας του 1960, δηλαδή την περίοδο του Ψυχρού Πολέμου στα πλαίσια ενός διπολικού κόσμου: Οι Ηνωμένες Πολιτείες και η Σοβιετική Ένωση ανταγωνίζονταν να επεκτείνουν την επιρροή τους, βλέποντας η μια την άλλη με έντονη καχυποψία. Στις 4 Οκτωβρίου 1957, η Σοβιετική Ένωση εκτόξευσε τον πρώτο διαστημικό δορυφόρο, τον Sputnik. Η επιτυχία του Sputnik απαιτούσε από την κοινή γνώμη της εποχής ανάλογη αμερικανική αντίδραση. Το Υπουργείο Άμυνας των ΗΠΑ ανταποκρίθηκε με την ίδρυση του Advanced Research Projects Agency με στόχο την προώθηση της έρευνας, διασφαλίζοντας ότι οι ΗΠΑ θα ανταγωνίζονταν και θα υπερείχαν έναντι της ΕΣΣΔ σε θέματα τεχνολογίας. Η αποστολή της ARPA ήταν η παραγωγή καινοτόμων ερευνητικών ιδεών και μη συμβατικών τεχνολογικών εξελίξεων μέσω της ανάπτυξης πρωτότυπων συστημάτων. Ένα από τα γραφεία της ARPA ήταν το Γραφείο Τεχνικής Επεξεργασίας Πληροφοριών (IPTO) μέσω του οποίου χρηματοδοτήθηκε η έρευνα στην επιστήμη των υπολογιστών, απώτερο στόχο την κινητοποίηση των αμερικανικών πανεπιστημίων και ερευνητικών εργαστηρίων για τη δημιουργία ενός στρατηγικού δικτύου επικοινωνίας που θα καθιστούσε διαθέσιμες τις δυνατότητες ανταλλαγής μηνυμάτων στις κυβερνητικές υπηρεσίες ακόμα και σε ακραίες περιπτώσεις πολέμου (Cohen, 2011). Ένας δημοφιλής μύθος υποστηρίζει ότι οι επιστήμονες του Υπουργείου Άμυνας πίστευαν ότι εάν οι Σοβιετικοί ήταν σε θέση να εκτοξεύσουν δορυφόρους, θα μπορούσαν κάλλιστα επίσης να εκτοξεύσουν πυρηνικούς πυραύλους μεγάλων αποστάσεων. Επειδή τα δίκτυα εκείνη την εποχή βασίζονταν εν γένει σε κεντρικό έλεγχο, η κύρια ανησυχία ήταν η ευπάθεια των δικτύων κατά τη διάρκεια επίθεσης, δηλαδή αν το κεντρικό σημείο ελέγχου του δικτύου σταματούσε να λειτουργεί, ολόκληρο το δίκτυο θα ήταν άχρηστο. Οι επιστήμονες επιδίωκαν τη διατήρηση του δικτύου ακόμα και μετά από επίθεση σε ένα ή περισσότερα από τα κέντρα επικοινωνίας τους [79].

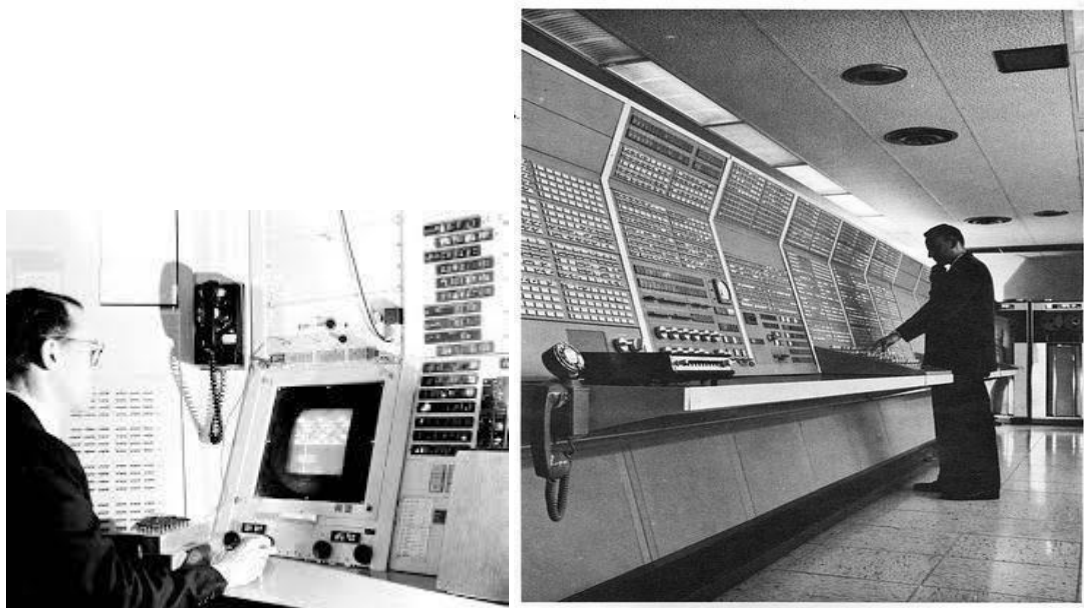
Η πρώτη καταγεγραμμένη περιγραφή των κοινωνικών αλληλεπιδράσεων που θα μπορούσαν εν γένει να ενεργοποιηθούν μέσω κάποιου είδους τεχνολογικής δικτύωσης ήταν μια σειρά υπομνημάτων που γράφτηκαν από τον J.C.R. Licklider (εικόνα 1) του MIT τον Αύγουστο του 1962. Ο Licklider οραματίστηκε ένα παγκόσμιο διασυνδεδεμένο σύνολο υπολογιστών μέσω των οποίων όλοι θα μπορούσαν γρήγορα

να έχουν πρόσβαση σε δεδομένα και προγράμματα από οποιοδήποτε σημείο, ιδέα που παραπέμπει στην σημερινή μορφή του διαδικτύου. Ο Licklider ήταν ο επικεφαλής του ερευνητικού προγράμματος DARPA, που ξεκίνησε τον Οκτώβριο του 1962.



Εικόνα 1. O J.C.R. Licklider

Ο Leonard Kleinrock του MIT δημοσίευσε την πρώτη θεωρητική εργασία σχετικά με τη μεταγωγή πακέτων τον Ιούλιο του 1961 και το πρώτο σχετικό βιβλίο το 1964. Ο Kleinrock έπεισε για τη θεωρητική σκοπιμότητα των επικοινωνιών χρησιμοποιώντας πακέτα και όχι κυκλώματα, ένα σημαντικό βήμα στην πορεία προς την υπολογιστική δικτύωση. Το άλλο βασικό βήμα ήταν η δυνατότητα «συνομιλίας» μεταξύ των υπολογιστών. Έτσι το 1965 σε συνεργασία με τον Thomas Merrill, ο Lawrence Gilman Roberts συνέδεσε τον υπολογιστή TX-2 στην Μασαχουσέτη με τον Q-32 (εικόνα 2) στην Καλιφόρνια μέσω τηλεφωνικής γραμμής χαμηλής ταχύτητας, δημιουργώντας το πρώτο δίκτυο υπολογιστών ευρείας περιοχής που κατασκευάστηκε ποτέ. Το αποτέλεσμα αυτού του πειράματος ήταν η συνειδητοποίηση ότι οι υπολογιστές θα μπορούσαν να λειτουργούν συνεργατικά και να εκτελούν από κοινού προγράμματα και να ανακτούν δεδομένα αλλά και ότι η τηλεφωνική υποδομή ήταν εντελώς ανεπαρκής για τις συγκεκριμένες ανάγκες [64].



Εικόνα 2. Ο TX-2 και ο Q-32

Το ARPANET, αν και ιδρύθηκε τους τελευταίους μήνες της δεκαετίας του 1960, η πρώτη μεγάλη επίδειξη των δυνατοτήτων του πραγματοποιήθηκε στην Ουάσιγκτον, το 1972. Το Υπουργείο Άμυνας των ΗΠΑ ενδιαφερόταν έντονα εκείνη την περίοδο να συστηματοποιήσει την χρήση των Η/Υ στις υπηρεσίες του στρατού . Σε αντίθεση με το ARPANET, το οποίο χρησιμοποιούσε αποκλειστικές τηλεφωνικές γραμμές για τη σύνδεση μεταξύ των υπολογιστών, ο αμερικανικός στρατός επιθυμούσε ένα κινητό δίκτυο ικανό να συνδέει μαζί τανκς, αεροπλάνα, πλοία κ.α. Αυτή η ικανότητα απαιτούσε τη χρήση ραδιοφωνικών και δορυφορικών συστημάτων. Περί το 1973, οι ερευνητές της DARPA είχαν καταλήξει σε τέσσερις διαφορετικές τεχνολογίες μεταγωγής πακέτων. Ο Δρ. Vint Cerf, διευθυντής του Γραφείου Τεχνικών Επεξεργασίας Πληροφοριών (IPTO) του DARPA άρχισε να εργάζεται πάνω σε αυτό το θέμα, το οποίο τελικά θα εξελισσόταν στο γνωστό πλέον Πρωτόκολλο TCP/IP.



Εικόνα 3. Το router του ARPANET γνωστό ως Interface Message Processors

Η αρχική εφαρμογή του πρωτοκόλλου TCP / IP πραγματοποιήθηκε στο Στάνφορντ το 1975. Καθώς η εξέλιξη του πρωτοκόλλου προχώρησε τα επόμενα χρόνια, άρχισε να βρίσκει εφαρμογή σε έναν εκθετικά αυξανόμενο αριθμό υπολογιστικών συστημάτων σε όλο τον κόσμο. Τον Ιανουάριο του 1983, αρκετά μεμονωμένα δίκτυα είχαν συνδεθεί μεταξύ τους ώστε να μπορεί να θεωρηθεί ότι το ARPANET είχε εξελιχθεί ουσιαστικά σε Διαδίκτυο, αν και το ίδιο το αρχικό ARPANET παροπλίστηκε το 1990. Στις αρχές της δεκαετίας του 1980, οι βασικές αρχές του τι θα εξελισσόταν στο σημερινό Διαδίκτυο είχαν ήδη τεθεί σε ισχύ. Αυτό το νέο και αναπτυσσόμενο δίκτυο, με τη συνεχή υποστήριξη της DARPA, έγινε διαθέσιμο στην ακαδημαϊκή κοινότητα, αλλά και σταδιακά και σε άλλες κυβερνητικές δομές (Darpa n.d). Το δίκτυο επεκτάθηκε σε ιδρύματα, όπως το Χάρβαρντ, το MIT, το Carnegie Mellon, το Case Western Reserve και το Πανεπιστήμιο του Ιλινόις στο Urbana. Μέσα σε δεκαέξι μήνες υπήρχαν περισσότεροι από δέκα ιστότοποι με περίπου 2.000 χρήστες και τουλάχιστον δύο διαδρομές μεταξύ οποιωνδήποτε δύο ιστότοπων για τη μετάδοση πακέτων [80].

Το 1983, 500 κεντρικοί υπολογιστές συνδέθηκαν στο Διαδίκτυο. Το 1984, ο αριθμός των κεντρικών υπολογιστών αυξήθηκε σε 1024. Καθώς περισσότεροι ερευνητές συνέδεσαν τους υπολογιστές και τα δίκτυα υπολογιστών τους με το ARPANET, το ενδιαφέρον για το δίκτυο αυξήθηκε στην ακαδημαϊκή κοινότητα. Ένας λόγος για το αυξημένο ενδιαφέρον ήταν η προσήλωσή του σε μια φιλοσοφία ανοικτής αρχιτεκτονικής: Κάθε δίκτυο θα μπορούσε να συνεχίσει να χρησιμοποιεί τα δικά του πρωτόκολλα και μεθόδους μεταφοράς δεδομένων εσωτερικά. Αυτή η φιλοσοφία ανοικτής αρχιτεκτονικής ήταν επαναστατική για εκείνη την εποχή. Οι περισσότερες εταιρείες χρησιμοποιούσαν τα δίκτυά τους ξεχωριστά και ασύμβατα με άλλα δίκτυα, φοβούμενες τον ανταγωνισμό και προσπαθούσαν να κάνουν τα προϊόντα τους απρόσιτα στους ανταγωνιστές. Η μετάβαση σε μια ανοιχτή αρχιτεκτονική προσέγγιση είναι ένα από τα πιο γνωστά χαρακτηριστικά του Διαδικτύου [83].

Το 1988, ο Cerf, ο τότε αντιπρόεδρος της Corporation for National Research Initiatives, έλαβε άδεια από το Federal Networking Council για τη σύνδεση της υπηρεσίας MCI Mail, η οποία παρείχε εμπορικές υπηρεσίες ηλεκτρονικού ταχυδρομείου μέσω τηλεφωνικών γραμμών με χρήση μόντεμ από το 1983. Αυτή η εξουσιοδότηση βοήθησε έτσι ώστε να αρθεί ο περιορισμός που απαγόρευε στις εμπορικές ηλεκτρονικές επικοινωνίες να συνυπάρχουν με τις κυβερνητικές υπηρεσίες. Με την έναρξη της συγκεκριμένης υπηρεσίας που ξεκίνησε το 1989, άνοιξαν τις πύλες και για άλλους εμπορικούς παίκτες. Οι σημαντικότεροι πάροχοι email της εποχής (συμπεριλαμβανομένων των AOL, CompuServe και Telemet's Telemail), οι οποίοι παρείχαν μηνύματα μέσω τηλεφωνικών μόντεμ, ακολούθησαν το παράδειγμα της MCI Mail και μετέφεραν τις υπηρεσίες τους στο αναδυόμενο Διαδίκτυο [16].

Το 1989 ο Άγγλος Tim Berners Lee (εικόνα 4), ερευνητής του Europeenne pour la Recherche Nucleaire (CERN) στη Γενεύη, πρότεινε ένα διεθνές σύστημα πρωτοκόλλων που περιελάμβανε την δημιουργία ενός κατανεμημένου διακομιστή υπερμέσων. Ο Berners-Lee το ονόμασε World Wide Web (WWW), δημιούργησε τον πρώτο WWW client (ένα πρόγραμμα περιήγησης) και το μεγαλύτερο μέρος του λογισμικού επικοινωνιών, καθορίζοντας τις διευθύνσεις URL (Uniform Resource Locator), HTTP (Hypertext Transfer Protocol) και HTML. Το λογισμικό υπερμέσων επέτρεψε στους χρήστες να έχουν πρόσβαση, να συνδέονται και να επικοινωνούν σε έναν ενιαίο παγκόσμιο ιστό πληροφοριών. Ο παγκόσμιος ιστός σηματοδότησε έτσι την ένωση τριών διαφορετικών μορφών καινοτομίας: Προσωπικός υπολογιστής, δικτύωση

και λογισμικό σύνδεσης [14]. Χρησιμοποιώντας υπερσυνδέσμους ενσωματωμένους μέσα στο υπερκείμενο, οι χρήστες ενεργούσαν ως παραγωγοί πληροφοριών συνδέοντας αρχεία που περιέχουν κείμενο, ήχο και γραφικά για τη δημιουργία ιστοσελίδων. Οι πηγές πληροφοριών που συνδέονται με αυτόν τον τρόπο μπορούσαν να εντοπιστούν σε οποιονδήποτε υπολογιστή που είναι επίσης μέρος του δικτύου. Κάθε πηγή πληροφοριών μπορεί από μόνη της να συνδέεται με έναν απεριόριστο αριθμό ιστοσελίδων. Το υπερκείμενο και οι υπερσύνδεσμοι επιτρέπουν στους χρήστες να περιηγηθούν άκοπα από μια πηγή πληροφοριών σε μια άλλη, αποφασίζοντας ποιες πληροφορίες επιθυμούν να προβληθούν στο πρόγραμμα περιήγησής τους και ποιο σύνδεσμο θέλουν να εξερευνήσουν ή να παραλείψουν [3].



Εικόνα 4. Tim Berners-Lee

Κατά τη δεκαετία του 1990 παρατηρήθηκε μία μαζική επέκταση του διαδικτύου. Η προσβασιμότητα στο Internet, οι πολλαπλές χρήσεις του και η αποκεντρωμένη φύση του ήταν καθοριστικής σημασίας για αυτήν την ταχεία ανάπτυξη. Επιχειρηματικοί και προσωπικοί υπολογιστές με διαφορετικά λειτουργικά συστήματα μπορούσαν να ενταχθούν στο καθολικό αυτό δίκτυο. Το Διαδίκτυο έγινε παγκόσμιο φαινόμενο, περισσότερες χώρες και άνθρωποι ενώθηκαν και πρωτοπόροι της εποχής επέκτειναν τους ορίζοντες της πλατφόρμας με νέες, ευφάνταστες καινοτομίες. Το 1990, το project ARPANET τελείωσε επίσημα όταν παρέδωσε τον έλεγχο του backbone του Διαδικτύου στο Εθνικό Ίδρυμα Επιστημών [14]. Το 1991, ιδρύθηκε το Internet Society και χώρες

όπως η Κροατία, το Χονγκ Κονγκ , η Ουγγαρία, η Πολωνία, η Πορτογαλία , η Σιγκαπούρη, η Νότια Αφρική, η Ταϊβάν και η Τυνησία εντάχθηκαν στο δίκτυο NSFnet του οποίου η ραχοκοκαλιά αναβαθμίστηκε σε DS-3 (44.736 Mbps) καθώς η κίνηση ανέβηκε σε 1 τρισεκατομμύριο byte και 10 δισεκατομμύρια πακέτα το μήνα. Εκείνη τη χρονιά, το 1991, υπήρξε επίσης ορόσημο καθώς το δημοφιλές πρόγραμμα κρυπτογράφησης PGP (Pretty Good Privacy) κυκλοφόρησε από τον Philip Zimmerman.

Το 1992, ο αριθμός των Internet hosts έφτασε το 1 εκατομμύριο με σχεδόν 50 ιστοσελίδες. Το 1993, υπήρχαν 623 Ιστοσελίδες στον κόσμο. Ο Παγκόσμιος Ιστός πολλαπλασιάστηκε με ετήσιο ρυθμό αύξησης κατά 341.634%. Στα τέλη του 1993, υπήρχαν 2,1 εκατομμύρια Internet hosts. Το 1995, σημαντικοί φορείς όπως η British Telecom, η France Telecom, η Deutsche Telekom, η Swedish Telecom, η Norwegian Telecom και η Finnish Telecom, μεταξύ άλλων, παρείχαν υπηρεσίες διαδικτύου. Περισσότεροι από 30.000 ιστότοποι λειτουργούσαν και ο αριθμός διπλασιαζόταν κάθε δύο μήνες [10]. Ο αριθμός των Internet hosts υπερδιπλασιάστηκε σε ένα έτος, φθάνοντας τα 6,6 εκατομμύρια. Τα μέσα της δεκαετίας του 1990 ήταν τα χρόνια που το Διαδίκτυο καθιερώθηκε ως το επίκεντρο της επικοινωνίας, της ενημέρωσης και των επιχειρήσεων, ενώ ο browser Netscape κατείχε την 3η μεγαλύτερη αξία μετοχής στον NASDAQ. Ταυτόχρονα, πολλοί άνθρωποι άρχισαν να δημιουργούν τις δικές τους προσωπικές ιστοσελίδες. Το Διαδίκτυο συνέχισε να αναπτύσσεται με ταχύ ρυθμό, προσελκύοντας όλο και περισσότερους ανθρώπους χρησιμοποιώντας το καθημερινά για: έρευνα, επιχειρηματικότητα, εμπόριο, ψυχαγωγία, ταξίδια και ουσιαστικά οποιαδήποτε ανάγκη. Για κάθε αναδυόμενη ανάγκη υπήρχε ο αντίστοιχος επιχειρηματίας που εκμεταλλευόταν την ευκαιρία ανοίγοντας ένα ιστότοπο για να την ικανοποιήσει.

1.2. Η σημερινή μορφή του διαδικτύου

Το Διαδίκτυο έχει οδηγήσει και αναμένεται να οδηγήσει σε περαιτέρω αλλαγές στον τρόπο επικοινωνίας των ανθρώπων, στον τρόπο εργασίας αλλά και στην αξιοποίηση του ελεύθερου χρόνου τους. Τα στοιχεία δείχνουν ότι το Διαδίκτυο έχει αλλάξει τους ρυθμούς της καθημερινής ζωής στην εργασία, στα σχολεία, στα πανεπιστήμια και στα νοσοκομεία. Χρησιμοποιείται για μια ευρεία ποικιλία σκοπών, όπως αναζήτηση πληροφοριών, τα διαδικτυακά παιχνίδια και η επικοινωνία.

Η τρέχουσα επιστημονική έρευνα καταδεικνύει ότι το Διαδίκτυο χρησιμοποιείται σήμερα από περισσότερα άτομα, σε περισσότερες χώρες, με πολλούς διαφορετικούς τρόπους:

- Η χρήση του Διαδικτύου έχει διαδοθεί από κυρίως λευκούς και νεαρούς Βορειοαμερικανούς άντρες σε όλο τον υπόλοιπο κόσμο. Το φύλο και η ηλικία έπαψαν να αποτελούν εμπόδια. Αν και ο αριθμός των οικονομικά αδυνάτων, λιγότερο μορφωμένων και μη λευκών που χρησιμοποιούν το Διαδίκτυο είναι ακόμα σχετικά μικρός, το ψηφιακό χάσμα μεταξύ τέτοιων ομάδων και παραδοσιακών χρηστών του Διαδικτύου κλείνει [93].
- Οι περισσότεροι χρήστες του Διαδικτύου στέλνουν και λαμβάνουν email, ενώ η ηλεκτρονική αλληλογραφία χρησιμοποιείται πλέον ευρύτερα από το τηλέφωνο.
- Τον Σεπτέμβριο του 2001, οι χρήστες του Διαδικτύου πέρασαν κατά μέσο όρο 10 ώρες και 19 λεπτά στο διαδίκτυο, αύξηση 7% από τις εννέα ώρες και 14 λεπτά που καταγράφηκαν ένα χρόνο νωρίτερα [53].

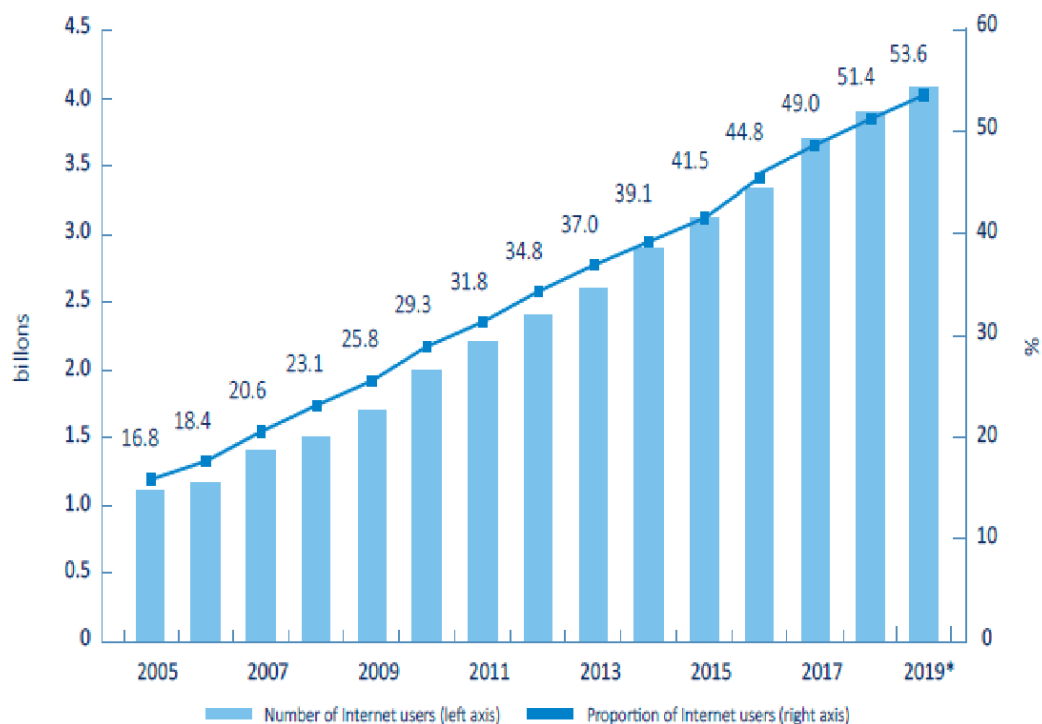
Το Διαδίκτυο δεν είναι μια μονοδιάστατη τεχνολογία. Αντίθετα, συγχωνεύει πολλές τεχνολογίες σε ένα μέσο. Ένα σύνολο τρεχουσών και αναμενόμενων αλλαγών δημιουργεί δυνατότητες - κοινωνικά και οικονομικά - για το πώς το Διαδίκτυο δύναται να επηρεάσει την καθημερινή ζωή:

- ✓ Υψηλότερες ταχύτητες: Η ευρυζωνική επικοινωνία διευκολύνει την ταχύτερη ανταλλαγή μεγάλων ποσοτήτων δεδομένων, άμεσων μηνυμάτων, ανατροφοδότησης, συνημμένων εγγράφων εικόνας, φωνής και τηλεδιασκέψεων.
- ✓ Μόνιμη συνδεσιμότητα: Η διαρκής σύνδεση στο διαδίκτυο χωρίς ή με ελάχιστο κόστος αποτέλεσε βασικό παράγοντα εξάπλωσης της εν λόγω τεχνολογίας.
- ✓ Εξατομίκευση: Οι υπολογιστικές επικοινωνίες αναπτύσσονται με γνώμονα την εξατομίκευση, δηλαδή με περισσότερο έλεγχο ως προς το με ποιους επικοινωνούμε, πότε και για τι. Αυτή η μορφή επικοινωνίας και οι επακόλουθες αλληλεπιδράσεις προσαρμόζονται περισσότερο στις ατομικές προτιμήσεις και ανάγκες.
- ✓ Ασύρματη φορητότητα: Η ασύρματη συνδεσιμότητα επιτρέπει την πρόσβαση στο Διαδίκτυο οπουδήποτε και εν κινήσει.
- ✓ Παγκοσμιοποιημένη συνδεσιμότητα. Η παγκόσμια διάδοση του Διαδικτύου αποτελεί και έναν εν δυνάμει παράγοντα συρρίκνωσης των κοινωνικό-οικονομικών αποκλίσεων μεταξύ αναπτυγμένων και αναπτυσσόμενων χωρών.

Οι επιστήμονες συμφωνούν ότι η χρήση του διαδικτύου μετασχηματίζει τον τρόπο επικοινωνίας των κοινωνιών όπως τον ξέραμε μέχρι σήμερα με έντονα αντικρουόμενους τρόπους. Ειδικότερα:

- Το Διαδίκτυο περιορίζει την δια ζώσης επικοινωνία: Το Διαδίκτυο μέσω των δυνατοτήτων ψυχαγωγίας και αναζήτησης πληροφοριών, απομακρύνει τους ανθρώπους από την οικογένεια και τους φίλους τους. Επιπλέον, διευκολύνοντας την παγκόσμια επικοινωνία, μειώνει το ενδιαφέρον για την συμμετοχή στα τοπικά δρώμενα και την ενασχόληση με την πολιτική [62].

- Το Διαδίκτυο βελτιώνει την επικοινωνία: Το Διαδίκτυο παρέχει τα μέσα για φθηνή και εύκολη επικοινωνία με άλλες απομακρυσμένες κοινότητες κοινού ενδιαφέροντος [4]. Μέσω του χαμηλού κόστους και της ασύγχρονης φύσης του, μεγιστοποιεί την επικοινωνία μεταξύ φίλων και οικογενειών, ειδικά την επαφή με εκείνους που βρίσκονται μακριά.
- Το Διαδίκτυο αλλάζει τον τρόπο επικοινωνίας: Μια τρίτη προοπτική βλέπει το Διαδίκτυο ως ένα άλλο μέσο επικοινωνίας για τη διευκόλυνση των υπάρχουσών κοινωνικών σχέσεων και ακολουθώντας μοτίβα αστικής κοινωνικοποίησης. Οι άνθρωποι χρησιμοποιούν το Διαδίκτυο για να διατηρήσουν τις υπάρχουσες κοινωνικές τους επαφές με εναλλακτικούς τρόπους έναντι του τηλεφώνου ή της δια ζώσης επικοινωνίας.



Note: * ITU estimate. Source: ITU.

Εικόνα 5. Αριθμός χρηστών Διαδικτύου από το 2005 έως το 2019

Αναφορικά με την επίδραση του διαδικτύου στα κοινωνικά δρώμενα, σχεδόν 3 δισεκατομμύρια συνδεδεμένοι καταναλωτές και επιχειρηματίες αναζητούν, ψωνίζουν, συμμετέχουν σε κοινωνικά δίκτυα, συναλλάσσονται και αλληλεπιδρούν καθημερινά χρησιμοποιώντας προσωπικούς υπολογιστές και όλο και περισσότερο κινητές συσκευές (Euromonitor International). Η ψηφιακή οικονομία, η οποία συνέβαλε με 2,3 τρισεκατομμύρια δολάρια στο ΑΕΠ των G20 το 2010 και 4 τρισεκατομμύρια δολάρια το 2016, αυξάνεται με 10% ετησίως - σημαντικά ταχύτερα από τη συνολική οικονομία των G20. Η ανάπτυξη είναι ακόμη υψηλότερη στις αναπτυσσόμενες οικονομίες, με 15-25% ετησίως. Η ψηφιακή οικονομία δεν είναι μόνο μία σημαντική πηγή θέσεων εργασίας, αλλά και οι ψηφιακές τεχνολογίες επιτρέπουν επίσης εκτεταμένες κοινωνικές και πολιτικές αλλαγές.

Ο αντίκτυπος του Διαδικτύου εκτείνεται πολύ πέρα από το ΑΕΠ. Όλα τα είδη οικονομικής δραστηριότητας, όπως το ηλεκτρονικό εμπόριο, η διαδικτυακή διαφήμιση και άλλες οικονομικές δραστηριότητες καταναλωτών, δεν καταγράφονται ικανοποιητικά στα στοιχεία του ΑΕΠ. Το Διαδίκτυο έχει τεράστιο αντίκτυπο στην παραγωγικότητα, δίνοντας στις επιχειρήσεις πρόσβαση σε νέες αγορές, πελάτες και προμηθευτές. Επιτρέπει νέα επιχειρηματικά μοντέλα και εξοικονομεί χρόνο και ενέργεια για αμέτρητα άτομα κάθε μέρα. Υπάρχουν επίσης ευρύτερες κοινωνικές επιπτώσεις. Οι ψηφιακές τεχνολογίες ήδη μετασχηματίζουν βασικές κοινωνικές υπηρεσίες, όπως η εκπαίδευση και η υγειονομική περίθαλψη, και η συναλλαγή με τις κυβερνητικές δομές. Επιπλέον, οι δυνατότητες για μαζικές βελτιώσεις σε χρηστικές υπηρεσίες, όπως οι μεταφορές, και η παροχή ενέργειας είναι σαφείς.

Τέλος το Internet of Things αποτελεί τη νέα τεχνολογική εξέλιξη στο Διαδίκτυο, που αναμένεται να αλλάξει τον κόσμο όπως τον γνωρίζουμε μέχρι σήμερα. Το Internet of Things αναφέρεται στη γενική ιδέα καθημερινών αντικειμένων, τα οποία είναι αναγνώσιμα, εντοπίσιμα και διευθυνσιοδοτούμενα μέσω συσκευών ανίχνευσης πληροφοριών ή / και ελεγχόμενα μέσω του Διαδικτύου, ανεξάρτητα από τα μέσα επικοινωνίας (είτε μέσω RFID, ασύρματου LAN, δίκτυα ευρείας περιοχής ή άλλα μέσα). Τα αντικείμενα αυτά περιλαμβάνουν όχι μόνο ηλεκτρονικές συσκευές ή προϊόντα ανώτερης τεχνολογικής ανάπτυξης, όπως οχήματα και εξοπλισμό, αλλά και πράγματα που συνήθως δεν θεωρούμε ηλεκτρονικά - όπως φαγητό, ρούχα, καρέκλες, ζώα, δέντρα, νερό κ.λπ.

Τα βασικά χαρακτηριστικά του IoT είναι τα εξής:

- Διασυνδεσιμότητα: Όσον αφορά το IoT, οτιδήποτε μπορεί να διασυνδεθεί με την παγκόσμια υποδομή πληροφοριών και επικοινωνιών.
- Things-related Υπηρεσίες: Το IoT είναι σε θέση να παρέχει υπηρεσίες που σχετίζονται με αντικείμενα εντός προφανώς των περιορισμών της φύσης των αντικειμένων.
- Ετερογένεια: Οι συσκευές στο IoT είναι ετερογενείς καθώς βασίζονται σε διαφορετικές πλατφόρμες και δίκτυα υλικού. Μπορούν να αλληλεπιδράσουν με άλλες συσκευές ή πλατφόρμες υπηρεσιών μέσω διαφορετικών δικτύων.
- Δυναμικές αλλαγές: Η κατάσταση των συσκευών αλλάζει δυναμικά, π.χ. ενεργοποίηση και απενεργοποίηση, σύνδεση ή / και αποσύνδεση, το περιβάλλον των συσκευών, συμπεριλαμβανομένης της θέσης και της ταχύτητας. Επιπλέον, ο αριθμός των συσκευών μπορεί να αλλάξει δυναμικά.
- Τεράστια κλίμακα: Ο αριθμός των διαχειρίσιμων συσκευών που επικοινωνούν μεταξύ τους ενδέχεται να είναι τάξης μεγέθους μεγαλύτερου από τις συσκευές που είναι συνδεδεμένες στο τρέχον Διαδίκτυο. Ακόμη πιο κρίσιμη θα είναι η διαχείριση των δεδομένων που παράγονται καθώς και η ερμηνεία τους.
- Ασφάλεια: Η ανάπτυξη του IoT θέτει επιπλέον καίρια ζητήματα ασφάλειας, που κατά κύριο λόγο έχουν να κάνουν με την προστασία των προσωπικών δεδομένων.
- Συνδεσιμότητα: Η συνδεσιμότητα περιλαμβάνει την πρόσβαση καθώς και τη συμβατότητα του δικτύου.

Οι πιθανές εφαρμογές του IoT είναι πολυάριθμες και ποικίλες, που διαπερνούν σχεδόν όλους τους τομείς της καθημερινής ζωής των ατόμων και των επιχειρήσεων. Οι εφαρμογές του IoT καλύπτουν «έξυπνα» περιβάλλοντα σε τομείς όπως: μεταφορές, σπίτια, πόλεις, γεωργία, βιομηχανία, αλυσίδες εφοδιασμού, υγειονομική περίθαλψη, πολιτισμός και τουρισμός, περιβάλλον και ενέργεια.

1.3. Κοινωνικά δίκτυα

Η έννοια των κοινωνικών δικτύων, που καταγράφεται για πρώτη φορά το 1954 από τον J. A. Barnes (εικόνα 6) στο προφητικό άρθρο του «Class and Committees in a Norwegian Island Parish», αποτελεί κλάδο μελέτης πολλαπλών επιστημών όπως της κοινωνιολογίας, της ανθρωπολογίας, της γεωγραφίας, της κοινωνικής ψυχολογίας, και της πληροφορικής τις τελευταίες δεκαετίες.



Εικόνα 6. J.A. Barnes

Ο άνθρωπος που δημιούργησε το σύγχρονο πρότυπο των κοινωνικών δικτύων ήταν ο Stanley Milgram. Μελέτησε το πρόβλημα του μικρόκοσμου το οποίο περιγράφεται μέσω έμμεσων σχέσεων, δηλαδή ακόμα κι αν δύο άτομα δεν γνωρίζονται μεταξύ τους άμεσα, μπορούν να μοιραστούν μια αμοιβαία σχέση μέσω ενός άλλου κοινού ατόμου [59]. Το θεωρητικό μοντέλο του προβλήματος δημιουργήθηκε από τους Pool και Kochen και χρησίμευσε ως βασικό στοιχείο για την έρευνα του Milgram η οποία ήταν καθαρά εικονογραφική. Ο Stanley Milgram πραγματοποίησε δύο πειράματα (Kansas Study and Nebraska Study) στα οποία ζήτησε από ένα σημαντικό αριθμό ατόμων από μια πόλη να διαβιβάσουν ένα γράμμα σε ένα επιλεγμένο άτομο σε μια άλλη

απομακρυσμένη πόλη, δίνοντας την επιστολή σε ένα άτομο που γνώριζαν σε ικανοποιητικό βαθμό. Στη συνέχεια, ανέλυσε τις διαδρομές προώθησης των επιστολών και κατέληξε στο συμπέρασμα ότι οι άνθρωποι στις ΗΠΑ σχηματίζουν ένα κοινωνικό δίκτυο και συνδέονται με αυτό το δίκτυο με «έξι βαθμούς διαχωρισμού», γεγονός που σημαίνει ότι ένα μήνυμα σε ένα τέτοιο δίκτυο παραδίδεται κατά μέσο όρο μέσω πέντε ενδιάμεσων.

Η συνεχώς αυξανόμενη δημοτικότητα του Παγκόσμιου Ιστού και του Διαδικτύου συσχετίζεται με έναν εκθετικά αυξανόμενο αριθμό διαφόρων τύπων υπηρεσιών. Τα άτομα που χρησιμοποιούν αυτές τις υπηρεσίες έχουν δημιουργήσει ένα νέο είδος εικονικών κοινωνιών που συνήθως ονομάζονται κοινωνικά δίκτυα ή εικονικές κοινότητες. Τα κύρια χαρακτηριστικά που διακρίνουν τα κοινωνικά δίκτυα στο Διαδίκτυο από τα δίκτυα που δημιουργούνται βάσει αλληλεπιδράσεων στον πραγματικό κόσμο είναι τα εξής:

- Έλλειψη φυσικής επαφής
- Συνήθως η έλλειψη σαφούς και αξιόπιστης συσχέτισης μεταξύ της ταυτότητας του μέλους στην εικονική κοινότητα και της ταυτότητάς τους στον πραγματικό κόσμο.
- Η δυνατότητα πολυτροπικής επικοινωνίας, ταυτόχρονα με πολλά μέλη.
- Η απλότητα δημιουργίας ή διάλυσης επαφών ή σχέσεων.
- Η σχετικά υψηλή ευκολία συλλογής δεδομένων σχετικά με την επικοινωνία ή τις κοινές δραστηριότητες και την περαιτέρω επεξεργασία τους.
- Χαμηλότερη αξιοπιστία των δεδομένων σχετικά με τους χρήστες. Οι χρήστες υπηρεσιών Διαδικτύου παρέχουν συχνά ψεύτικα προσωπικά δεδομένα λόγω ανησυχιών περί απορρήτου.

Οι κυριότερες κατηγορίες κοινωνικών δικτύων σήμερα στο Διαδίκτυο θα μπορούσαν να συνοψιστούν στις εξής παρακάτω:

➤ Υπηρεσίες ηλεκτρονικού ταχυδρομείου

Τα συστήματα ηλεκτρονικού ταχυδρομείου αποτελούν έναν αμφίδρομο και ασύγχρονο τρόπο επικοινωνίας επιτρέποντας σε χρήστες, από διαφορετικά μέρη και με διαφορετικό λογισμικό, να επικοινωνούν μεταξύ τους ανταλλάσσοντας μηνύματα [94]. Το μοντέλο αυτό αποτελεί την βάση για τη δημιουργία ενός κοινωνικού δικτύου, στο οποίο οι διευθύνσεις ηλεκτρονικού ταχυδρομείου αντιπροσωπεύουν φυσικές κοινωνικές οντότητες. Η σχέση σε ένα κοινωνικό δίκτυο που βασίζεται σε email μπορεί να προέλθει τόσο από την επικοινωνία μεταξύ αποστολέων και παραληπτών όσο και από τα βιβλία διευθύνσεων που διατηρούν οι χρήστες. Οι καταχωρημένες διευθύνσεις ηλεκτρονικού ταχυδρομείου και οι πληροφορίες σχετικά με την επικοινωνία (αρχεία καταγραφής διακομιστών SMTP) καθώς και ορισμένες πληροφορίες σχετικά με τα ιδιωτικά βιβλία διευθύνσεων που είναι αποθηκευμένα στους servers μπορούν να ληφθούν από ξεχωριστούς, κατανεμημένους διακομιστές αλληλογραφίας, π.χ. Gmail, Yahoo! Mail, MSN Hotmail, AOL Mail, κ.λπ. Από την άλλη πλευρά, πολλοί χρήστες email χρησιμοποιούν δικούς τους τοπικούς email agents (MTA) διατηρώντας τα βιβλία διευθύνσεων μόνο σε τοπικό χώρο αποθήκευσης. Προφανώς, αυτά τα δεδομένα δεν είναι διαθέσιμα για εξωτερική επεξεργασία

➤ Instant messengers

Τα instant messengers (IM) όπως το ICQ, το Skype, το Windows Live Messenger (πρώην MSN Messenger), το AOL Instant Messenger (AIM), το Yahoo! Messenger, το Google Talk (GTalk) εξυπηρετούν την ανταλλαγή πληροφοριών μεταξύ δύο ατόμων ή περιορισμένης ομάδας ατόμων. Η ραγδαία ανάπτυξη συνδέσεων υψηλής ταχύτητας βοήθησε στην αποστολή όχι μόνο μηνυμάτων κειμένου αλλά φωνής και βίντεο. Αυτά τα χαρακτηριστικά ενσωματώνονται σε πολλά συστήματα VoIP, π.χ. Skype ή Ventrillo, συμβάλλοντας στην αύξηση της κοινωνικής παρουσίας [94]. Σήμερα, οι περισσότεροι IMs υποστηρίζουν και άλλα είδη καναλιών επικοινωνίας. Ωστόσο, ο πρωταρχικός στόχος τους υπήρξε αποκλειστικά η ανταλλαγή πληροφοριών κειμένου. Σε αντίθεση με τα συστήματα email, ένα instant messenger παρέχει ευκολότερο τρόπο συνεργασίας, επειδή προσφέρει επικοινωνία σε πραγματικό χρόνο. Επιπλέον, ο κάθε χρήστης έχει την δυνατότητα να ελέγχει εάν άλλα άτομα από τη λίστα επαφών τους είναι διαθέσιμα ή όχι καθώς δίνεται η δυνατότητα ορισμού της κατάστασης του

χρήστη, π.χ. online, away, not available. Δεδομένου ότι τα περισσότερα δεδομένα που σχετίζονται με μεμονωμένους χρήστες αποθηκεύονται τοπικά στους υπολογιστές τους, η απόκτηση δεδομένων επικοινωνίας που είναι απαραίτητα για τη δημιουργία του κοινωνικού δικτύου από τους IMs μπορεί να είναι πολύ δύσκολη. Παρόλα αυτά, ορισμένοι χειριστές IM παρέχουν τη δυνατότητα μεταφοράς και διατήρησης ορισμένων τοπικών δεδομένων στον κεντρικό διακομιστή.

➤ Blogs

Οι υπηρεσίες blogs όπως το WordPress, το Blogger, το LiveJournal ή το Windows Live Spaces, δεν λειτουργούν αποκλειστικά ως διαδικτυακά ημερολόγια, αλλά μπορούν επίσης να θεωρηθούν ως κοινωνικό δίκτυο [34]. Η σχέση μεταξύ δύο χρηστών μπορεί να δημιουργηθεί με βάση τη λίστα των αγαπημένων, κοινά χρησιμοποιούμενα tags ή με βάση τα σχόλια που γίνονται στο blog. Αρκετά παρόμοιες λειτουργίες παρέχουν υπηρεσίες microblog όπως το Twitter [39], εκτός από το περιορισμένο μήκος των δημοσιευμένων μηνυμάτων, π.χ. έως 160 χαρακτήρες.

➤ Site κοινωνικής δικτύωσης

Τα τελευταία χρόνια, η δημοτικότητα των ιστότοπων κοινωνικής δικτύωσης (SNS) έχει αυξηθεί ραγδαία. Ο κύριος στόχος τους είναι η δημιουργία, η διατήρηση και η παρουσίαση κοινωνικών σχέσεων στους χρήστες τους, καθώς και το πιθανό κοινωνικό ταίριασμα μεταξύ τους. Για να το επιτύχουν, κάνουν χρήση ορισμένων πρόσθετων υπηρεσιών επικοινωνίας όπως email, chat, instant messaging. Τυπικά παραδείγματα ιστότοπων κοινωνικής δικτύωσης είναι: Facebook, Friendster, Orkut, Tribe, Ecademy, MySpace και LinkedIn, τα οποία δημιουργούνται και συντηρούνται από εμπορικές εταιρείες. Τα κύρια χαρακτηριστικά των ιστότοπων κοινωνικής δικτύωσης είναι η αυτοέκφραση (διατήρηση προσωπικών προφίλ), η παρουσίαση προσωπικών επιτευγμάτων, σχέσεων με άλλους και αμοιβαίας επικοινωνίας. Υπάρχουν διάφοροι τρόποι επικοινωνίας μεταξύ των χρηστών σε αυτούς τους διαδικτυακούς ιστότοπους δικτύωσης, οι οποίοι ποικίλλουν ανάλογα με τη λειτουργικότητα της πύλης: email, chat, φόρουμ, blog, σχόλια, μαρτυρίες, άλμπουμ φωτογραφιών / ταινιών κ.λπ. Συνολικά, όσο περισσότερα κανάλια επικοινωνίας υποστηρίζονται από το δίκτυο, τόσο

αυξάνει και η χρηστικότητα της υπηρεσίας, παρέχοντας περισσότερες ευκαιρίες για τη δημιουργία νέων και τη διατήρηση υπαρχουσών σχέσεων εντός του συστήματος.

➤ Συστήματα κοινής χρήσης πολυμέσων

Τα συστήματα κοινής χρήσης ή δημοσίευσης πολυμέσων (π.χ. Flickr, YouTube, Photobucket, ImageShack, Break.com, Google Video, Metacafe, OneWorldTV) επιτρέπουν στον χρήστη να ανεβάζει και να διαχειρίζεται το δικό του περιεχόμενο πολυμέσων, όπως φωτογραφίες, βίντεο, κινούμενα σχέδια. Κάθε ένα από τα αντικείμενα πολυμέσων μπορεί να επισημανθεί από τον δημιουργό. Με άλλα λόγια, ένας χρήστης μπορεί να περιγράψει το περιεχόμενο του με μία ή περισσότερες σύντομες φράσεις που συνήθως δηλώνουν το περιεχόμενο αυτού του στοιχείου. Αυτές οι ετικέτες που χρησιμοποιούνται από τα μέλη μπορούν να αποτελέσουν τη βάση για τη δημιουργία ενός κοινωνικού δικτύου, δημιουργώντας μία σχέση μεταξύ δύο μελών εάν και οι δύο έχουν χρησιμοποιήσει τουλάχιστον μία κοινή ετικέτα για να περιγράψουν τα αντικείμενα των πολυμέσων τους. Ταυτόχρονα, οι χρήστες έχουν την ευκαιρία να αλληλεπιδράσουν, να συνεργαστούν και να επηρεάσουν ο ένας τον άλλον με διαφορετικούς τρόπους. Ως εκ τούτου, δεν μπορούν μόνο να επισημάνουν τα στοιχεία που έχουν δημοσιεύσει, αλλά και να σχολιάσουν αντικείμενα που έχουν προστεθεί από άλλους, να τα συμπεριλάβουν στα αγαπημένα τους κ.λπ. Επιπλέον, οι χρήστες έχουν την ευκαιρία να δημιουργήσουν νέες, άμεσες σχέσεις με άλλους χρήστες του συστήματος.

➤ Συστήματα δημοπρασίας

Ο κύριος στόχος των συστημάτων δημοπρασίας είναι να επιτρέπουν στους χρήστες να πωλούν και να αγοράζουν προϊόντα από και προς άλλους χρήστες. Παραδείγματα τέτοιων συστημάτων είναι το eBay ή το OnSale, όπου άνθρωποι καθώς και επιχειρήσεις μπορούν να αγοράσουν και να πουλούν τα αγαθά και υπηρεσίες παγκοσμίως. Προφανώς, κάθε άτομο που θέλει να χρησιμοποιήσει ένα τέτοιο σύστημα πρέπει να εγγραφεί με ένα μοναδικό όνομα που γίνεται η ταυτότητα του. Μετά τη σύνδεση στο σύστημα, τα μέλη μπορούν να δημιουργήσουν νέους πλειστηριασμούς, καθώς και να αγοράσουν προϊόντα ή υπηρεσίες, δημιουργώντας φυσικές σχέσεις μεταξύ αγοραστών και πωλητών. Ωστόσο, αυτός δεν είναι ο μόνος τύπος σχέσεων που μπορεί να προσδιοριστεί στα συστήματα αυτού του είδους. Οι πιθανοί αγοραστές

μπορούν να υποβάλουν στον πωλητή μια ερώτηση αναφορικά με τα προϊόντα που προσφέρει χρησιμοποιώντας πρόσθετες λειτουργίες του συστήματος. Συνήθως, οι πωλητές μπορούν να καταργήσουν ορισμένες προσφορές που παρέχονται από αναξιόπιστους χρήστες. Επιπλέον, οι χρήστες έχουν τη δυνατότητα να καλέσουν άμεσα ορισμένα επιλεγμένα μέλη να συμμετάσχουν στις δημοπρασίες που διαχειρίζονται. Μόλις ολοκληρωθεί η δημοπρασία, τόσο ο νικητής όσο και ο πωλητής μπορούν να σχολιάσουν την ποιότητα της υπηρεσίας [91].

➤ Εικονικοί κόσμοι και διαδικτυακά παιχνίδια για πολλούς παίκτες

Οι εικονικοί κόσμοι και τα online παιχνίδια για πολλούς παίκτες (Second Life, Sims, World of Warcraft) είναι παραδείγματα συστημάτων, στα οποία οι χρήστες διατηρούν τα δικά τους είδωλα που τους αντιπροσωπεύουν στον εικονικό κόσμο. Οι άνθρωποι μπορούν να δημιουργήσουν όχι μόνο το είδωλό τους αλλά και ολόκληρη τη γειτονιά στην οποία θέλουν να ζήσουν, οδηγώντας σε μία κατάσταση που οι κοινωνικές οντότητες δημιουργούν από μόνες τους μία δεύτερη ζωή παράλληλη με την πραγματική. Στα διαδικτυακά παιχνίδια, οι χρήστες μπορούν να συνεργαστούν με άλλους παίκτες, συμμετέχοντας σε κοινές αποστολές. Αρκετές φορές ορίζονται αποστολές που δεν μπορούν να επιτευχθούν αποκλειστικά από ένα άτομο [21].

➤ Συστήματα ανταλλαγής γνώσης

Οι αγορές γνώσης (Experts-Exchange, Mahalo Answers, Yahoo! Answers, Knowledge Search, ChaCha.com, Answly.com) είναι παραδείγματα κοινωνικών δικτύων που επιτρέπουν στους χρήστες, αφενός, να δημοσιεύουν ένα αίτημα και να ορίζουν ένα αντίτιμο για τη σχετική απάντηση καθώς και από την άλλη να απαντήσουν σε ερωτήσεις που έχουν υποβάλει άλλοι με το αντίστοιχο αντίτιμο. Επιπλέον, οι χρήστες έχουν την ευκαιρία να αξιολογήσουν και να σχολιάσουν τις απαντήσεις που έχουν λάβει από άλλους [50].

1.4. Ιδιωτικότητα στο διαδίκτυο

Το Διαδίκτυο είναι ένα διεθνές και σε μεγάλο βαθμό ανεξέλεγκτο δίκτυο. Αυτό σημαίνει ότι οι νόμοι οποιασδήποτε χώρας δεν ισχύουν συνήθως για δραστηριότητες Διαδικτύου που προέρχονται από άλλες χώρες. Το απόρρητο των προσωπικών δεδομένων υφίσταται όταν ελέγχεται η χρήση και η διανομή των προσωπικών πληροφοριών. Οι παραβιάσεις της ιδιωτικής ζωής συμβαίνουν όταν τα άτομα δεν μπορούν να διατηρήσουν ουσιαστικό κάποιο βαθμό ελέγχου των προσωπικών τους πληροφοριών και της χρήσης τους. Η ανάπτυξη του Διαδικτύου με την ταχεία πρόοδο της τεχνολογίας εγείρει τις έντονες ανησυχίες των χρηστών αναφορικά με το προσωπικό απόρρητο ενώσω είναι συνδεδεμένοι στο διαδίκτυο [51].

Το Διαδίκτυο επιτρέπει την αποτελεσματική, φθηνή συλλογή πληροφοριών χωρίς τη απαραίτητη πάντα συγκατάθεση των χρηστών του. Δύναται να «παρακολουθεί» τους χρήστες με μοναδικούς τρόπους, όπως τις προτιμήσεις και τα ενδιαφέροντα τους ή ακόμη και τα στοιχεία της πιστωτικής τους κάρτας. Σε σχετική έρευνα η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) των ΗΠΑ ανακάλυψε ότι το 92,8 τοις εκατό των ιστότοπων συγκεντρώνει τουλάχιστον έναν τύπο πληροφοριών αναγνώρισης (όνομα, διεύθυνση ηλεκτρονικού ταχυδρομείου, ταχυδρομική διεύθυνση), ενώ το 56,8 τοις εκατό συλλέγει τουλάχιστον έναν τύπο δημογραφικών πληροφοριών (φύλο και προτιμήσεις). Η χρηματική αξία αυτών των πληροφοριών εξηγεί γιατί οι ιστότοποι συλλέγουν προσωπικά στοιχεία.

Οι απειλές προστασίας του ιδιωτικού απορρήτου κυρίως περιλαμβάνουν:

- Αν επισκέψεις σε ιστότοπους παρακολουθούνται κρυφά.
- Αν οι διευθύνσεις ηλεκτρονικού ταχυδρομείου και άλλες προσωπικές πληροφορίες θα καταγράφονται και θα χρησιμοποιούνται για εμπορικούς ή άλλους σκοπούς χωρίς άδεια.
- Αν τα προσωπικά στοιχεία θα πωληθούν σε τρίτους χωρίς άδεια.
- Κλοπή πιστωτικών καρτών

Επιπλέον οι εξελίξεις στο τομέα της τεχνολογίας βάσεων δεδομένων αυξάνουν τα ζητήματα απορρήτου των πληροφοριών καθώς τα εργαλεία και οι υπηρεσίες εξόρυξης δεδομένων καθίστανται ευρύτερα διαθέσιμα.

Τα cookies χρησιμοποιούνται πλέον ευρέως για την ταυτοποίηση χρηστών σε έναν ιστότοπο. Στον χρήστη θα ζητηθούν πληροφορίες όπως το φύλο, η ηλικία, οι προτιμήσεις αγοράς ή ακόμη και η διεύθυνση email. Οι πληροφορίες αυτές αποθηκεύονται με τη μορφή ενός αρχείου κειμένου και στέλνονται στον σκληρό δίσκο του χρήστη, όπου αποθηκεύονται για μελλοντική του αναγνώριση. Το πρόγραμμα περιήγησης του χρήστη θα στείλει το cookie στον διακομιστή όταν ο χρήστης μεταβεί στον ίδιο ιστότοπο. Ο server μπορεί να χρησιμοποιήσει τις πληροφορίες του cookie για να δημιουργήσει προσαρμοσμένες ιστοσελίδες σύμφωνα με τα ενδιαφέροντα και τις προτιμήσεις του χρήστη. Χρησιμοποιώντας cookies, οι επιχειρήσεις μπορούν να αποκτήσουν προσωπικά στοιχεία, όπως αγοραστικές συνήθειες, διεύθυνση e-mail ή τμήματα του ιστότοπου που επισκέφθηκε ο χρήστης. Αυτές οι πληροφορίες μπορούν να συνδυαστούν σε λίστες αλληλογραφίας για σκοπούς άμεσου μάρκετινγκ ή μπορούν να πωληθούν σε τρίτους [43].

Τα web bugs είναι ένα άλλο ευρέως χρησιμοποιούμενο εργαλείο παρακολούθησης στο διαδίκτυο. Τα web bugs είναι «αόρατα» κομμάτια κώδικα που μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, από την κρυφή παρακολούθηση των διαδικτυακών ταξιδιών των ατόμων, έως και τη διάθεση ηλεκτρονικών αρχείων. Ένα εκτελέσιμο bug μπορεί να εγκατασταθεί τοπικά στο σκληρό δίσκο για τη συλλογή πληροφοριών όποτε ο χρήστης είναι συνδεδεμένος ή να λάβει οποιοδήποτε έγγραφο από τον υπολογιστή του χρήστη χωρίς προηγούμενη προειδοποίηση. Μπορούν επίσης να παρακολουθούν το ιστορικό των επισκεπτών στον ιστό και να ελέγχουν απομακρυσμένα τον υπολογιστή του θύματος. Π.χ. ένα web bug μπορεί να εκκινεί πολλά παράθυρα του προγράμματος περιήγησης όταν ένα χρήστης προσπαθεί να εξέλθει από ένα ιστότοπο. Πολλές ιστοσελίδες και διαδικτυακές διαφημιστικές εταιρείες τοποθετούν bugs στις σελίδες τους για τη συλλογή πληροφοριών, όπως ποιες σελίδες διαβάζονται συχνότερα. Τα bugs μπορούν να χρησιμοποιηθούν με πιο «ωμό» τρόπο, όπως για παράδειγμα, για τη λήψη της IP διεύθυνσης ή την εγκατάσταση επιβλαβών αρχείων στον σκληρό δίσκο του επισκέπτη. Σχετική έκθεση δείχνει ότι 16 εκατομμύρια σελίδες από τα 51 εκατομμύρια που σαρώθηκαν περιέχουν τουλάχιστον ένα bug που είχε επισυναφθεί από τρίτο μέρος, όπως ένα διαφημιστικό δίκτυο [84].

Ένα άλλο ζήτημα απορρήτου είναι το ταίριασμα των εγγραφών των βάσεων δεδομένων των πελατών εταιρειών με τις εγγραφές βάσεων δεδομένων που λαμβάνουν από τα cookies. Το DoubleClick είχε ήδη δημιουργήσει μια βάση δεδομένων για τις συνήθειες

περιήγησης των καταναλωτών στο Διαδίκτυο χρησιμοποιώντας cookies. Όπως γίνεται εμφανές υπάρχει σημαντική πιθανότητα δόλιων δραστηριοτήτων στο Διαδίκτυο, καθώς υπάρχουν λίγα κανονιστικά πρότυπα. Η ασφάλεια των πληροφοριών των πιστωτικών καρτών για διαδικτυακές αγορές αποτελεί επίσης ένα θέμα που εντάσσεται στα θέματα απορρήτου. Η Bibliofind, θυγατρική της Amazon.com παραδέχθηκε ότι χάκερ έκλεψαν 98.000 αριθμούς πιστωτικών καρτών. Οι χάκερ κατά καιρούς δημοσιεύουν λίστες με κλεμμένους αριθμούς πιστωτικών καρτών και άλλες σχετικές πληροφορίες στο Διαδίκτυο [35].

Τα ζητήματα απορρήτου που σχετίζονται με τη χρήση ιστότοπων κοινωνικής δικτύωσης συνήθως σχετίζονται με δημιουργία πλαστών προφίλ και ετικετών. Η προσθήκη ετικετών είναι μια δυνατότητα που επιτρέπει σε φίλους να συσχετίζονται μεταξύ τους με δραστηριότητες, εκδηλώσεις ή φωτογραφίες χωρίς προηγούμενη ειδοποίηση. Επιπλέον, για την δημιουργία ενός προφίλ σε οποιονδήποτε ιστότοπο κοινωνικής δικτύωσης, απαιτείται μόνο μια έγκυρη διεύθυνση email, επιτρέποντας σε οποιονδήποτε να προσποιείται ότι είναι κάποιος που στην πραγματικότητα δεν είναι. Τα πλαστά προφίλ και οι ετικέτες, σε συνδυασμό με αδύναμες πολιτικές απορρήτου, μπορούν να θέσουν σε κίνδυνο την ιδιωτικότητα ενός ατόμου. Π.χ. κάποιος θα μπορούσε να επισημανθεί με ετικέτα σε μια εικόνα μη επαγγελματικής φύσης ορατή σε έναν υποψήφιο εργοδότη. Η επακόλουθη συνέπεια θα μπορούσε να είναι η απώλεια μιας ευκαιρίας εργασίας.

Το ζήτημα του απορρήτου στο ηλεκτρονικό εμπόριο έγκειται στο γεγονός ότι οι πληροφορίες χρέωσης και αποστολής ενός ατόμου συνήθως αποθηκεύονται στο διαδίκτυο, μαζί με το ιστορικό αγορών του. Ως αποτέλεσμα, εάν υπάρξει πρόβλημα με την ασφάλεια των συστημάτων των υπηρεσιών πληρωμών ή εάν ο χρήστης δεν ήταν προσεκτικός, ένα άλλο άτομο θα μπορούσε να θέσει σε κίνδυνο τα στοιχεία σύνδεσης του συγκεκριμένου ατόμου και να αποκτήσει πρόσβαση στις προσωπικές του πληροφορίες και τις χρεώσεις. Σύμφωνα με την Ομάδα Εργασίας Anti-Phishing (APWG) ο κλάδος των υπηρεσιών πληρωμών ήταν ο δεύτερος υψηλότερος στόχος για επιθέσεις ηλεκτρονικού ψαρέματος (phishing), μεταξύ των μηνών Αυγούστου και Δεκεμβρίου του έτους 2010 [2]. Το ηλεκτρονικό ψάρεμα (phishing) είναι μια τεχνική με την οποία ένα άτομο παραπλανάται για την παροχή ευαίσθητων πληροφοριών, μέσω επεξεργασμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή ψευδών ιστότοπων που μοιάζουν με αυτούς των πραγματικών διαδικτυακών παρόχων υπηρεσιών. Οι

συνέπειες μιας επίθεσης ηλεκτρονικού ψαρέματος (phishing) μπορεί δυνητικά να καταστρέψουν οικονομικά το θύμα και να είναι τόσο σοβαρές όσο π.χ. η κλοπή ταυτότητας, ανάλογα με την έκταση των πληροφοριών που διέρρευσαν στο Διαδίκτυο.

Η βιβλιογραφική επισκόπηση σε θέματα ιδιωτικότητας, υποδεικνύει άμεση σχέση μεταξύ της ανησυχίας ενός ατόμου σε θέματα ασφαλείας και του επιπέδου γνώσης σχετικά με το Διαδίκτυο. Οι ερευνητές έχουν επίσης προσδιορίσει ότι ορισμένοι παράγοντες, όπως το φύλο και η εκπαίδευση, επηρεάζουν τα επίπεδα ανησυχίας των χρηστών στο διαδίκτυο [63].

1.5. Εγχώρια και διεθνής νομοθεσία

1.5.1. Ελλάδα

Η ελληνική νομοθεσία έχει ένα πλήθος διαφορετικών διατάξεων αναφορικά με τα εγκλήματα στον κυβερνοχώρο. Ενδεικτικά αναφέρονται οι Νόμοι 370 και 370^A του Ποινικού Κώδικα περί ποινικής προστασίας του απορρήτου, που μεταξύ άλλων αφορούν:

- Αθέμιτη εισχώρηση σε ξένα απόρρητα γραπτά (ανάγνωση – αντιγραφή – αποτύπωση με οποιοδήποτε τρόπο), που τιμωρείται με φυλάκιση μέχρι 1 έτος.
- Αθέμιτη παγίδευση ή παρέμβαση σε συσκευή, σύνδεση ή δίκτυο – υλικό – λογισμικό με σκοπό γνώση – αποτύπωση επικοινωνίας- δεδομένων κίνησης, που τιμωρείται με κάθειρξη μέχρι 10 έτη.
- Αθέμιτη παρακολούθηση με ειδικά τεχνικά μέσα – αποτύπωση συνομιλίας ή μη δημόσιας πράξης άλλου, που τιμωρείται με κάθειρξη μέχρι 10 έτη.
- Χρήση πληροφορίας/υλικού φορέα, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

Επίσης, ο Νόμος 292^A μεταξύ άλλων αφορά:

- Χωρίς δικαίωμα πρόσβαση σε σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας, που τιμωρείται με φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή (20.000-50.000 ευρώ).
- Παραβίαση διάταξης Κανονισμού ΑΔΑΕ ή Γενικής Άδειας ΕΕΤΤ, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (100.000 - 500.000 ευρώ).
- Παράλειψη αποτροπής παράνομης πρόσβασης, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (20.000 - 50.000 ευρώ).

Στη συνέχεια, αναφέρονται Νόμοι της Ελληνικής Νομοθεσίας, Προεδρικά Διατάγματα και Άρθρα Ποινικού Κώδικα, που είναι σχετικά με το ηλεκτρονικό έγκλημα και το κυβερνοέγκλημα [55]:

N.2225/1994	«Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
N. 2246/1994	«Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»
N.2472/1997	«Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
N. 2672/1998	«Διακίνηση εγγράφων με ηλεκτρονικά μέσα»
N.2774/1999	«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
N.2867/2000	«Οργάνωση και λειτουργία των τηλεπικοινωνιών»
N .3115/2003	«Αρχή διασφάλισης του απορρήτου των επικοινωνιών»
N.3431/2006	«Περί ηλεκτρονικών επικοινωνιών»
N. 3471/2006	«Προστασία Δεδομένων Προσωπικού Χαρακτήρα»

Πίνακας 1.Νόμοι για το ηλεκτρονικό έγκλημα

Π.Δ. 150/2001	«Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».
Π.Δ. 342/2002	«Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο»
Π.Δ. 131/2003	«Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά»
Π.Δ.47/2005	«Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών»

Πίνακας 2.Προεδρικά Διατάγματα για το ηλεκτρονικό έγκλημα.

Άρθρο 3 48Α ΠΚ	Πορνογραφία ανηλίκων
Άρθρο 370Α	Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
Άρθρο 370 Β	Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα
Άρθρο 370Γ	Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών
Άρθρο 386Α	Απάτη με υπολογιστή

Πίνακας 3.Άρθρα Ποινικού Κώδικα για το ηλεκτρονικό έγκλημα.

1.5.2. Ευρωπαϊκή Ένωση

Οι κανόνες προστασίας δεδομένων της ΕΕ εγγυώνται την προστασία των προσωπικών δεδομένων οποτεδήποτε αυτά συλλέγονται - για παράδειγμα, online αγορές, αίτηση για εργασία ή τραπεζικό δάνειο. Αυτοί οι κανόνες ισχύουν τόσο για τις εταιρείες όσο και για οργανισμούς (δημόσιους και ιδιωτικούς) στην ΕΕ και εκείνους που εδρεύουν εκτός ΕΕ που όμως προσφέρουν αγαθά ή υπηρεσίες εντός ΕΕ, όπως το Facebook ή το Amazon, οποτεδήποτε αυτές οι εταιρείες ζητούν ή επαναχρησιμοποιούν προσωπικά δεδομένα ατόμων εντός ΕΕ., χωρίς να έχει σημασία ποια μορφή παίρνουν τα δεδομένα - ψηφιακά ή σε μορφή φυσικού εγγράφου.

Οι κανόνες προστασίας δεδομένων της ΕΕ, γνωστοί επίσης ως Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (ή GDPR), περιγράφουν διαφορετικές καταστάσεις όπου μια εταιρεία ή ένας οργανισμός επιτρέπεται να συλλέγει ή να επαναχρησιμοποιεί προσωπικά στοιχεία:

- ύπαρξη συμβολαίου - για παράδειγμα, μια σύμβαση προμήθειας αγαθών ή υπηρεσιών ή μια σύμβαση εργαζομένου
- όταν η επεξεργασία των δεδομένων αποτελεί νομική απαίτηση, για παράδειγμα ο εργοδότης δίνει πληροφορίες για τον μηνιαίο μισθό στην αρχή κοινωνικής ασφάλισης.
- όταν η επεξεργασία δεδομένων είναι υπέρ των συμφερόντων του χρήστη
- για την ολοκλήρωση μιας δημόσιας εργασίας - κυρίως σχετίζεται με τα καθήκοντα των δημόσιων διοικήσεων, όπως σχολεία, νοσοκομεία και δήμοι
- όταν υπάρχουν νόμιμα συμφέροντα - για παράδειγμα, εάν μία τράπεζα χρησιμοποιεί προσωπικά δεδομένα για να ελέγξει εάν πληρούνται οι προϋποθέσεις για άνοιγμα τραπεζικού λογαριασμού.

Σε όλες τις άλλες περιπτώσεις, η εταιρεία ή ο οργανισμός πρέπει να ζητήσει τη συγκατάθεση του χρήστη προτού μπορέσει να συλλέξει ή να χρησιμοποιήσει ξανά προσωπικά δεδομένα. Όταν μια εταιρεία ή ένας οργανισμός ζητά τη συγκατάθεσή του χρήστη, αυτός πρέπει προβεί σε μια σαφή ενέργεια συναίνεσης, για παράδειγμα υπογράφοντας κατάλληλη φόρμα ή επιλέγοντας θετικά ανάμεσα από μία επιλογή ναι /

όχι σε κάποια ιστοσελίδα. Θα πρέπει επίσης να δοθούν οι ακόλουθες πληροφορίες προτού ο χρήστης αποφασίσει:

- πληροφορίες σχετικά με την εταιρεία / οργανισμό που θα επεξεργαστεί τα δεδομένα, συμπεριλαμβανομένων των στοιχείων επικοινωνίας τους, και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων (DPO) εάν υπάρχει
- ο λόγος για τον οποίο η εταιρεία / οργανισμός θα χρησιμοποιήσει τα προσωπικά δεδομένα
- πόσο καιρό σκοπεύουν να διατηρήσουν τα προσωπικά δεδομένα
- λεπτομέρειες για οποιαδήποτε άλλη εταιρεία ή οργανισμό που θα λάβει τα προσωπικά δεδομένα
- πληροφορίες σχετικά με τα δικαιώματα προστασίας δεδομένων (πρόσβαση, διόρθωση, διαγραφή, καταγγελία, ανάκληση συγκατάθεσης)

Όλες αυτές οι πληροφορίες πρέπει να παρουσιάζονται με σαφή και κατανοητό τρόπο. Εάν προηγουμένως ο χρήστης έδωσε τη συγκατάθεσή του σε μια εταιρεία ή οργανισμό να χρησιμοποιήσει τα προσωπικά του δεδομένα, μπορεί να επικοινωνήσει με τον υπεύθυνο επεξεργασίας δεδομένων (το πρόσωπο ή τον οργανισμό που χειρίζεται τα προσωπικά δεδομένα) και να ανακαλέσει την άδειά ανά πάσα στιγμή. Μόλις ανακληθεί η άδεια, η εταιρεία ή ο οργανισμός δεν θα μπορούν πλέον να χρησιμοποιούν τα προσωπικά δεδομένα.

Όταν ένας οργανισμός επεξεργάζεται τα προσωπικά δεδομένα με βάση το δικό του νόμιμο συμφέρον ή ως μέρος μιας εργασίας δημοσίου συμφέροντος ή για μια επίσημη αρχή, ο πολίτης ενδέχεται να έχει το δικαίωμα να αντιταχθεί. Σε ορισμένες περιπτώσεις, ενδέχεται να επικρατήσει το δημόσιο συμφέρον και η εταιρεία ή ο οργανισμός να μπορούν να συνεχίσουν να χρησιμοποιούν τα προσωπικά δεδομένα. Για παράδειγμα, αυτό θα μπορούσε να ισχύει για την επιστημονική έρευνα και τις στατιστικές, έργο που εκτελείται ως μέρος του επίσημου ρόλου μιας δημόσιας αρχής.

Για απευθείας μηνύματα μάρκετινγκ που προωθούν συγκεκριμένες μάρκες ή προϊόντα, απαιτείται η προηγούμενη συγκατάθεσή του πολίτη. Ωστόσο, εάν αυτός είναι υφιστάμενος πελάτης μιας συγκεκριμένης εταιρείας, μπορεί να λάβει μηνύματα μάρκετινγκ ηλεκτρονικού ταχυδρομείου σχετικά με παρόμοια προϊόντα ή υπηρεσίες. Διατηρεί το δικαίωμα να αντιταχθεί ανά πάσα στιγμή οπότε και η εταιρεία πρέπει να

σταματήσει να χρησιμοποιεί τα δεδομένα αμέσως. Σε όλες τις περιπτώσεις, θα πρέπει πάντα να παρέχονται πληροφορίες σχετικά με το δικαίωμα ένστασης στη χρήση των προσωπικών δεδομένων την πρώτη φορά που η εταιρεία ή ο οργανισμός επικοινωνεί με τον χρήστη.

Εάν ανήλικοι θέλουν να χρησιμοποιούν διαδικτυακές υπηρεσίες, όπως κοινωνικά μέσα, λήψη μουσικής ή παιχνιδιών, συχνά χρειάζονται έγκριση από τους γονείς ή τον νόμιμο κηδεμόνα τους, καθώς αυτές οι υπηρεσίες χρησιμοποιούν τα προσωπικά δεδομένα του παιδιού. Τα παιδιά δεν χρειάζονται πλέον γονική συγκατάθεση όταν είναι άνω των 16 ετών (σε ορισμένες χώρες της ΕΕ αυτό το όριο ηλικίας μπορεί να είναι ακόμη και 13 ετών). Τα στοιχεία για τον έλεγχο της γονικής συγκατάθεσης πρέπει να είναι αποτελεσματικά, για παράδειγμα χρησιμοποιώντας ένα μήνυμα επαλήθευσης που αποστέλλεται στη διεύθυνση ηλεκτρονικού ταχυδρομείου ενός γονέα.

Ο χρήστης μπορεί να ζητήσει πρόσβαση στα προσωπικά δεδομένα που έχει μια εταιρεία ή ένας οργανισμός και έχει το δικαίωμα να λάβει ένα αντίγραφο των δεδομένων δωρεάν, σε προσιτή μορφή. Θα πρέπει το αίτημα να απαντηθεί εντός 1 μηνός και πρέπει να αποσταλεί αντίγραφο προσωπικών δεδομένων και τυχόν σχετικές πληροφορίες σχετικά με τον τρόπο με τον οποίο τα δεδομένα χρησιμοποιήθηκαν ή χρησιμοποιούνται.

Εάν τα προσωπικά δεδομένα δεν χρειάζονται πλέον ή χρησιμοποιούνται παράνομα, τότε ο πολίτης μπορεί να ζητήσει τη διαγραφή των δεδομένων. Αυτοί οι κανόνες ισχύουν επίσης και για μηχανές αναζήτησης, όπως η Google. Ο πολίτης μπορεί να αιτηθεί την κατάργηση συνδέσμων προς ιστοσελίδες, συμπεριλαμβανομένου του ονόματός του, από αποτελέσματα της μηχανής αναζήτησης, εάν οι πληροφορίες είναι ανακριβείς, ανεπαρκείς, άσχετες ή υπερβολικές.

Εάν μια εταιρεία έχει διαθέσει τα προσωπικά δεδομένα στο διαδίκτυο και ζητάται η διαγραφή τους, η εταιρεία πρέπει επίσης να ενημερώσει τυχόν άλλους ιστότοπους στους οποίους έχουν κοινοποιηθεί ότι έχει ζητηθεί η διαγραφή των δεδομένων. Για την προστασία άλλων δικαιωμάτων, όπως η ελευθερία της έκφρασης, ορισμένα δεδομένα ενδέχεται να μην διαγράφονται αυτόματα.

Οποιοσδήποτε ιστότοπος επιθυμεί να χρησιμοποιήσει cookies πρέπει να λάβει τη συγκατάθεσή του χρήστη προτού τα εγκαταστήσει στον υπολογιστή ή την κινητή του συσκευή. Δεν επιτρέπεται σε έναν ιστότοπο να ενημερώνει απλώς ότι χρησιμοποιεί

cookies ή να εξηγεί πώς μπορεί να απενεργοποιηθούν. Οι ιστότοποι πρέπει να εξηγούν πώς θα χρησιμοποιηθούν οι πληροφορίες cookies. Θα πρέπει επίσης ο χρήστης να μπορεί να ανακαλεί την συγκατάθεσή του.

Δεν απαιτούν όλα τα cookies τη συγκατάθεσή του χρήστη. Τα cookies που χρησιμοποιούνται με αποκλειστικό σκοπό τη διασφάλιση της επικοινωνίας δεν απαιτούν συγκατάθεση. Περιλαμβάνουν π.χ. τα cookies που χρησιμοποιούνται για load balancing (επιτρέποντας την κατανομή των αιτημάτων ενός web server). Τα cookies που είναι απολύτως απαραίτητα για την παροχή μιας διαδικτυακής υπηρεσίας επίσης δεν χρειάζονται συγκατάθεση, όπως για παράδειγμα, τα cookies που χρησιμοποιούνται για την συμπλήρωση μιας ηλεκτρονικής φόρμας ή όταν χρησιμοποιείται ένα καλάθι αγορών [27].

1.5.3. Ηνωμένες Πολιτείες Αμερικής

Το νομοθετικό πλαίσιο των ΗΠΑ για την προστασία των προσωπικών δεδομένων αποτελεί γενικά ένα συνονθύλευμα σκόρπιων διατάξεων ανά κλάδο. Σε αντίθεση με άλλες περιπτώσεις, οι ΗΠΑ δεν διαθέτουν ειδικό νόμο για την προστασία των δεδομένων, αλλά αντίθετα υπάρχουν ρυθμίσεις κατά κύριο λόγο τη βιομηχανία, ανά τομέα. Υπάρχουν πολλές νομικές αναφορές περί απορρήτου στις ΗΠΑ, συμπεριλαμβανομένων νόμων και κανονισμών που έχουν αναπτυχθεί σε ομοσπονδιακό και πολιτειακό επίπεδο. Αυτοί οι νόμοι και οι κανονισμοί μπορούν να επιβληθούν από τις ομοσπονδιακές και πολιτειακές αρχές, και παρέχουν στα άτομα δικαίωμα να ασκήσουν αγωγές εναντίον οργανώσεων που πιστεύουν ότι παραβιάζουν το νόμο.

Σε ομοσπονδιακό επίπεδο, η ρυθμιστική αρχή που είναι υπεύθυνη για την εποπτεία κινείται με βάση το εκάστοτε νομοθετικό πλαίσιο. Στο πλαίσιο των χρηματοπιστωτικών υπηρεσιών, για παράδειγμα, το Γραφείο Χρηματοοικονομικής Προστασίας των Καταναλωτών και διάφοροι ρυθμιστικοί φορείς χρηματοοικονομικών υπηρεσιών (καθώς και οι ρυθμιστικές αρχές κρατικής ασφάλισης) έχουν υιοθετήσει πρότυπα σύμφωνα με τον Νόμο Gramm-Leach-Bliley (GLB) που υπαγορεύει τον τρόπο με τον οποίο οι επιχειρήσεις μπορούν να συλλέγουν, να χρησιμοποιούν και να αποκαλύπτουν προσωπικά στοιχεία. Ομοίως, στο πλαίσιο της υγειονομικής περίθαλψης, το Υπουργείο Υγείας και Ανθρωπίνων Υπηρεσιών είναι υπεύθυνο για την επιβολή του νόμου Health Insurance Portability and Accountability Act του 1996 (HIPAA).

Εκτός του παραπάνω πλαισίου, η Ομοσπονδιακή Επιτροπή Εμπορίου (FTC) είναι ο κύριος ομοσπονδιακός ρυθμιστής απορρήτου στις ΗΠΑ. Το άρθρο 5 της νομοθεσίας του FTC, είναι ένας γενικός νόμος για την προστασία των καταναλωτών που απαγορεύει «άδικες ή παραπλανητικές πράξεις ή πρακτικές που επηρεάζουν το εμπόριο», και αποτελεί το κύριο εργαλείο επιβολής της FTC σε ενέργειες ενάντια της ιδιωτικής ζωής. Το FTC έχει κινηθεί πολλαπλές φορές εναντίον παραβιάσεων της ιδιωτικής ζωής σε ένα ευρύ φάσμα φερόμενων παραβιάσεων με πρακτικές που έχουν κριθεί παραπλανητικές. Το νομοθετικό πλαίσιο επιτρέπει στην Επιτροπή να ασκεί μέτρα επιβολής εναντίον παραβατών, μέσω διαταγμάτων που απαγορεύουν στις

ελεγχόμενες εταιρείες μελλοντικά παραπτώματα και συχνά απαιτούν ελέγχους ανά διετία για έως και 20 χρόνια, ενώ το FTC μπορεί να επιβάλλει και χρηματικά πρόστιμα.

Σε πολιτειακό επίπεδο, οι γενικοί εισαγγελείς έχουν επίσης τη δυνατότητα να ασκήσουν αγωγές για αθέμιτες ή παραπλανητικές εμπορικές πρακτικές ή να επιβάλουν ποινές περί συγκεκριμένων κρατικών νόμων περί απορρήτου. Σε γενικές γραμμές, οι παραβιάσεις των ομοσπονδιακών και πολιτειακών νόμων περί απορρήτου οδηγούν σε αστικές και όχι ποινικές κυρώσεις. Οι κύριες εξαιρέσεις είναι οι νόμοι που αφορούν τις δραστηριότητες παρακολούθησης και τα εγκλήματα ηλεκτρονικών υπολογιστών. Οι παραβιάσεις του ομοσπονδιακού νόμου περί απορρήτου ηλεκτρονικών επικοινωνιών (ECPA) (ο οποίος αποτελείται από τον νόμο Wiretap, τον νόμο Stored Communications και τον νόμο Pen Register Act) ή τον νόμο περί απάτης και κατάχρησης υπολογιστών (CFAA) μπορεί να οδηγήσουν σε ποινικές κυρώσεις και αστικές ευθύνες. Επιπλέον, πολλά κράτη έχουν θεσπίσει νόμους επιτήρησης που περιλαμβάνουν ποινικές κυρώσεις, εκτός από την αστική ευθύνη. Εκτός του πλαισίου επιτήρησης, το Υπουργείο Δικαιοσύνης των ΗΠΑ εξουσιοδοτείται να διώξει ποινικά σοβαρές παραβιάσεις ιδιωτικού απορρήτου, όπως π.χ. αν ένα άτομο παραβιάζει εν γνώσει του νόμους περί απαγόρευσης απόκτησης και αποκάλυψης νομικά γνωστών πληροφοριών για την υγεία.

Η ομοσπονδιακή CFAA (Computer Fraud and Abuse Act) απαγορεύει επίσης ορισμένες δραστηριότητες παρακολούθησης, αλλά επικεντρώνεται πρωτίστως στον περιορισμό άλλων δραστηριοτήτων που σχετίζονται με τη χρήση Η/Υ. Σε πολιτειακό επίπεδο, οι περισσότερες πολιτείες διαθέτουν νόμους που ρυθμίζουν την παρακολούθηση των επικοινωνιών. Το διαφημιστικό ηλεκτρονικό ταχυδρομείο ρυθμίζεται σε ομοσπονδιακό επίπεδο από τον νόμο Controlling the Assault of Non-Solicited Pornography and Marketing Act του 2003 (CAN-SPAM). Το τηλεμάρκετινγκ ρυθμίζεται σε ομοσπονδιακό επίπεδο από τον Telephone Consumer Protection Act του 1991 (TCPA) και τον Νόμο περί αποτροπής απάτης των καταναλωτών, καθώς και κανονισμούς που εφαρμόζονται από το FTC και την Ομοσπονδιακή Επιτροπή Επικοινωνιών (FCC)[44].

Εκτός από τους νόμους που αναφέρονται παραπάνω, υπάρχουν πολλοί άλλοι ομοσπονδιακοί και πολιτειακοί νόμοι που αντιμετωπίζουν διάφορα θέματα απορρήτου, όπως:

- προσωπικά δεδομένα καταναλωτών: Νόμος για την Έκθεση Πιστωτικής Πιστοποίησης (FCRA) και Νόμος για τις Δίκαιες και Ακριβείς Πιστωτικές Συναλλαγές του 2003 (FACTA).
- προσωπικά δεδομένα ανηλίκων: Νόμος για την προστασία της ιδιωτικής ζωής των παιδιών στο Διαδίκτυο (COPPA).
- προσωπικά δεδομένα οδηγών: Νόμος περί προστασίας της ιδιωτικής ζωής του οδηγού του 1994 (DPPA).
- δεδομένα αναφορικά με την ενοικίαση βίντεο: Νόμος προστασίας απορρήτου βίντεο (VPPA) και
- δραστηριότητες ομοσπονδιακής κυβέρνησης: Νόμος περί απορρήτου του 1974 [44].

1.5.4. Υπόλοιπος κόσμος

Στην Δανία η νομοθεσία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ισχύει από το 2000 και εφαρμόζεται από τη Δανική Υπηρεσία Προστασίας Δεδομένων. Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να ενημερώσουν την υπηρεσία πριν ξεκινήσουν οποιαδήποτε επεξεργασία (με κάποιες μικρές εξαιρέσεις). Οι Δανοί οφείλουν να ενημερώσουν για:

- το όνομα και τη διεύθυνσή τους, καθώς και εκείνα οποιουδήποτε εκπροσώπου ή άλλου υπευθύνου επεξεργασίας δεδομένων, τις κατηγορίες και τους σκοπούς της επεξεργασίας ·
- γενική περιγραφή της επεξεργασίας ·
- τις κατηγορίες των υποκειμένων των δεδομένων και τις κατηγορίες των δεδομένων που υποβάλλονται σε επεξεργασία σχετικά με αυτά ·
- σε ποιον θα αποκαλυφθούν τα δεδομένα ·
- προτεινόμενες υπεράκτιες προσωπικές μεταφορές δεδομένων καθώς και μια περίληψη των βημάτων που θα διασφαλίσουν την ασφαλή επεξεργασία.
- ημερομηνία έναρξης επεξεργασίας · και
- ημερομηνία καταστροφής για τα δεδομένα. (Privacy International's Privacy Reports)

Στο Ηνωμένο Βασίλειο, το Αγγλικό Κοινοβούλιο ψήφισε τον Νόμο περί Προστασίας Δεδομένων τον Ιούλιο του 1998, με ισχύ από την 1η Μαρτίου 2000 με τον Επίτροπο Προστασίας Δεδομένων να επιβλέπει την εφαρμογή. Αυτός ο νόμος (με ορισμένες εξαιρέσεις) απαιτεί από μη κυβερνητικούς οργανισμούς επεξεργασίας δεδομένων υποχρεωτικά να ενημερώνουν το γραφείο του Επιτρόπου Προστασίας Δεδομένων πριν από την επεξεργασία πληροφοριών. Ενώ η υποβολή ειδοποιήσεων κοστίζει μόνο 35 £ ετησίως, η απαίτηση ειδοποίησης σημαίνει ότι ακόμη και η διαδικασίες όπως προσλήψεις, αρχειοθετήσεις, πωλήσεις πελατών και το ηλεκτρονικό ταχυδρομείο είναι ενέργειες παράνομες στην Αγγλία έως ότου καταχωρηθεί η ειδοποίηση δεδομένων. Η ειδοποίηση πρέπει να αναφέρει:

- το όνομα και τη διεύθυνση του υπευθύνου επεξεργασίας δεδομένων ·

- το όνομα και τη διεύθυνση οποιουδήποτε «αντιπροσώπου» που ορίζεται από την εταιρεία δεδομένων ·
- περιγραφή των προσωπικών δεδομένων που πρόκειται να υποβληθούν σε επεξεργασία, καθώς και τις κατηγορίες των υποκειμένων των δεδομένων που επηρεάζονται ·
- μια εξήγηση γιατί υποβάλλονται τα δεδομένα σε επεξεργασία ·
- ταυτοποίηση του ποιος θα λάβει τα δεδομένα(Data Protection Act).

Το σύνταγμα της Αργεντινής, όπως και πολλά αντίστοιχα στη Νότια Αμερική, επιδιώκει να διασφαλίσει το δικαίωμα προστασίας της ιδιωτικής ζωής: Το άρθρο 43 εγγυάται το δικαίωμα προστασίας των προσωπικών δεδομένων. Σύμφωνα με αυτήν την αρχή, ο καθένας μπορεί να υποβάλει αγωγή για να λάβει πληροφορίες σχετικά με τα προσωπικά του δεδομένα και τον σκοπό καταχώρισης τους σε δημόσια ή ιδιωτικά αρχεία. Το 2000, η Αργεντινή ενίσχυσε περαιτέρω αυτό το συνταγματικό δικαίωμα κωδικοποιώντας τον Νόμο για την Προστασία των Προσωπικών Δεδομένων, ακολουθώντας τις οδηγίες της ΕΕ: Η νέα νομοθεσία σε γενικές γραμμές περιλαμβάνει:

- προσφέρει γενικές διατάξεις προστασίας δεδομένων ·
- καθορίζει τα δικαιώματα και τα καθήκοντα των υποκειμένων των δεδομένων και των ελεγκτών ·
- εγκαينιάζει μια υπηρεσία εποπτείας, την Εθνική Διεύθυνση Προστασίας Προσωπικών Δεδομένων και
- συμπληρώνει περαιτέρω διαδικασίες σχετικά με τα προσωπικά δεδομένα

Η νομοθεσία της Αργεντινής, σύμφωνη με τους κανόνες της ΕΕ, απαγορεύει επίσης τη μεταφορά δεδομένων προσωπικού χαρακτήρα υπεράκτια σε χώρες χωρίς επαρκή προστασία, όπως οι Ηνωμένες Πολιτείες [68].

Η Αυστραλία ξεκίνησε τη διαδικασία ρύθμισης απορρήτου δεδομένων ήδη από το 1988, όταν πέρασε τον Νόμο περί απορρήτου που περιέχει έντεκα αρχές απορρήτου πληροφοριών, σχετικά με τη συλλογή, την αποθήκευση, την ασφάλεια, την πρόσβαση και τη χρήση προσωπικών δεδομένων, αλλά μόνο στον δημόσιο τομέα της Αυστραλίας - τις έξι πολιτείες της. Προκειμένου να εκπληρώσει τις υποχρεώσεις που απορρέουν από ένα σύνολο συνθηκών που έχει υπογράψει η χώρα, αυτός ο νόμος απέφυγε πολλά

βασικά ζητήματα απορρήτου. Αργότερα η Αυστραλία συμπλήρωσε ορισμένα κενά, ψηφίζοντας τους ακόλουθους νόμους [56]:

- Νόμος αντιστοίχισης δεδομένων (1990)
- Κώδικας δεοντολογίας πιστωτικής αναφοράς (1991)
- Νόμος περί τηλεπικοινωνιών (1997)
- Νόμος περί ανεπιθύμητων μηνυμάτων (2003)
- Κώδικας απορρήτου αγοράς και κοινωνικής έρευνας (2003)
- Νόμος περί προστασίας της ιδιωτικής ζωής σε μη Αυστραλούς πολίτες (2004)

Παρ' όλα αυτά, μέχρι την εκτεταμένη τροποποίηση του 2000, η Αυστραλία περιόρισε το νόμο περί προστασίας της ιδιωτικής ζωής στο δημόσιο τομέα. Το 2000 επέβαλε στις ιδιωτικές επιχειρήσεις δέκα νέες «εθνικές αρχές απορρήτου» (NPP) όπου πέρα των υποχρεώσεων των δημοσίων οργανισμών καθορίστηκαν και οι υποχρεώσεις του ιδιωτικού τομέα αναφορικά με τη χρήση, αποκάλυψη και διαχείριση προσωπικών δεδομένων - καθώς και θέματα ανωνυμίας και υπεράκτιων μεταφορών δεδομένων. Καθορίστηκαν θέματα όπως:

- Ποιότητα δεδομένων
- τρόποι ανωνυμοποίησης δεδομένων.
- Πολιτικές εξαίρεσης
- εξαιρεί τις «μικρές επιχειρήσεις» (αυτή η εξαίρεση φτάνει το 94% όλων των επιχειρήσεων στην Αυστραλία)

Η Βραζιλία δεν διαθέτει ολοκληρωμένο νόμο περί απορρήτου δεδομένων, αλλά κάποιες βασικές νομικές αρχές δημιουργώντας ένα υποτυπώδες σύστημα προστασίας της ιδιωτικής ζωής. Όπως και άλλες χώρες της Νότιας Αμερικής, τα συνταγματικά δικαιώματα απορρήτου της Βραζιλίας θεωρητικά φαίνονται ικανοποιητικά: Το σύνταγμα θεωρεί το δικαίωμα της ιδιωτικής ζωής «απαραβίαστο» και εγγυάται χρηματικές αποζημιώσεις σε όσους υποστούν περιουσιακές ή ηθικές ζημιές που προκύπτουν από παραβίαση. Η Βραζιλία δίνει το δικαίωμα στους υποκείμενους την επεξεργασία, να έχουν πρόσβαση στα αρχεία που τους αφορούν σε κυβερνητικές βάσεις δεδομένων, καθώς και τρόπους επιδιόρθωσης τους [8].

Ο Καναδάς έχει θεσπίσει έναν ολοκληρωμένο ομοσπονδιακό νόμο περί προστασίας δεδομένων, τον Νόμο περί Προστασίας Προσωπικών Πληροφοριών και Ηλεκτρονικών Εγγράφων (PIPEDA), ο οποίος τέθηκε σε ισχύ σταδιακά από την 1η Ιανουαρίου 2001.

Το PIPEDA ρυθμίζει τη συλλογή, τη χρήση και την αποκάλυψη προσωπικών πληροφοριών αναφορικά με εμπορικές δραστηριότητες και ισχύει για κάθε οργανισμό που εμπλέκεται σε εμπορικές δραστηριότητες, ανεξάρτητα από το μέγεθός του. Η PIPEDA καθιερώνει ένα σύνολο δέκα αρχών που πρέπει να ακολουθούν οι εταιρείες κατά την επεξεργασία προσωπικών πληροφοριών.

- Ευθύνη. Μια εταιρεία είναι υπεύθυνη για τις προσωπικές πληροφορίες που συλλέγει και ελέγχει. Η εταιρεία πρέπει να ορίσει ένα άτομο εντός της εταιρείας που θα επιβλέπει και θα είναι υπεύθυνο για τη συμμόρφωση με το PIPEDA.
- Προσδιορισμός σκοπών. Η εταιρεία πρέπει να προσδιορίσει τους λόγους για τους οποίους συλλέγει τις πληροφορίες, είτε πριν είτε ταυτόχρονα με τη συλλογή των προσωπικών πληροφοριών.
- Συγκατάθεση. Όπου ενδείκνυται, η εταιρεία πρέπει να ζητήσει τη συγκατάθεση του ατόμου κατά την επεξεργασία, την αποθήκευση και τη συλλογή των προσωπικών πληροφοριών. Η συγκατάθεση πρέπει να είναι ρητή όταν οι πληροφορίες είναι ευαίσθητης φύσης, αλλά οι περισσότερες κατηγορίες προσωπικών πληροφοριών ενδέχεται να απαιτούν μόνο κάποιου είδους σιωπηρής συγκατάθεσης. Η ρητή συγκατάθεση θα μπορούσε να αποκτηθεί προφορικά ή μέσω την συμπλήρωσης ενός πλαισίου ελέγχου.
- Περιορισμένη συλλογή. Μόνο προσωπικές πληροφορίες που είναι απαραίτητες για τον δηλωμένο σκοπό μπορούν να συλλεχθούν και πρέπει να συλλέγονται νόμιμα.
- Περιορισμός χρήσης, αποκάλυψης και διατήρησης. Οι προσωπικές πληροφορίες δεν μπορούν να χρησιμοποιηθούν για σκοπούς διαφορετικούς από τον επιδιωκόμενο σκοπό της συλλογής, εκτός εάν το άτομο έχει συναινέσει στην εξαίρεση ή τέτοια εναλλακτική χρήση απαιτείται από το νόμο. Επιπλέον, οι προσωπικές πληροφορίες πρέπει να διατηρούνται μόνο για όσο διάστημα απαιτείται για την εκπλήρωση των επιδιωκόμενων σκοπών.
- Ακρίβεια. Οι προσωπικές πληροφορίες πρέπει να είναι ακριβείς, πλήρεις και ενημερωμένες.
- Προστατευτικά μέτρα. Τα προσωπικά στοιχεία πρέπει να προστατεύονται επαρκώς ανάλογα με το επίπεδο ευαισθησίας των δεδομένων.

- Ανοικτότητα. Οι εταιρείες πρέπει να ορίσει την πολιτική απορρήτου της και να ενημερώσει για το πώς συλλέγει, αποθηκεύει και επεξεργάζεται προσωπικά στοιχεία.
- Ατομική πρόσβαση. Κάθε άτομο μπορεί να αποκτήσει πρόσβαση σε σχετικές προσωπικές πληροφορίες και να έχει την ευκαιρία να διορθώσει τυχόν ανακριβείς πληροφορίες (Canada's Personal Information Protection and Electronic Documents Act).

Τέλος οι νόμοι περί απορρήτου δεδομένων της Κίνας είναι στην καλύτερη περίπτωση ιδιαίτερα περιστασιακοί. Το κινεζικό σύνταγμα αναφέρεται έμμεσα στην προστασία της ιδιωτικής ζωής, εγγυώμενο τα δικαιώματα της ιδιωτικής ζωής στην οικία και την προσωπική αλληλογραφία. Ωστόσο, η Κίνα δεν διαθέτει επαρκή νομική υποδομή για την προστασία της ιδιωτικής ζωής. Έχει εκδώσει ορισμένους νόμους περί απορρήτου:

- Ο Ποινικός Κώδικας επιβάλλει έως και ένα έτος φυλάκιση σε όσους παραβιάζουν τα δικαιώματα της ελευθερίας της επικοινωνίας των πολιτών και έως και τρία χρόνια σε όσους αναζητούν παράνομα κατοικία.
- Οι Γενικές Αρχές του Αστικού Δικαίου απαγορεύουν τις προσβολές, τη συκοφαντία και την καταστροφή της φήμης.
- Ο νόμος για την προστασία των ανηλίκων απαγορεύει τη συλλογή προσωπικών δεδομένων ανηλίκων.

Η Κίνα δεν προσφέρει επί του παρόντος κανένα νόμο περί προστασίας δεδομένων που σχετίζεται με το Διαδίκτυο, αν και στην πραγματικότητα η Κίνα αναγνωρίζεται ως ο παγκόσμιος ηγέτης στην κυβερνητική παρακολούθηση και λογοκρισία στην χρήση του Διαδικτύου από τους πολίτες [48].

➤ ΚΕΦΑΛΑΙΟ 2. Διαδικτυακός εκφοβισμός - εκμετάλλευση

Στο παρόν κεφάλαιο εξετάζεται το ιδιαίτερα ανησυχητικό και εκθετικά αυξανόμενο φαινόμενο του διαδικτυακού εκφοβισμού-εκμετάλλευσης. Στο πρώτο υποκεφάλαιο γίνεται μία σύντομη ιστορική ανασκόπηση, στο δεύτερο υποκεφάλαιο παρουσιάζονται οι διάφορες μορφές που δύναται να πάρει το φαινόμενο, το τρίτο υποκεφάλαιο εστιάζει κυρίως στα κοινωνικά δίκτυα που αποτελούν πλέον και τον συνηθέστερο τόπο εκφοβιστικών συμπεριφορών, ενώ τέλος στο τέταρτο υποκεφάλαιο καταγράφονται σημαντικές υποθέσεις διαδικτυακού εκφοβισμού που απασχόλησαν την εγχώρια και τη διεθνή κοινότητα.

2.1 Ιστορία

Ο διαδικτυακός εκφοβισμός είναι μια νέα και ιδιαίτερα ύπουλη μορφή εκφοβισμού. Το 2007, περισσότεροι από 900.000 μαθητές δευτεροβάθμιας εκπαίδευσης ανέφεραν ότι έχουν εκφοβιστεί στο διαδίκτυο [79]. Ο εκφοβισμός στον κυβερνοχώρο επιτρέπει στους θύτες να προβαίνουν σε αυτές τις πράξεις από απόσταση, έξω από σχολεία, μπροστά σε ένα ευρύ κοινό και μερικές φορές υπό την προστασία της ανωνυμίας. Οι νέες τεχνολογίες παρέχουν στους εκφοβιστές νέα εργαλεία για να προκαλέσουν βλάβη με νέους τρόπους. Ο εκφοβισμός στον κυβερνοχώρο αποτελεί καίριο ζήτημα σε πολλές χώρες σε όλο τον κόσμο. Για παράδειγμα, στη Νότια Κορέα, μια φοιτήτρια άφησε τον σκύλο της να αφοδεύσει εντός του μετρό. Αφού το κορίτσι αρνήθηκε να καθαρίσει τις ακαθαρσίες, ένας άλλος επιβάτης στο τρένο πήρε τη φωτογραφία της χρησιμοποιώντας το κινητό της και τη δημοσίευσε στο διαδίκτυο. Τους επόμενους μήνες το κορίτσι «Dog Poop» έγινε στόχος ακραίας παρενόχλησης. Πολλά άτομα ανακάλυψαν το όνομα και τη διεύθυνσή της και σύντομα αναγκάστηκε να αποσυρθεί από το σχολείο και να μετακομίσει σε άλλη περιοχή της χώρας [87].

Ο εκφοβισμός αποτελεί μια επίδειξη ανταγωνιστικών κακόβουλων δραστηριοτήτων. Σύμφωνα με τον Dake, Price και Telljohann [15], ο εκφοβισμός συμβαίνει όταν «πράξεις που προκαλούν τραυματισμό ή δυσφορία διαπράττονται σε άλλο άτομο». Η συναισθηματική και σωματική βλάβη του εκφοβισμού έχει κινητοποιήσει παγκόσμια τις κοινωνίες για την ανάληψη νομικών δράσεων εναντίον του φαινομένου. Ο εκφοβισμός έχει εξελιχθεί από την διά ζώσης μορφή του σε αλληλεπίδραση πολυμέσων που μπορούν να μεταδοθούν μέσω πολλαπλών ηλεκτρονικών πηγών. Η εξέλιξη της ηλεκτρονικής επικοινωνίας είναι το θεμέλιο του εκφοβισμού στον κυβερνοχώρο. Ο εκφοβισμός στον κυβερνοχώρο συμβαίνει μέσω κινητών τηλεφώνων, μέσω μηνυμάτων κειμένου και του Διαδικτύου.

Σύμφωνα με τους Hinduja και Patchin [67] ο εκφοβισμός λαμβάνει χώρα μεταξύ των παιδιών εδώ και αρκετές γενιές. Η τελευταία γενιά, ωστόσο, κατάφερε να χρησιμοποιήσει την τεχνολογία για να επεκτείνει την εμβέλεια και το εύρος εφαρμογής. Ο εκφοβισμός στον κυβερνοχώρο, ορίζεται ως ηθελημένη και επαναλαμβανόμενη βλάβη που προκαλείται μέσω της χρήσης υπολογιστών, κινητών τηλεφώνων και άλλων ηλεκτρονικών συσκευών.

Επιπλέον, η διόγκωση χρήσης των μέσων κοινωνικής δικτύωσης αποτελεί συχνό θέμα στα μέσα ενημέρωσης αναφορικά με τη χρήση τους στα σχολεία και τον χώρο εργασίας. Παρόλο που ο εκφοβισμός αποτελεί διαχρονικό φαινόμενο, η αύξηση της δημοσιότητας οφείλεται κατά κύριο λόγο στην αύξηση των ανθρωποκτονιών και των αυτοκτονιών που σχετίζονται με τον εκφοβισμό στον κυβερνοχώρο. Π.χ. Το ABC News παρουσίασε ειδική δώρη εκπομπή με τίτλο "Bullied to Death in America's Schools" [22]. Το ντοκιμαντέρ ανέφερε ότι τουλάχιστον 14 έφηβοι αυτοκτόνησαν σε ένα χρόνο ως αποτέλεσμα του εκφοβισμού. Ο Dilmac [20] έχει πραγματοποιήσει αρκετές έρευνες οι οποίες καταδεικνύουν ότι ο εκφοβισμός στον κυβερνοχώρο είναι ένα διεθνές πρόβλημα.

Ο Dan Olweus, που θεωρείται πρωτοπόρος στην έρευνα του εκφοβισμού, έχει εκδώσει αρκετές μελέτες με βάση την εμπειρία του σε αυτόν τον τομέα. Ο Olweus δημοσίευσε το πρώτο του βιβλίο το 1973 με τίτλο, «Aggression on the Schools: Bullies and Whipping Boys». Στα ευρήματά του ο Olweus υποστήριξε ότι ο εκφοβισμός συνεπάγεται ανισορροπία δυνάμεων. Ο Olweus σημειώνεται ως ο πρώτος που εφάρμοσε προγράμματα κατά του εκφοβισμού [9]. Ο σχεδιασμός του κατά του εκφοβισμού καλύπτει διαδικασίες στις αίθουσες διδασκαλίας και μπορεί επίσης να χρησιμοποιηθεί στο χώρο εργασίας για να βοηθήσει στην αντιμετώπιση φαινομένων εκφοβισμού. Στις αρχές της δεκαετίας του 1980, ο Olweus ξεκίνησε μια εκστρατεία για τη διαμόρφωση νόμων κατά του εκφοβισμού στα σχολεία. Λόγω της έρευνας του, ορισμένα σχολεία έχουν μειώσει κατά 50% τον εκφοβισμό. Οι εκπαιδευτικοί δήλωσαν ότι η δουλειά που έκανε ο Olweus βελτίωσε την προστασία των μαθητών.

Σε έκθεση του Secret Service των ΗΠΑ που ερευνά τα χαρακτηριστικά των μαθητών που έχουν διαπράξει εγκλήματα, ανακάλυψε τον εκφοβισμό ως έναν από τους βασικούς παράγοντες που οδηγούν στις εγκληματικές δραστηριότητες [15]. Σε 12 από 15 πυροβολισμούς σε πανεπιστημιούπολεις κατά τη διάρκεια της δεκαετίας του 1990, οι δράστες είχαν παρελθόν εκφοβισμού. Στο παρελθόν, ο εκφοβισμός συνίστατο ως χειραγώγηση και σωματική επιθετικότητα εναντίον του ασθενέστερου αντιπάλου. Ο εκφοβισμός ήταν πιο εμφανής στα σχολεία ή κατά τη διάρκεια της ημέρας [43].

Ωστόσο, στο σημερινό κόσμο του διαδικτυακού εκφοβισμού, το θύμα συχνά μπορεί να διασυνθεί δημόσια. Μέσα σε λίγα δευτερόλεπτα, οποιαδήποτε φήμη, αληθής ή ψευδής, μπορεί να κυκλοφορήσει στο σχολείο ή την κοινότητα πριν κάποιος επαληθεύσει την εγκυρότητά της. Οι πληροφορίες μπορούν να εξαπλωθούν τόσο γρήγορα ώστε

εκατομμύρια άνθρωποι σε ολόκληρο τον κόσμο να τις δουν πριν καταργηθούν. Για παράδειγμα, πριν από λίγα χρόνια ένας φοιτητής του Πανεπιστημίου του Rutgers πήδηξε από τη γέφυρα George Washington επειδή οι σεξουαλικές του δραστηριότητες με ένα άλλο άνδρα μαγνητοσκοπήθηκαν και αναρτήθηκαν σε βίντεο στο Internet [75].

Ο εκφοβισμός δεν είναι μόνο πρόβλημα των παιδιών ή των εφήβων. Πολλοί ενήλικες βιώνουν εκφοβισμό στο χώρο εργασίας με τα αποτελέσματα να είναι εξίσου καταστροφικά. Σήμερα τα σχολεία και οι χώροι απασχόλησης θεωρητικά δείχνουν μηδενική ανοχή στον εκφοβισμό οποιασδήποτε μορφής. Ο εκφοβισμός στο χώρο εργασίας μπορεί να οδηγήσει σε μείωση της απόδοσης του εργαζομένου [46]. Ο αρνητικός αντίκτυπος δεν είναι μόνο επιβλαβής για το άτομο ή το θύμα, αλλά δύναται να επηρεάσει την παραγωγικότητα στο χώρο εργασίας. Στον χώρο της υγειονομικής περίθαλψης, οι νοσοκόμες αντιμετωπίζονται συχνά με λιγότερο σεβασμό από τους γιατρούς και τους ζητείται να εκτελέσουν εργασίες που δεν εντάσσονται στα καθήκοντα που τους ανατίθενται. Σύμφωνα με τους Hutchinson, Vickers, Jackson και Wilkes [42], «ο εκφοβισμός μπορεί να προκαλέσει όχι μόνο ψυχολογική βλάβη αλλά και σωματική ασθένεια» του υπαλλήλου. Αρκετοί υπάλληλοι χρησιμοποίησαν παραπλανητικές μεθόδους με στόχο την εργασιακή τους εξέλιξη. Παράδειγμα εκφοβισμού στο χώρο εργασίας αποτελούν τα υποτιμητικά μηνύματα ηλεκτρονικού ταχυδρομείου ή οι προφορικές αντιπαραθέσεις σε συναδέλφους.

Το φαινόμενο φαίνεται να διατρέχει το σύνολο των χωρών του πλανήτη. Στη Νέα Ζηλανδία, ο εκφοβισμός στον κυβερνοχώρο προκαλεί όλο και μεγαλύτερη ανησυχία λόγω της εξάπλωσης των κινητών τηλεφώνων μεταξύ νέων. Σε σχετική έρευνα σε 1.530 άτομα ηλικίας 11 έως 18 ετών, η μελέτη διαπίστωσε ότι το 43% των συμμετεχόντων ανέφεραν ότι βίωσαν κάποιο περιστατικό εκφοβισμού στο διαδίκτυο [73].

Σχετική έρευνα έχει πραγματοποιηθεί και στο Ηνωμένο Βασίλειο σε 1.429 μαθητές σχετικά με την πρόθεση του επιτιθέμενου και την ανισορροπία ισχύος μεταξύ τους και του επιτιθέμενου [41]. Οι ηλικίες των ερωτηθέντων ήταν μεταξύ 8 και 13 ετών όπου περιέγραψαν τις μεθόδους αντιμετώπισής τους κατά του εκφοβισμού. Το Ηνωμένο Βασίλειο έχει πραγματοποιήσει μελέτες που δείχνουν το αυξανόμενο πρόβλημα του εκφοβισμού στα σχολεία ως υποκατηγορία επιθετικής συμπεριφοράς [45]. Μια ταινία κινουμένων σχεδίων επίλυσης συγκρούσεων με τίτλο "Bully Dance" παρουσιάστηκε

σε βρετανικά σχολεία για να εντοπίσει συμπεριφορές εκφοβισμού και στρατηγικές αντιμετώπισης για τα παιδιά σχολικής ηλικίας.

Μερικά κοινά λάθη που κάνουν συνήθως τα θύματα είναι ότι δεν αποκαλύπτουν ότι έχουν εκφοβιστεί. Ορισμένα θύματα θεωρούν ότι η ηλεκτρονική επικοινωνία δεν είναι ανιχνεύσιμη όταν είναι ανώνυμη, οπότε δεν χρειάζεται να αναφερθεί το αδίκημα. Σύμφωνα με τους Junonen και Gross [46], «θεωρητικά, τα εργαλεία ηλεκτρονικής επικοινωνίας επιτρέπουν στους εκφοβιστές να παραμένουν ανώνυμοι». Ωστόσο στον σημερινό τεχνολογικό κόσμο πολλά προγράμματα ελέγχου έχουν επινοήσει μεθόδους ανίχνευσης ανώνυμων μεταδόσεων. Πολλά θύματα προσπαθούν να αποκρύψουν τα γεγονότα από τις αρμόδιες αρχές ή από τους οικείους τους με το φόβο αντιπoinων από τον δράστη ή τον χλευασμό από συναδέλφους που θα τους αντιμετώπιζαν αρνητικά [46].

Ο Smith (2007) παρείχε προτάσεις για να σταματήσει ο εκφοβισμός στον κυβερνοχώρο αναφορικά με τον αποκλεισμό την αγνόηση του εκφοβισμού, την έλλειψη αντίποινων και την ενημέρωση των αρχών. Άλλες προτάσεις περιλαμβάνουν δημοσίευση του συμβάντος και εκστρατείες κατά του εκφοβισμού. Η ευαισθητοποίηση είναι βασικός παράγοντας της πρόληψης του διαδικτυακού εκφοβισμού. Σύμφωνα με τους Diamanduros, Downs και Jenkins [19] «είναι σημαντικό για τους γονείς και τους δασκάλους να εκπαιδεύσουν τα παιδιά τους σχετικά με τον αντίκτυπο που μπορούν να έχουν οι διαδικτυακές συνομιλίες, τα άμεσα μηνύματα, τα μηνύματα κειμένου και οι ιστότοποι κοινωνικής δικτύωσης όπως το MySpace στην κοινωνική τους ζωή».

2.2 Είδη διαδικτυακού εκφοβισμού

Ο διαδικτυακός εκφοβισμός λαμβάνει πολλές μορφές. Οι βασικότερες μορφές που μπορεί να λάβει ο διαδικτυακός εκφοβισμός είναι κατά κύριο λόγο οι εξής:

- **Αποκλεισμός:** Ο αποκλεισμός συνίσταται στην σκόπιμη απόρριψη κάποιου από γεγονότα ή συναθροίσεις. Ο αποκλεισμός μπορεί να συμβεί διά ζώσης, αλλά τελείται επίσης στο διαδίκτυο για στόχευση και εκφοβισμό. Π.χ. ένα παιδί θα μπορούσε να αποκλειστεί από ομάδες ή πάρτι, ενώ βλέπει άλλους φίλους να καλούνται ή να παραλείπεται από συνομιλίες που περιλαμβάνουν αμοιβαίους φίλους.
- **Παρενόχληση:** Η παρενόχληση είναι μια ευρεία κατηγορία στην οποία εμπίπτουν πολλοί τύποι εκφοβισμού στον κυβερνοχώρο, αλλά γενικά αναφέρεται σε ένα συνεχές και σταθερό μοτίβο επιβλαβών ή απειλητικών διαδικτυακών μηνυμάτων που αποστέλλονται με την πρόθεση να βλάψουν κάποιον.
- **Outing/Doxing:** Το outing, αναφέρεται στην πράξη της ανοιχτής αποκάλυψης ευαίσθητων ή προσωπικών πληροφοριών για κάποιον χωρίς τη συγκατάθεσή του με στόχο την ενόχληση ή την ταπείνωση του θύματος. Το γεγονός μπορεί να κυμαίνεται από τη διάδοση προσωπικών φωτογραφιών ή εγγράφων δημόσιων προσώπων έως την κοινή χρήση των αποθηκευμένων προσωπικών μηνυμάτων ενός ατόμου σε μια διαδικτυακή ιδιωτική ομάδα. Το βασικό σημείο είναι η έλλειψη συναίνεσης από το θύμα.
- **Trickery:** Παρόμοιο με το outing, με ένα επιπλέον στοιχείο εξαπάτησης. Σε αυτές τις καταστάσεις, ο θύτης θα προσεγγίσει τον στόχο του ξεγελώντας το δημιουργώντας μια ψευδή αίσθηση ασφάλειας. Μόλις ο θύτης αποκτήσει την εμπιστοσύνη του στόχου του, κάνει κατάχρηση αυτής της εμπιστοσύνης και μοιράζεται τα μυστικά και τις προσωπικές πληροφορίες του θύματος με τρίτα άτομα.
- **Cyberstalking:** Το Cyberstalking είναι μια ιδιαίτερα σοβαρή μορφή διαδικτυακού εκφοβισμού που μπορεί να επεκταθεί σε απειλές σωματικής βλάβης στο άτομο που στοχεύει. Μπορεί να περιλαμβάνει παρακολούθηση, ψευδείς κατηγορίες, απειλές και συχνά συνοδεύεται από καταδίωξη εκτός

σύνδεσης. Είναι ποινικό αδίκημα και μπορεί να οδηγήσει σε περιοριστική εντολή ακόμη και χρόνο φυλάκισης για τον δράστη.

- **Fraping:** Το fraping συμβαίνει όταν ο δράστης χρησιμοποιεί λογαριασμούς κοινωνικής δικτύωσης του θύματος για να δημοσιεύσει ακατάλληλο περιεχόμενο με το όνομά του. Μπορεί γενικά να είναι ακίνδυνο όταν φίλοι γράφουν αστείες αναρτήσεις στα προφίλ του άλλου, αλλά γενικά μπορεί να αποδειχτεί εξαιρετικά επιβλαβές, π.χ. ο δράστης να δημοσιεύει φυλετικές / ομοφοβικές συκοφαντίες μέσω του προφίλ κάποιου άλλου για να καταστρέψει τη φήμη του.
- **Masquerading:** Συμβαίνει όταν ο δράστης δημιουργεί ένα ψεύτικο προφίλ ή ταυτότητα στο διαδίκτυο με μοναδικό σκοπό τον εκφοβισμό κάποιου στον κυβερνοχώρο. Υλοποιείται κυρίως μέσω της δημιουργίας ψεύτικου λογαριασμού email, ψεύτικου προφίλ κοινωνικών μέσων και την επιλογή νέας ταυτότητας και φωτογραφιών για να ξεγελάσει το θύμα. Σε αυτές τις περιπτώσεις, ο δράστης τείνει να είναι κάποιος που το θύμα γνωρίζει πολύ καλά.
- **Dissing:** Το Dissing αναφέρεται σε πράξη εκφοβισμού μέσω της διάδοσης πληροφοριών σχετικά με το θύμα μέσω δημόσιων ή ιδιωτικών μηνυμάτων με στόχο την καταστροφή της φήμη του ή τις σχέσεις του με άλλους ανθρώπους. Σε αυτές τις καταστάσεις, ο δράστης τείνει να έχει προσωπική σχέση με το θύμα.
- **Trolling:** Το trolling συμβαίνει όταν ο δράστης επιδιώκει να εκνευρίσει σκόπιμα άλλους, δημοσιεύοντας ειρωνικά σχόλια στο διαδίκτυο. Το trolling μπορεί να μην είναι πάντα μια μορφή εκφοβισμού στον κυβερνοχώρο, αλλά μπορεί να χρησιμοποιηθεί ως εργαλείο εκφοβισμού όταν γίνεται με κακόβουλη και επιβλαβή πρόθεση.
- **Flaming:** Αυτός ο τύπος διαδικτυακού εκφοβισμού υλοποιείται μέσω ανάρτησης ή άμεσης αποστολής προσβολών και βωμολοχιών στον στόχο τους. Το Flaming είναι παρόμοιο με το trolling, αλλά συνήθως είναι μια πιο άμεση επίθεση εναντίον του θύματος για να τον υποκινήσει σε διαδικτυακές αντιπαραθέσεις.

2.3 Ο διαδικτυακός εκφοβισμός στα κοινωνικά δίκτυα

Ο εκφοβισμός στον κυβερνοχώρο μπορεί να συμβεί με πολλούς τρόπους όπως e-mail, ανταλλαγή άμεσων μηνυμάτων, αίθουσες συνομιλίας, πίνακες συζητήσεων, κοινωνικά δίκτυα, ιστολόγια, μηνύματα κειμένου ή εικόνες και βίντεο που αποστέλλονται σε κινητά τηλέφωνα [1]. Η χρήση των κοινωνικών δικτύων είναι ευρέως διαδεδομένη σε εφήβους, νεαρούς ενήλικες και ηλικιωμένους. Στο πλαίσιο του προγράμματος Internet and American Life του Pew Research Center, οι Madden et al. [54] αναφέρουν ότι το 81% των Αμερικανών συμμετεχόντων ηλικίας 12-17 ετών χρησιμοποιούν SNS (Social networking service). Στο πλαίσιο του ίδιου έργου, οι Duggan και Smith [24] ανέφεραν ότι το 73% των ενηλίκων (άνω των 18 ετών) έχουν τουλάχιστον έναν λογαριασμό σε κοινωνικά δίκτυα. Πιο συγκεκριμένα, οι συμμετέχοντες ηλικίας 18-29 ετών ανέφεραν τη μεγαλύτερη χρήση κοινωνικών δικτύων σε σύγκριση με τις μεγαλύτερες ηλικιακές ομάδες σε Facebook, Twitter, Instagram και Pinterest. Τα κοινωνικά δίκτυα φαίνεται επίσης να χρησιμοποιούνται με υψηλή συχνότητα. Οι Madden et al. [54] ανέφεραν ότι το 73% των παιδιών ηλικίας 14-17 ετών έχουν καθημερινή πρόσβαση στους λογαριασμούς τους και οι Duggan και Smith [24] ανέφεραν ότι το ποσοστό αυτό αγγίζει το 63% στα άτομα άνω των 18 ετών.

Σε μια από τις πρώτες μελέτες που εστιάζουν σε συγκεκριμένους κινδύνους από την χρήση κοινωνικών δικτύων, οι Ybarra και Mitchell [96] διερεύνησαν εάν τα κοινωνικά δίκτυα αποτελούν περιβάλλοντα στα οποία οι νέοι ήταν ευάλωτοι σε σεξουαλική παρενόχληση ή και θυματοποίηση. Η σεξουαλική προσέγγιση ορίστηκε η παροχή σεξουαλικών πληροφοριών ή αιτήματα διαλόγου για σεξ ή παρακίνηση σε σεξουαλική δραστηριότητα. Η παρενόχληση ορίστηκε ως η διάδοση φημών ή εκφορά αγενών ή υβριστικών σχολίων στο διαδίκτυο. Συνολικά, το 14,7% των συμμετεχόντων (10-15 ετών) ανέφεραν ότι ήταν θύματα ανεπιθύμητης σεξουαλικής προσέλκυσης και 34% ανέφεραν ότι βίωσαν παρενόχληση στο Διαδίκτυο κατά το προηγούμενο έτος. Από εκείνους που ανέφεραν ότι υπήρξαν θύματα, το 33,6% ανέφερε ότι δέχτηκαν σεξουαλική παρενόχληση και το 27,3% ανέφερε απλή παρενόχληση στο Διαδίκτυο που συνέβη ειδικά στα κοινωνικά δίκτυα.

Οι Lenhart et al. (2011) διερεύνησε επίσης τον διαδικτυακό εκφοβισμό στο SNS. Αν και το 69% των 12-17 ετών εφήβων ανέφερε ότι οι χρήστες είναι ως επί το πλείστον

ευγενικοί με άλλους χρήστες στο SNS, το 88% ανέφερε ότι υπήρξαν μάρτυρες κακής και σκληρής συμπεριφοράς από άλλους χρήστες στο SNS [54]. Επιπλέον, το 15% των εφήβων και το 13% των ενηλίκων (18 ετών και άνω) ανέφεραν ότι υπήρξαν στόχος της «διαδικτυακής κακίας» στο SNS τους τελευταίους 12 μήνες. Αυτές οι εμπειρίες στο SNS φέρεται να οδήγησαν σε διάφορα αρνητικά αποτελέσματα, όπως τερματισμούς φιλιών, προβλήματα οικογενειακά, νεύρα στο σχολικό περιβάλλον και φυσικές διαμάχες με άλλους [54]. Υπάρχουν έντονες ανησυχίες από γονείς, εκπαιδευτικό προσωπικό και νομοθέτες σχετικά με τη φύση των συναντήσεων εκφοβισμού στον κυβερνοχώρο μεταξύ εφήβων στο SNS. Οι Jaishankar και Shariff (2008) εξέτασαν το φαινόμενο του διαδικτυακού εκφοβισμού σε πολλές χώρες και σημείωσαν ότι απαιτείται έρευνα προκειμένου να καλυφθεί το κενό πολιτικής που υπάρχει διεθνώς, για την καλύτερη διαχείριση αυτής της μορφής παρενόχλησης.

Τα μέσα κοινωνικής δικτύωσης συνέβαλαν σημαντικά στην αύξηση του διαδικτυακού εκφοβισμού την τελευταία δεκαετία. Ο Esin [26] διαπίστωσε ότι μεταξύ του 2003 και 2007, η δημοτικότητα των κοινωνικών μέσων αυξήθηκε καθώς έγινε πιο εύκολη η χρήση τους, με νέους τρόπους επικοινωνίας και ανταλλαγής πληροφοριών. Με την αυξημένη χρήση των κοινωνικών μέσων ως προτιμώμενη μέθοδο επικοινωνίας, ο εκφοβισμός κατέστη πιο εύκολος. Οι Whitaker και Kowalski [95] έδειξαν ότι το Twitter και το Facebook ήταν οι δύο περισσότερο χρησιμοποιούμενοι ιστότοποι στους οποίους διαπράττεται εκφοβισμός στον κυβερνοχώρο. Επιπλέον, ο Mesch [64] έδειξε ότι οι νέοι είχαν περισσότερες πιθανότητες να αναφέρουν ότι έχουν υπάρξει διαδικτυακό θύμα σε πλατφόρμες κοινωνικών μέσων (π.χ. αίθουσες συνομιλίας και ιστότοποι κοινωνικής δικτύωσης) παρά σε χώρους μη κοινωνικών μέσων (π.χ. διαδικτυακό παιχνίδι). Συνολικά, αυτά τα ευρήματα υποδηλώνουν ότι η θυματοποίηση στον κυβερνοχώρο είναι πιο πιθανό να συμβεί σε πλατφόρμες κοινωνικών μέσων. Ωστόσο, υπάρχει έλλειψη σχετικών ερευνών που να εξετάζουν τη σχέση μεταξύ της συμμετοχής στα μέσα κοινωνικής δικτύωσης και της διάπραξης του εκφοβισμού στον κυβερνοχώρο.

Οι πολιτικές ενάντια του εκφοβισμού στον κυβερνοχώρο επιβάλλονται μέσω μηχανισμών αυτορρύθμισης που διαθέτουν οι εταιρείες κοινωνικών μέσων για την αντιμετώπιση περιστατικών στις πλατφόρμες τους. Αυτοί οι μηχανισμοί μπορούν να περιλαμβάνουν εργαλεία αναφοράς, λογισμικό αποκλεισμού και φιλτραρίσματος, γεώφραξη, ανθρώπινα ή αυτοματοποιημένα συστήματα εποπτείας, καθώς και

εκπαιδευτικό υλικό για την καταπολέμηση του φαινομένου. Οι εταιρείες τείνουν να παρέχουν εργαλεία στους χρήστες τους για την αναφορά ενός χρήστη ή περιεχομένου που θεωρούν καταχρηστικό. Αφού εξετάσει την υπόθεση, η εταιρεία μπορεί να αποφασίσει εάν το αναφερόμενο περιεχόμενο παραβιάζει την πολιτική της και ως εκ τούτου αν θέλει να αποκλείσει τον χρήστη που το δημοσίευσε, να καταργήσει το καταχρηστικό περιεχόμενο ή να προβεί σε κάποια άλλη ενέργεια [64]. Έτσι π.χ. το Facebook παρέχει τις παρακάτω δυνατότητες στους χρήστες του, σε περίπτωση παρενόχλησης:

- Μπλοκάρισμα μηνυμάτων
- Υποβολή αναφοράς για απειλητικό μήνυμα
- Παράβλεψη, διαγραφή συζήτησης
- Μπλοκάρισμά χρήστη
- Υποβολή αναφοράς για ανάρμοστα post ή και φωτογραφίες
- Υποβολή αναφοράς για πλαστοπροσωπία
- Κ.α.

Αντίστοιχη πολιτική ακολουθείται και στο Twitter, δίνοντας την δυνατότητα στους χρήστες του να αναφέρουν ένα συγκεκριμένο tweet ως υβριστικό ή ακόμα και να αναφέρουν συνολικά το προφίλ ως χρήστη ως κακόβουλο ή με συνεχείς κακόβουλες ενέργειες. Τέλος και στο Instagram οι χρήστες μπορούν να προβούν σε αναφορά εναντίον μίας δημοσίευσης ή ενός χρήστη παρέχοντας γραπτώς λεπτομέρειες αναφορικά με τη φύση της ανεπιθύμητης συμπεριφοράς. Ορισμένες εταιρείες αναπτύσσουν επίσης εκπαιδευτικό υλικό σε συνεργασία με μη κυβερνητικούς οργανισμούς ηλεκτρονικής ασφάλειας που διδάσκουν στα παιδιά τις θετικές διαδικτυακές σχέσεις σε μια προσπάθεια πρόληψης του εκφοβισμού.

Αναφορικά με την συνεργασία των εταιρειών κοινωνικής δικτύωσης με τις δικαστικές και αστυνομικές αρχές, κατά κύριο λόγο ακολουθείται η κείμενη νομοθεσία της κάθε χώρας. Έτσι π.χ. το Facebook αναφέρει στον ιστότοπο του ότι:

«Κοινοποιεί στοιχεία λογαριασμών αποκλειστικά και μόνο σύμφωνα με τους όρους χρήσης του και την ισχύουσα νομοθεσία, συμπεριλαμβανομένου του ομοσπονδιακού νόμου των ΗΠΑ περί αποθηκευμένων επικοινωνιών (SCA), άρθρο 18 U.S.C., παράγραφοι 2701-2712. Σύμφωνα με το δίκαιο των ΗΠΑ: Για την κοινοποίηση βασικών στοιχείων των συνδρομητών (όπως ορίζεται στο άρθρο 18 U.S.C.,

παράγραφος 2703(c)(2)), τα οποία μπορεί να περιλαμβάνουν το ονοματεπώνυμο, τη διάρκεια συνδρομής, στοιχεία πιστωτικών καρτών, διευθύνσεις email και πρόσφατες διευθύνσεις IP σύνδεσης/αποσύνδεσης, εφόσον υπάρχουν, απαιτείται έγκυρη κλήτευση, εκδοθείσα στο πλαίσιο επίσημης ανακριτικής έρευνας. Για την κοινοποίηση συγκεκριμένων στοιχείων ή άλλων πληροφοριών που αφορούν το λογαριασμό, εξαιρουμένου του περιεχομένου επικοινωνιών, που μπορεί να περιλαμβάνουν κεφαλίδες μηνυμάτων και διευθύνσεις IP, εκτός από τα βασικά στοιχεία που αναφέρονται πιο πάνω, απαιτείται δικαστική απόφαση εκδοθείσα σύμφωνα με το άρθρο 18 U.S.C., παράγραφος 2703(d). Για την κοινοποίηση αποθηκευμένων πληροφοριών λογαριασμού, π.χ. μηνυμάτων, φωτογραφιών, βίντεο, δημοσιεύσεων χρονολογίου και πληροφοριών τοποθεσίας, απαιτείται ένταλμα έρευνας εκδοθέν σύμφωνα με τις διαδικασίες που προβλέπουν οι ομοσπονδιακοί κανόνες ποινικής δικονομίας ή τις αντίστοιχες διαδικασίες κάθε πολιτείας για την έκδοση ενταλμάτων κατόπιν απόδειξης πιθανής αιτίας. Με βάση την ερμηνεία που έχουμε υιοθετήσει όσον αφορά τη διάταξη περί εγγράφων εθνικής ασφάλειας, το Facebook υποχρεούται να παρέχει μόνο δύο κατηγορίες πληροφοριών: το ονοματεπώνυμο και τη διάρκεια της συνδρομής»».

Αντίστοιχα το twitter μπορεί να δεχτεί αιτήματα δικαστικών αρχών για διατήρηση αρχείων που αποτελούν δυνητικά σχετικά αποδεικτικά στοιχεία σε νομικές διαδικασίες. Διατηρεί αλλά δεν αποκαλύπτει, ένα προσωρινό στιγμιότυπο των σχετικών εγγραφών λογαριασμού για 90 ημέρες.

Τα αιτήματα διατήρησης, σύμφωνα με την ισχύουσα νομοθεσία, πρέπει:

- να υπογραφούν από τον αιτούντα υπάλληλο ·
- να υπάρχει μια έγκυρη επίσημη διεύθυνση ηλεκτρονικού ταχυδρομείου επιστροφής.
- αποστέλλεται σε επίσημο κρατικό επιστολόχαρτο σε μη επεξεργάσιμη μορφή ·

συμπεριλαμβάνοντας το @ όνομα χρήστη και τη διεύθυνση URL του σχετικού προφίλ Twitter (π.χ. [@twittersafety](https://twitter.com/twittersafety)) ή / και τον μοναδικό, δημόσιο αριθμό αναγνώρισης χρήστη (UID) του λογαριασμού Twitter.

Αν και οι επίσημες πολιτικές των εταιρειών κοινωνικών μέσων τείνουν να καταγράφονται στους ιστότοπους τους, αυτές οι πολιτικές δεν εξηγούν πάντα πώς λειτουργούν οι μηχανισμοί κατά του εκφοβισμού. Οι πλατφόρμες κοινωνικών μέσων

είναι διαδικτυακοί διαμεσολαβητές που επιτρέπουν την προβολή περιεχόμενου που δημιουργείται από χρήστες καθώς και διαδραστικότητα μεταξύ χρηστών και άμεση αλληλεπίδραση με το περιεχόμενο [18]. Στις Ηνωμένες Πολιτείες, σύμφωνα με την Ενότητα 230 του Communications Decency Act, οι διαδικτυακοί διαμεσολαβητές απαλλάσσονται από την ευθύνη για συμβάντα εκφοβισμού στον κυβερνοχώρο που λαμβάνουν χώρα στις πλατφόρμες τους, γεγονός που σημαίνει ότι δεν εμπλέκονται με περιεχόμενο. Σε ορισμένες χώρες, συγκεκριμένοι νόμοι έχουν διατάξεις που ζητούν από τις εταιρείες να συνεργαστούν με την επιβολή του νόμου για να αποκαλύψουν την ταυτότητα των δραστών [25] ή να καταργήσουν συγκεκριμένο περιεχόμενο κατόπιν αιτήματος εκπροσώπων της κυβέρνησης. Ωστόσο, κανένας νόμος δεν ορίζει ποιοι μηχανισμοί πρέπει να αναπτύξει κάθε εταιρεία κοινωνικών μέσων για την αντιμετώπιση του εκφοβισμού.

2.4 Σημαντικές υποθέσεις διαδικτυακού εκφοβισμού

Στο κεφάλαιο αυτό παρουσιάζονται κάποιες από τις πλέον γνωστές υποθέσεις διαδικτυακού εκφοβισμού τόσο σε παγκόσμιο όσο και σε τοπικό επίπεδο, ξεκινώντας ίσως με την πιο γνωστή αλλά και ιδιαίτερος τραγική ιστορία του Ryan Halligan. Ο Ryan Halligan ήταν ένα 13χρονο αγόρι που ζούσε στο Essex Junction του Βερμόντ.

Στις 7 Οκτωβρίου 2003, αυτοκτόνησε ως αποτέλεσμα του πόνου και της ταλαιπωρίας που είχε βιώσει από τους συμμαθητές του στο γυμνάσιο. Ο πατέρας του Ryan περιέγραψε τις δυσκολίες της καθημερινής ζωής που αντιμετώπισε ο Ryan, συμπεριλαμβανομένης μιας φιλίας με ένα νεαρό αγόρι που ο Ryan πίστευε ότι ήταν καλός του φίλος. Ο Ryan αντιμετώπιζε σημαντικές μαθησιακές δυσκολίες από νεαρή ηλικία. Κατά τη διάρκεια των σπουδών του στο γυμνάσιο, ο Ryan δέχτηκε φυσικές απειλές από έναν άλλο μαθητή, με τον οποίο στη συνέχεια ανέπτυξε φιλική σχέση. Ωστόσο, η εκμυστήρευση ενός ιατρικού γεγονότος προς τον φίλο του, οδήγησε σε γεγονότα ταπείνωσης μέσω κοινοποιήσεων σε αρκετούς άλλους μαθητές στα κοινωνικά δίκτυα. Το αποκορύφωμα του συναισθηματικού στρες και της αγωνίας οδήγησε τον Ryan στην αυτοκτονία.

Η Megan Meier ήταν ένα υπέρβαρο 13χρονο κορίτσι που μαχόταν με τη χαμηλή αυτοεκτίμηση και την κατάθλιψη. Έπεισε τη μητέρα της να της επιτρέψει να έχει λογαριασμό στο MySpace. Η μητέρα της Μέγκαν ήταν αρχικά απρόθυμη, αλλά παρακολουθούσε τις δραστηριότητες της κόρης της ενώ είχε και τον κωδικό πρόσβασης στον λογαριασμό της. Τον Οκτώβριο του 2006 η Megan ήρθε σε επαφή με τον 16χρονο Josh Evans μέσω του MySpace. Κολακευμένη από την προσοχή του η μαμά της Μέγκαν συμφώνησε ότι θα μπορούσε να προσθέσει τον Τζος ως φίλο. Αφού κέρδισε την εμπιστοσύνη και την αγάπη της Μέγκαν, ο Τζος μετά από λίγο καιρό είπε ότι δεν ήθελε πλέον να είναι φίλος της λόγω του τρόπου με τον οποίο αντιμετωπίζει τους φίλους της. Ο Josh και άλλοι άρχισαν να δημοσιεύουν στο MySpace χαρακτηρισμούς ενάντια στην Megan αποκαλώντας την «παχιά» και «τσούλα». Έπειτα έλαβε ένα μήνυμα από το «Josh» που της είπε «ο κόσμος θα ήταν ένα καλύτερο μέρος χωρίς αυτήν». Η Μέγκαν κρεμάστηκε στην ντουλάπα της κρεβατοκάμαράς της και πέθανε στο νοσοκομείο την επόμενη μέρα. Μετά το θάνατο της Μέγκαν αποκαλύφθηκε ότι ο Josh τελικά ήταν η Sarah Drew, πρώην φίλη και γείτονα της Μέγκαν, η οποία δημιούργησε εικονικό λογαριασμό με αποκλειστικό σκοπό να βλάψει την Μέγκαν. Η υπόθεση απασχόλησε τα μέσα μαζικής ενημέρωσης της εποχής, αρκετό καιρό μετά το θάνατο της Μέγκαν.



Εικόνα 7. Η είδηση της αυτοκτονίας της Μέγκαν σε άρθρο σε εφημερίδα

Η Τζέσικα Λόγκαν ήταν μια ιδιαίτερα όμορφη μαθήτρια γυμνασίου, η οποία φιλοδοξούσε να σπουδάσει γραφιστική στο Πανεπιστήμιο του Σινσινάτι. Δυστυχώς, μια γυμνή φωτογραφία της Τζέσικα φέρεται να στάλθηκε στο φίλο της, και όταν η σχέση τελείωσε, η εικόνα σύντομα έγινε viral σε τέσσερα γυμνάσια. Μαθητές παρενοχλούσαν για μήνες την Τζέσικα, αποκαλώντας την «πόρνη» ενώ ενίοτε της πετούσαν και αντικείμενα. Παρόλο που ο τοπικός αξιωματικός της αστυνομίας, η διεύθυνση του σχολείου και το γραφείο του τοπικού εισαγγελέα γνώριζαν τον εκφοβισμό της Τζέσικα, ο καθένας είπε ότι δεν μπορούσε να ασκήσει κατηγορίες εναντίον των παιδιών. Ο αξιωματικός της αστυνομίας δήλωσε ότι βοήθησε στην επίλυση της κατάστασης ζητώντας από τους μαθητές να διαγράψουν το βίντεο και ενθάρρυνε την Τζέσικα να δημοσιοποιήσει την ιστορία της, χωρίς να συμβουλευτεί τη μητέρα της. Λίγο μετά την συνέντευξη της Τζέσικα, εντούτοις, η κακοποίηση

εντατικοποιήθηκε. Μετά από μήνες αίσθησης κατάθλιψης και φόβου η Τζέσικα τερμάτισε τη ζωή της βρισκόμενη κρεμασμένη στην κρεβατοκάμαρά της (Albin, 2012).

Ο Tyler Clementi ήταν ένας 18χρονος πρωτοετής φοιτητής στο Πανεπιστήμιο Rutgers που αυτοκτόνησε στις 22 Σεπτεμβρίου 2010, σύμφωνα με πληροφορίες μετά από εκφοβισμό στον κυβερνοχώρο από τον συγκάτοικο του στο κολλέγιο, Dharun Ravi. Λίγο μετά τη μετακίνηση στους πανεπιστημιακούς κοιτώνες, ο Κλεμέντι ζήτησε ιδιωτική χρήση του κοινόχρηστου δωματίου τους για να δεχτεί έναν επισκέπτη, γνωστό σε δικαστικά έγγραφα ως M.B. Ο Ravi ισχυριζόμενος ότι ανησυχεί για την ασφάλεια των αντικειμένων του στο δωμάτιο, απενεργοποίησε το φως στην κάμερα του, βάζοντας την να δείχνει στο πλάι του δωματίου του Κλεμέντι και την ενεργοποίησε από τον υπολογιστή ενός φίλου του όταν έφυγε από το δωμάτιο. Όταν ενεργοποίησε την κάμερα, παρατήρησε για λίγο τον Κλεμεντί να φιλάει τον M.B. πριν τερματίσει τη σύνδεση. Ο Ράβι έστειλε έπειτα ένα tweet αναφέροντας ότι ο συγκάτοικος του φιλούσε κάποιον. Λίγες μέρες αργότερα, όταν ο Clementi ζήτησε και πάλι ιδιωτική χρήση του δωματίου, ο Ravi συμφώνησε, αλλά δημοσίευσε ένα μήνυμα στον λογαριασμό του στο Twitter, ζητώντας από τους ακολούθους του να συνομιλήσουν μέσω βίντεο εκείνο το βράδυ κατά τη διάρκεια του χρόνου που ο Clementi ζήτησε το δωμάτιο. Ο Κλέμεντι είχε ήδη ανακαλύψει ότι ο Ράβι τον κατασκοπεύει αφού διάβασε το πρώτο του tweet και απενεργοποίησε τον υπολογιστή του Ravi πριν από τη δεύτερη συνάντηση με τον M.B. Την ίδια ημέρα, ο Κλεμέντι υπέβαλε αίτημα αλλαγής δωματίου στο πανεπιστήμιο και διαμαρτυρήθηκε για τις ενέργειες του Ράβι. Την επόμενη μέρα ο Κλεμέντι πήδηξε από τη γέφυρα George Washington και πνίγηκε στον ποταμό Χάντσον. Ο Ράβι δεν κατηγορήθηκε για το θάνατο του Κλεμέντι, αλλά διώχθηκε και κρίθηκε ένοχος για 15 παραβιάσεις της ιδιωτικής ζωής, παρεμπόδιση της δίωξης και εκφοβισμό, που θεωρείται έγκλημα μίσους. Παρά το γεγονός ότι αντιμετώπισε πιθανότητα 10 ετών στη φυλακή, καταδικάστηκε τελικά σε 30 ημέρες [7].

Η δεκαπεντάχρονη Amanda Todd κρεμάστηκε στο σπίτι της στο Port Coquitlam, στον Καναδά στις 10 Οκτωβρίου του 2012, ένα μήνα μετά από τα 16α γενέθλιά της και πέντε εβδομάδες μετά την ανάρτηση ενός τραγικού βίντεο στο YouTube, στο οποίο περιγράφεται λεπτομερώς το πώς παρενοχλήθηκε και εκφοβίστηκε στο διαδίκτυο. Το βίντεο που δημοσίευσε στο YouTube είχε τον τίτλο «Η ιστορία μου: αγώνες, εκφοβισμός, αυτοκτονία και αυτοτραυματισμός». Το βίντεο που ήταν ασπρόμαυρο, δείχνει την Amanda να λέει την ιστορία της σε μια σειρά από κάρτες flash [23].

Σε μια διαδικτυακή συνομιλία μέσω βίντεο με έναν άγνωστο άντρα, αφού δέχτηκε τα κομπλιμέντα του, ζήτησε από την Amanda να του δείξει το στήθος και εκείνη δυστυχώς δέχτηκε. Ένα χρόνο αργότερα, επικοινωνήσε με τον άντρα μέσω Facebook, όπου την απείλησε ότι αν δεν του έκανε μία αντίστοιχη παράσταση, θα έστελνε τη φωτογραφία στην οικογένεια, τους φίλους και τους συμμαθητές της, έχοντας καταφέρει να αποκτήσει όλες τις προσωπικές της πληροφορίες: προφίλ Facebook, διεύθυνση, όνομα σχολείου, ονόματα μελών της οικογένειας, ονόματα φίλων κ.λπ. Η Amanda αρνήθηκε. Κατά τη διάρκεια των Χριστουγέννων, η αστυνομία εμφανίστηκε στην πόρτα της στις 4 π.μ. ρωτώντας για τη φωτογραφία της. Προφανώς, η φωτογραφία είχε σταλεί σε όλους, όπως είχε απειλήσει ο άντρας. Ως αποτέλεσμα, η Amanda παρουσίασε κατάθλιψη και άγχος, στράφηκε στο αλκοόλ και τα ναρκωτικά για να αντιμετωπίσει αυτήν την κατάσταση.

Η Αμάντα κατέληξε να αλλάζει σχολεία, αλλά ο διαδικτυακός εκφοβισμός συνεχίστηκε. Ο άντρας που την είχε απειλήσει δημιούργησε μια σελίδα στο Facebook με την εικόνα του στήθους της Amanda ως φωτογραφία προφίλ του. Οι συμμαθητές της άρχισαν να την κοροϊδεύουν. Η Amanda άρχισε να αυτοτραυματίζεται και προσπάθησε να αυτοκτονήσει πίνοντας χλωρίνη. Μεταφέρθηκε στο νοσοκομείο όπου και επέζησε.

Όταν έμαθαν για την απόπειρα αυτοκτονίας της, οι φίλοι της στο Facebook δημοσίευσαν σκληρά σχόλια. Μετακόμισε με τη μητέρα της σε μια νέα πόλη και σε ένα νέο σχολείο και σκέφτηκε ότι τα πράγματα μπορεί να γίνουν καλύτερα, αλλά οι βασανιστές της, την ακολούθησαν. Σχόλια στη σελίδα της στο Facebook ανέφεραν ότι έπρεπε να αυτοκτονήσει και περιελάμβανε φωτογραφίες λευκών μπουκαλιών και τάφρων με ετικέτα στο προφίλ της. Το άγχος της αυξήθηκε σε τέτοιο επίπεδο που ξεκίνησε θεραπεία με αντικαταθλιπτικά και άρχισε συμβουλευτική. Μετά από υπερβολική δόση που απαιτούσε διήμερη παραμονή στο νοσοκομείο, αποφάσισε να δημιουργήσει βίντεο με την εμπειρία της.

Το βίντεο ξεκινούσε με τις παρακάτω φράσεις:

Παλεύω να μείνω σε αυτόν τον κόσμο, γιατί όλα με αγγίζουν τόσο βαθιά. Δεν το κάνω για προσοχή. Το κάνω για να εμπνεύσω και να δείξω ότι μπορώ να είμαι δυνατός. Έκανα πράγματα στον εαυτό μου για να κάνω τον πόνο να φύγει, γιατί προτιμώ να βλάψω τον εαυτό μου παρά κάποιον άλλο. Οι κακοί είναι κακοί αλλά παρακαλώ μην

μισείτε. Ελπίζω να σας δείξω ότι ο καθένας έχει μια ιστορία, και το μέλλον κάθε ατόμου θα είναι λαμπρό μια μέρα. Είμαι ακόμα εδώ, έτσι δεν είναι; [23].



Εικόνα 8. Στιγμιότυπο από το συγκλονιστικό βίντεο της Amanda Todd στο Youtube

Επίσης σύμφωνα με Tech Transparency Project, μία μη κερδοσκοπική οργάνωση αποτελούμενη από επιφανείς δημοσιογράφους, ακαδημαϊκούς κ.α. με κύριο στόχο την ανίχνευση της επιρροής της τεχνολογίας σε διάφορες εκφάνσεις της κοινωνικής ζωής, σε πρόσφατη έρευνα αναφέρει ότι το Facebook έχει χρησιμοποιηθεί ευρέως από παιδόφιλους για τη σεξουαλική κακοποίηση παιδιών. Μετά από επανειλημμένες εκκλήσεις από επιζώντες κακοποίησης και τους γονείς τους, η εταιρεία υποσχέθηκε να αποτρέψει τη χρήση της πλατφόρμας της από εγκληματίες που στοχεύουν παιδιά. «Η εκμετάλλευση παιδιών είναι μια από τις πιο σοβαρές απειλές στις οποίες εστιάζουμε»,

δήλωσε ο διευθύνων σύμβουλος Mark Zuckerberg στους νομοθέτες τον Οκτώβριο του 2019. «Χτίζουμε εξελιγμένα συστήματα για να εντοπίσουμε αυτήν τη συμπεριφορά».

Ωστόσο, η έρευνα έδειξε ότι τα συστήματα του Facebook αποτυγχάνουν να εξαλείψουν τέτοια χρήση. Χρησιμοποιώντας έναν προσαρμοσμένο κώδικα, το TTP σάρωσε το κείμενο των ανακοινώσεων του Υπουργείου Δικαιοσύνης των ΗΠΑ και συνέλεξε ό, τι ανέφερε το Facebook. Στη συνέχεια, οι αναλυτές εντόπισαν 366 μεμονωμένες ποινικές υποθέσεις που αφορούσαν φερόμενους παιδόφιλους που χρησιμοποίησαν το κοινωνικό δίκτυο για εκμετάλλευση παιδιών, συμπεριλαμβανομένης της διανομής εικόνων σεξουαλικής κακοποίησης, της στρατολόγησης παιδιών και της σωματεμπορίας. Στη συντριπτική πλειονότητα αυτών των περιπτώσεων, το Facebook δεν παρείχε την αρχική ενημέρωση στις αρχές. Αντίθετα, αξιωματούχοι δήλωσαν ότι βασίστηκαν σε πληροφορίες από το κοινό, προϊστάμενους από άλλες έρευνες ή επιχειρήσεις για να εντοπίσουν υπόπτους. Οι υποθέσεις που αναλύθηκαν από το Υπουργείο Δικαιοσύνης έλαβαν χώρα στο σύνολο των ΗΠΑ. Περιλαμβάνουν έναν άνδρα από το Κεντάκι που κατηγορείται ότι έστειλε χιλιάδες μηνύματα σε πολλά παιδιά μέσω Facebook, έναν άντρα από το Ρόουντ Άιλαντ που φέρεται να παριστάνει την έφηβη για να παρασύρει αγόρια σε σεξουαλική δραστηριότητα ζωντανής ροής στο Facebook Messenger και έναν καταδικασμένο για σεξουαλικά αδικήματα από το Μιζούρι που φέρεται να χρησιμοποίησε το Facebook Messenger για επικοινωνία με ένα 13χρονο κορίτσι. Μεταξύ των κορυφαίων ευρημάτων από την ανάλυση της TTP, η οποία εξέτασε τα δελτία τύπου του Υπουργείου Δικαιοσύνης από τον Ιανουάριο του 2013 έως τον Δεκέμβριο του 2019:

- Η έρευνα εντόπισε 366 ομοσπονδιακές ποινικές υποθέσεις για επτά χρόνια, όπου οι ύποπτοι χρησιμοποιούν Facebook για εκμετάλλευση παιδιών.
- Διαπιστώθηκε επίσης ότι τέτοιες περιπτώσεις γίνονται συχνότερες, από 10 ανά τρίμηνο το 2013 σε έως 23 ανά τρίμηνο το 2019. (Κατά την ίδια περίοδο, ο αριθμός των χρηστών του Facebook αυξήθηκε επίσης σημαντικά.)
- Μόνο το 9% των περιπτώσεων διερευνήθηκαν επειδή το Facebook δεν τις ανέφερε στις αρχές, θέτοντας ερωτήματα σχετικά με την αποτελεσματικότητα της παρακολούθησης της εγκληματικής δραστηριότητας που στοχεύει τα παιδιά στο Facebook.
- Ο αριθμός των περιπτώσεων τις οποίες το Facebook ανέφερε αυξήθηκε μετά την έγκριση του νόμου FOSTA-SESTA, ο οποίος για πρώτη φορά έκανε την

εταιρεία να υπόκειται σε αστικές κυρώσεις για την εμπορία σεξ στην πλατφόρμα της. Αυτό υποδηλώνει ότι το Facebook μπορεί να έχει γίνει πιο επιφυλακτικό λόγω της πιθανότητας δικαστικών διαφορών, παρά την αρχική αντίθεσή του στο νόμο.[85]

Επιπλέον των παραπάνω, τα social media καταγράφονται να παίζουν ένα σημαντικό αυξανόμενο ρόλο στο φαινόμενο human trafficking. Ενδεικτικά αναφέρονται κάποιες από τις υποθέσεις που είτε είδαν το φως της δημοσιότητας είτε αναδείχθηκαν στα πλαίσια ερευνητικής προσπάθειας [49].

Ο Campbell Fraser στην έρευνα του για το ρόλο των social media στο human trafficking καταγράφει πλήθος περιπτώσεων τις οποίες και έζησε από κοντά. Ο Sahring είναι ένας 51χρονος Ινδονήσιος μεσίτης που προμηθεύει αλιευτικά με πληρώματα. Προμηθεύει εργασία σε όλη τη Νοτιοανατολική Ασία, αλλά το μεγαλύτερο μέρος της εργασίας του προέρχεται τώρα από μεσίτες με τους οποίους έχει συνεργασίες στην Καμπότζη. Ο Sahring ισχυρίζεται ότι προσφέρει μια «τελευταία ευκαιρία» για τους κατοίκους της Καμπότζης που έχουν χάσει τον δρόμο τους λόγω χρέους ή ναρκωτικών και πιστεύει ότι απαιτείται ένα αυστηρό καθεστώς για να διατηρήσει την τάξη και να βοηθήσει αυτούς τους άντρες να βελτιώσουν τη ζωή τους. Ο Sahring ισχυρίζεται ότι οι καπετάνιοι επιλέγουν τους εργάτες του καθώς γνωρίζουν ότι συμμορφώνονται με όλα τα αιτήματα που υποβάλλουν. Άλλοι μεσίτες προσφέρουν λιγότερο πειθαρχημένη εργασία, και οι καπετάνιοι, σύμφωνα με τον Sahring, είναι λιγότερο ικανοποιημένοι με αυτούς. Ο Sahring επικοινωνεί με ένα δίκτυο μεσιτών που βασίζεται σε μέσα κοινωνικής δικτύωσης σε κάθε πόλη της Καμπότζης και τους αποστέλλει ηλεκτρονικά μια προμήθεια για κάθε μετανάστη εργαζόμενο που στέλνουν. Χρησιμοποιεί επίσης άλλους μεσίτες στο δίκτυο κοινωνικών μέσων του για τη μεταφορά των μεταναστών στην τοποθεσία των καπεταναίων [30].

Σε μία ακόμα πιο ακραία περίπτωση ο Fraser αναφέρεται στον Siong ένας 56χρονος άνδρας πολίτης των ΗΠΑ κινεζικής εθνικότητας. Έχοντας αγοράσει ένα νεφρό στην Κίνα το 2010, έχει αναπτύξει ένα εκτεταμένο δίκτυο μεσιτείας που στέλνει κυρίως Αμερικανούς και Καναδούς πολίτες στην Κίνα για μεταμόσχευση. Πολλοί από τους πελάτες του προέρχονται απευθείας από γιατρούς ειδικούς στα νεφρά, οι οποίοι είναι κυρίως κινεζικής καταγωγής και παραπέμπουν σε αυτόν ασθενείς που χρειάζονται μεταμόσχευση. Αυτοί οι γιατροί επικοινωνούν με τη Siong μέσω e-mail και μέσω κοινωνικής δικτύωσης. Στη συνέχεια, έρχεται σε επαφή με τον χειρουργό που

πραγματοποίησε τη δική του μεταμόσχευση και εισπράττει προμήθεια για κάθε αγοραστή. Ο Siong παραδέχεται ότι γνώριζε ότι ο νεφρός του ανήκε σε έναν εκτελεσμένο κρατούμενο, αλλά τώρα οι νεφροί στην Κίνα προέρχονται από ζωντανούς δότες. Οι πιο οργανωμένοι χειρουργοί παράνομων μεταμοσχεύσεων έχουν παγκόσμια δίκτυα αξιόπιστων μεσιτών που ελπίζουν να τους προσφέρουν σταθερή προσφορά νέων πελατών.

Τα social media αποτελούν επίσης χώρο τέλεσης εκβιαστικών συμπεριφορών με στόχο κυρίως την αποκόμιση οικονομικού οφέλους. Το Δεκέμβριο του 2020 η αστυνομία στο Νέο Δελχί συνέλαβε 26χρονο με κατηγορίες εκβιασμού για αποκόμιση χρημάτων από περισσότερες από 100 γυναίκες, παραποιώντας τις φωτογραφίες τους και απειλώντας να τις δημοσιεύσει στα κοινωνικά μέσα. Ο κατηγορούμενος Sumit Jha συνήθιζε να κατεβάζει και να παραποιεί τις φωτογραφίες προφίλ των γυναικών από τους λογαριασμούς κοινωνικών μέσων, να δημιουργεί πλαστά προφίλ στην ίδια πλατφόρμα και να στέλνει απειλητικά μηνύματα στις γυναίκες ότι οι γυμνές φωτογραφίες τους θα δημοσιεύονταν στο διαδίκτυο σε περίπτωση που δεν πληρώσουν χρήματα. Σύμφωνα με την αστυνομία, το ζήτημα έγινε γνωστό, όταν μια γυναίκα διευθυντής τράπεζας παραπονέθηκε για διαδικτυακή παρενόχληση και απειλές εκβιασμού για να μην ανέβει η γυμνή εικόνα της στον λογαριασμό της στο Instagram. Ο κατηγορούμενος απαίτησε επίσης χρήματα από την καταγγέλλουσα, καθώς και από τις επαφές της στα κοινωνικά μέσα. "Ο κατηγορούμενος χρησιμοποιούσε κλήσεις VOIP μέσω WhatsApp και άλλων εφαρμογών για να αποφύγει τον εντοπισμό[61].

Σε μια συγκλονιστική υπόθεση τον Ιανουάριο του 2021, ένας 26χρονος άνδρας φέρεται να παραβίασε λογαριασμούς στα μέσα κοινωνικής δικτύωσης περίπου 400 κοριτσιών και στη συνέχεια να τα εκβίαζε για χρήματα. Ο κατηγορούμενος, που ταυτοποιήθηκε ως Vinit Mishra, κατηγορήθηκε από αξιωματούχους της μονάδας εγκλήματος στον κυβερνοχώρο της αστυνομίας του Lucknow και πάλι στην Ινδία, μετά από καταγγελία ενός από τα θύματά του. Σύμφωνα με την αστυνομία, πρόσφατα, ένα κορίτσι υπέβαλε καταγγελία, δηλώνοντας ότι ένας άγνωστος άντρας την εκβίαζε για χρήματα χρησιμοποιώντας φωτογραφίες της στις οποίες είχε πρόσβαση μετά από παραβίαση του λογαριασμού της στο Facebook. Μετά από αυτό, ξεκίνησε έρευνα, η οποία οδήγησε στη σύλληψη του Mishra[86].

Στις 7 Ιουλίου 2017, το περιφερειακό δικαστήριο των ΗΠΑ στη Βόρεια Περιφέρεια του Τέξας καταδίκασε τον Robert Dion Ables σε 80 χρόνια σε ομοσπονδιακή φυλακή

μετά την αποδοχή της ενοχής του. Ένα δελτίο τύπου του Τμήματος Δικαιοσύνης αναφέρει ότι, σύμφωνα με έγγραφα του δικαστηρίου, ο Ables έπεισε πολλές ανήλικες γυναίκες να του στείλουν γυμνές φωτογραφίες τους μέσω των κοινωνικών μέσων και στη συνέχεια απείλησε να διαδώσει τις εικόνες στο διαδίκτυο εάν τα θύματα δεν παρείχαν περισσότερο υλικό. Σύμφωνα με το Dallas Morning News, ο Ables παραδέχτηκε ότι εκτός από τη στόχευση κοριτσιών, εκβίασε και ενήλικες άνδρες για χρήματα αφού τους έπεισε να ανταλλάξουν γυμνές φωτογραφίες μαζί του. Το Γραφείο Εισαγγελέων των ΗΠΑ στη Νότια Περιοχή της Νέας Υόρκης ανακοίνωσε στις 14 Φεβρουαρίου 2017 ότι ο Kelvin Acosta καταδικάστηκε σε ποινή φυλάκισης 25 ετών μετά την παραδοχή του για παραγωγή παιδικής πορνογραφίας. Το δελτίο τύπου του Υπουργείου Δικαιοσύνης ισχυρίζεται ότι ο Acosta εξαπάτησε γυναίκες θύματα, ηλικίας 13 έως 25 ετών, για την παροχή προσωπικών πληροφοριών μέσω κοινωνικών μέσων, τα οποία στη συνέχεια του επέτρεψαν να παραβιάσει τους λογαριασμούς email τους. Βρίσκοντας φωτογραφίες ή βίντεο στους λογαριασμούς τους, ο Acosta φέρεται να εκβίασε πολλούς ανηλίκους με στόχο πορνογραφικές συζητήσεις και βίντεο, χρήματα ή και τα δύο.[95]

2.5 Σημαντικές υποθέσεις διαδικτυακού εκφοβισμού στον Ελλαδικό χώρο

Στην Ελλάδα, αν και το φαινόμενο δεν έχει λάβει τις διαστάσεις άλλων χωρών, εντούτοις τα τελευταία χρόνια υπάρχει σημαντική αύξηση των υποθέσεων. Παρακάτω

παρατίθενται κάποιες από τις σοβαρότερες υποθέσεις cyberbullying, όπως τις παραθέτουν αστυνομικοί της δίωξης ηλεκτρονικού εγκλήματος. Η πρώτη υπόθεση αφορά την ερωτική ηλεκτρονική συνεύρεση 13χρονης μαθήτριας με 14χρονο συμμαθητή της. Η μαθήτρια όντας ερωτευμένη με τον 14χρονο πείστηκε στο να προβεί σε «cyber sex» χωρίς να γνωρίζει ότι καταγράφεται από τον συνομήλικό της. Το βίντεο εν συνεχεία κυκλοφόρησε στο διαδίκτυο με την μαθήτρια να υφίσταται τεράστιο ψυχολογικό σοκ, οδηγώντας την σε αλλαγή σχολικού περιβάλλοντος. Σύμφωνα με πληροφορίες, πλέον διαμένει σε πόλη της επαρχίας χωρίς να έχει πλήρως ξεπεράσει αυτό που συνέβη. Σε μεγάλη πόλη της περιφέρειας, μονταρισμένο βίντεο εμφάνιζε μαθήτρια να πρωταγωνιστεί σε ταινία πορνό. Το βίντεο κυκλοφόρησε άμεσα και έγινε γνωστό στο στενό κύκλο της μαθήτριας, με αποτέλεσμα να της ασκηθεί τεράστια ψυχολογική πίεση. Μετά από σχετική καταγγελία, η δίωξη ηλεκτρονικού εγκλήματος εντόπισε τον δράστη και κατέβαλε το βίντεο από το διαδίκτυο [54].

Στην Πελοπόννησο 14χρονος μαθητής κατάφερε να χακάρει την κάμερα συμμαθήτριας του, με αποτέλεσμα να καταγράψει όλες τις κινήσεις της. Ο μαθητής απειλούσε την κοπέλα ότι το υλικό θα δημοσιευθεί στο διαδίκτυο. Οι γονείς της κοπέλας κατήγγειλαν το περιστατικό στην αστυνομία. Πρόσφατα ήλθε στην δημοσιότητα ακόμη μία υπόθεση διαδικτυακού εκφοβισμού στην Ρόδο, με θύμα ένα 12χρονο κορίτσι, το οποίο έπεσε θύμα αγνώστου χρήστη μέσω της εφαρμογής chat «discord». Ο άγνωστος έπεισε την νεαρή κοπέλα να του στέλνει γυμνές φωτογραφίες καθώς και να αυτοτραυματίζεται με ξυράφι. Η κοπέλα αποπειράθηκε να αυτοκτονήσει αλλά ευτυχώς οι γονείς πρόλαβαν το μοιραίο. Η υπόθεση βρίσκεται υπό διερεύνηση [54].

Στην Καλαμάτα διεστραμμένος ζαχαροπλάστης κατάφερε να παραβιάσει λογαριασμούς μαθητριών και να τις καταγράψει με κάμερα χωρίς ρούχα, ζητώντας κατόπιν εκβιαστικά να συναντηθούν μαζί του προκειμένου οι φωτογραφίες να μην διαρρεύσουν στο διαδίκτυο. Οι γονείς μίας εκ των μαθητριών απευθύνθηκε στην Δίωξη Ηλεκτρονικού Εγκλήματος, ο ζαχαροπλάστης συνελήφθη και σχηματίστηκε σε βάρος του δικογραφία ενώ ακόμα κυκλοφορεί ελεύθερος [70]. Σε απόπειρα αυτοκτονίας οδηγήθηκε μαθήτρια η οποία είδε τον εαυτό της να ποζάρει σε εμφανώς παραποιημένο βίντεο σεξουαλικής φύσεως. Η υπόθεση η οποία είδε και τα φώτα της δημοσιότητας τελικά εξιχνιάστηκε και πάλι από τη δίωξη του ηλεκτρονικού εγκλήματος. Θύτης ήταν ένας συμμαθητής της κοπέλας, με βάση τα ηλεκτρονικά ίχνη που άφησε πίσω του. Η

αιτία με βάση όσα αποκαλύφθηκαν ήταν η ηθική απαξίωση της νεαρής καθώς ήταν η καλύτερη μαθήτρια της τάξης με εκείνον να ακολουθεί δεύτερος [70]. Αντίστοιχα σε ιδιωτικό σχολείο των βορείων προαστίων της Αθήνας, νεαρή είδε να διακινείται άσεμνο περιεχόμενο με παραποιημένες φωτογραφίες από το λογαριασμό της στο Facebook. Η δίωξη ηλεκτρονικού εγκλήματος αποκάλυψε ότι ο ένοχος ήταν συμμαθήτρια της κοπέλας, η οποία παραδέχτηκε ότι οι ενέργειες βασίζοντας σε λόγους αντιζηλίας [40].

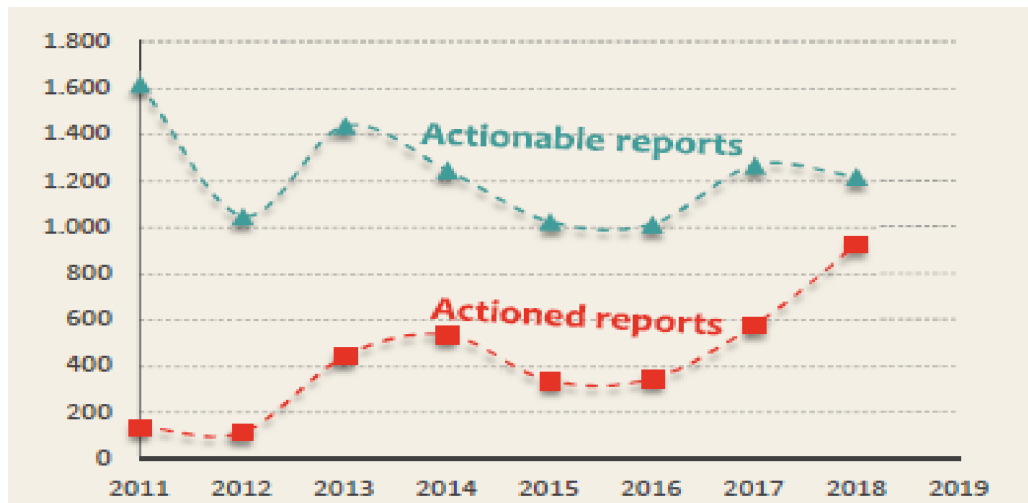
Η πρώτη cyber bullying αυτοκτονία στην Ελλάδα καταγράφεται το φθινόπωρο του 2016. Η Λίνα Γαλήνη, φοιτήτρια του ΤΕΦΑΑ Θεσσαλονίκης, θα πηδήξει από τον 9^ο όροφο της εστίας του Πανεπιστημίου, δίνοντας τέλος στην ζωή της. Λίγο πριν θα αναρτήσει στο λογαριασμό της στον Instagram «Κάποτε θα φύγει εκείνος που διώχνεις. Θα φύγει και θα πάρει μαζί του ό,τι σου έδωσε και δεν το εκτίμησες, όλα όσα θεώρησες δεδομένα. Κάποτε θα πάψει να περπατά μόνος σε έναν δρόμο για δύο, θα σφίξει τα δόντια, θα γλείψει τις πληγές του και θα σου αδειάσει τη γωνιά. Θα φύγει, μην αμφιβάλεις... Από αξιοπρέπεια δεν έμεινε κανείς. Μονάχα από αγάπη. Μα κι αυτή κάποτε, από αξιοπρέπεια αποχωρεί». Αιτία φαίνεται να είναι ο άνθρωπος με τον οποίο διατηρούσε σχέση και ο οποίος την έπεισε να ποζάρει γυμνή ή ημίγυμνη με την υπόσχεση ότι θα την κάνει μοντέλο. Η Λίνα έκπληκτη θα δει εν συνεχεία τις φωτογραφίες της να «ταξιδεύουν» στο διαδίκτυο ενώ κατόπιν θα αρχίσει να δέχεται υβριστικά μηνύματα ή πρόστυχες προτάσεις από άγνωστους άντρες, με κάποιους από αυτούς να της προτείνουν ερωτική συνεύρεσή. Και ενώ η νέα της σχέση με άντρα από την Καλαμαριά φαίνεται να αποτελεί την αρχή του τέλους για τα προβλήματα της, εντούτοις η νέα της σχέση απειλεί να διαρρεύσει στο διαδίκτυο βίντεο με τις ερωτικές τους περιπτώξεις αν εκείνη δεν ενδώσει στην απαίτηση του να συνευρεθούν ερωτικά με περισσότερα άτομα. Με τις απειλές να γίνονται συνεχώς πιο έντονες η Λίνα, ενημερώνει τις συμμαθήτριες στην εστία ότι θα ανέβει στον 9^ο όροφο της εστίας για ένα τσιγάρο, όπου και έδωσε τέλος στην ζωή της. Αν και η μητέρα της κοπέλας μέσω του δικηγόρου της έδωσε μεγάλο αγώνα προκειμένου η υπόθεση να φτάσει στην δικαιοσύνη, εντούτοις η υπόθεση τελικά αρχειοθετήθηκε, αφού σύμφωνα με το σκεπτικό της απόφασης ο θάνατος αποδίδεται σε αυτοκτονία. Σύμφωνα με τον κο. Σφακιανάκη, πρώην επικεφαλή της Δίωξης Ηλεκτρονικού Εγκλήματος, στην υπόθεση καταγράφονται αρκετές παραλείψεις και κενά τα οποία οφείλονται εν γένει στην άγνοια χειρισμού τέτοιων υποθέσεων [69].

Κοινό χαρακτηριστικό της πλειονότητας των περιπτώσεων που εξιχνιάστηκαν και κατέληξαν στην δικαιοσύνη ήταν η εμπλοκή της δίωξης ηλεκτρονικού εγκλήματος. Η υπηρεσία ιδρύθηκε με το Π.Δ. 178/2014 ενώ η αποστολή της περιλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η ίδρυση της υπηρεσίας και η στελέχωση της από εξειδικευμένο προσωπικό είχε ως αποτέλεσμα το ψηφιακό έγκλημα να καταπολεμηθεί αποτελεσματικότερα με σύγχρονες μεθόδους έναντι των κλασσικών μεθόδων της ελληνικής αστυνομίας. Στην εσωτερική της δομή, αποτελείται από πέντε τμήματα που συμπληρώνουν όλο το φάσμα προστασίας του χρήστη και ασφάλειας του Κυβερνοχώρου, ήτοι από: α. Τμήμα Διοικητικής Υποστήριξης και Διαχείρισης Πληροφοριών, β. Τμήμα Καινοτόμων Δράσεων και Στρατηγικής, γ. Τμήμα Ασφάλειας Ηλεκτρονικών και Τηλεφωνικών Επικοινωνιών και Προστασίας Λογισμικού και Πνευματικών Δικαιωμάτων, δ. Τμήμα Διαδικτυακής Προστασίας Ανηλίκων και Ψηφιακής Διερεύνησης και ε. Τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών Οικονομικών Εγκλημάτων. Επιπλέον λειτουργεί και τον ιστότοπο cyberkid.gr που απευθύνεται στη σωστή χρήση του διαδικτύου από τους ανήλικους, ενώ διαθέτει λογαριασμό και στα μέσα κοινωνικής δικτύωσης όπως Facebook και Twitter [13].

Πέρα από τη Δίωξη Ηλεκτρονικού Εγκλήματος, από το 2013 ξεκίνησε τη λειτουργία της η μοναδική γραμμή καταγγελιών παράνομου περιεχομένου στο Διαδίκτυο και επίσημο μέλος του INHOPE (Διεθνής Σύνδεσμος Ανοικτών Γραμμών Διαδικτύου) SafeLine. Σύμφωνα με τον ίδιο τον οργανισμό: «Βασική μέριμνα της SafeLine είναι η εξάλειψη φωτογραφιών και βίντεο που απεικονίζουν κακοποίηση ανηλίκων, καθώς και η προάσπιση του δικαιώματος της ασφαλούς πλοήγησης του παιδιού στο Διαδίκτυο. Στα παραπάνω προστίθεται και η αντιμετώπιση της παρενόχλησής του μέσω του κυβερνοχώρου ή του κινητού τηλεφώνου αλλά και η αντιμετώπιση περιεχομένου που αφορά τη βία, το ρατσισμό, την ξενοφοβία και γενικά καθετί το οποίο αντιβαίνει στην Ελληνική Νομοθεσία». Σύμφωνα με την ετήσια αναφορά του για το 2018, για την Ελλάδα καταγράφονται:

- Ο συνολικός αριθμός των αναφορών που έλαβε η SafeLine αυξήθηκε κατά μέσο όρο κατά 185 ετησίως.
- Ο αριθμός των αναφορών που πραγματοποίησε η SafeLine αυξάνεται, κατά μέσο όρο κατά 88% ανά έτος.

- Κατά τα τελευταία 8 χρόνια, η αναλογία ενεργειών που η Safeline ανέλαβε δράση προς αυτών που σκοπεύει να κινηθεί νομικά, αυξάνεται με τάση 7,7% έτος, φθάνοντας το 76% το 2018. Αυτός ο λόγος δεν μπορεί, προφανώς, να διατηρηθεί να αυξάνεται, οπότε η τάση αναμένεται να μειωθεί τα επόμενα 2-3 χρόνια.
- Ο αριθμός των αναφορών που χαρακτηρίζονται από την SafeLine ως ικανών προς καταγγελία, μειώθηκε κατά 38 κατά μέσο όρο ετησίως(εικόνα 1)[76].



Εικόνα 1. Τάση Actioned και Actionable reports Safeline

➤ ΚΕΦΑΛΑΙΟ 3. Η ταυτότητα των κακόβουλων χρηστών

Στο παρόν κεφάλαιο εξετάζεται το προφίλ των θυτών και θυμάτων του διαδικτυακού εκφοβισμού. Ειδικότερα στο πρώτο κεφάλαιο διερευνώνται τα βαθύτερα αίτια του φαινομένου, στο δεύτερο υποκεφάλαιο το ψυχολογικό προφίλ των ατόμων που ασκούν τον εκφοβισμό, ενώ τέλος στο τρίτο υποκεφάλαιο η ανάλυση μεταφέρεται στο χώρο των θυμάτων και των ιδιαίτερων ψυχολογικών χαρακτηριστικών τους.

3.1. Τα αίτια του διαδικτυακού εκφοβισμού

Τα αίτια για τον εκφοβισμό στον κυβερνοχώρο έχουν διερευνηθεί από τους Varjas, Talley, Meyers, Parris και Cutts [90] σε ποιοτική έρευνα χρησιμοποιώντας συνεντεύξεις σε 20 μαθητές ηλικίας 15-19 ετών. Διαπίστωσαν ότι τα αίτια θα μπορούσαν να χαρακτηριστούν είτε εσωτερικά - εκδίκηση, πλήξη, ζήλια, δοκιμή νέας προσωπικότητας ή εξωτερικά - χωρίς συνέπειες, μη αντιπαραθετικά (όταν ένας θύτης δεν θέλει να αντιμετωπίσει πρόσωπο με πρόσωπο το θύμα) ή όταν το θύμα παρουσίαζε διαφορετικά χαρακτηριστικά από τα συνηθισμένα π.χ. εμφάνιση.

Το ερευνητικό ενδιαφέρον στην Ελλάδα αναφορικά με το φαινόμενο του εκφοβισμού ξεκινάει περίπου στις αρχές του 2000. Ένας σημαντικός αριθμός φορέων, οργανισμών, πανεπιστημιακών σχολών κ.α. αρχίζει να ασχολείται συστηματικά με το θέμα, ενώ η Ελλάδα συμμετέχει σε ευρωπαϊκές δράσεις για την αντιμετώπιση του φαινομένου. Η πρώτη συστηματική μελέτη για τον διαδικτυακό εκφοβισμό στην Ελλάδα υλοποιείται στα πλαίσια της Ευρωπαϊκής δράσης SAFE NET HOME εν έτη 2005, μεταξύ 450 μαθητών καταγράφοντας το εντυπωσιακό ποσοστό του 54% να απαντάει θετικά στην ερώτηση στο κατά πόσο έχει πέσει θύμα διαδικτυακού εκφοβισμού. Το 2007 σε έρευνα της μονάδας εφηβικής υγείας της Β παιδιατρικής κλινικής του νοσοκομείου Παίδων Αγλαΐα Κυριακού με συμμετοχή 900 εφήβων, μόλις το 4.2% καταγράφεται να έχει δεχθεί κάποιου είδους ψηφιακό εκφοβισμό. Τέλος στα πλαίσια του προγράμματος «Δαφνη III» το 2012 με τη συμμετοχή 997 μαθητών, ένα ποσοστό της τάξης του 10% δηλώνει θύμα διαδικτυακού εκφοβισμού. Οι σημαντικές αυτές αποκλίσεις μεταξύ των ερευνών προδίδουν κατά κύριο λόγο σύμφωνα με τους ερευνητές ελλιπή ψυχομετρικά ερωτηματολόγια [93].

Όλες οι μορφές εκφοβισμού έχουν αρνητικές επιπτώσεις στα θύματα, και γενικότερα σε όλους τους εμπλεκόμενους. Ωστόσο, ο αντίκτυπος του παραδοσιακού και του διαδικτυακού εκφοβισμού μπορεί να επηρεαστεί από τις σημαντικές διαφορές μεταξύ τους, που συνοψίζονται παραπάνω. Ορισμένοι παράγοντες, όπως ο κοινωνικός περίγυρος ή η ανωνυμία, μπορεί να συμβάλλουν ιδιαίτερα στον αρνητικό αντίκτυπο [92], αλλά μερικές φορές οι διαφορές μεταξύ του παραδοσιακού εκφοβισμού και του διαδικτυακού εκφοβισμού μπορούν να λειτουργήσουν είτε θετικά ή αρνητικά, όσον αφορά το θύμα ή το κίνητρο για τον δράστη. Για παράδειγμα, το δυνητικά μεγάλο μέγεθος κοινού που μπορεί να προσελκύσει ο εκφοβισμός στον κυβερνοχώρο, θα

μπορούσε να σημαίνει ότι το θύμα αισθάνεται χειρότερα λόγω αισθημάτων αμηχανίας και ντροπής [81]. Ωστόσο, μια θετική πτυχή είναι ότι, λόγω του μεγάλου κοινού, το θύμα μπορεί να λάβει ευκολότερα βοήθεια, καθώς συνήθως οι ενήλικες μπορούν να ενημερωθούν για το συμβάν, γεγονός που επίσης συμβάλει σε ελαφρότερη συναίσθηση μοναξιάς στα θύματα.

Εάν ο δράστης δεν έχει οπτική επαφή με το θύμα, τότε μπορεί να έχει λιγότερη επίγνωση των συνεπειών και των επιπτώσεων που προκαλούν οι ενέργειές του, γεγονός που ερμηνεύεται δισδιάστατα. Από τη μία πλευρά, η ικανοποίηση του να βλέπεις το θύμα να υποφέρει ή η δημόσια παρουσία της δύναμης στην ομάδα των ομοτίμων, μπορεί να είναι λιγότερο διαθέσιμη για να παρακινήσει τον δράστη. Από την άλλη πλευρά, χωρίς την άμεση ανατροφοδότηση που μπορεί να προσφέρει ο παραδοσιακός εκφοβισμός μπορεί να υπάρχουν λιγότερες ευκαιρίες για ενσυναίσθηση ή τύψεις [82] και ως εκ τούτου ο εκφοβισμός μπορεί να συνεχιστεί για περισσότερο. Σε συνεντεύξεις μαθητών υπήρχαν κάποιες ενδείξεις ότι τα περιστατικά του εκφοβισμού στον κυβερνοχώρο συνεχίστηκαν για μεγαλύτερες περιόδους από τα περιστατικά του παραδοσιακού εκφοβισμού.

Ο Ortega et al.[66] συνέκριναν τα διαφορετικά συναισθήματα που θα μπορούσαν να νιώσουν τα θύματα αν είχαν βιώσει τον παραδοσιακό εκφοβισμό (άμεσος, έμμεσος) ή τον διαδικτυακό εκφοβισμό (κινητό, Διαδίκτυο). Τα συναισθήματα που αναφέρθηκαν ήταν κυρίως ντροπή, θυμός, αναστάτωση, άγχος, ανησυχία, φόβος και κατάθλιψη. Περισσότερα από τα αρνητικά συναισθήματα αναφέρθηκαν στην περίπτωση του παραδοσιακού εκφοβισμού, ιδίως στα θύματα άμεσου εκφοβισμού, παρά στον εκφοβισμό στον κυβερνοχώρο. Άλλες έρευνες [6] δείχνουν ότι τα θύματα εκφοβισμού στον κυβερνοχώρο εκφράζουν μια ποικιλία συναισθημάτων όπως: θυμός, θλίψη, απογοήτευση, αμηχανία, άγχος, φόβο, μοναξιά και κατάθλιψη. Οι Hay, Meldrum και Mann [36] βρήκαν μεγαλύτερο αντίκτυπο της θυματοποίησης στον κυβερνοχώρο σε σύγκριση με την παραδοσιακή θυματοποίηση με συνέπειες όπως αυτοτραυματισμό και αυτοκτονικό ιδεασμό.

Δύο αιτίες περιγράφονται συχνά ως βασικοί μηχανισμοί, λειτουργίες ή συστηματικά κίνητρα για επιθετική συμπεριφορά: οργανική και αντιδραστική επιθετικότητα. Η έννοια της αντιδραστικής επιθετικότητας έχει τις ρίζες της στη θεωρία της απογοήτευσης. Το να βλάψεις κάποιον άλλο συμβαίνει ως «αντίδραση» σε μια (αντιληπτή) πρόκληση, απειλή ή απογοήτευση και συνήθως συνοδεύεται από έντονα

συναισθήματα θυμού. Έτσι, η αντιδραστική επιθετικότητα πυροδοτείται από τη μη επίτευξη στόχων και το κύριο κίνητρό της είναι να αντιδράσει στο ερέθισμα της οργής-απογοήτευσης και να βλάψει τον δράστη της πρόκλησης ή της απειλής. Αντίθετα, η έννοια της οργανικής επιθετικότητας βασίζεται στη θεωρία της κοινωνικής μάθησης. Το να βλάψεις κάποιον άλλο είναι μια προμελετημένη, υπολογισμένη συμπεριφορά που χρησιμοποιείται ως «μέσο» για την επίτευξη συγκεκριμένων στόχων. Τα κυρίαρχα συναισθήματα που εμπλέκονται σε αυτόν τον τύπο επιθετικότητας είναι η ευχαρίστηση και η διέγερση. Η αντιδραστική επιθετικότητα βρέθηκε να είναι ιδιαίτερα συσχετισμένη με άλλες συμπεριφορές. Περίπου τα μισά από τα παιδιά που εμφανίζουν επιθετική συμπεριφορά βρέθηκαν να είναι τόσο αντιδραστικά όσο και επιθετικά, περίπου το ένα τρίτο βρέθηκε συνήθως να είναι μόνο αντιδραστικά επιθετικό και μόνο μια μειονότητα (περίπου 15%) των παιδιών βρέθηκε να είναι μόνο οργανικά επιθετικό. Συνήθως, τα αγόρια λαμβάνουν υψηλότερη βαθμολογία τόσο στην αντιδραστική όσο και στην οργανική επιθετικότητα σε σύγκριση με τα κορίτσια [52].

Οι Raskauskas και Stoltz [72] σε μελέτη στις ΗΠΑ ζήτησαν τους λόγους για τους οποίους οι ηλεκτρονικοί δράστες διαπράττουν ηλεκτρονικό εκφοβισμό. Από τους 84 συμμετέχοντες ηλικίας 14 έως 18 ετών, οι 18 ταυτοποιήθηκαν ως ηλεκτρονικοί εκφοβιστές και 16 από αυτούς απάντησαν στην ερώτηση σχετικά με την αιτία του ηλεκτρονικού εκφοβισμού. Έξι ερωτηθέντες το έκαναν για λόγους διασκέδασης, τέσσερις ερωτηθέντες λόγω θυμού και ένας έφηβος το έκανε λόγω χαμηλής εκτίμησης για τον εαυτό του. Πέντε ερωτηθέντες δεν γνώριζαν τα κίνητρα για τη συμπεριφορά τους.

Οι Gradinger, Strohmeier και Spiel [33] εξέτασαν 761 εφήβους ηλικίας 14 έως 19 ετών στην Αυστρία και συνέκριναν τα επίπεδα της αντιδραστικής και οργανικής επιθετικότητας σε θύτες και θύματα εκφοβισμού. Οι συγγραφείς διαφοροποίησαν τις ομάδες εκφοβιστών ανάλογα με τη συμμετοχή τους στον παραδοσιακό εκφοβισμό και τον εκφοβισμό στον κυβερνοχώρο. Οι μαθητές που εκφοβίζουν τους άλλους τόσο παραδοσιακά όσο και στον κυβερνοχώρο ορίστηκαν ως συνδυασμένοι εκφοβιστές. Οι μαθητές που εκφοβίστηκαν αλλά και εκφόβισαν άλλους τόσο παραδοσιακά όσο και στον κυβερνοχώρο χαρακτηρίστηκαν ως συνδυασμένα θύματα εκφοβισμού. Οι συνδυασμένοι εκφοβιστές έδειξαν τα υψηλότερα επίπεδα στην αντιδραστική και οργανική επιθετικότητα σε σύγκριση με τους παραδοσιακούς εκφοβιστές και τους μη εκφοβιστές. Τα συνδυασμένα θύματα εκφοβισμού έδειξαν τα υψηλότερα επίπεδα

αντιδραστικής και οργανικής επιθετικότητας σε σύγκριση με τα παραδοσιακά θύματα εκφοβισμού και τους μη κατηγοριοποιημένους εφήβους.

Οι πρόσφατες έρευνες έχουν τονίσει τη σχέση μεταξύ των της κοινωνικής συμπεριφοράς και του εκφοβισμού. Σε ψυχολογικό επίπεδο, ο εκφοβισμός έχει συνδεθεί με προσπάθεια επίτευξης στόχων και με στρεβλώσεις σε κοινωνικό επίπεδο. Οι εκφοβιστές επιδιώκουν περισσότερους αντικοινωνικούς στόχους από τους μη εκφοβιστές και χρησιμοποιούν τον εκφοβισμό ως μέσο για την εδραίωση κυρίαρχων θέσεων. Αυτά τα ευρήματα, μαζί με μελέτες που παρέχουν κάποιες ενδείξεις ότι οι εκφοβιστές δεν είναι κοινωνικά ανίκανοι, αλλά έχουν καλές κοινωνικές δεξιότητες, υποστηρίζουν την άποψη των εκφοβιστών ως προσανατολισμένων στην κυριαρχία και είναι επιρρεπείς στο να χρησιμοποιήσουν τις δεξιότητές τους προκειμένου να χειριστούν αποτελεσματικά τους συνομηλίκους τους για να επιτύχουν τους δικούς τους στόχους. Αυτή η προοπτική είναι σύμφωνη με τον αρχικό ορισμό του Olweus που θεωρεί τον εκφοβισμό ως εσκεμμένη συμπεριφορά που ασκείται από νέους με υψηλότερη (σωματική, ψυχολογική ή κοινωνική) δύναμη από τα θύματά τους [65].

Ο εκφοβισμός έχει συσχετιστεί με διάθεση Μακιαβελικής προσωπικότητας, που θεωρείται μη παθολογικό χαρακτηριστικό της προσωπικότητας που χαρακτηρίζεται από την πεποίθηση ότι οι άνθρωποι είναι χειραγωγητικοί και χειραγωγήσιμοι. Κατά συνέπεια, η κοινωνική χειραγωγήση μπορεί να χρησιμοποιηθεί από Μακιαβελικές προσωπικότητες για να επιτύχουν τους κοινωνικούς τους στόχους. Δεδομένου ότι ο εκφοβισμός έχει συνδεθεί με την επιδίωξη στόχων κυριαρχίας ιδιαίτερα στην εφηβεία και οι εκφοβιστές αντιλαμβάνονται αυτήν τη συμπεριφορά ως ένα αποτελεσματικό εργαλείο για τη διαχείριση σχέσεων με συνομηλίκους, οι έφηβοι με υψηλότερο δείκτη Μακιαβελισμού ενδέχεται να διατρέχουν μεγαλύτερο κίνδυνο εμφάνισης συμπεριφοράς εκφοβισμού [32].

Ο εκφοβισμός είναι επίσης ομαδικό φαινόμενο. Από κοινωνική σκοπιά, μελέτες δείχνουν ότι οι εκφοβιστές μπορούν να είναι δημοφιλείς στις ομότιμες ομάδες τους και ότι ο εκφοβισμός μπορεί να χρησιμοποιηθεί για την επίτευξη κοινωνικών στόχων. Κατά συνέπεια, υπάρχουν κάποιες ενδείξεις ότι στην εφηβεία η δημοφιλία μπορεί να λειτουργήσει ως ένα επιπλέον, κοινωνικό κίνητρο για εκφοβισμό. Ο εκφοβισμός και ευρύτερα η επιθετικότητα έχει επίσης αποδειχθεί ότι εξαρτώνται από το πλαίσιο των συνομηλίκων, ιδίως από τους κανόνες ομάδων ομότιμων. Οι έρευνες υποστηρίζουν ότι συμπεριφορές και πεποιθήσεις που μοιράζονται σε επίπεδο ομάδας και οι κανόνες

κύρους (συμπεριφορά που παρουσιάζεται από άτομα υψηλού επιπέδου εντός της ομάδας) θέτουν το αρχικό στάδιο για τον εκφοβισμό , δημιουργώντας ένα κοινωνικό πλαίσιο που ομαλοποιεί, αποδέχεται ή ακόμη και εκτιμά αυτές τις συμπεριφορές [82].

Αρκετές μελέτες αποδίδουν επίσης την ανάπτυξη εκφοβιστικών συμπεριφορών σε γνωστικούς και συναισθηματικούς μηχανισμούς που συνδέονται με τον αυτοέλεγχο και την αυτορρύθμιση. Η ηθική έγκριση του του εκφοβισμού, ηθική αποστασιοποίηση, η έλλειψη ενοχών και ανάληψης ευθυνών σε βίαιες καταστάσεις, η τάση να αποδυναμώνουν τον αντίκτυπο της συμπεριφοράς τους σε άλλους, τα υψηλά επίπεδα ηθικής δικαιολόγησης και τα χαμηλά επίπεδα ενσυναισθηματικής ανταπόκρισης είναι άρρηκτα συνδεδεμένα με τη διάπραξη διαδικτυακού εκφοβισμού, ενώ η γνωστική και συναισθηματική ενσυναίσθηση έχουν υπάρξει προστατευτικοί παράγοντες κατά τη διάπραξη του διαδικτυακού εκφοβισμού. Ένας επιπλέον παράγοντας που προκύπτει από την διεθνή βιβλιογραφία είναι η σημαντική έκθεση στην ηλεκτρονική βία η οποία δύναται να οδηγήσει σε επιθετικές συμπεριφορές. Τέλος πέρα του Μακιαβελισμού που αναφέρθηκε προηγουμένως, ο εκφοβισμός ενίοτε οφείλεται είτε σε φαινόμενα ναρκισσισμού, δηλαδή σε τάση του ατόμου να αναγνωρίζει τον εαυτό του ως ανώτερο των άλλων ή ακόμη και σε ψυχοπάθειες δηλαδή σε συμπεριφορές που στερούνται ενσυναίσθησης των δεινών που προκαλούν [94].

3.2. Ψυχολογικό προφίλ κακόβουλων χρηστών

Αναφορικά με τους μεμονωμένους παράγοντες, η διάπραξη του εκφοβισμού έχει συσχετιστεί με ψυχοπαθητικές τάσεις, υποστήριξη αρρενωπών χαρακτηριστικών, προβλήματα συμπεριφοράς, αντικοινωνικά χαρακτηριστικά προσωπικότητας, ευαισθησία στο άγχος της πίεσης και κατάθλιψη. Μερικοί από τους εκφοβιστές έχουν βρεθεί με υψηλότερη κοινωνική νοημοσύνη αλλά και κοινωνικό status, με ερευνητές να τους διακρίνουν μεταξύ κοινωνικά ολοκληρωμένων και κοινωνικά περιθωριοποιημένων εκφοβιστών [28].

Δεδομένης της πολυκατευθυντικότητας του κοινωνικό-οικολογικού μοντέλου και των αρχών της ισοτιμίας και της πολυμορφικότητας [11], είναι πιθανό ότι το κοινωνικό πλαίσιο επηρεάζει το βαθμό στον οποίο αυτοί οι μεμονωμένοι παράγοντες λειτουργούν ως συνέπειες της συμμετοχής στον εκφοβισμό. Μια επιθετική νεότητα που διαγιγνώσκεται με διαταραχή συμπεριφοράς δύναται να οδηγήσει σε εκφοβισμό λόγω προδιάθεσης. Εναλλακτικά, οι νέοι που «ανταμείβονται» για συμπεριφορές εκφοβισμού (π.χ. μέσω βελτιωμένου status ή δημοτικότητας, πρόσβαση σε αγαθά) μπορεί να συνεχίσουν τον εκφοβισμό, να αναπτύξουν περαιτέρω επιθετικές συμπεριφορές και τελικά να πληρούν τα κριτήρια για τη διάγνωση διαταραχής συμπεριφοράς. Οι ντροπαλοί νέοι μπορεί να φαίνονται πιο ευάλωτοι, καθιστώντας τους ελκυστικούς στόχους θυματοποίησης. Εναλλακτικά, κάποιος που εκφοβίζεται μπορεί να αναπτύξει μια ντροπαλή και ίσως ανήσυχη συμπεριφορά ως αποτέλεσμα αυτής της αντίδρασης. Έτσι, η κατανόησή για την ψυχολογία του εκφοβισμού / θυματοποίησης μοιάζει πολύ με το αίνιγμα «η κότα έκανε το αυγό ή το αυγό την κότα».

Ο εκφοβισμός έχει μελετηθεί περισσότερο στο σχολικό πλαίσιο και κατά πόσο το θετικό ή αρνητικό κλίμα του σχολείου επηρεάζει τη συχνότητα του εκφοβισμού και της θυματοποίησης. Τα υψηλότερα επίπεδα εκφοβισμού και θυματοποίησης έχουν συνδεθεί με ακατάλληλες συμπεριφορές εκπαιδευτικών, έλλειψη υποστήριξης των εκπαιδευτικών και έλλειψη συμμετοχής σε σχολικές δραστηριότητες. Οι μαθητές είναι επίσης λιγότερο πιθανό να αναφέρουν τον εκφοβισμό εάν θεωρούν το σχολικό τους κλίμα αρνητικό [89]. Η σχέση μεταξύ του σχολικού κλίματος και του εκφοβισμού / θυματοποίησης μπορεί να είναι αμφίδρομη, με το κακό σχολικό κλίμα να συμβάλλει στον εκφοβισμό και αντίστροφα.

Πέρα από τις οικογένειες, τους συνομηλίκους και τα σχολεία, υπάρχει η επιρροή και της ευρύτερης κοινωνίας, με υψηλότερα επίπεδα εκφοβισμού να συνδέονται με μη ασφαλείς γειτονίες και φτώχεια. Η έρευνα έχει επίσης συνδέσει τη διάπραξη του εκφοβισμού με την έκθεση σε βίαια τηλεοπτικά προγράμματα και βιντεοπαιχνίδια [29]. Γενικά, ο αυξημένος εκφοβισμός και η θυματοποίηση βρίσκονται σε κοινότητες στις οποίες η βία είναι εγκαθιδρυμένη ή και συγχωρούμενη, αν και πάλι η αιτιώδης φύση αυτών των σχέσεων παραμένει ασαφής.

Οι εκφοβιστές χαρακτηρίζονται συνήθως ως επιθετικοί, εχθρικοί, παρορμητικοί και με ελλειπείς κοινωνικές δεξιότητες. Τείνουν να συμπεριφέρονται με σταθερό και επίμονο τρόπο και να εμφανίζουν φαινόμενα ψυχωτισμού. Επίσης, οι εκφοβιστές δυσκολεύονται να ανιχνεύσουν βασικά συναισθήματα όπως φόβο ή θλίψη και να αναγνωρίσουν τον ψυχισμό των θυμάτων τους ως συνέπεια των συμπεριφορών τους. Απολαμβάνουν να κυριαρχούν στους άλλους ενώ έχουν κακές ακαδημαϊκές επιδόσεις και απορρίπτουν το σχολικό περιβάλλον. Οι οικογένειες των εκφοβιστών συχνά αντιμετωπίζουν προβλήματα, οι γονείς υποστηρίζουν τη χρήση της φυσικής πειθαρχίας και είναι εχθρικοί, απορρίπτουν και είναι αδιάφοροι για τα παιδιά τους ενώ είναι ανεκτικοί στην επιθετική παιδική συμπεριφορά [17].

Όπως δείχνουν αυτά τα ευρήματα, ο εκφοβισμός και η θυματοποίηση δεν εμφανίζονται μεμονωμένα. Αντίθετα, ο εκφοβισμός προέρχεται από πολύπλοκες αλληλεπιδράσεις μεταξύ ατόμων και των πλαισίων στα οποία λειτουργούν, τόσο εγγύς (δηλαδή, οικογένεια, συνομηλίκους, σχολικό κλίμα) όσο και απομακρυσμένες (δηλαδή κοινωνικές, πολιτιστικές επιρροές) [37].

3.3. Ψυχολογικό προφίλ θυμάτων

Ενώ οι αυτοκτονίες που φέρονται ως αποτέλεσμα του διαδικτυακού εκφοβισμού έχουν συγκεντρώσει πολλή προσοχή στα μέσα ενημέρωσης τα τελευταία χρόνια, η αυτοκτονία δεν είναι ούτε ο πιο πιθανός ούτε ο πιο διαδεδομένος τύπος επιπτώσεων στα θύματα. Στην πραγματικότητα, ορισμένοι ερευνητές υποστηρίζουν ότι ακόμη και σε περιπτώσεις όπου οι νέοι αυτοκτόνησαν μετά από εμπειρίες εκφοβισμού στον κυβερνοχώρο, η αυτοκτονία δεν μπορεί να αποδοθεί άμεσα (ή αποκλειστικά) στα περιστατικά εκφοβισμού στον κυβερνοχώρο, καθώς υπήρχαν και άλλα σημαντικά ζητήματα που επηρεάζουν την ψυχική υγεία αυτών των νέων θυμάτων πριν από το θάνατό τους [47].

Υπάρχουν, ωστόσο, πολλές αρνητικές επιπτώσεις που προέρχονται από την θυματοποίηση του διαδικτυακού εκφοβισμού που έχουν τεκμηριωθεί στην ερευνητική βιβλιογραφία, πολλές από αυτές αλληλεπικαλύπτονται με τις επιπτώσεις που έχουν παρατηρηθεί σε προηγούμενες μελέτες σχετικά με τον παραδοσιακό εκφοβισμό, όπως κατάθλιψη, κακή αυτοεκτίμηση, άγχος, αυτοκτονικός ιδεασμός και ψυχοσωματικά προβλήματα όπως πονοκεφάλους και διαταραχές του ύπνου [65].

Χαρακτηριστικά του εκφοβισμού στον κυβερνοχώρο, όπως η ανωνυμία, επηρεάζουν επίσης τον αντιληπτό αντίκτυπο. Παρόλο που ορισμένοι πιστεύουν ότι τα ανώνυμα μηνύματα είναι χειρότερα από τα επώνυμα, άλλοι υποστηρίζουν ότι ο εκφοβισμός στον κυβερνοχώρο από κάποιον γνωστό είναι πιο επιζήμιος. Επομένως, τόσο η γνώση όσο και η μη γνώση του δράστη έχουν αντίκτυπο, αλλά η αντίληψη ποικίλλει. Η αόρατη παρουσία όσων κάνουν τον εκφοβισμό μπορεί να δημιουργήσει ένα αίσθημα ευπάθειας για τα θύματα που μπορεί να αισθάνονται ότι δεν μπορούν να διαφύγουν του εκφοβισμού. Επίσης, το εύρος του δυνητικού κοινού στον εκφοβισμό στον κυβερνοχώρο μπορεί να δράσει ως παράγοντας επιδείνωσης των αισθημάτων ταπείνωσης και απομόνωσης των θυμάτων. Τέλος, η έλλειψη συνειδητοποίησης των συνεπειών των ενεργειών κάποιου αναφέρεται από τους Smith και Slonje ως ένα άλλο χαρακτηριστικό του διαδικτυακού εκφοβισμού. Ο έμμεσος εκφοβισμός επιτρέπει την ηθική απεμπλοκή, αλλά για τους εκφοβιστές που απολαμβάνουν να βλέπουν τα δεινά ή να επιδεικνύουν τη δύναμή τους μπροστά σε άλλους, ο εκφοβισμός στον κυβερνοχώρο μπορεί να μην τους προσφέρει αυτή την δυνατότητα [24].

Οι επιπτώσεις κυμαίνονται από ασήμαντες έως σοβαρές, ανάλογα με τη συχνότητα, τη διάρκεια και τη σοβαρότητα του διαδικτυακού εκφοβισμού. Τα αποτελέσματα μπορεί να μεγεθυνθούν σε σύγκριση με τον παραδοσιακό εκφοβισμό λόγω της πεποίθησης των θυμάτων ότι δεν μπορούν να ξεφύγουν από τον εκφοβισμό στον κυβερνοχώρο χωρίς να αποκοπούν από το δίκτυο κοινωνικής επικοινωνίας [58]. Επίσης, η δημόσια φύση του διαδικτυακού εκφοβισμού και το να μην είναι γνωστό ποιος και πόσα άτομα έχουν δει ή διαπράξει εκφοβισμό μπορεί να επηρεάσει την αντίληψη των θυμάτων. Επιπλέον, ένα θύμα μπορεί να βρίσκεται σε πραγματικό κίνδυνο εάν κάποιος άλλος έχει δημοσιεύσει μηνύματα μέσω πλαστοπροσωπίας (γιατί μπορεί να αντιμετωπίσει φυσικά αντίποινα). Ο βαθμός του αντίκτυπου μπορεί επίσης να επηρεαστεί από το ευρύ κοινό, την ανωνυμία και τη μονιμότητα επανάληψης ενός μηνύματος [57].

Αναφορικά με τους μαθητές, υπάρχουν διάφοροι τρόποι με τους οποίους ο εκφοβισμός στον κυβερνοχώρο μπορεί να επηρεάσει την ακαδημαϊκή απόδοση όπως: Μειωμένη συγκέντρωση, αποφυγή του σχολείου, αυξημένες σχολικές απουσίες, απομόνωση, αποξένωση, χαμηλότερα ακαδημαϊκά επιτεύγματα, αρνητικές αντιλήψεις για το σχολικό κλίμα, έλλειψη αισθήματος ασφάλειας στο σχολείο, υψηλότερος κίνδυνος για σχολικά προβλήματα και μεγαλύτερη πιθανότητα μεταφοράς όπλων στο σχολείο [38].

Υπάρχουν επίσης πολλά τεκμηριωμένα αποτελέσματα του διαδικτυακού εκφοβισμού στην ψυχική υγεία των θυμάτων, συμπεριλαμβανομένων συναισθημάτων όπως θλίψη, πόνος, θυμός, απογοήτευση, σύγχυση, άγχος, αγωνία και μοναξιά, συμπεριλαμβανομένων πιο έντονων επιπτώσεων όπως: Κατάθλιψη, χαμηλή αυτοεκτίμηση, αδυναμία, κοινωνικό άγχος, αυτοκτονικός ιδεασμός, συναισθηματικά προβλήματα, φόβος, αίσθημα ευπάθειας και μοναξιάς, μειωμένη αυτοεκτίμηση, σοβαρή διαταραχή των σχέσεων, συναισθηματικά προβλήματα. Ορισμένες μελέτες έχουν επίσης επισημάνει ψυχοσωματικά παράπονα (πονοκεφάλους, κοιλιακούς πόνους), δυσκολίες στον ύπνο, σωματική συμπτωματολογία [73]. Επιπλέον, τα θύματα εκφοβισμού στον κυβερνοχώρο μπορούν να γίνουν επιθετικοί ή μπορούν επίσης να είναι θύματα και σε άλλες καταστάσεις.

Η εμπειρία της θυματοποίησης στον κυβερνοχώρο σχετίζεται με αυξημένα επίπεδα κατάθλιψης. Οι Mitchell, Ybarra και Finkelhor [60] σε έρευνα για την ασφάλεια των νέων, σε 1.500 χρήστες του Διαδικτύου ηλικίας μεταξύ 10 και 17 ετών, διαπίστωσαν ότι οι νέοι που εκφοβίστηκαν στον κυβερνοχώρο είχαν 2,5 φορές περισσότερες πιθανότητες να αναφέρουν καταθλιπτικά συμπτώματα από εκείνους που δεν είχαν

υποστεί εκφοβισμό. Οι Schneider, O'Donnell, Stueve και Coulter [79] σε έρευνα σε 20.406 μαθητές ανέφεραν ότι το 33,9% των θυμάτων του εκφοβισμού στον κυβερνοχώρο είχαν καταθλιπτικά συμπτώματα και ότι τα θύματα είχαν 3,26 φορές μεγαλύτερη πιθανότητα να αναπτύξουν καταθλιπτική συμπεριφορά από τα μη θύματα. Όχι μόνο μεταξύ των νέων αλλά και μεταξύ των φοιτητών, τα θύματα του διαδικτυακού εκφοβισμού βρέθηκε να εμφανίζουν υψηλότερο επίπεδο καταθλιπτικών συμπτωμάτων από εκείνους που δεν βίωσαν εκφοβισμό στον κυβερνοχώρο [77]. Επιπλέον, ο κίνδυνος κατάθλιψης είναι υψηλότερος για τα θύματα εκφοβισμού στον κυβερνοχώρο από ό, τι για τα θύματα του παραδοσιακού εκφοβισμού. Οι Schneider et al.[78] ανέφεραν ότι περισσότερα θύματα εκφοβισμού στον κυβερνοχώρο είχαν περισσότερα καταθλιπτικά συμπτώματα από τα θύματα του παραδοσιακού εκφοβισμού (33,9% έναντι 26,6%). Επιπλέον, σε μια διαχρονική μελέτη 845 εφήβων μεταξύ 13 και 17 ετών, οι Gámez-Guadix et al. [31] διαπίστωσαν ότι η εμπειρία της θυματοποίησης του διαδικτυακού εκφοβισμού προέβλεπε υψηλότερα επίπεδα συμπτωμάτων κατάθλιψης 6 μήνες μετά την εμπειρία.

Η εμπειρία της θυματοποίησης στον κυβερνοχώρο σχετίζεται με αυξημένα επίπεδα άγχους. Οι Junonen και Gross [46] διερεύνησαν τη συχνότητα της θυματοποίησης του διαδικτυακού εκφοβισμού και το προκύπτον επίπεδο άγχους μεταξύ 1.454 νέους από 12 έως 17 ετών. Διαπίστωσαν ότι τα θύματα του εκφοβισμού στον κυβερνοχώρο είχαν υψηλότερο επίπεδο κοινωνικού άγχους από εκείνα που δεν βίωναν τον εκφοβισμό. Επιπλέον, οι φοιτητές που εκφοβίστηκαν στον κυβερνοχώρο βρέθηκαν να εμφανίζουν υψηλότερο επίπεδο άγχους από εκείνους που δεν είχαν βιώσει κάτι ανάλογο [71].

Μαζί με την κατάθλιψη και το άγχος, η χαμηλή αυτοεκτίμηση αποτελεί ένδειξη προβλημάτων που επηρεάζουν άμεσα και έμμεσα την κοινωνική συμπεριφορά των θυμάτων. Η αυτοεκτίμηση ορίζεται ως ευνοϊκή ή δυσμενής στάση απέναντι στον εαυτό. Η αυτοεκτίμηση είναι σημαντική όχι μόνο επειδή μπορεί να είναι ένας από τους πιο σημαντικούς παράγοντες που σχετίζονται με την ευημερία, αλλά και επειδή η αυτοεκτίμηση σχετίζεται με το άγχος [88]. Επειδή η θυματοποίηση του διαδικτυακού εκφοβισμού αποτελεί μία αγχωτική κατάσταση, μπορεί να έχει αρνητική επίδραση στην αυτοεκτίμηση. Ωστόσο, μόνο μία μελέτη για τον εκφοβισμό στον κυβερνοχώρο διαπίστωσε ότι τα θύματα είχαν σημαντικά χαμηλότερη αυτοεκτίμηση από εκείνα που δεν είχαν εμπειρία με τον εκφοβισμό στον κυβερνοχώρο [38].

➤ ΚΕΦΑΛΑΙΟ 4. Συμπεράσματα – προτάσεις

Ο εικονικός κόσμος συνδυάζει την οικειότητα και την απόσταση με έναν μοναδικό τρόπο που δημιουργεί νέα ερωτήματα σχετικά με την κοινωνική και προσωπική ανάπτυξη των ανθρώπων [12]. Αν και υπάρχει ο κίνδυνος για κάποιο βαθμό λογοκρισίας, αναγνωρίζεται η ανάγκη για τους εκπαιδευτικούς και τους γονείς να παρέχουν στα παιδιά και τους νέους την ικανότητα να διαχειρίζονται αποτελεσματικά τον κίνδυνο, να γνωρίζουν πώς να προστατεύουν τον εαυτό τους και να υποστηρίξουν ευάλωτους συνομηλίκους τους που υφίστανται κακομεταχείριση στο διαδίκτυο. Με άλλα λόγια, ενώ υπάρχουν πολιτικές και ποινές, αυτές δεν είναι αποτελεσματικές χωρίς την δύναμη της συνεργασίας και των συναισθημάτων που βρίσκονται στο επίκεντρο των κοινωνικών αλληλεπιδράσεων όλων των ανθρώπων. Η σύνδεση στο διαδίκτυο σε μια κοινότητα αποτελεί ουσιαστικό μέρος της κοινωνικής πραγματικότητας των νέων. Η σημασία του δεν μπορεί να υποτιμηθεί ως σημαντική πτυχή της καθημερινής δραστηριότητας όλων των νέων.

Η πλειονότητα των κρατών έχει θεσπίσει κάποιου είδους νομοθεσία για την καταπολέμηση του εκφοβισμού και πιο πρόσφατα του διαδικτυακού εκφοβισμού. Ένας αυξανόμενος αριθμός πολιτών αναγνωρίζουν τη σημασία της ανάπτυξης πολιτικών και της εφαρμογής προγραμμάτων που θα σχεδιαστούν για την αντιμετώπιση του φαινομένου. Ειδικότερα στα πλαίσια της εκπαίδευσης κρίνεται αναγκαίο σε όλους τους μαθητές να διδαχθούν τρόπους προκειμένου να ανταποκριθούν κατάλληλα στον διαδικτυακό εκφοβισμό και οι πιθανοί εκφοβιστές πρέπει να είναι ενήμεροι ότι υπάρχουν σοβαρές συνέπειες που σχετίζονται με τέτοια συμπεριφορά, συμπεριλαμβανομένης της σχολικής τιμωρίας, της δικαστικής προσφυγής, και της ποινικής δίωξης [5].

Μέχρι να γίνουν γνωστές περισσότερες πληροφορίες για αποδεδειγμένα αποτελεσματικούς τρόπους για την καταπολέμηση του εκφοβισμού, πρέπει να ληφθεί μέριμνα για την παρακολούθηση των αποτελεσμάτων των τρεχουσών πρακτικών για να διασφαλιστεί ότι θα έχουν τα επιθυμητά αποτελέσματα [83]. Οι ερευνητές δείχνουν τη σημασία της διάκρισης μεταξύ δευτερευόντων και σοβαρών περιστατικών

εκφοβισμού στον κυβερνοχώρο. Πιθανώς οι περισσότερες από τις μικρές περιπτώσεις μπορούν να αντιμετωπιστούν ως ρουτίνα προτού μετατραπούν σε κάτι πιο σοβαρό.

Η έρευνα δείχνει επίσης ότι ο εκφοβισμός στον κυβερνοχώρο είναι συχνά επέκταση του εκφοβισμού στον πραγματικό κόσμο. Ενώ είναι δελεαστικό να πιστεύουμε ότι η αυστηρότερη ρύθμιση και οι αυστηρότερες κυρώσεις θα έχουν αντίκτυπο στα ποσοστά του εκφοβισμού, μπορεί να είναι πιο παραγωγικό η ολιστική συνεργασία της κοινωνίας και του σχολείου, προκειμένου να αναπτυχθεί αυξημένη ευαισθητοποίηση σχετικά με τις συνέπειες του εκφοβισμού. καθώς και ενσυναίσθηση απέναντι σε αυτούς που πλήττονται σοβαρά. Συμπερασματικά, οι Rivers και Noret[74] επισημαίνουν ότι οι εικονικές αλληλεπιδράσεις δεν θα πρέπει να θεωρούνται φαντασιώσεις, καθώς είναι πραγματικές για τους νέους που ασχολούνται με αυτές και πρέπει να κατανοήσουμε περισσότερα για τις κοινότητες στις οποίες πραγματοποιούνται αυτές. Υπάρχει ανάγκη να ολοκληρωθεί περισσότερη έρευνα στο πλαίσιο του διαδικτυακού εκφοβισμού, συμπεριλαμβανομένης της αποτελεσματικότητας των προτεινόμενων προγραμμάτων πρόληψης και παρέμβασης.

Η ανάγκη για συνεργασία με εκείνους που επηρεάζονται από τον εκφοβισμό στον κυβερνοχώρο περιλαμβάνει τη διασφάλιση ότι οι μαθητές, το κράτος, οι γονείς και τα μέλη της κοινότητας γνωρίζουν και εκπαιδεύονται σχετικά με τον εκφοβισμό. Είναι σημαντικό τα θύματα του εκφοβισμού να γνωρίζουν ότι μπορούν να ενημερώνουν τους ενήλικες σε περίπτωση εκφοβισμού. Οι γονείς πρέπει να γνωρίζουν ότι η παρακολούθηση της διαδικτυακής δραστηριότητας του παιδιού τους, η τοποθέτηση του υπολογιστή σε κοινόχρηστο δωμάτιο αντί στην κρεβατοκάμαρα του και η συζήτηση με το παιδί τους σχετικά με τον εκφοβισμό μπορεί να συμβάλει στη μείωση της εμφάνισης του διαδικτυακού εκφοβισμού στο σπίτι τους. Τα σχολεία πρέπει να εφαρμόσουν προγράμματα anticyberbully όπως το CyberSmart! για να αυξήσουν την ευαισθητοποίηση σχετικά με τον εκφοβισμό, να αναπτύξουν πολιτικές σχετικά με τη χρήση υπολογιστών και τις συνέπειες για εκείνους που εκφοβίζουν. Τα σχολεία μπορούν επίσης να εφαρμόσουν κυτίο ανώνυμων καταγγελιών γύρω από το σχολείο στο οποίο οι μαθητές θα μπορούν να αναφέρουν ανώνυμα περιπτώσεις εκφοβισμού που έχουν δει ή έχουν εμπλακεί.

Τα ευρήματα δείχνουν ότι ο εκφοβισμός στον κυβερνοχώρο γίνεται πιο διαδεδομένος καθώς οι νέοι ξοδεύουν όλο και περισσότερο χρόνο χρησιμοποιώντας τεχνολογία που τους κρατά online σχεδόν στο σύνολο της ημέρας. Υπάρχουν πολλοί διαφορετικοί

τρόποι με τους οποίους οι εκφοβιστές προσεγγίζουν τα θύματά τους, συμπεριλαμβανομένων των άμεσων μηνυμάτων μέσω του Διαδικτύου, των ιστότοπων κοινωνικής δικτύωσης, των μηνυμάτων κειμένου και των τηλεφωνικών κλήσεων σε κινητά τηλέφωνα. Υπάρχουν διάφορες μορφές εκφοβισμού στον κυβερνοχώρο, συμπεριλαμβανομένων ενδεικτικά, της παρενόχλησης, της πλαστοπροσωπίας και του cyberstalking. Έχει βρεθεί ότι υπάρχουν διαφορές μεταξύ όχι μόνο της επικράτησης του διαδικτυακού εκφοβισμού μεταξύ ανδρών και γυναικών, αλλά και των τρόπων με τους οποίους άνδρες και γυναίκες εκφοβίζουν. Όπως και ο παραδοσιακός εκφοβισμός, ο εκφοβισμός στον κυβερνοχώρο είναι ένα σοβαρό πρόβλημα που μπορεί να προκαλέσει στο θύμα αισθήματα προσωπικής ανεπάρκειας, οδηγώντας ακόμα και στην αυτοκτονία. Αποτελεί συνολικό χρέος της κοινωνίας να ενημερωθεί και να υιοθετήσει τις κατάλληλες πολιτικές για την αντιμετώπιση του φαινομένου. Όπως και σε άλλα παρόμοια προβλήματα, η καταλληλότερη λύση φαίνεται να πηγάζει πάντα από τον ίδιο χώρο: παιδεία.

➤ ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Agatston, P., Kowalski, R., & Limber, S. (2012). Youth views on cyberbullying. In J. W. Patchin, & S. Hinduja (Eds.), *Cyberbullying prevention and response: Expert perspectives* (pp. 57–71). New York, NY: Routledge.
- [2] Anti-Phishing Working Group (APWG). (2010). *Phishing Activity Trends Report 2nd Half 2010*. Manning, Ronnie.
- [3] Αθανασίου Κ., 2020. *Διαπολιτισμικές συγκρίσεις του διαδικτυακού εκφοβισμού μεταξύ ευρωπαϊκών χωρών*. Αθήνα: Πανεπιστήμιο Αθηνών.
- [4] Barlow, J. P., S. Birkets, K. Kelly and M. Slouka (1995). “What Are We Doing On-Line?” *Harper's*. 291: 35-46.
- [5] Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What school administrators (and parents) can do. *Clearing House*, 81(1), 8-12. DOI: 10.3200/TCHS.81.1.8-12
- [6] Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing*, 1, 15–33.
- [7] Byers, D. (2013). Do they see nothing wrong with this?: Bullying, bystander complicity, and the role of homophobic bias in the Tyler Clementi case. *Families in Society: The Journal of Contemporary Social Services*, 94(4), 251–258. <http://dx.doi.org/10.1606/1044-3894.4325>
- [8] C.F. art. 5 (Brazil) (Constituição Federal), with reforms through 1998 (hereinafter BRAZ. CONST.), available at www.georgetown.edu/pdba/Constitutions/Brazil/btitle1.html.
- [9] Carey, T. A. (2003). Improving the success of anti-bullying intervention programs: A tool for matching programs with purposes. *International Journal of Reality Therapy*, 22(2), 16.
- [10] Cerf, V. G. (1995). *Computer networking: Global infrastructure for the 21st century*. Retrieved from <http://www.cs.washington.edu/homes/lazowska/cra/networks.html>
- [11] Cicchetti, D., & Rogosch, F. A. (1996). Equifinality and multifinality in developmental psychopathology. *Development and Psychopathology*, 8, 597–600. <http://dx.doi.org/10.1017/S0954579400007318>
- [12] Cowie, H., & Colliety, P. (2010). Cyberbullying: Sanctions or sensitivity? *Pastoral Care in Education*, 28(4), 261-268. DOI: 10.1080/02643944.2010.528017.
- [13] Crime Times. *Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος*, . viewed 14 February 2021 <https://www.crimetimes.gr/%CE%B4%CE%B9%CE%B5%CF%8D%CE%B8%CF%>

85%CE%BD%CF%83%CE%B7-
%CE%B4%CE%AF%CF%89%CE%BE%CE%B7%CF%82-
%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%
CE%B9%CE%BA%CE%BF%CF%8D-
%CE%B5%CE%B3%CE%BA%CE%BB%CE%AE/

[14] Curran, J., & Seaton, J. (2009). *Power without responsibility*. London, UK: Routledge.

[15] Dake, J. A., Price, J. H., & Telljohann, S. K. (2003). The nature and extent of bullying at school. *Journal of School Health*, 73(5), 173.

[16] Darpa (n.d.). Arpanet. Retrieved from https://www.darpa.mil/attachments/ARPANET_final.pdf Euromonitor International, June 2014

[17] Demaray, M., & Malecki, C. (2003). Perceptions of the frequency and importance of social support by students classified as victims, bullies, and bully/victims in an urban middle school. *School Psychology Review*, 32(3): 471 -489

[18] DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press

[19] Diamanduros, T., Downs, E., & Jenkins, S. J. (2008). The role of school psychologists in the assessment, prevention, and intervention of cyberbullying. *Psychology In The Schools*, 45(8), 693-704.

[20] Dilmac, B. (2009). Psychological needs as a predictor of cyber bullying: A preliminary report on college students. *Educational Sciences: Theory & Practice*, 9(3), 1307-1325.

[21] Ducheneaut, N., Yee, N., Nickell, E., Moore, R.J.: "Alone together?": exploring the social dynamics of massively multiplayer online games, In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp. 407–416. (2006)

[22] Dubreuil, J., & McNiff, E. (2010). *Bullied to death in America's schools*. Retrieved from http://abcnews.go.com/2020/TheLaw/school-bullying-epidemic-turningdeadly/story?id=11880841#.Tyass5ity_c

[23] Dufour, K. (2012). *Amanda Todd case highlights issue of online bullying*. The Telegraph.

[24] Duggan, M., & Smith, A. (2014). Pew Research Center - Social Media Update 2013. Retrieved from <http://pewinternet.org/Reports/2013/Social-Media-Update/MainFindings.aspx>

[25] Dyer, E. (2014, October 20). *Cyberbullying bill draws fire from diverse mix of critics*. CBC News.

- [26] Esin, J. O. (2017). *System overview of cyber-technology in a digitally connected global society*. Bloomington, IN: Authorhouse.
- [27] European Union. Data protection and online privacy.
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm
- [28] Farmer, T. W., Petrin, R., Robertson, D., Fraser, M., Hall, C., Day, S., & Dadisman, K. (2010). Peer relations of bullies, bully-victims, and victims: The two social worlds of bullying in second-grade classrooms. *The Elementary School Journal*, 110, 364–392. [http://dx.doi.org/ 10.1086/648983](http://dx.doi.org/10.1086/648983)
- [29] Ferguson, C. J., & Dyck, D. (2012). Paradigm change in aggression research: The time has come to retire the general aggression model. *Aggression and Violent Behavior*, 17, 220–228. [http://dx.doi.org/ 10.1016/j.avb.2012.02.007](http://dx.doi.org/10.1016/j.avb.2012.02.007)
- [30] Fraser, C. (2016). An analysis of the emerging role of social media in human trafficking. *International Journal of Development Issues*, 15 (2), 98-112.
- [31] Gámez-Guadix, M., Orue, I., Smith, P. K., & Calvete, E. (2013). Longitudinal and reciprocal relations of cyberbullying with depression, substance use, and problematic internet use among adolescents. *Journal of Adolescent Health*(0). doi: <http://dx.doi.org/10.1016/j.jadohealth.2013.03.030>
- [32] Garandeau, C. F., & Cillessen, A. H. (2006). From indirect aggression to invisible aggression: A conceptual view on bullying and peer group manipulation. *Aggression and Violent Behavior*, 11(6), 612-625. doi: 10.1016/j.avb.2005.08.005
- [33] Gradingier, P., Strohmeier, D., & Spiel, C. (2009). Traditional bullying and cyberbullying: Identification of risk groups for adjustment problems. *Zeitschrift für Psychologie / Journal of Psychology*, 217, 205-213.
- [34] Han, L., Cen, S., Ma, J., Ma, Y.: Identify intimate social relationship in blogosphere, lecture notes of the institute for computer sciences. *Soc. Inform. Telecommun. Eng.* 18, 14–25 (2009)
- [35] Hancock, W. (1997). *Cookies on your hard drive*. American Agent & Broker. 69(6): 8-10. 1997 Jun.
- [36] Hay, C., Meldrum, R., & Mann, K. (2010). Traditional bullying, cyber bullying, and deviance: A general strain theory approach. *Journal of Contemporary Criminal Justice*, 26, 130–147.
- [37] Hendricks, L.; Lumadue, R.; Waller, L.R. The evolution of bullying to cyber bullying: An overview of the best methods for implementing a cyber bullying preventive program. *National Forum J. Counsel. Addict.* 2012, 1, 1–9
- [38] Hinduja, S., & Patchin, J. W. (2011). *Cyberbullying identification, prevention, and response*. Retrieved from:
http://www.cyberbullying.us/cyberbullying_identification_prevention_response.php

- [39] Huberman, B.A., Romero, D.M., Wu, F.: Social networks that matter: Twitter under the microscope. *First Monday* 14(1) (2009)
- [40] Huffpost, Οι 12 σοβαρές υποθέσεις διαδικτυακού bullying στην Ελλάδα, , viewed 14 February 2021
https://www.huffingtonpost.gr/2015/05/29/koinonia_n_7466008.html
- [41] Hunter, S. C., Boyle, J. E., & Warden, D. (2007). Perceptions and correlates of peer-victimization and bullying. *British Journal of Educational Psychology*, 77(4), 797-810.
- [42] Hutchinson, M., Vickers, M.H., Jackson, D., & Wilkes, L. (2010). Bullying as circuits of power: An Australian nursing perspective. *Administrative Theory and Praxis*, 32(1), 24-47.
- [43] James, G. (2000). *The price of privacy*. Upside. 12(4): 182-190. 2000 Apr.
- [44] Jay R.(2015). Data Protection & Privacy 2015. Law Business Research: London.
- [45] Jennifer, D., Cowie, H., & Bray, D. (2006). ‘Bully Dance’: Animation as a tool for conflict resolution. *Pastoral Care in Education*, 24(1), 27-32.
- [46] Juvonen, J., & Gross, E. F. (2008). Extending the school grounds?—Bullying experiences in cyberspace. *Journal of School Health*, 78(9), 496-505.
- [47] Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age* (2nd ed)). Malden, MA: Wiley-Blackwell.
- [48] Law on the Protection of Minors, 1991 (P.R.C.), available at www.unescap.org/esid/psis/population/database/poplaws/law_china/ch_record009.htm.
- [49] Lawfare, *New Data on Sextortion: 124 Additional Public Cases*, viewed 8 February 2021 < <https://www.lawfareblog.com/new-data-sextortion-124-additional-public-cases>>
- [50] Leskovec, J., Backstrom, L., Kumar, R., Tomkins, A.: Microscopic evolution of social networks, In Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ACM, 462–470 (2008)
- [51] Lim, E. (2000). “Electronic Commerce and the Law”. Bcom(Hons) Dissertation, MSIS, University of Auckland.
- [52] Little, T. D., Jones, S. M., Henrich, C. C., & Hawley, P. H. (2003). Disentangling the "whys" from the "whats" of aggressive behavior. *International Journal of Behavioral Development*, 27, 122-133.
- [53] Macaluso, N. (2001). "Nearly 60% of Homes are Online." *E-Commerce Times*, Aug. 13. Available online at: <http://www.ecommercetimes.com/perl/sto12743.html>.

- [54] Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy
- [55] Μαυρίδης, Ι. 2015. *Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα*. Στο Μαυρίδης, Ι. 2015. Ασφάλεια πληροφοριών στο διαδίκτυο. [ηλεκτρ. βιβλ.] Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ. 13. Διαθέσιμο στο: <http://hdl.handle.net/11419/1037>
- [56] Media Release, Office of the Privacy Commissioner (Austl.), Privacy Commissioner approves market research code (Aug. 27, 2003), available at www.privacy.gov.au/news/media/03_11_print.html
- [57] Menesini, E., & Nocentini, A. (2012). Peer education intervention: Face-to-face versus online. In A. Costabile, & B. A. Spears (Eds.), *The impact of technology on relationships in educational settings* (pp. 139–150). New York, NY: Routledge.
- [58] Menesini, E., Palladino, B., & Nocentini, A. (2015). Emotions of moral disengagement, class norms, and bullying in adolescence: A multilevel approach. *MerrillPalmer Quarterly*, 61, 1, 124-143. Doi: 10.13110/merrpalmquar1982.61.1.0124
- [59] Milgram, S.: The small-world problem. *Psychol. Today* 2, 60–67 (1967)
- [60] Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreat*, 12(4), 314-324. doi: 10.1177/1077559507305996
- [61] National Herald 2020, *Man held for 'blackmailing' over 100 women on social media*, viewed 8 February 2021, <<https://www.nationalheraldindia.com/national/man-held-for-blackmailing-over-100-women-on-social-media/>>.
- [62] Nie, N. H. (2001). “Sociability, Interpersonal Relations, and the Internet: Reconciling Conflicting Findings.” *American Behavioral Scientist*, 45(3), 426-437.
- [63] O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review*, 19(1), 17-31
- [64] O'Neill, B. (2014, April). *The ICT Coalition: First report on the implementation of the ICT Principles*. Dublin, Ireland: Dublin Institute of Technology. Retrieved from http://www.ictcoalition.eu/gallery/75/ICT_REPORT.pdf
- [65] Olweus, D. (2012). Cyberbullying: An overrated phenomenon? *European Journal of Developmental Psychology*, 9, 520–538, doi:10.1080/17405629.(2012).682358
- [66] Ortega, R., Elipe, P., Mora-Merchan, J. A., Calmaestra, J., & Vega, E. (2009). The emotional impact on victims of traditional bullying and cyberbullying: A study of Spanish adolescents. *Zeitschrift fur Psychologie/Journal of Psychology*, 217 } , 197–204. Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, 4, 148–169.

- [67] Patchin, J. W., & Hinduja, S. (2011). Cyberbullying and self-esteem. *Journal of School Health*, 80(12), 614-621. doi: 10.1111/j.1746-1561.2010.00548.x
- [68] Personal Data Protection Act No. 25,326 (Oct. 4, 2000) (Arg.), available at www.privacyinternational.org/countries/argentina/argentine-dpa.html.
- [69] Πρώτο Θέμα. Λίνα Κοεμτζή: *Η πρώτη cyber bullying αυτοκτονία*. viewed 14 February 2021, <https://www.protothema.gr/greece/article/739934/lina-koemtzi-i-proti-cyber-bullying-autoktonia/>
- [70] Πρώτο Θέμα. Λίνα Κοεμτζή: *Επτά άγνωστες περιπτώσεις bullying*, <https://www.protothema.gr/greece/article/462154/7-agnostes-periptoseis-bullying/>
- [71] R. Cohen-Almagor(2011). *Internet history*. *Int. J. Technoeth.*, vol. 2, no. 2, pp. 45–64, Apr./Jun. 2011
- [72] Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology*, 43, 564-575.
- [73] Raskauskas, J. (2010). Text-bullying: Associations with traditional bullying and depression among New Zealand adolescents. *Journal of School Violence*, 9(1), 74-97.
- [74] Rivers, I., & Noret, N. (2010). *British Educational Research Journal*, 36(4), 643-671.
- [75] Rochman, B. (2010, October 1). *Cyberbullying? Homophobia? Tyler Clementi's Death highlights online lawlessness*. Retrieved from <http://healthland.time.com/2010/10/01/cyberbullying-homophobia-tyler-clementis-deathhighlights-online-lawlessness/>
- [76] Safeline, *Annual Report*, viewed 14 February 2021, https://www.safeline.gr/wp-content/uploads/2020/08/safeline_annualreport2018.pdf
- [77] Schenk, A. M. (2011). *Psychological Impact of Cyberbully Victimization among College Students*. M.S. 1501716, West Virginia University, United States -- West Virginia. ProQuest Dissertations & Theses A&I database.
- [78] Schneider, G. P., & Evans, J. (2007). *Newperspectives on the Internet: Comprehensive (6th ed.)*. Boston, MA: Thomson.
- [79] Schneider, S. K., O'Donnell, L., Stueve, A., & Coulter, R. W. S. (2011). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *Am J Public Health*, 102(1), 171-177. doi: 10.2105/ajph.2011.300308
- [80] Slevin, J. (2000). *The Internet and society*. Oxford, UK: Polity Press
- [81] Slonje, R. (2011). *The nature of cyberbullying in Swedish schools: Processes, feelings of remorse by bullies, impact on victims and age and gender differences*. Unpublished PhD thesis, Goldsmiths, University of London, UK.

- [82] Slonje, R., Smith, P. K., & Frisen, A. (2012). Processes of cyberbullying, and feelings of remorse by bullies: A pilot study. *European Journal of Developmental Psychology*, 9, 244–259.
- [83] Snakenborg, J., Van Acker, R., & Gable, R. A. Cyberbullying: Prevention and intervention to protect our children and youth. *Preventing School Failure*, 55(2), 88-95. DOI: 10.1080/1045988X.2011.539454.
- [84] Stefanie, O. (2001). “Reversal of fortune – tracking web trackers”. *ZD Net News*, Mar 5, 2001. <http://www.zdnet.com/zdnn/stories/news/0,4586,2692472,00.html>
- [85] Tech Transparency Project(2020). Broken Promises: Sexual Exploitation of Children on Facebook.
- [86] TimesNowNews.com, Shocking! *Class 8 dropout from UP hacks social media accounts of 400 girls, blackmails them for money*, viewed 8 February 2021 <
<https://www.timesnownews.com/india/article/shocking-class-8-dropout-from-up-hacks-social-media-accounts-of-400-girls-blackmails-them-for-money/712927>>
- [87] Tippet, N., & Kwak, K. (2012). Cyberbullying in South Korea. In Q. Li, D. Cross, & P. K. Smith (Eds.), *Cyberbullying in the global playground: Research from international perspectives* (pp. 202–219). Chichester, England: Wiley-Blackwell.
- [88] Twenge, J. M., & Campbell, W. K. (2001). Age and birth cohort differences in self-esteem: A cross-temporal meta-analysis. *Personality and Social Psychology Review*, 5(4), 321-344. doi: 10.1207/s15327957pspr0504_3
- [89] Unnever, J. D., & Cornell, D. G. (2004). Middle school victims of bullying: Who reports being bullied? *Aggressive Behavior*, 30, 373– 388. <http://dx.doi.org/10.1002/ab.20030>
- [90] Varjas, K., Talley, J., Meyers, J., Parris, L., & Cutts, H. (2010). High school students’ perceptions of motivations for cyberbullying: An exploratory study. *Western Journal of Emergency Medicine*, 3, 269–273.
- [91] Wang, J.C., Chiu, C.C.: Recommending trusted online auction sellers using social network analysis. *Expert Syst. Appl.* 34(3), 1666–1679 (2008)
- [92] Wang, J., Iannotti, R. J., & Nansel, T. R. (2009). School bullying among adolescents in the United States: Physical, verbal, relational, and cyber. *Journal of Adolescent Health*, 45, 368–375.
- [93] Wellman, B., R. Wilkes, E. Fong, and M. Kew. (2003). “Fathoming the Digital Divide.” *Studies in Internet Communication: Theory and Practice*, 19, forthcoming.
- [94] Wellman, B., Salaff, J., Dimitrova, D., Garton, L., Gulia, M., Haythornthwaite, C.: Computer networks as social networks: collaborative work, telework, and virtual community. *Annu. Rev. Sociol.* 22(1), 213–238 (1996)

[95] Whitaker E, Kowalski RM. (2015). Cyberbullying via social media. *J Sch Violence*. 14, 11–29.

[96] Ybarra, M. (2009, August). Issues of language and frequency in measuring cyberbullying: Data from the Growing up with Media survey. Presented at the meeting of COST ACTION IS0801: Cyberbullying: Coping with negative and enhancing positive uses of new technologies, in relationships in educational settings, Lithuania