



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΗΘΙΚΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΙΑ ΚΡΙΤΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

ΒΟΥΛΗΣ ΧΡΗΣΤΟΣ ΡΑΦΑΗΛ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Ραγάζου Βασιλική
Λέκτορας

(Απόκτηση ακαδημαϊκής διδακτικής εμπειρίας σε νέους επιστήμονες κατόχους
διδακτορικού)

Λαμία 2023



ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΗΘΙΚΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ: ΜΙΑ ΚΡΙΤΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

ΒΟΥΛΗΣ ΧΡΗΣΤΟΣ ΡΑΦΑΗΛ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Ραγάζου Βασιλική
Λέκτορας

(Απόκτηση ακαδημαϊκής διδακτικής εμπειρίας σε νέους επιστήμονες κατόχους
διδακτορικού)

Λαμία 2023



UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

CYBER ETHICS AND CYBER CRIME: A CRITICAL REVIEW

VOULIS CHRISTOS RAFAIL

FINAL THESIS

ADVISOR

Ragazou Vasiliki

Lecturer

(Acquisition of Academic Teaching Experience for young Phd holders)

Lamia 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις ⁽¹⁾, που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων Συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάστηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.
2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.
3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια
4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: ...16.../...11.../2023.....

Ο – Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Στη σύγχρονη εποχή, η τεχνολογία και η πληροφορική έχουν αποκτήσει κεντρικό ρόλο στο εμπόριο, στη βιομηχανία, στη διακυβέρνηση, στην ιατρική, στην εκπαίδευση, στην ψυχαγωγία, καθώς και στην κοινωνία, γενικότερα. Ωστόσο, η τεχνολογία και η πληροφορική μπορεί να επιφέρει αρνητικές συνέπειες στην κοινωνία, διότι η χρήση τους δημιουργεί ηθικά προβλήματα, που σχετίζονται κυρίως με την προστασία της ιδιωτικότητας, την ασφαλή πρόσβαση και την αντιμετώπιση επιβλαβών και επικίνδυνων ενεργειών. Η ευρεία χρήση της τεχνολογίας έχει δημιουργήσει νέες μορφές εγκληματικότητας, όπως το κυβερνοέγκλημα, το οποίο μπορεί να εκδηλωθεί με απρόβλεπτες συνέπειες για τους χρήστες. Στο πλαίσιο αυτό, λοιπόν, διαμορφώνεται ο στόχος της εργασίας αυτής που είναι η διερεύνηση της ηθικής στον κυβερνοχώρο και παράλληλα η διερεύνηση του ίδιου του κυβερνοεγκλήματος. Η μέθοδος που ακολουθείται είναι η βιβλιογραφική επισκόπηση και τα ευρήματα της εργασίας έδειξαν ότι το Διαδίκτυο είναι μια ανεξάντλητη πηγή πληροφοριών και ένα περιβάλλον, εντός του οποίου υπάρχουν πολλές ευκαιρίες να εκδηλωθούν εγκληματικές ενέργειες. Η συνεισφορά της έρευνας στην ακαδημαϊκή κοινότητα έγκειται στο γεγονός ότι καλύπτει ένα ευρύ ερευνητικό φάσμα του κυβερνοεγκλήματος και προτείνει λύσεις για την αποτροπή του.

Λέξεις κλειδιά: *Διαδίκτυο, Ηθική, εμπιστοσύνη, ασφάλεια, Κυβερνοέγκλημα, Νομοθεσία, Παραδείγματα, Αντιμετώπιση*

ABSTRACT

Nowadays, technology and information technology have acquired a central role in commerce, industry, government, medicine, education, entertainment, and society in general. However, technology and information technology can bring negative consequences to society, because their use creates ethical problems, mainly related to the protection of privacy, secure access, and dealing with harmful and dangerous actions. The widespread use of technology has created new forms of crime, such as cybercrime, which can manifest itself with unpredictable consequences for users. In this context, therefore, the goal of this work is formed, which is the investigation of ethics in cyberspace and at the same time the investigation of cybercrime itself. The method followed is the literature review and the findings of the work showed that the Internet is an inexhaustible source of information and an environment, within which there are many opportunities to manifest criminal actions. The contribution of the research to the academic community lies in the fact that it covers a wide research spectrum of cybercrime and proposes solutions to prevent it.

Keywords: *Internet, Ethics, trust, security, Cybercrime, Legislation, Examples, Coping*

Περιεχόμενα

ΠΕΡΙΛΗΨΗ	I
ABSTRACT	III
ΚΕΦΑΛΑΙΟ 1 ΕΙΣΑΓΩΓΗ.....	2
1.2 ΣΚΟΠΟΣ ΚΑΙ ΕΡΕΥΝΗΤΙΚΑ ΕΡΩΤΗΜΑΤΑ	3
1.3 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.....	3
ΚΕΦΑΛΑΙΟ 2 ΗΘΙΚΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ	6
2.1 Η ΗΘΙΚΗ ΩΣ ΣΤΟΙΧΕΙΟ ΤΟΥ ΚΟΣΜΟΥ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ	6
2.2 ΗΘΙΚΗ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΑΚΥΒΕΡΝΗΣΗ	9
2.3 ΗΘΙΚΗ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ	11
2.4 ΜΕΘΟΔΟΙ ΓΙΑ ΤΗ ΒΕΛΤΙΩΣΗ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΗΣ ΗΘΙΚΗΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ	15
2.4.1 ΚΑΤΟΧΥΡΩΣΗ ΤΗΣ ΕΜΠΙΣΤΟΣΥΝΗΣ	15
2.4.2 ΥΛΟΠΟΙΗΣΗ ΤΗΣ ΚΟΙΝΩΝΙΑΣ ΤΗΣ ΓΝΩΣΗΣ.....	16
2.4.3 ΑΠΟΦΥΓΗ ΤΗΣ ΨΗΦΙΑΚΗΣ ΔΙΑΙΡΕΣΗΣ.....	17
2.4.4 ΔΗΜΙΟΥΡΓΙΑ ΜΙΑΣ ΑΝΟΙΚΤΗΣ ΚΟΙΝΩΝΙΑΣ.....	18
ΚΕΦΑΛΑΙΟ 3 ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ.....	20
3.1 ΤΑ ΚΥΡΙΟΤΕΡΑ ΕΙΔΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.....	20
3.1.1. ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ, ΔΙΑΔΙΚΤΥΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ	20
3.1.2 ΠΡΟΠΑΓΑΝΔΑ ΜΙΣΟΥΣ	22
3.1.3 ΔΙΑΔΙΚΤΥΑΚΟΣ ΕΚΦΟΒΙΣΜΟΣ	23
3.1.4 ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ.....	24
3.1.5 ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ.....	26
3.1.6 ΨΑΡΕΜΑ (PHISING, PHARMING).....	26
3.1.7 ΒΑΝΔΑΛΙΣΜΟΣ ΔΙΑΔΙΚΤΥΑΚΩΝ ΤΟΠΩΝ.....	28
3.2 ΝΟΜΟΘΕΣΙΑ ΚΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ	29
3.2.1. Η ΕΥΡΩΠΑΪΚΗ ΠΡΟΣΤΑΣΙΑ ΚΑΤΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.....	29
3.2.2 Το ΕΛΛΗΝΙΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ	30
3.2.3 Η ΝΟΜΟΘΕΣΙΑ ΤΟΥ ΠΟΙΝΙΚΟΥ ΚΩΔΙΚΑ ΓΙΑ ΤΗΝ ΠΑΤΑΞΗ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.....	32
ΚΕΦΑΛΑΙΟ 4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ.....	35
4.1 ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΕ ΕΥΡΩΠΑΪΚΕΣ ΠΕΤΡΕΛΑΪΚΕΣ ΕΓΚΑΤΑΣΤΑΣΕΙΣ	35
4.2 Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΣΤΗΝ UBER.....	36
4.3 Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΣΤΗ NASA ΤΟ 1999	37
4.4 Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΣΤΗ SONY PLAYSTATION NETWORK	38

4.5 Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΣΤΗΝ ΟΥΚΡΑΝΙΑ ΣΤΟ ΔΙΚΤΥΟ ΗΛΕΚΤΡΙΚΗΣ ΕΝΕΡΓΕΙΑΣ .	39
4.6 Η ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΣΤΗΝ ΕΛΛΗΝΙΚΗ ΤΡΑΠΕΖΑ ΘΕΜΑΤΩΝ ΕΞΕΤΑΣΕΩΝ ΤΟΥ ΥΠΟΥΡΓΕΙΟΥ ΠΑΙΔΕΙΑΣ.....	40
<u>ΚΕΦΑΛΑΙΟ 5 ΜΕΘΟΔΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ.....</u>	<u>42</u>
5.1 ΠΡΟΛΗΠΤΙΚΑ ΕΡΓΑΛΕΙΑ.....	42
5.2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ	43
5.3 ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΠΕΡΙΓΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.....	44
<u>ΚΕΦΑΛΑΙΟ 6 ΣΥΜΠΕΡΑΣΜΑΤΑ.....</u>	<u>46</u>
<u>ΒΙΒΛΙΟΓΡΑΦΙΑ</u>	<u>50</u>

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Η σημερινή εποχή είναι η εποχή του «αυτοματισμού», καθώς ο άνθρωπος, για να ολοκληρώσει τη δουλειά του, βασίζεται σε μεγάλο βαθμό στις μηχανές. Η Τεχνολογία Υπολογιστών βοηθά τον ανθρώπινο πολιτισμό σε τόσο μεγάλο βαθμό που η ζωή χωρίς υπολογιστές φαίνεται να είναι αδύνατη. Μιλώντας με παραδείγματα, σιδηροδρομικές κρατήσεις, μεταφορές αεροσκαφών, κάρτες αποτελεσμάτων εξετάσεων, σήματα κυκλοφορίας, τηλεφωνικές επικοινωνίες, τραπεζικές συναλλαγές, όλα γίνονται με τη βοήθεια υπολογιστών και κάθε στοιχείο έχει αποκτήσει ηλεκτρονική μορφή και μπορεί να κινείται μέσα από τις οπτικές ίνες. Ακόμη, η παραγωγή προϊόντων εξαρτάται σε μεγάλο βαθμό από την τεχνολογία των υπολογιστών.

Ωστόσο, η τεχνολογία των υπολογιστών παρουσιάζει μειονεκτήματα, καθώς τα πλεονεκτήματα χάνονται υπό την απειλή του κυβερνοεγκλήματος. Χαρακτηριστικές περιπτώσεις εγκλημάτων στον κυβερνοχώρο είναι η παρέμβαση σε οποιαδήποτε ενέργεια τελείται ηλεκτρονικά, προκαλώντας σύγχυση και παρακωλύοντας το τελικό αποτέλεσμα. Για παράδειγμα, ένας εγκληματίας μπορεί να σταματήσει οποιονδήποτε σιδηρόδρομο όπου και αν κινείται, μπορεί να παραπλανήσει τα αεροπλάνα με λάθος σήματα, ή μπορεί να σταματήσει τα ηλεκτρονικά μέσα.

Ως έγκλημα στον κυβερνοχώρο μπορεί να οριστεί κάθε έγκλημα που τελείται με τη βοήθεια τεχνολογίας υπολογιστών και τηλεπικοινωνιών, με σκοπό να επηρεάσει τη λειτουργία των υπολογιστών ή των συστημάτων υπολογιστών. Το έγκλημα στον κυβερνοχώρο είναι η πιο διαδεδομένη «επιδημία» που αντιμετωπίζει ο πλανήτης αυτή τη χιλιετία. Με την αυξανόμενη και ευρεία χρήση του Διαδικτύου, αναμένεται ότι το έγκλημα στον κυβερνοχώρο θα επηρεάσει μεγάλο μέρος των χρηστών, είτε άμεσα, είτε έμμεσα, καθώς δεν υπάρχει εργασία που να μην υλοποιείται, έστω έως ένα βαθμό, με την αξιοποίηση της τεχνολογίας.

1.2 Σκοπός και Ερευνητικά Ερωτήματα

Η ηθική στον κυβερνοχώρο αποτελεί το βασικό ζητούμενο στην έρευνα αυτή και παράλληλα είναι απαραίτητο να εξεταστεί το κυβερνοέγκλημα. Επομένως, τα ερευνητικά ερωτήματα που γεννιούνται είναι τα ακόλουθα:

- Ποιες είναι οι μέθοδοι για τη βελτίωση της ποιότητας της ηθικής στο διαδίκτυο;
- Ποια είναι τα είδη του κυβερνοεγκλήματος;
- Η νομοθεσία κατά του κυβερνοεγκλήματος είναι επαρκής;

Για να απαντηθούν όλα αυτά όμως είναι απαραίτητο να παρατεθούν τα βασικά στοιχεία του Διαδικτύου και του διαδικτυακού εγκλήματος.

1.3 Βασικά Στοιχεία του Διαδικτύου και του Διαδικτυακού Εγκλήματος

Το Διαδίκτυο είναι ένα ολόένα και πιο σημαντικό μέρος της καθημερινής ζωής για τους ανθρώπους σε όλο τον κόσμο και απαρτίζεται από ένα παγκόσμιο δίκτυο δισεκατομμυρίων υπολογιστών και άλλων ηλεκτρονικών συσκευών. Με το Διαδίκτυο, είναι δυνατή η πρόσβαση σχεδόν σε οποιαδήποτε πληροφορία, η επικοινωνία με οποιονδήποτε άλλον άνθρωπο στον κόσμο και πολλά περισσότερα (Michael, 2020).

Το Διαδίκτυο ξεκίνησε το 1969 ως μια υπηρεσία προηγμένων ερευνητικών έργων του Υπουργείου Άμυνας των ΗΠΑ, με στόχο να παρέχει άμεση επικοινωνία εντός του Υπουργείου σε περίπτωση πολέμου. Στη συνέχεια, εγκαταστάθηκαν υπολογιστές σε πανεπιστήμια των ΗΠΑ. Καθώς οι μελετητές άρχισαν να συνδέονται στο διαδίκτυο, η χρήση του που ήταν κυρίως στρατιωτική, άλλαξε σε επιστημονική. Καθώς το δίκτυο μεγάλωνε, η διαχείριση του συστήματος διανεμήθηκε σε διάφορους οργανισμούς, συμπεριλαμβανομένου του Εθνικού Ιδρύματος Επιστημών (NSF). Αυτή η μετατόπιση ξεκίνησε τη μετατροπή του επιστημονικού προσανατολισμού προς το Διαδίκτυο με στόχο την εμπορική διάθεση και τη χρηματοδότηση που χρησιμοποιείται από εκατομμύρια άτομα σήμερα (Troia, 2020).

Το Διαδίκτυο λειτουργεί ως αγωγός για τη μεταφορά ηλεκτρονικών μηνυμάτων από το ένα δίκτυο στο άλλο. Στην καρδιά των περισσότερων δικτύων

βρίσκεται ένας διακομιστής, ένας γρήγορος υπολογιστής με μεγάλες ποσότητες μνήμης και αποθηκευτικού χώρου. Ο διακομιστής ελέγχει την επικοινωνία πληροφοριών μεταξύ των συσκευών που είναι συνδεδεμένες σε ένα δίκτυο, όπως υπολογιστές, εκτυπωτές ή άλλους διακομιστές (Hill & Marion, 2016).

Ένας πάροχος υπηρεσιών Διαδικτύου (ISP) επιτρέπει στο χρήστη πρόσβαση στο Διαδίκτυο μέσω του διακομιστή του. Πολλοί εκπαιδευτικοί χρησιμοποιούν μια σύνδεση μέσω ενός τοπικού πανεπιστημίου επειδή είναι δωρεάν. Άλλοι πάροχοι υπηρεσιών Internet, όπως η America Online, εταιρείες τηλεφωνίας ή καλωδιακές εταιρείες παρέχουν πρόσβαση στο Διαδίκτυο στα μέλη τους. Το ίδιο συμβαίνει και στην Ελλάδα, καθώς είναι δυνατόν για όλους να συνδεθούν στο Διαδίκτυο μέσω τηλεφωνικών γραμμών, καλωδιακών μόντεμ, κινητών τηλεφώνων και άλλων φορητών συσκευών (Manjikian, 2019).

Η ραγδαία τεχνολογική ανάπτυξη και οι εξελίξεις έχουν προσφέρει νέες ευκαιρίες και παραγωγικές πηγές για οργανισμούς όλων των μεγεθών. Η τεχνολογική ανάπτυξη υποστηρίζεται κυρίως από το Διαδίκτυο και οι νέες τεχνολογίες έχουν φέρει απειλές στον κυβερνοχώρο. Το έγκλημα στον κυβερνοχώρο είναι μια σοβαρή πρόκληση για την κοινωνία και είναι επιβλαβής (Manjikian, 2019).

Το έγκλημα στον κυβερνοχώρο αποτελεί απειλή για τη σημερινή κοινωνία που εξαρτάται από το Διαδίκτυο και αποτελεί αυξανόμενο πρόβλημα. Οι χρήστες χρησιμοποιούν διαδικτυακές τραπεζικές συναλλαγές, ηλεκτρονικές αγορές και διαδικτυακή κοινωνική δικτύωση, καθώς η ψηφιακή τεχνολογία παρέχει οφέλη, αλλά ταυτόχρονα δημιουργεί ένα πλούσιο περιβάλλον για εγκληματικές δραστηριότητες, με στόχο την κλοπή ταυτότητας και την κλοπή απόρρητων κρατικών πληροφοριών, γνωστή και ως hacking. Μερικά σύντομα παραδείγματα περιλαμβάνουν την αγορά και πώληση παράνομου λογισμικού και κακόβουλου λογισμικού, την παραβίαση διακομιστών, την καταστροφή συστημάτων που θα μπορούσαν να κοστίσουν δισεκατομμύρια σε άτομα, οργανισμούς και κυβερνήσεις (Chowbe, 2023).

Ως κυβερνοέγκλημα νοείται κάθε έγκλημα που διαπράττεται με χρήση υπολογιστή ή ηλεκτρονικής συσκευής, κυρίως μέσω του Διαδικτύου, καθώς το Διαδίκτυο προσφέρει πολλές ευκαιρίες για κατανάλωση και πρόσβαση σε

πληροφορίες. Οι κυβερνοεπιθέσεις έχουν προκαλέσει σημαντικές ζημιές στις τραπεζικές συναλλαγές με χρήση πιστωτικής κάρτας και απάτες πληρωμών. Οι χάκερ συνήθως στρέφονται σε ιστότοπους κοινωνικής δικτύωσης που βασίζονται στο Διαδίκτυο. Σήμερα, οποιοσδήποτε μπορεί να στείλει και να λάβει οποιαδήποτε μορφή δεδομένων, είτε πρόκειται για email, ήχο ή βίντεο, κάνοντας απλώς ένα «κλικ». Το Διαδίκτυο είναι πράγματι η ταχύτερα αναπτυσσόμενη υποδομή στην καθημερινή ζωή και οι τελευταίες τεχνολογίες αλλάζουν το πρόσωπο της ανθρωπότητας. Ενώ το Διαδίκτυο είναι μια καταπληκτική εφεύρεση, έχει γίνει ένα απαραίτητο μέρος της ζωής μας, αλλά υπάρχουν πολλά εκεί έξω που θα μπορούσαν να προκαλέσουν σοβαρά προβλήματα (Chowbe, 2023).

Το κυβερνοέγκλημα περιλαμβάνει εγκλήματα όπως «ψάρεμα» (phishing), απάτες με πιστωτικές κάρτες, παράνομη λήψη δεδομένων, βιομηχανική κατασκοπεία, παιδική πορνογραφία, απάτες και κυβερνοτρομοκρατία. Ορισμένα εγκλήματα που διαπράχθηκαν στο Διαδίκτυο έχουν αποκαλυφθεί και μερικά παραμένουν άλυτο μυστήριο. Οι άνθρωποι προσπαθούν να λύσουν προβλήματα ιών εγκαθιστώντας λογισμικό προστασίας. Η πραγματικότητα όμως είναι ότι οι ένοχοι για τα εγκλήματα του Διαδικτύου, σε πολλές περιπτώσεις, είναι δύσκολο να εντοπιστούν και να συλληφθούν. Άρα, οι χρήστες του Διαδικτύου θα πρέπει να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν μέτρα, όπως να χρησιμοποιούν μοναδικούς κωδικούς πρόσβασης, να έχουν λογισμικό προστασίας από ιούς και λογισμικό αντικατασκοπείας (Mishra, 2020).

ΚΕΦΑΛΑΙΟ 2 ΗΘΙΚΗ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

2.1 Η ηθική ως Στοιχείο του Κόσμου της Πληροφορίας

Η ηθική είναι βασική αξία της κοινωνίας. Αλλά η πραγματικότητα είναι ότι η ηθική χρησιμεύει περισσότερο ως αρετή παρά ως πρότυπο για να εφαρμόζεται στην πραγματική ζωή. Σε σχέση με πολλά διαφορετικά σε απευθείας σύνδεση κοινωνικά δίκτυα, είναι εμφανές ότι η ανάγκη για σαφή ηθικά πρότυπα είναι μεγάλη και θα πρέπει να δοθεί έμφαση στην προστασία του απορρήτου των χρηστών (Vasiliu- Feltes & Thomason, 2021).

Ο όρος «ήθος» όπως χρησιμοποιείται στην Αρχαία Ελλάδα περιλαμβάνει δύο διαφορετικές έννοιες — ανάλογα με το ποια από τις παραλλαγές της λέξης που επέλεξε κανείς να χρησιμοποιήσει — δηλαδή συνήθεια και έθιμο, ή χαρακτήρας και ήθη. Συνεπώς, το ήθος αντανakλά κατευθυντήριες πεποιθήσεις ή ιδανικά που διέπουν την κοινότητα, όπως οι πρακτικές δεξιότητες, η σοφία, η αρετή, η καλοσύνη και η καλή θέληση. Σαν αποτέλεσμα, το ήθος έχει ως τελεολογικό στόχο την επιδίωξη μιας καλής ζωής. Στην αρχαιότητα, η ηθική ήταν συνδεδεμένη με το φυσικό δίκαιο. Από αυτή την άποψη, η ηθική συμπεριφορά θεωρείται ως αντανakλαση βασικών κανονιστικών αρχών. Οι επακόλουθες προσδοκίες οδηγούν φυσικά σε τεκμήρια για τις επιθυμητές ενέργειες και όλα αυτά αποκρυσταλλώνονται σε ένα σύστημα κανόνων και θεσμών που στηρίζουν την κοινωνία των πολιτών (Vasiliu- Feltes & Thomason, 2021).

Σε πιο σύγχρονες εποχές, το ήθος άρχισε να γίνεται μια σημαντική έννοια για τους νομικούς και τους φιλοσόφους του 17^{ου} αιώνα. Ο Χομπς εξέφρασε την άποψη ότι η ανθρώπινη ταυτότητα θεμελιώνεται λιγότερο στη συλλογική κοινωνική τάξη, παρά στα αυτόνομα δικαιώματα ενός ατόμου να ασκήσει τις δικές του φυσικές δεξιότητες. Σύμφωνα με τον Λοκ, η ταυτότητα που έχει ένα άτομο που διαθέτει αυτοσυντηρούμενα χαρακτηριστικά αντανakλά τη φυσική ελευθερία. Μόνο ο Ρουσσώ άλλαξε τον λόγο που υποστηρίζει τη μεταμόρφωση του ατόμου σε κοινωνικό άνθρωπο. Κατά την οπτική του Καντ, η ηθική αξιοπρέπεια του ατόμου πρέπει να αναπτυχθεί, αφού η ανθρωπότητα αντανakλά η ίδια την αξιοπρέπεια. Με άλλα λόγια, για τον Καντ, η ηθική αναφέρεται στη «σωστή» ή «λάθος» συμπεριφορά ως μέρος της φιλοσοφίας της ανθρώπινης συμπεριφοράς (Rachels & Rachels, 2012).

Η ηθική συνεπάγεται ότι κάποιος ενεργεί ηθικά. Από μια γενική σκοπιά, τα ήθη αναφέρονται στις εμπειρικά έγκυρες κοινωνικά συμβάσεις σε οποιαδήποτε κοινωνική ομάδα. Η ηθική περιλαμβάνει τα «κοινωνικά έγκυρα ηθικά δικαιώματα και τις υποχρεώσεις και τα πρότυπα συμπεριφοράς που προκύπτουν από μια συγκεκριμένη κουλτούρα και παράδοση. Το ήθος επομένως θεωρείται ως η προσωπική πεποίθηση ενός ατόμου, η «αυτοαντίληψη του όσον αφορά την ταυτότητα και τη νομιμότητα». Έτσι τα άτομα πρέπει να δικαιολογήσουν τις ηθικές αρχές στις οποίες βασίζεται η ζωή τους(Rachels & Rachels, 2012).

Η ηθική ως ακαδημαϊκή επιστήμη αξιολογεί κανονιστικές αξιώσεις από μια διαφανή και αμερόληπτη προοπτική. Η ηθική έτσι αντιμετωπίζει αρχές ή κανόνες που δηλώνουν κάτι για τις καλές ανθρώπινες πράξεις. Τρεις τύποι ηθικών αξιών εντοπίζονται: η ηθική περιγράφει το εφαρμοστέο πεδίο εφαρμογής της. Πρώτον, η περιγραφική ή εμπειρική ηθική σκιαγραφεί στο πολλαπλάσιο τις εμφανίσεις των ασκούμενων ηθών και των εθίμων των ατόμων, των θεσμών και των πολιτισμών. Δεύτερον, κανονιστικά, η ηθική εξετάζει τις υπάρχουσες στάσεις απέναντι στην ηθική και πλαισιώνει κανόνες προσανατολισμένους στη δράση. Όσον αφορά τη μεταηθική, αυτή εξετάζει εξονυχιστικά τις ηθικές μεθόδους και τις επεκτείνει(Rachels & Rachels, 2012).

Στο πλαίσιο αυτό, η ηθική αντιμετωπίζει αρκετές ανησυχίες. Αρχικά, η ηθική σκέψη πρέπει να αντικατοπτρίζει τη θέση αυτών που επηρεάζονται από έγκυρους ηθικούς ισχυρισμούς και η κριτική αξιολόγηση των πρακτικών διαδικασιών ενθαρρύνουν την προσοχή σε θέματα κοινωνικής ευθύνης και ηθικής επάρκειας. Η ηθική ενισχύει επίσης μια μακροπρόθεσμη άποψη των επιχειρηματικών σχέσεων, δηλαδή της πίστης, της εμπιστοσύνης και της υπευθυνότητας που βασίζεται στην έννοια της ευσέβειας (Rachels & Rachels, 2012).

Οι ακόλουθες θεμελιώδεις ηθικές αξίες σχετίζονται με την ανάπτυξη της κοινωνίας της πληροφορίας:

- Δικαιοσύνη/ισότητα: Κάθε άτομο έχει αναφαίρετη την αξιοπρέπεια και δικαιούται ίσα δικαιώματα. Ο σεβασμός του ενός για τον άλλον καλλιεργεί τη Δικαιοσύνη και η δίκαιη και ισότιμη πρόσβαση στην πληροφόρηση επιτρέπει στα μέλη της κοινωνίας των πολιτών να επιτευχθεί διμερής κατανόηση.

- **Ελευθερία:** Η ανθρώπινη αξιοπρέπεια απαιτεί την ανάπτυξη διαφόρων ελευθεριών: στο πλαίσιο του Διαδικτύου, για παράδειγμα, η ελευθερία της έκφρασης, των πεποιθήσεων και πρόσβασης σε πληροφορίες είναι σημαντική. Ως αποτέλεσμα, η ελευθερία, η ισότητα και η ευθύνη πρέπει να ισορροπούν μεταξύ τους.
- **Φροντίδα και συμπόνια:** Η ενσυναίσθηση και ο σεβασμός οδηγεί στην αλληλεγγύη και την αμοιβαία υποστήριξη
- **Κοινή χρήση:** Η ανταλλαγή πληροφοριών και γνώσεων στο πλαίσιο του Διαδικτύου επιτρέπει και οδηγεί σε βιώσιμες σχέσεις μεταξύ των ανθρώπων και, ως αποτέλεσμα, ενισχύει τις κοινότητες.
- **Βιωσιμότητα:** Μακροπρόθεσμα, τα βιώσιμα έργα είναι σημαντικά για την προστασία του περιβάλλοντος για όλα τα ανθρώπινα όντα.
- **Υπευθυνότητα:** Η ανάληψη ευθύνης για τις προσωπικές δράσεις είναι βασική απαίτηση σε ένα κοινωνικό περιβάλλον. Το επίπεδο ευθύνης πρέπει να αντιστοιχεί στα επίπεδα της δύναμης, της ικανότητας και των ικανοτήτων του ατόμου (Krieger & Belliger, 2021).

Αυτές οι διαφορετικές ηθικές αξίες είναι αλληλένδετες και μπορούν να ισορροπήσουν η μια την άλλη. Σε αντίθεση με τα αποκλίνοντα ανθρώπινα δικαιώματα (για παράδειγμα, η ελευθερία έκφρασης έναντι της ιδιωτικότητας) και οι άμεσες συγκρούσεις προσφέρουν ένα νέο πεδίο συζητήσεων, διότι τα ανθρώπινα δικαιώματα μπορούν να θεωρηθούν ως επισημοποιημένη ηθική (Krieger & Belliger, 2021).

Η πραγματοποίηση της ηθικής εξαρτάται από τις ευκαιρίες και την προθυμία των ατόμων να τα εφαρμόσουν όλα αυτά στην πρακτική ζωή. Η ηθική δείχνει ξεκάθαρα, ότι ουσιαστικά δεν υπάρχει χώρος στις πληροφορίες και η κοινωνία βρίσκεται έξω από τους κανόνες συμπεριφοράς που μπορούν να καθοδηγήσουν τις ηθικές πράξεις. Δεδομένου ότι οι ηθικές αξίες είναι αλληλένδετες, το πεδίο εφαρμογής είναι σχεδόν απεριόριστο (Krieger & Belliger, 2021).

Όσον αφορά τη σημασία των πρακτικών περιστάσεων, δύο περιπτώσιολογικές μελέτες έχουν γίνει και μπορούν να βοηθήσουν στον εντοπισμό των πραγματικών προκλήσεων. Η πρώτη μελέτη περίπτωσης εξετάζει την αντιμετώπιση της ηθικής στις πολλές και ποικίλες δηλώσεις διακυβέρνησης του Διαδικτύου που εγκρίθηκαν

κατά την τελευταία δεκαετία. Η δεύτερη μελέτη εξετάζει το κοινωνικό δίκτυο συμμόρφωσης των παρόχων με τα πρότυπα δεοντολογίας. Κάθε μελέτη δείχνει τις πρακτικές προκλήσεις στην εφαρμογή της ηθικής και περαιτέρω προτείνει πώς ορισμένα από τα οφέλη ηθικής συμπεριφοράς μπορούν να επιτευχθούν (Krieger & Belliger, 2021).

Αυτές οι δύο περιπτώσιολογικές μελέτες έχουν επιλεγεί σκόπιμα, διότι απευθύνονται σε διαφορετικούς κοινωνικούς τομείς. Η διακυβέρνηση του Διαδικτύου αποτελεί ένα παγκόσμιο ζήτημα που αφορά πολλούς ενδιαφερόμενους και απαιτεί το σχεδιασμό γενικών κανόνων, δηλαδή, η διακυβέρνηση του Διαδικτύου να εφαρμόζεται στο μακροεπίπεδο. Αντίθετα, οι σχέσεις μεταξύ κοινωνικών δικτύων και οι χρήστες τους βασίζονται σε συμβάσεις, όποια και αν είναι η μορφή τους, καθώς αυτές οι σχέσεις λαμβάνουν χώρα σε μικροεπίπεδο (Krieger & Belliger, 2021).

2.2 Ηθική στην Ηλεκτρονική Διακυβέρνηση

Ο ρόλος της ηθικής έχει αναδειχθεί στη διακυβέρνηση του Διαδικτύου και σε συζητήσεις σε διάφορα φόρουμ. Η «Δήλωση των Αρχών» της Γενεύης επιδιώκει να διασφαλίσει αυτό που όλοι μπορούν να επωφεληθούν από τις ευκαιρίες ενημέρωσης και τις Τεχνολογίες Πληροφορίας και Επικοινωνιών (ΤΠΕ). Αυτό δηλώνει αντιμετώπιση των ηθικών διαστάσεων της πληροφορίας και η κοινωνία αποτελεί βασική αρχή για όλους τους ενδιαφερομένους στην οικοδόμηση μια κοινωνίας της πληροφορίας χωρίς αποκλεισμούς. Η δήλωση αυτή προτρέπει την κοινωνία της πληροφορίας να σεβαστεί την ειρήνη και την υποστήριξη θεμελιωδών αξιών όπως η ελευθερία, η αλληλεγγύη και οι κοινές ευθύνες υπογραμμίζοντας τη σημασία της ηθικής για την κοινωνία της πληροφορίας, ενώ παράλληλα καλεί όλους τους φορείς να λάβουν τα κατάλληλα μέτρα και τις δράσεις για την πρόληψη των γεγονότων (Xie, 2020).

Στο πλαίσιο αυτό, η Διακήρυξη απαιτεί την υπεύθυνη χρήση και αντιμετώπιση των πληροφοριών από τα μέσα ενημέρωσης σύμφωνα με τα υψηλότερα ηθικά πρότυπα. Εξάλλου, η υποστήριξη μιας κοινωνίας της πληροφορίας που υπόκειται σε οικουμενικές αξίες, προάγει το κοινό καλό και αποτρέπει την

καταχρηστική εξάρτηση από τις ΤΠΕ. Έτσι, το «Σχέδιο Δράσης της Γενεύης» καλεί όλα τα ενδιαφερόμενα μέρη να αυξήσουν την επίγνωσή τους για τις ηθικές διαστάσεις της χρήσης του Διαδικτύου, ενώ παράλληλα περαιτέρω ενθαρρύνει όλα τα ενδιαφερόμενα μέρη να συνεχίσουν να ερευνούν τις ηθικές διαστάσεις των ΤΠΕ (Xie, 2020).

Η UNESCO θεωρείται ο σημαντικότερος οργανισμός που προσφέρει συνεχή ανασκόπηση των θεμάτων δεοντολογίας. Η «UNESCO και οι ηθικές διαστάσεις της κοινωνίας της ενημέρωσης» της 14ης Σεπτεμβρίου 2012, απευθύνεται στο βασικό ρόλο στην ανάπτυξη ηθικών προοπτικών για να καταστεί δυνατή η κοινωνική και η ανθρώπινη πρόοδος για την κοινωνία της πληροφορίας. Η συμβολή της στη διεθνή συζήτηση για τις ηθικές διαστάσεις της κοινωνίας της πληροφορίας, οι συνεχιζόμενες παγκόσμιες προσπάθειες στον τομέα των ηθικών διαστάσεων της κοινωνίας της πληροφορίας και οι προτάσεις για πιθανούς τρόπους με τους οποίους η UNESCO θα μπορούσε να αντιμετωπίσει τις ηθικές διαστάσεις της κοινωνίας της πληροφορίας είναι τα βασικά ζητήματα για την αντιμετώπιση των διαστάσεων του ζητήματος (Σφακιανάκης, 2016).

Το Διαδίκτυο έχει αναπτυχθεί για μεγάλο χρονικό διάστημα χωρίς ρύθμιση. Ο καθορισμός πρωτοκόλλων και προτύπων ήταν το πιο σημαντικό στοιχείο για μεγάλο χρονικό διάστημα και αυτό ανέπτυξε τη ρυθμιστική δραστηριότητα. Τα πρότυπα και η διαχείριση δρομολόγησης, η κρυπτογράφηση, η ψηφιακή υπογραφή, η αδειοδότηση παρόχων υπηρεσιών Διαδικτύου, τα δικαιώματα ιδιοκτησίας και τα εγκλήματα που προκύπτουν μέσα από το Διαδίκτυο ήταν ερωτήματα που τέθηκαν μόλις το ηλεκτρονικό εμπόριο ήρθε στο προσκήνιο. Ειδικότερα, εξετάζεται η διαχείριση ονομάτων και διευθύνσεων στο Διαδίκτυο ως κρίσιμης σημασίας στοιχείο για τη σταθερότητα και τη διαλειτουργικότητα του Διαδικτύου. Η κατανομή των ονομάτων είναι υψίστης σημασίας για τους ενδιαφερόμενους οργανισμούς, τους χρήστες και τους κατόχους εμπορικών σημάτων (Σφακιανάκης, 2016).

Η συζήτηση για το συγκεκριμένο ζήτημα είναι πάντα επίκαιρη, καθώς υπάρχουν ορισμένα εξαιρετικά ευαίσθητα χαρακτηριστικά περιβάλλουν την έννοια της διακυβέρνηση του Διαδικτύου. Η εκστρατεία της μπλε κορδέλας και παρόμοιες εκδηλώσεις κατά της λογοκρισίας έρχονται πίσω στην αρχή, όταν το Διαδίκτυο ήταν κυρίως εργαλείο έρευνας και εκπαίδευσης, δηλαδή λειτουργώντας σύμφωνα με την

αρχή της «ακαδημαϊκής ελευθερίας». Επομένως, το ερώτημα που προκύπτει είναι αν το Διαδίκτυο χρειάζεται περισσότερη ρύθμιση. Αυτοί που υποστηρίζουν την περισσότερη ρύθμιση αισθάνονται ότι το Διαδίκτυο σήμερα είναι χαοτικό και ανεξέλεγκτο, όπως επίσης και αυτορυθμιζόμενο (Babadac, 2015).

Η ηθική στην Ηλεκτρονική διακυβέρνηση είναι απαραίτητη, διότι:

- Η πληροφορική είναι ένα ισχυρό και συνεχώς εξελισσόμενο εργαλείο,
- Η πληροφορική διαπερνά όλες τις πτυχές της ζωής μας,
- Η εξάρτηση από το IT δημιουργεί ευπάθεια σε μεγάλη κλίμακα,
- Η εξέλιξη και η χρήση της πληροφορικής ξεπερνούν τη διατύπωση και την εφαρμογή των πολιτικών και των νομικών μέσων (Σφακιανάκης, 2016).

Υπάρχει μια σχετικά εύκολη συναίνεση ότι η ηθική είναι απαραίτητη στο διαδίκτυο, όταν μιλάμε για προστασία των ανηλίκων και της ανθρώπινης αξιοπρέπειας. Η δράση και το σχέδιο για την προώθηση της ασφαλέστερης χρήσης του Διαδικτύου» αποτελεί μέρος ενός συνεκτικού συνόλου σε επίπεδο Ευρωπαϊκής Ένωσης (ΕΕ) για την αντιμετώπιση παράνομου και επιβλαβούς περιεχομένου στο Ίντερνετ (Σφακιανάκης, 2016).

2.3 Ηθική στα Μέσα Κοινωνικής Δικτύωσης

Διαδικτυακά κοινωνικά δίκτυα όπως Facebook, Google, Twitter και άλλα έχουν όχι μόνο ευρεία οικονομική έκταση, αλλά και κοινωνικές και πολιτιστικές επιπτώσεις στο διαδικτυακό κόσμο. Έχοντας τεράστια αύξηση σε μέλη και χρήστες κατά το παρελθόν, τα διαδικτυακά κοινωνικά δίκτυα έχουν πλέον αναγνωρίσει τη συμμόρφωση με τις ηθικές αρχές και είναι ζήτημα φήμης. Ενεργώντας σύμφωνα με τις ηθικές αρχές βελτιώνεται η φήμη των κοινωνικών δικτύων, η οποία με τη σειρά της βοηθά στην απόκτηση της εμπιστοσύνης των χρηστών και κάνει τους παρόχους υπηρεσιών πιο ελκυστικούς σε πιθανούς πελάτες. Φυσικά, κερδίζοντας και διατηρώντας περισσότερα οι πελάτες ενισχύουν επίσης τα διαφημιστικά έσοδα των δικτύων (Dover et al., 2017).

Ως εκ τούτου, τουλάχιστον ρητορικά, τα κοινωνικά δίκτυα όλο και περισσότερο διακηρύσσουν τα ηθικά πρότυπα που ακολουθούν, καθώς και τις αρχές της εταιρικής κοινωνικής ευθύνης. Οι δημόσιες δηλώσεις των κοινωνικών δικτύων

αναγκαστικά συμπίπτουν με την πραγματικότητα. Γύρω από αυτό το λόγο, αξίζει να εξεταστεί η συμμόρφωση των κοινωνικών δικτύων με ηθικές αρχές στην πράξη και στο μικροεπίπεδο ηθικής (Dover et al., 2017).

Οι δημόσιες ανακοινώσεις των κοινωνικών δικτύων με υψηλά ηθικά πρότυπα πρέπει να αντικατοπτρίζεται στην πραγματικότητα. Δηλαδή η πρακτική εφαρμογή των προτύπων πρέπει να υπόκεινται σε επανεξέταση. Για παράδειγμα, οι δραστηριότητες του Twitter και άλλοι ιστότοποι κοινωνικής δικτύωσης αξιολογούνται, διότι αυτοί οι πάροχοι προσφέρουν ευκαιρίες σε χρήστες από όλο τον κόσμο να μοιράζονται προσωπικές πληροφορίες και να συμμετέχουν στη δημόσια συνομιλία. Ωστόσο, οι εμπορικές επιταγές και ιδιαίτερα τα συμφέροντα του κλάδου της διαφήμισης τείνουν να κατευθύνουν τη συμμετοχή των χρηστών σε μια ασύμμετρη ιδιωτική ρύθμιση, κυρίως εκφρασμένη με τους όρους υπηρεσίας των κοινωνικών δικτύων, οι οποίοι το κάνουν, με στόχο να λαμβάνονται απαραίτητα υπόψη τα συμφέροντα των χρηστών, για παράδειγμα, η αποφυγή επεξεργασίας μεγάλης κλίμακας στα προσωπικά δεδομένα. Αυτοί οι όροι παροχής υπηρεσιών ρυθμίζουν τα δικαιώματα των χρηστών, για παράδειγμα, όσον αφορά το απόρρητο των πληροφοριών και της πνευματικής ιδιοκτησίας, με τρόπο που δεν περιορίζει τις δραστηριότητες μάρκετινγκ των κοινωνικών δικτύων. Τέτοια συμπεριφορά θεωρείται προβληματική, γιατί αυτά τα κοινωνικά δίκτυα ενεργούν ως οιονεί κυβερνητικές ρυθμιστικές αρχές (Matei & Bruneau, 2011).

Το Twitter προσελκύει χρήστες του Διαδικτύου και αποκτά νέα μέλη προσφέροντας συμμετοχή σε μια «πληροφόρηση σε πραγματικό χρόνο που υποστηρίζει την ελευθερία του Λόγου. Το Διαδικτυακό κοινωνικό δίκτυο μεταξύ άλλων δηλώνει ότι η ανοιχτή ανταλλαγή πληροφοριών μπορεί να έχει θετική παγκόσμια επιρροή. Δεν μπορεί να αγνοηθεί ότι το Twitter και άλλα κοινωνικά δίκτυα συχνά φαίνεται να αφυπνίζουν μια εργαλειακή προσέγγιση στο ήθος που δεν αντικατοπτρίζει σωστά τα ηθικά δικαιώματα, τις ευθύνες και τις στρατηγικές προκλήσεις που οι ΤΠΕ αντιμετωπίζουν όταν αλληλεπιδρούν με τους ενδιαφερόμενους. Επιπλέον, ο ρυθμιστικός ρόλος που διαδραματίζουν τα κοινωνικά δίκτυα στο διαδικτυακό περιβάλλον δυσκολεύει τη σκέψη για τις πραγματικές επιπτώσεις του ρόλου τους ως οιονεί ρυθμιστικές αρχές των δικαιωμάτων των χρηστών (Matei & Bruneau, 2011).

Επομένως, υπάρχει μια σημαντική διαφορά μεταξύ των κοινωνικών δικτύων τυπικά και στην πραγματικότητα. Η ηθική συμπεριφορά λειτουργεί με εργαλειακό τρόπο, μιας που ο ρόλος των κοινωνικών δικτύων και του Ίντερνετ γενικότερα είναι δημόσιος, χρηστοκεντρικός και από την άλλη οδηγεί σε μια βασισμένη στα δικαιώματα προσέγγιση που επικεντρώνεται σε ζητήματα, όπως το απόρρητο των χρηστών και τα δικαιώματα πνευματικής ιδιοκτησίας. Ωστόσο, αυτά τα δικαιώματα περιορίζονται ουσιαστικά. Ειδικότερα, η ενοποιητική επιχειρηματική ηθική δεν εφαρμόζεται ως μια σημαντική ηθική πειθαρχία. Επιπλέον, η λογοδοσία και οι μηχανισμοί θα πρέπει να βελτιωθούν ουσιαστικά, η έλλειψη και η ανεπαρκής λογοδοσία αποτελεί αδυναμία της μη συμμόρφωσης με τις δηλωμένες ηθικές αρχές, επομένως η εταιρική ηθική αφήνει περιθώριο για περισσότερα πρότυπα ηθικής συμπεριφοράς(Roche, 2016).

Τα κοινωνικά δίκτυα παίζουν προφανώς ρόλο ως φύλακες και μεσάζοντες γιατί είναι έτσι σε θέση να υποβάλουν λογοκρισία, τόσο με θετικό, όσο και με αρνητικό τρόπο. Δεδομένου ότι τα υπάρχοντα κοινωνικά δίκτυα, μέχρι στιγμής, έχουν δομικό ρόλο, θα έλεγε κανείς ότι είναι οι «κυρίαρχοι του κυβερνοχώρου». Επιπλέον, κοινωνικά οι πλατφόρμες Διαδικτύου μπορούν να καθορίσουν τι μπορούν να κάνουν οι χρήστες στις αντίστοιχες διαδικτυακές περιοχές τους. Κατά συνέπεια, το Facebook και η Google επικρίνονται ως όντα έκφρασης μιας «νέας φεουδαρχίας». Αυτό σημαίνει ότι οι εταιρείες ΤΠΕ και τα κοινωνικά δίκτυα ασκούν μια «οιονεί κυβερνητική» λειτουργία σε δύο επίπεδα. Το πρώτο επίπεδο αφορά τα βασικά επιχειρηματικά τους μοντέλα (δηλαδή πώς βγάζουν χρήματα) και έχουν άμεση επιρροή στα ενδιαφερόμενα μέρη τους. Το δεύτερο επίπεδο δείχνει τον τρόπο με τον οποίο τα επιχειρηματικά μοντέλα αλληλεπιδρούν έμμεσα με τα ενδιαφερόμενα μέρη τους (Roche, 2016).

Λαμβάνοντας υπόψη αυτές τις εξελίξεις, τα διαδικτυακά κοινωνικά δίκτυα θεωρείται ότι έχουν εφαρμόσει και αναγνωρίζουν νόμιμους κανονισμούς ως εταιρικοί παράγοντες. Τα κοινωνικά δίκτυα πρέπει να συνειδητοποιήσουν και να αντιμετωπίσουν την πραγματικότητα, καθώς όλα δείχνουν ότι έχουν γίνει de facto πολιτικοί ρυθμιστές και η νομιμότητά τους αμφισβητείται συνεχώς. Επιπλέον, είναι απαραίτητο τα κοινωνικά δίκτυα να βελτιώσουν τις διαδικασίες λήψης αποφάσεων,

με στόχο να αποκτήσουν νομιμότητα και είναι απαραίτητο να διεξάγουν έναν άνευ όρων διάλογο με τα ενδιαφερόμενα μέρη τους(Lavorgna & Holt, 2021).

Δεδομένου ότι τα διαδικτυακά κοινωνικά δίκτυα εξαρτώνται από τη συμμετοχή των μελών τους, οι χρήστες του Διαδικτύου πρέπει να αποδεχτούν τη δική τους ευθύνη. Οι χρήστες για να γίνονται σεβαστοί στο διαδίκτυο, πρέπει να υπερασπίζονται τα δικαιώματά τους και να δημιουργήσουν έναν πληροφοριακό περιβάλλον συμβατό με τον πολίτη. Με άλλα λόγια, οι χρήστες πρέπει να σταματήσουν να συμπεριφέρονται σαν παθητικοί πελάτες και πρέπει να αρχίσουν να ενεργούν σαν υπεύθυνοι χρήστες του Διαδικτύου. Όσο περισσότεροι χρήστες του Διαδικτύου χρησιμοποιούν ενεργά τα δικαιώματά τους, τόσο πιο δύσκολο είναι οι κυβερνήσεις και οι εταιρείες να μειώσουν τις ελευθερίες τους(Lavorgna & Holt, 2021).

Γνωρίζοντας τη σημασία της δράσης σύμφωνα με τις ηθικές αρχές, τουλάχιστον τα περισσότερα διαδικτυακά κοινωνικά δίκτυα προσποιούνται ότι συμφωνούν με την έννοια της εταιρικής κοινωνικής ευθύνης. Ωστόσο, ορισμένες από τις πρακτικές τους φαίνεται να είναι ηθικά προβληματικές, όπως, για παράδειγμα, η κοινή πρακτική του κέρδους από τη συλλογή και τη χρήση των προσωπικών στοιχείων πελατών για διαφημιστικούς σκοπούς. Στην πραγματικότητα, τα κοινωνικά δίκτυα δεν ανταποκρίνονται στις καθιερωμένες ηθικές αρχές, όπως η Δικαιοσύνη ή η Λογοδοσία. Στην πραγματικότητα μόνο σε κάποιο βαθμό συμμορφώνονται με την εταιρική ηθική. Επιπλέον, αφού λειτουργούν ως οιονεί κυβερνητικές ρυθμιστικές αρχές, τα διαδικτυακά κοινωνικά δίκτυα θα πρέπει να υποχρεωθούν να βελτιώσουν τη νομιμότητά τους εμπλέκοντας σε άνευ όρων διάλογο όλα τα ενδιαφερόμενα μέρη (Lavorgna & Holt, 2021).

Από την παραπάνω ανάλυση αυτό που μπορούμε να συμπεράνουμε είναι ότι τα ηθικά ζητήματα δεν παραμελούνται εντελώς στις αντίστοιχες συζητήσεις, αλλά η πρακτική συμμόρφωση με τις θεωρητικές αρχές δεν ανταποκρίνεται στις προσδοκίες των εμπλεκόμενων μερών. Επομένως, είναι απαραίτητο να βρεθούν μέθοδοι για τη βελτίωση της ποιότητας της ηθικής στον κυβερνοχώρο.

2.4 Μέθοδοι για τη βελτίωση της ποιότητας της ηθικής στον κυβερνοχώρο

2.4.1 Κατοχύρωση της Εμπιστοσύνης

Ανεξάρτητα από τον σχεδιασμό του, ένα τεχνολογικό σύστημα θα πρέπει να εμπνέει εμπιστοσύνη. Από ηθικής άποψης, η εμπιστοσύνη ενισχύει τη συνεργασία και προωθεί τις αμοιβαίες σχέσεις. Κατά συνέπεια, η βελτιωμένη ηθική για τις αναδυόμενες τεχνολογίες απαιτείται και θα πρέπει να σχεδιαστούν εφαρμογές Διαδικτύου με τέτοιο τρόπο που θεωρούνται αξιόπιστες στα μάτια της κοινωνίας των πολιτών. Επομένως, στο πλαίσιο της διακυβέρνησης του Διαδικτύου, θα πρέπει να δοθεί ιδιαίτερη προσοχή σε θέματα ασφάλειας δεδομένων και απαιτήσεις λογοδοσίας(Σφακιανάκης, 2016).

Επιπλέον, η εμπιστοσύνη συνδέεται επίσης με την «εξάρτηση». Εάν ένα άτομο βασίζεται σε κάτι ή σε κάποιον για να επιδείξει ένα χαρακτηριστικό ή συμπεριφορά, τότε αυτό το άτομο ενεργεί με τέτοιο τρόπο που διαμορφώνεται από μια σίγουρη πίστη στο άλλο μέρος. Η εμπιστοσύνη είναι ιδιαίτερα σημαντική στο πλαίσιο των απειλών στον κυβερνοχώρο και της ασφάλειας στον κυβερνοχώρο. Για παράδειγμα, η οικοδόμηση εμπιστοσύνης μπορεί να βελτιωθεί με την καλύτερη ανταλλαγή πληροφοριών ή με την εισαγωγή περισσότερο κατάλληλων προτύπων εμπιστοσύνης(Σφακιανάκης, 2016).

Η εμπιστοσύνη θα πρέπει επιπλέον να προβάλλεται μέσα από το φακό της αυτοπεποίθησης. Οποιαδήποτε εμπιστευτική αλληλεπίδραση πρέπει να καθιερώνει τη διαδικασία ανταλλαγής διαπιστευτηρίων. Στο δυναμικό πλαίσιο του Διαδικτύου, όπου οι αλληλεπιδράσεις αλλάζουν γρήγορα, η εμπιστοσύνη και οι σχέσεις πρέπει να οδηγούν στη χρήση συστημάτων φήμης, τα οποία μπορεί να συμβάλλουν στην καθιέρωση αξιοπιστίας στον εικονικό κόσμο (για παράδειγμα, στα κοινωνικά δίκτυα). Το άλλο στοιχείο κρίσιμο για την οικοδόμηση εμπιστοσύνης είναι η υπευθυνότητα — δηλαδή η αναγνώριση και ανάληψη ευθύνης για δράσεις, αποφάσεις και πολιτικές εντός του πεδίου εφαρμογής του καθορισμένου ρόλου. Η λογοδοσία συνίσταται στην υποχρέωση του ατόμου σε άλλον, σύμφωνα με την οποία το πρώτο πρέπει να λογοδοτήσει, να εξηγήσει και να αιτιολογήσει τις πράξεις του ή τις αποφάσεις με κριτήρια του ίδιου είδους, καθώς και τα άτομα να λαμβάνουν ευθύνη για οποιαδήποτε βλάβη (Σφακιανάκης, 2016).

2.4.2 Υλοποίηση της Κοινωνίας της Γνώσης

Ακόμη, στο πλαίσιο αυτό εντάσσεται και η υλοποίηση της κοινωνίας της γνώσης. Ηθικές εκτιμήσεις καθιστούν επιτακτικό ότι η κοινωνία της πληροφορίας εξελίσσεται σε κοινωνία της γνώσης. Επομένως, έξι πλευρές πρέπει να ληφθούν υπόψη:

- Προσέγγιση με βάση την αξία: Η γνώση πρέπει να μοιράζεται δίκαια, ισότιμα, ελεύθερα και προς όφελος της φροντίδας βιώσιμων κοινοτήτων, σεβόμενη έτσι την ποικιλομορφία των πολιτισμών, των γλωσσών, των θρησκειών και των οικονομικών – πολιτικών συστημάτων
- Ανθρωποκεντρικό πλαίσιο: Η τεχνολογία δεν πρέπει να είναι ένας στόχος από μόνος του, αλλά θα πρέπει να εξυπηρετεί τα άτομα στην προσωπική τους ανάπτυξη
- Κοινότητες και λύσεις προσανατολισμένες στις ταυτότητες: το Διαδίκτυο έχει την τάση να αυξάνει τον ατομικισμό, ωστόσο οι ανάγκες και τα δικαιώματα των ατόμων και των κοινοτήτων θα πρέπει να είναι ισορροπημένα, ιδιαίτερα επειδή η πλημμύρα των πληροφοριών οδηγεί σε συνεχή κατασκευή και ανασυγκρότηση ταυτοτήτων
- Προσέγγιση με επίκεντρο την εκπαίδευση: Η ηθική της πληροφόρησης απαιτεί την υπεύθυνη αντιμετώπιση των πληροφοριών. Η εκπαίδευση στην κρίσιμη κατανάλωση μέσων, συμπεριλαμβανομένης της χρήσης των μέσων κοινωνικής δικτύωσης μπορεί να βοηθήσει τους ενδιαφερόμενους να αντιμετωπίσουν τις πληροφορίες
- Σχεδιασμός με γνώμονα το φύλο: η ισότητα είναι μια σημαντική διάσταση μιας περιεκτικής και ανθρωποκεντρικής κοινωνίας. Η διασφάλιση της ισότητας των γυναικών περιλαμβάνει την πρόσβαση σε πληροφορίες, επικοινωνία, γνώση και λήψη αποφάσεων
- Πλαίσιο ευαίσθητο στη γενιά: ο τεχνολογικός γραμματισμός βοηθά στην αύξηση της συμμετοχής όλων των ατόμων σε κοινωνικά ζητήματα και ιδιαίτερα διευκολύνει την ανταλλαγή γνώσεων μεταξύ γενεών (Matei & Bruneau, 2011).

Η βελτίωση της παραγωγής και ανταλλαγής γνώσεων αναφέρεται σε μεγάλο αριθμό στη διακυβέρνηση του Διαδικτύου. Εντούτοις, το ουσιαστικό περιεχόμενο

αυτών παραμένουν σχετικά ασαφείς. Η εφαρμογή με βάση τις δεοντολογικές κατευθυντήριες γραμμές όπως περιγράφονται παραπάνω στο πλαίσιο για μια κοινωνία της γνώσης είναι πιο συγκεκριμένες και η υλοποίηση των αντίστοιχων στόχων περισσότερο πιθανές. Ως εκ τούτου, θα πρέπει να δοθεί μεγαλύτερη προσοχή σε θέματα όπως η εκπαίδευση, η πολυγλωσσία και ο πολιτισμός με την ποικιλομορφία που τον διακρίνει. Η έμφαση στη γνώση που αποκτάται και μοιράζεται μπορεί να συμβάλει στην επίτευξη των ηθικών στόχων της συμμετοχής και κυρίως του μοιράσματος, που οδηγεί σε ενισχυμένες κοινότητες και βιώσιμες σχέσεις μεταξύ των ανθρώπων (Matei & Bruneau, 2011).

2.4.3 Αποφυγή της Ψηφιακής Διαιρέσης

Συναφές με τα παραπάνω είναι τα ηθικά πρότυπα που σχετίζονται με την κοινωνική δικαιοσύνη. Ανάμεσα σε πολλές και διαφορετικές αντιλήψεις, η κοινωνική δικαιοσύνη σημαίνει τη δίκαιη κατανομή των οφελών και των βαρών, καθώς και των ίσων ευκαιριών με στόχο να επωφεληθούν από τις τεχνολογικές εξελίξεις όλα τα άτομα. Έτσι, η κοινωνική δικαιοσύνη μπορεί να συμβάλει στην κοινωνική ακεραιότητα και την πρόληψη των κοινωνικών ανισοτήτων (Dover et al., 2017).

Ένα βασικό ζήτημα είναι η πρόσβαση στον εικονικό κόσμο. Το ιδανικό είναι να αποφεύγονται τα μειονεκτήματα και η αδικία στην πρόσβαση όσον αφορά τη γνώση, την ενδυνάμωση και άλλους ζωτικούς πόρους για την ευημερία των ατόμων. Τα εικονικά δίκτυα έχουν γίνει ο δημόσιος χώρος για ιδιωτικές επικοινωνίες και επιχειρηματικές συναλλαγές, καθώς και για σχέσεις μεταξύ κυβερνήσεων και κοινωνίας των πολιτών. Ο αποκλεισμός από αυτόν το χώρο στερεί από τους ενδιαφερόμενους τη συμμετοχή στα κοινωνικά δίκτυα και την αστική ζωή (Dover et al., 2017).

Το ψηφιακό χάσμα συζητείται για περισσότερα από 10 χρόνια. Πέρα από την υπέρβαση του ψηφιακού χάσματος, απαιτεί και η ηθική να αποτρέψουμε το «χάσμα πρόσβασης» σε πόρους γνώσης. Αυτό σημαίνει ενίσχυση της ελεύθερης και δίκαιης πρόσβασης στη γνώση υποστηρίζοντας την ανοιχτή πρόσβαση στα αποθετήρια (συμπεριλαμβανομένης της εκπαίδευσης και της υποστήριξης), την ανάπτυξη σε περιφερειακούς κόμβους που στηρίζουν αποθετήρια ανοιχτής πρόσβασης και υλοποίηση ανοιχτών εκδοτικών πρωτοβουλιών, συμπεριλαμβανομένων της

παγκόσμιας διαφάνειας, της προσβασιμότητας και των αξιών. Παρ' όλο που υπάρχουν στοιχεία ότι τα επίπεδα πρόσβασης στο Διαδίκτυο αυξάνονται στις ανεπτυγμένες χώρες, ένα μεγάλο μέρος της ανθρωπότητας εξακολουθεί να είναι αποκλεισμένο από το Διαδίκτυο(Σφακιανάκης, 2016).

Η υπέρβαση του χάσματος πρόσβασης μπορεί επίσης να φανεί στο πλαίσιο για την ενίσχυση της δημοκρατίας και των δημοκρατικών θεσμών παρέχοντας στο κοινό επαρκείς ευκαιρίες για αποτελεσματική δημόσια διαβούλευση και συμμετοχή στις δημοκρατικές διαδικασίες. Η δίκαιη συμμετοχή όλων των ενδιαφερομένων από όλες τις περιοχές του κόσμου, αναγνωρίζοντας παράλληλα την ποικιλομορφία των πολιτισμών, θα επιτρέψει επίσης στα άτομα να ανταποκριθούν στις ηθικές προκλήσεις της κοινωνίας της πληροφορίας. Από τη συμμετοχή και την κοινή χρήση που αποτελούν βασικούς ηθικούς στόχους, μεγαλύτερη προσοχή πρέπει να δοθεί στην καταπολέμηση του ψηφιακού χάσματος, διότι αυτή η πτυχή θα βελτιώσει την ηθική του Ίντερνετ αποτελεσματικότερα (Σφακιανάκης, 2016).

2.4.4 Δημιουργία μιας Ανοικτής Κοινωνίας

Οι πρόσφατες τεχνολογικές εξελίξεις και η αυξανόμενη συμμετοχή της κοινωνίας των πολιτών στον κυβερνοχώρο μπορεί να οδηγήσει στην ίδρυση και ανάπτυξη μιας ανοικτής κοινωνίας. Παράλληλα, θεμελιώδεις ηθικές αξίες, όπως η αναφαίρετη ανθρώπινη αξιοπρέπεια, οι βασικές ελευθερίες, η κοινωνική ευθύνη και η δικαιοσύνη έχουν επίσης παγκόσμια εμβέλεια και μπορεί να προωθήσει δημόσια τη συνειδητοποίηση αυτών των αρχών(Schoenherr, 2022).

Η έννοια της ανοικτής κοινωνίας, όπως διατυπώθηκε από τον Karl Popper το 1945 προσπαθεί να διατηρήσει και την ατομική ελευθερία ως το ιδανικό του πολιτικοϊδεολογικού πλουραλισμού. Η σκέψη εστιάζεται στο άνοιγμα και την αποδοχή άλλων προσεγγίσεων που περιέχουν λύσεις για προβλήματα, τα οποία συμβάλλουν σε ένα περιβάλλον που θα επέτρεπε την καλύτερη εναλλακτική λύση για να εδραιωθεί η ανοικτή κοινωνία. Η ανοικτή κοινωνία προσφέρει ιδανικά χώρο για πρόσβαση στα άτομα με τις υπάρχουσες επιλογές, ενώ υπολογίζονται οι συνέπειές τους και αναλαμβάνονται η ευθύνη για την τελική έκβαση των επιλογών τους(Schoenherr, 2022).

Στον ψηφιακό κόσμο, δημόσια φόρουμ που επιτρέπουν ανταλλαγές γνώμης είναι διαθέσιμα και επιτρέπουν τη συμμετοχή των συμμετεχόντων με διαφορετικά υπόβαθρα και πολλές και διαφορετικές ιδέες. Δεδομένου ότι οι νέες δυνατότητες για συμμετοχή μπορεί να αναπτυχθούν και οι προηγούμενες διαδικασίες μπορεί να βελτιωθούν, υπάρχει μια σοβαρή πιθανότητα ότι μπορεί ο κυβερνοχώρος χρησιμεύει ως κατάλληλο εργαλείο για μια ανοιχτή κοινωνία (Schoenherr, 2022) .

Δεδομένου ότι η ψηφιακή εποχή κερδίζει ολοένα και περισσότερο έδαφος, το κοινό πρέπει να εστιάζεται όλο και περισσότερο στις ηθικές πτυχές του Twitter, του Facebook, του Google και άλλων μορφών κοινωνικών δικτύων. Όλα αυτά όμως απαιτούν άμεση προσοχή και κοινή πρακτική δημιουργίας εσόδων των διαδικτυακών κοινωνικών δικτύων, με αποτέλεσμα να υπάρχουν τα προσωπικά στοιχεία πελατών για διαφημιστικούς σκοπούς και τις οιονεί κυβερνητικές λειτουργίες τους. Τα διαδικτυακά κοινωνικά δίκτυα πρέπει να «βιώνουν» την ηθική συμπεριφορά και την εταιρική κοινωνική ευθύνη βάζοντας το μάρκετινγκ σε δεύτερη μοίρα (Schoenherr, 2022).

Με βάση όλα τα παραπάνω, η ηθική παίρνει τη μορφή οδηγιών συμπεριφοράς που απορρέουν από αξίες όπως η Δικαιοσύνη και η Ισότητα, η φροντίδα , η συμπόνια και η ευθύνη. Αυτές οι αξίες δε χρειάζονται μόνο προσοχή σε έγγραφα όπως διεθνείς κατευθυντήριες γραμμές και πλαίσια, αλλά και συγκεκριμένη εφαρμογή στην καθημερινή ζωή. Συνεχείς συζητήσεις για το σχέδιο και το σχήμα της κοινωνία της πληροφορίας παρέχει ένα κατάλληλο φόρουμ για να καταστεί δυνατή η βαθύτερη κατανόηση των ηθικών θεωρήσεων.

ΚΕΦΑΛΑΙΟ 3 ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

3.1 Τα Κυριότερα Είδη Ηλεκτρονικού Εγκλήματος

3.1.1. Παιδική Πορνογραφία, Διαδικτυακή Τρομοκρατία

Η παιδική πορνογραφία είναι μια μορφή σεξουαλικής εκμετάλλευσης παιδιών και ορίζεται ως οποιαδήποτε οπτική απεικόνιση σεξουαλικής συμπεριφοράς που περιλαμβάνει έναν ανήλικο (άτομα κάτω των 18 ετών). Οι εικόνες παιδικής πορνογραφίας αναφέρονται επίσης ως εικόνες σεξουαλικής κακοποίησης παιδιών. Έτσι, ο νόμος απαγορεύει την παραγωγή, διανομή, εισαγωγή, λήψη ή κατοχή οποιασδήποτε εικόνας παιδικής πορνογραφίας. Επειδή ο όρος «παιδική πορνογραφία» χρησιμοποιείται επίσης συνήθως από νομοθέτες, ερευνητές και το κοινό για να περιγράψει αυτή τη μορφή σεξουαλικής εκμετάλλευσης παιδιών, αυτός ο όρος αποτυγχάνει να περιγράψει την αληθινή φρίκη που αντιμετωπίζουν αμέτρητα παιδιά κάθε χρόνο. Η παραγωγή παιδικής πορνογραφίας δημιουργεί ένα μόνιμο αρχείο της σεξουαλικής κακοποίησης ενός παιδιού. Όταν αυτές οι εικόνες τοποθετούνται στο Διαδίκτυο και διαδίδονται, η θυματοποίηση των παιδιών συνεχίζεται στο διηνεκές. Οι ειδικοί και τα θύματα συμφωνούν ότι τα θύματα που απεικονίζονται στην παιδική πορνογραφία συχνά υφίστανται επαναλαμβανόμενη θυματοποίηση για μια ζωή, γνωρίζοντας ότι οι εικόνες της σεξουαλικής τους κακοποίησης βρίσκονται για πάντα στο Διαδίκτυο. Αυτό συχνά δημιουργεί μόνιμες ψυχολογικές βλάβες στο παιδί, συμπεριλαμβανομένων διαταραχών στη σεξουαλική ανάπτυξη, την εικόνα του εαυτού του και την ανάπτυξη σχέσεων εμπιστοσύνης με άλλους στο μέλλον.

Η επέκταση του Διαδικτύου και της προηγμένης ψηφιακής τεχνολογίας βρίσκεται παράλληλα με την έκρηξη της αγοράς παιδικής πορνογραφίας. Οι εικόνες παιδικής πορνογραφίας είναι άμεσα διαθέσιμες μέσω Διαδικτύου, συμπεριλαμβανομένων ιστοτόπων κοινωνικής δικτύωσης, ιστοτόπων κοινής χρήσης αρχείων, ιστοτόπων κοινής χρήσης φωτογραφιών, συσκευών παιχνιδιών, ακόμη και εφαρμογών για κινητό. Οι παραβάτες παιδικής πορνογραφίας μπορούν επίσης να συνδεθούν σε φόρουμ και δίκτυα Διαδικτύου για να μοιραστούν τα ενδιαφέροντά τους, τις επιθυμίες και τις εμπειρίες τους κατά την κακοποίηση παιδιών, εκτός από την πώληση, την κοινή χρήση και την εμπορία εικόνων. Αυτές οι διαδικτυακές

κοινότητες έχουν προωθήσει την επικοινωνία και τη συνεργασία μεταξύ παραβατών παιδικής πορνογραφίας ενισχύοντας έτσι μια ευρύτερη σχέση που βασίζεται σε ένα κοινό σεξουαλικό ενδιαφέρον για τα παιδιά. Αυτό έχει ως αποτέλεσμα τη διάβρωση της ντροπής που τυπικά θα συνόδευε αυτή τη συμπεριφορά, καθώς και την απευαισθητοποίηση όσων εμπλέκονται στη σωματική και ψυχολογική βλάβη που προκαλείται στα παιδιά-θύματα. Για το λόγο αυτό, οι διαδικτυακές κοινότητες προσελκύουν και ενθαρρύνουν νέα άτομα να συμμετάσχουν μαζί τους στη σεξουαλική εκμετάλλευση παιδιών (Akdeniz, 2016).

Συναφές με το παραπάνω είναι η διαδικτυακή τρομοκρατία, η οποία είναι μια απειλή που έχει τραβήξει την προσοχή των μέσων μαζικής ενημέρωσης και της κοινότητας ασφάλειας και της βιομηχανίας Τεχνολογίας Πληροφοριών (IT). Δημοσιογράφοι, πολιτικοί, και ειδικοί σε διάφορους τομείς έχουν διαδώσει ένα σενάριο στο οποίο οι κυβερνοτρομοκράτες εισβάλλουν ηλεκτρονικά σε υπολογιστές που ελέγχουν φράγματα ή την εναέρια κυκλοφορία προκαλώντας τον όλεθρο και θέτοντας σε κίνδυνο όχι μόνο εκατομμύρια ζωές αλλά και την εθνική ασφάλεια (Marcum, 2019).

Επειδή οι περισσότερες κρίσιμες υποδομές στις δυτικές κοινωνίες είναι δικτυωμένες μέσω υπολογιστών, η πιθανή απειλή από την κυβερνοτρομοκρατία είναι, σίγουρα, πολύ ανησυχητική. Οι χάκερ, αν και δεν παρακινούνται από τους ίδιους στόχους που εμπνέουν τρομοκράτες, έχουν δείξει ότι είναι άτομα που μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες και στη λειτουργία κρίσιμων υπηρεσιών. Οι τρομοκράτες, τουλάχιστον θεωρητικά, θα μπορούσαν έτσι να ακολουθήσουν το παράδειγμα των χάκερ και στη συνέχεια, έχοντας εισβάλει σε κρατικά και ιδιωτικά συστήματα υπολογιστών, ακρωτηριάζουν ή τουλάχιστον απενεργοποιούν τους στρατιωτικούς, οικονομικούς και υπηρεσιακούς τομείς των προηγμένων οικονομιών.

Η αυξανόμενη εξάρτηση των κοινωνιών από την τεχνολογία της πληροφορίας έχει δημιουργήσει μια νέα μορφή ευπάθειας, δίνοντας στους τρομοκράτες την ευκαιρία να πλησιάσουν στόχους που διαφορετικά θα ήταν εντελώς απρόσβλητοι, όπως τα εθνικά αμυντικά συστήματα και τα συστήματα ελέγχου της κυκλοφορίας. Όσο πιο τεχνολογικά ανεπτυγμένη είναι μια χώρα, τόσο πιο ευάλωτη γίνεται σε κυβερνοεπιθέσεις κατά των υποδομών της (Marcum, 2019). Επομένως, η ανησυχία

για τον πιθανό κίνδυνο που ενέχει η κυβερνοτρομοκρατία είναι βάσιμη (Marcum, 2019).

3.1.2 Προπαγάνδα Μίσους

Ένας αυξανόμενος αριθμός επιθέσεων σε μετανάστες και άλλες μειονότητες έχει εγείρει νέες ανησυχίες σχετικά με τη σύνδεση μεταξύ του εμπρηστικού λόγου στο διαδίκτυο και των βίαιων πράξεων, καθώς και για το ρόλο των εταιρειών και του κράτους στην αστυνόμευση του Λόγου. Οι αναλυτές λένε ότι οι τάσεις στα εγκλήματα μίσους σε όλο τον κόσμο απηχούν αλλαγές στο πολιτικό κλίμα και ότι τα μέσα κοινωνικής δικτύωσης μπορούν να μεγεθύνουν τη διχόνοια. Στην πιο ακραία μορφή τους, οι φήμες και η επιθετικότητα που διαδίδονται στο Διαδίκτυο έχουν συμβάλει στη βία που εκτείνεται από το λιντσάρισμα έως την εθνοκάθαρση (Johnson, 2016).

Η ανταπόκριση ήταν άνιση και το καθήκον της απόφασης για το τι θα 'λογοκριθεί' έχει σε μεγάλο βαθμό πέσει στα χέρια των εταιρειών που ελέγχουν τις πλατφόρμες στις οποίες επικοινωνεί πλέον μεγάλο μέρος του κόσμου. Αλλά αυτές οι εταιρείες περιορίζονται από τους εσωτερικούς νόμους. Στις φιλελεύθερες δημοκρατίες, αυτοί οι νόμοι μπορούν να χρησιμεύσουν για την άμβλυνση των διακρίσεων και την αποτροπή της βίας κατά των μειονοτήτων. Αλλά τέτοιοι νόμοι μπορούν επίσης να χρησιμοποιηθούν για την καταστολή των μειονοτήτων και των διαφωνούντων (Johnson, 2016).

Περιστατικά έχουν αναφερθεί σχεδόν σε όλες τις ηπείρους. Μεγάλο μέρος του κόσμου πλέον επικοινωνεί στα μέσα κοινωνικής δικτύωσης, με σχεδόν το 1/3 του παγκόσμιου πληθυσμού να είναι ενεργό στο Facebook. Καθώς όλο και περισσότεροι άνθρωποι επικοινωνούν μέσω Διαδικτύου, υπάρχουν άτομα που τείνουν προς το ρατσισμό, το μισογυνισμό ή την ομοφοβία και έχουν βρει θέσεις που μπορούν να ενισχύσουν τις απόψεις τους και να τους οδηγήσουν στη βία. Οι πλατφόρμες μέσω κοινωνικής δικτύωσης προσφέρουν επίσης στους βίαιους παράγοντες την ευκαιρία να δημοσιοποιήσουν τις πράξεις τους (Johnson, 2016).

Στη Γερμανία βρέθηκε συσχέτιση μεταξύ των αναρτήσεων στο Facebook κατά των προσφύγων από το ακροδεξιό κόμμα «Εναλλακτική για τη Γερμανία» και των επιθέσεων σε πρόσφυγες. Οι μελετητές παρατήρησαν ότι οι αυξήσεις σε επιθέσεις, όπως ο εμπρησμός και οι επιθέσεις, ακολούθησαν αιχμές σε αναρτήσεις που

υποκινούν μίσος. Στις Ηνωμένες Πολιτείες, οι δράστες των επιθέσεων λευκής υπεροχής έχουν υπάρξει μεταξύ ρατσιστικών κοινοτήτων στο Διαδίκτυο και επέλεξαν τα μέσα κοινωνικής δικτύωσης για να δημοσιοποιήσουν τις πράξεις τους. Ο δράστης στη συναγωγή του Πίτσμπουργκ το 2018 συμμετείχε στο δίκτυο κοινωνικής δικτύωσης Gab, του οποίου οι χαλαροί κανόνες έχουν προσελκύσει εξτρεμιστές που έχουν απαγορευτεί από μεγαλύτερες πλατφόρμες. Η δικτύωση αυτή υποστήριξε τη συνωμοσία ότι οι Εβραίοι επιδίωκαν να φέρουν μετανάστες στις Ηνωμένες Πολιτείες και να καταστήσουν τους λευκούς μειονότητα (Edwards, 2019).

Στη Μιανμάρ, στρατιωτικοί ηγέτες και βουδιστές εθνικιστές χρησιμοποίησαν τα μέσα κοινωνικής δικτύωσης για να προσβάλουν και να δαιμονοποιήσουν τη μουσουλμανική μειονότητα των Ροχίνγκια πριν και κατά τη διάρκεια μιας εκστρατείας εθνοκάθαρσης. Αν και οι Ροχίνγκια αποτελούσαν ίσως το 2 % του πληθυσμού, οι εθνοεθνικιστές ισχυρίστηκαν ότι οι Ροχίνγκια σύντομα θα υποκαθιστούσαν τη βουδιστική πλειοψηφία. Η Σρι Λάνκα έχει δει παρόμοια επαγρύπνηση εμπνευσμένη από φήμες που διαδίδονται στο Διαδίκτυο, με στόχο τη μουσουλμανική μειονότητα των Ταμίλ. Κατά τη διάρκεια μιας σειράς βίας τον Μάρτιο του 2018, η κυβέρνηση απέκλεισε την πρόσβαση στο Facebook και στο WhatsApp, καθώς και στην εφαρμογή ανταλλαγής μηνυμάτων Viber, για μια εβδομάδα, λέγοντας ότι το Facebook δεν ανταποκρίθηκε επαρκώς κατά τη διάρκεια της έκτακτης ανάγκης (Edwards, 2019).

3.1.3 Διαδικτυακός Εκφοβισμός

Ο διαδικτυακός εκφοβισμός είναι ο εκφοβισμός με τη χρήση ψηφιακών τεχνολογιών και μπορεί να πραγματοποιηθεί σε μέσα κοινωνικής δικτύωσης, πλατφόρμες ανταλλαγής μηνυμάτων, πλατφόρμες παιχνιδιών και κινητά τηλέφωνα. Ο διαδικτυακός εκφοβισμός είναι επαναλαμβανόμενη συμπεριφορά, με στόχο να τρομάξει, να θυμώσει ή να ντροπιάσει όσους στοχοποιούνται. Τα παραδείγματα περιλαμβάνουν τη διάδοση ενοχλητικών φωτογραφιών ή βίντεο στα μέσα κοινωνικής δικτύωσης, την αποστολή βλαβερών ή απειλητικών μηνυμάτων, εικόνων ή βίντεο μέσω πλατφορμών ανταλλαγής μηνυμάτων, πλαστοπροσωπία κάποιου και αποστολή κακόβουλων μηνυμάτων σε άλλους για λογαριασμό τους ή μέσω ψεύτικων λογαριασμών (Hill & Marion, 2016).

Όταν ο εκφοβισμός συμβαίνει στο διαδίκτυο, μπορεί να νιώθει κανείς σα να δέχεται επίθεση από παντού, ακόμα και μέσα στο σπίτι του και μπορεί να φαίνεται ότι δεν υπάρχει διαφυγή. Οι επιπτώσεις μπορεί να διαρκέσουν πολύ και να επηρεάσουν ένα άτομο με πολλούς τρόπους:

- Διανοητικά – τα άτομα νιώθουν αναστατωμένα, ντροπιασμένα, ανόητα, ακόμη και θυμωμένα
- Συναισθηματικά – ντροπή ή απώλεια ενδιαφέροντος για τα πράγματα που αγαπάνε
- Σωματικά – κούραση (απώλεια ύπνου) ή συμπτώματα όπως πόνοι στο στομάχι και πονοκεφάλους.

Σε ακραίες περιπτώσεις, ο διαδικτυακός εκφοβισμός μπορεί να οδηγήσει ακόμη και στην αυτοκτονία ανθρώπων (Hill & Marion, 2016).

Η λύση που μπορεί να βρεθεί ωστόσο προκύπτει μέσα από τα ίδια τα κοινωνικά δίκτυα, μιας που κάθε πλατφόρμα κοινωνικής δικτύωσης προσφέρει διαφορετικά εργαλεία που επιτρέπουν να περιορίσουμε ποιος μπορεί να σχολιάσει ή να δει τις αναρτήσεις μας ή ποιος μπορεί να συνδεθεί αυτόματα ως φίλος και να αναφέρει περιπτώσεις εκφοβισμού. Πολλά από αυτά περιλαμβάνουν απλά βήματα για τον αποκλεισμό, τη σίγαση ή την αναφορά διαδικτυακού εκφοβισμού. Οι εταιρείες μέσων κοινωνικής δικτύωσης παρέχουν επίσης εκπαιδευτικά εργαλεία και καθοδήγηση σε παιδιά, γονείς και δασκάλους για να ενημερωθούν σχετικά με τους κινδύνους και τους τρόπους να παραμείνουν ασφαλείς στο διαδίκτυο (Hill & Marion, 2016).

3.1.4 Ξέπλυμα Χρήματος

Το ξέπλυμα βρώμικου χρήματος είναι η παράνομη διαδικασία δημιουργίας μεγάλων ποσών χρημάτων που παράγονται από εγκληματικές δραστηριότητες, όπως η διακίνηση ναρκωτικών ή η χρηματοδότηση της τρομοκρατίας. Το Ίντερνετ τα κάνει να φαίνονται ότι προέρχονται από νόμιμη πηγή. Τα χρήματα από την εγκληματική δραστηριότητα θεωρούνται βρώμικα και η διαδικασία τα «ξεπλένουν» για να φαίνονται καθαρά. Το ξέπλυμα βρώμικου χρήματος είναι ένα σοβαρό οικονομικό έγκλημα που χρησιμοποιείται από εγκληματίες και για το λόγο αυτό οι περισσότερες χρηματοπιστωτικές εταιρείες σήμερα εφαρμόζουν πολιτικές κατά της

νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML) για τον εντοπισμό και την πρόληψη αυτής της δραστηριότητας (Johnson, 2016).

Το ξέπλυμα χρήματος είναι απαραίτητο για εγκληματικές οργανώσεις που επιθυμούν να χρησιμοποιήσουν αποτελεσματικά χρήματα που αποκτήθηκαν παράνομα. Η αντιμετώπιση μεγάλων ποσών παράνομων μετρητών είναι αναποτελεσματική και επικίνδυνη. Οι εγκληματίες χρειάζονται έναν τρόπο να καταθέσουν χρήματα σε νόμιμα χρηματοπιστωτικά ιδρύματα, ωστόσο μπορούν να το κάνουν μόνο εάν φαίνεται ότι προέρχονται από νόμιμες πηγές (Johnson, 2016).

Το Διαδίκτυο έχει βάλει μια νέα τροπή στο παλιό έγκλημα. Η άνοδος των ηλεκτρονικών τραπεζικών ιδρυμάτων, των ανώνυμων διαδικτυακών υπηρεσιών πληρωμών και των μεταφορών peer-to-peer (P2P) με κινητά τηλέφωνα έχουν καταστήσει ακόμη πιο δύσκολο τον εντοπισμό της παράνομης μεταφοράς χρημάτων. Επιπλέον, η χρήση διακομιστών μεσολάβησης και λογισμικού ανωνυμοποίησης καθιστά σχεδόν αδύνατο να εντοπιστεί το συστατικό της νομιμοποίησης εσόδων από παράνομες δραστηριότητες, της ενοποίησης — τα χρήματα μπορούν να μεταφερθούν ή να αποσυρθούν με ελάχιστο ή καθόλου ίχνος διεύθυνσης πρωτοκόλλου Διαδικτύου (IP) (Akdeniz, 2016).

Τα χρήματα μπορούν επίσης να 'ξεπλυθούν' μέσω διαδικτυακών δημοπρασιών και πωλήσεων, ιστοσελίδων τυχερών παιχνιδιών και εικονικών ιστοσελίδων τυχερών παιχνιδιών, όπου τα παράνομα χρήματα μετατρέπονται σε νόμιμα τυχερών παιχνιδιών και στη συνέχεια σε πραγματικά, χρησιμοποιήσιμα και μη ανιχνεύσιμα «καθαρά» χρήματα. Το νεότερο σύνορο του ξεπλύματος χρήματος περιλαμβάνει κρυπτονομίσματα, όπως το Bitcoin. Αν και δεν είναι εντελώς ανώνυμα, χρησιμοποιούνται όλο και περισσότερο σε προγράμματα εκβιασμού, εμπόριο ναρκωτικών και άλλες εγκληματικές δραστηριότητες λόγω της σχετικής ανωνυμίας τους σε σύγκριση με πιο συμβατικές μορφές νομίσματος (Akdeniz, 2016).

Η καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες (AML) επιδιώκει να στερήσει τους εγκληματίες από κέρδη από τις παράνομες επιχειρήσεις τους εξαλείφοντας έτσι το κύριο κίνητρο για αυτούς να συμμετάσχουν σε τέτοιες άθλιες δραστηριότητες. Οι παράνομες και επικίνδυνες δραστηριότητες, όπως η διακίνηση ναρκωτικών, το λαθρεμπόριο ανθρώπων, η χρηματοδότηση της τρομοκρατίας, το λαθρεμπόριο, ο εκβιασμός και η απάτη, θέτουν σε κίνδυνο

εκατομμύρια ανθρώπους παγκοσμίως και επιβάλλουν τεράστιο κοινωνικό και οικονομικό κόστος στην κοινωνία. Καθώς τα έσοδα από τέτοιες δραστηριότητες νομιμοποιούνται από το ξέπλυμα βρώμικου χρήματος, η καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες μπορεί να οδηγήσει σε μείωση της εγκληματικής δραστηριότητας και, ως εκ τούτου, σε σημαντικό όφελος για την κοινωνία (Akdeniz, 2016).

3.1.5 Πειρατεία Λογισμικού

Η πειρατεία λογισμικού Διαδικτύου αναφέρεται σε οποιαδήποτε παράνομη ή/και μη εξουσιοδοτημένη χρήση ηλεκτρονικού υλικού που προστατεύεται από πνευματικά δικαιώματα μέσω σκόπιμης αντιγραφής ή/και διανομής, σκόπιμα ή όχι, ή για κέρδος/μη κερδοσκοπική. Τα συστήματα κοινής χρήσης αρχείων peer-to-peer (P2P) είναι ο κύριος ένοχος στην πειρατεία λογισμικού Διαδικτύου. Το πλαστό λογισμικό που πωλείται μέσω διαδικτυακών τοποθεσιών δημοπρασιών είναι μια άλλη μορφή πειρατείας λογισμικού στο Διαδίκτυο. Η πειρατεία λογισμικού Διαδικτύου συμβαίνει κάθε φορά που το Διαδίκτυο χρησιμοποιείται για ρητούς σκοπούς πώλησης, κοινής χρήσης ή με άλλο τρόπο απόκτησης προστατευμένων δημιουργικών έργων (Berlatsky, 2013).

Η πειρατεία λογισμικού στο Διαδίκτυο καλύπτει ένα πολύ ευρύ πεδίο. Πρέπει να διασφαλίζεται η κατάλληλη άδεια χρήσης για την αντιγραφή, διανομή ή χρήση ψηφιακού υλικού που προστατεύεται από πνευματικά δικαιώματα.

Η πειρατεία λογισμικού στο Διαδίκτυο είναι ένα έγκλημα που είναι σχεδόν αδύνατο να ελεγχθεί. Ωστόσο, βρίσκεται σε άνοδο, καθώς οι προσπάθειες των δραστών γίνονται πιο μυστικές και ποικίλες. Τόσο οι κακόβουλοι, όσο και οι καλόβουλοι χρήστες υλικού που προστατεύεται από ψηφιακά δικαιώματα μπορεί να καταδιωχθούν και να κατηγορηθούν για πειρατεία από υπηρεσίες που έχουν αναλάβει τη δίωξη αυτού του είδους του ηλεκτρονικού εγκλήματος (Berlatsky, 2013).

3.1.6 Ψάρεμα (Phising, pharming)

Η προέλευση του phishing και του pharming είναι μάλλον ενδιαφέρουσα διότι και τα δύο ξεκίνησαν από παραδοσιακές πηγές κερδών, την αλιεία και τη γεωργία, μέχρι

που λήφθηκαν σε ένα διαδικτυακό πλαίσιο και μετατράπηκαν σε τέχνασμα. Στην κλοπή στον κυβερνοχώρο, το phishing και το pharming είναι δύο απάτες που χρησιμοποιούν οι εγκληματίες για να χειραγωγήσουν τους ανθρώπους, ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες. Αυτές οι τακτικές είναι δύο από τις μεγαλύτερες απειλές στον κυβερνοχώρο και καθώς βελτιώνονται τα συστήματα ασφαλείας, βελτιώνονται και οι τακτικές κυβερνοεγκληματικότητας. Το phishing και το pharming έχουν τον ίδιο τελικό στόχο: την απόκτηση ευαίσθητων πληροφοριών(Jahankhani, 2018).

Το phishing είναι μια κοινωνική μηχανική που χειραγωγεί τους χρήστες, ώστε να αποκαλύψουν προσωπικές και εμπιστευτικές πληροφορίες. Οι χάκερ στέλνουν γενικά ένα πλαστό email με ένα νόμιμο όνομα πηγής για να ξεγελάσουν το θύμα να κάνει κλικ στον κακόβουλο σύνδεσμο ή το συνημμένο αρχείο. Όταν οι χρήστες το κάνουν αυτό, οι χάκερ αποκτούν πρόσβαση στις εμπιστευτικές πληροφορίες του στόχου τους. Οι απατεώνες χρησιμοποιούν λογισμικό ή ευπάθειες ασφαλείας που είναι εγκατεστημένες στη συσκευή του χρήστη για να κάνουν το τέχνασμα τους να λειτουργήσει. Ωστόσο, οι επιθέσεις phishing δεν περιορίζονται μόνο στο ηλεκτρονικό ταχυδρομείο και ένα παράδειγμα αυτού θα ήταν ένας κυβερνοεγκληματίας που προσποιείται ότι είναι υπάλληλος της τράπεζάς σας(Jahankhani, 2018).

Το pharming προκύπτει όταν οι εγκληματίες του κυβερνοχώρου εγκαθιστούν κακόβουλο κώδικα στη συσκευή του χρήστη ή σε έναν διακομιστή που τους ανακατευθύνει εν αγνοία τους σε δόλιες ιστοσελίδες. Αυτοί οι ψεύτικοι ιστότοποι μπορεί να φαίνονται νόμιμοι στην αρχή, αλλά έχουν ένα κρυφό κίνητρο κλοπής εμπιστευτικών πληροφοριών, όπως τα στοιχεία σύνδεσης του χρήστη, τα προσωπικά δεδομένα και οι τραπεζικές πληροφορίες. Επιπλέον, οι αυθεντικοί σύνδεσμοι και οι τομείς ενδέχεται επίσης να παραβιαστούν από χάκερ και να κλέψουν πληροφορίες χρηστών. Το Pharming μπορεί να είναι πιο επικίνδυνο για τους χρήστες του Διαδικτύου, καθώς η πιθανότητα εντοπισμού ενός κινδύνου που κρύβεται είναι χαμηλή, ειδικά επειδή επικρατούν οι απάτες κοινωνικής μηχανικής . Οι εισβολείς στον κυβερνοχώρο μπορούν επίσης να μιμηθούν έναν νόμιμο ιστότοπο, όπου οι χρήστες θα μοιράζουν εν αγνοία τους το όνομα χρήστη, τον κωδικό πρόσβασής τους και άλλες κρίσιμες πληροφορίες (Jahankhani, 2018).

3.1.7 Βανδαλισμός Διαδικτυακών Τόπων

Ο βανδαλισμός διαδικτυακών τόπων αποτελεί μια επίθεση κατά την οποία κακόβουλα μέρη διεισδύουν σε έναν ιστότοπο και αντικαθιστούν το περιεχόμενο του ιστότοπου με τα δικά τους μηνύματα. Τα μηνύματα μπορεί να μεταφέρουν ένα πολιτικό ή θρησκευτικό μήνυμα, βωμολοχίες ή άλλο ακατάλληλο περιεχόμενο που θα έφερνε σε δύσκολη θέση τους κατόχους ιστότοπων ή μια ειδοποίηση ότι ο ιστότοπος έχει παραβιαστεί από μια συγκεκριμένη ομάδα χάκερ. Οι περισσότεροι ιστότοποι αποθηκεύουν δεδομένα σε αρχεία περιβάλλοντος ή διαμόρφωσης, τα οποία επηρεάζουν το περιεχόμενο που εμφανίζεται στον ιστότοπο ή καθορίζουν πού βρίσκονται τα πρότυπα και το περιεχόμενο της σελίδας. Οι απροσδόκητες αλλαγές σε αυτά τα αρχεία μπορεί να σημαίνουν συμβιβασμό ασφαλείας και ενδέχεται να σηματοδοτούν μια επίθεση παραμόρφωσης (Marcum, 2019).

Οι θρησκευτικοί και κυβερνητικοί ιστότοποι στοχοποιούνται τακτικά από χάκερ προκειμένου να προβάλλουν πολιτικές ή θρησκευτικές πεποιθήσεις, ενώ αλλοιώνουν τις απόψεις και τις πεποιθήσεις των επίσημων ιστότοπων. Οι ιστότοποι δεν παραποιούνται μόνο για πολιτικούς λόγους, μιας που πολλοί χάκερ το κάνουν μόνο για τη συγκίνηση. Για παράδειγμα, υπάρχουν διαδικτυακοί διαγωνισμοί στους οποίους απονέμονται βαθμοί στους χάκερ για την παραμόρφωση του μεγαλύτερου αριθμού ιστοσελίδων σε καθορισμένο χρονικό διάστημα. Οι εταιρείες στοχοποιούνται επίσης πιο συχνά από άλλους ιστότοπους και συχνά επιδιώκουν να λάβουν μέτρα για να προστατευθούν από την παραβίαση. Οι ιστότοποι αντιπροσωπεύουν την εικόνα μιας εταιρείας ή οργανισμού για τον οποίο η παραμόρφωση μπορεί να προκαλέσει σημαντική απώλεια. Οι επισκέπτες μπορεί να χάσουν την πίστη τους σε ιστότοπους που δεν μπορούν να υποσχεθούν ασφάλεια και θα γίνουν επιφυλακτικοί, όσον αφορά την εκτέλεση ηλεκτρονικών συναλλαγών. Μετά την παραμόρφωση, οι ιστότοποι πρέπει να κλείσουν για επισκευές και έλεγχο ασφαλείας, μερικές φορές για μεγάλο χρονικό διάστημα, προκαλώντας έξοδα και απώλεια κέρδους (Marcum, 2019).

3.2 Νομοθεσία κατά του Ηλεκτρονικού Εγκλήματος

3.2.1. Η ευρωπαϊκή προστασία κατά του ηλεκτρονικού εγκλήματος

Με την ταχέως διευρυνόμενη ψηφιοποίηση της καθημερινής ζωής, που επιταχύνθηκε περαιτέρω από την πανδημία Covid-19, η προστασία από τις απειλές στον κυβερνοχώρο έχει καταστεί απαραίτητη για τη σωστή λειτουργία της κοινωνίας. Οι κυβερνοεπιθέσεις μπορεί να αποδειχθούν πολύ δαπανηρές. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, το ετήσιο κόστος του εγκλήματος στον κυβερνοχώρο για την παγκόσμια οικονομία εκτιμάται ότι έχει φτάσει τα 5,5 τρισεκατομμύρια ευρώ μέχρι το τέλος του 2020. Τον Νοέμβριο του 2022, το Ευρωπαϊκό Κοινοβούλιο ενημέρωσε τη νομοθεσία της ΕΕ για να ενισχύσει τις επενδύσεις σε ισχυρή κυβερνοασφάλεια για βασικές υπηρεσίες και ζωτικής σημασίας υποδομές και να ενισχύσει τους κανόνες σε όλη την ΕΕ (Ευρωπαϊκό Κοινοβούλιο, 2023).

Το Κοινοβούλιο ενίσχυσε επίσης την προστασία της βασικής υποδομής της ΕΕ, συμπεριλαμβανομένης της ψηφιακής υποδομής στις 22 Νοεμβρίου 2022, δίνοντας την τελική του έγκριση σε νομοθεσία που αυστηροποιεί τις εκτιμήσεις κινδύνου και τις απαιτήσεις αναφοράς για κρίσιμους οργανισμούς σε 11 βασικούς τομείς. Ο νέος νόμος διευρύνει το πεδίο των τομέων και δραστηριοτήτων που είναι κρίσιμες για την οικονομία και την κοινωνία, συμπεριλαμβανομένων της ενέργειας, των μεταφορών, των τραπεζών, της υγείας, των ψηφιακών υποδομών, της δημόσιας διοίκησης και του διαστήματος. Ωστόσο, δεν καλύπτει την εθνική και δημόσια ασφάλεια, την επιβολή του νόμου ή το δικαστικό σώμα. Ο νόμος ισχύει για τη δημόσια διοίκηση σε κεντρικό και περιφερειακό επίπεδο, αλλά όχι για τα κοινοβούλια και τις κεντρικές τράπεζες (Ευρωπαϊκό Κοινοβούλιο, 2023).

Επομένως, η νομοθεσία απαιτεί από περισσότερες οντότητες και κλάδους να λαμβάνουν μέτρα διαχείρισης κινδύνων στον κυβερνοχώρο, συμπεριλαμβανομένων των παρόχων δημόσιων υπηρεσιών ηλεκτρονικών επικοινωνιών, των χειριστών μέσων κοινωνικής δικτύωσης, των κατασκευαστών κρίσιμων προϊόντων (συμπεριλαμβανομένων των ιατρικών συσκευών) και των ταχυδρομικών υπηρεσιών και υπηρεσιών ταχυμεταφορών. Ο νόμος ορίζει αυστηρότερες υποχρεώσεις κυβερνοασφάλειας για τις χώρες της ΕΕ, όσον αφορά την εποπτεία και βελτιώνει την επιβολή αυτών των υποχρεώσεων, μεταξύ άλλων με την εναρμόνιση των κυρώσεων μεταξύ των κρατών – μελών. Στοχεύει επίσης στη βελτίωση της

συνεργασίας μεταξύ των χωρών της ΕΕ, συμπεριλαμβανομένων των περιστατικών μεγάλης κλίμακας, υπό την ομπρέλα του Οργανισμού της ΕΕ για την Κυβερνοασφάλεια (Enisa) (Ευρωπαϊκό Κοινοβούλιο, 2023).

Επειδή ο χρηματοοικονομικός τομέας εξαρτάται όλο και περισσότερο από λογισμικό και ψηφιακές διαδικασίες, χρειάζεται επίσης αυξημένη προστασία. Ο νόμος για την ψηφιακή επιχειρησιακή ανθεκτικότητα (Dora) θα διασφαλίσει ότι ο χρηματοπιστωτικός τομέας της ΕΕ είναι πιο ανθεκτικός σε σοβαρές λειτουργικές διακοπές και επιθέσεις στον κυβερνοχώρο. Το Κοινοβούλιο ενέκρινε τελικά τη νομοθεσία, η οποία είχε συμφωνηθεί προηγουμένως με το Συμβούλιο, στις 10 Νοεμβρίου 2022. Το Συμβούλιο ενέκρινε επίσημα τον κανονισμό στις 28 Νοεμβρίου 2022. Αναλυτικότερα, ο νόμος εισάγει και εναρμονίζει τις απαιτήσεις ψηφιακής επιχειρησιακής ανθεκτικότητας για τον τομέα των χρηματοπιστωτικών υπηρεσιών της ΕΕ υποχρεώνοντας τις εταιρείες να βεβαιωθούν ότι μπορούν να αντέξουν, να ανταποκριθούν και να ανακάμψουν από κάθε είδους διακοπές και απειλές που σχετίζονται με τις τεχνολογίες πληροφορίας και επικοινωνιών (ΤΠΕ). Οι νέοι κανόνες ισχύουν για όλες τις εταιρείες που παρέχουν χρηματοοικονομικές υπηρεσίες - όπως τράπεζες, παρόχους πληρωμών, παρόχους ηλεκτρονικών χρημάτων, εταιρείες επενδύσεων, παρόχους υπηρεσιών κρυπτογράφησης, καθώς και για σημαντικούς τρίτους παρόχους υπηρεσιών ΤΠΕ. Ωστόσο, οι εθνικές αρχές θα επιβλέπουν την εφαρμογή του νόμου (Ευρωπαϊκό Κοινοβούλιο, 2023).

Εκτός όμως από το ευρωπαϊκό πλαίσιο πολύ σημαντικό είναι να ερευνηθεί ο τρόπος μέσα από τον οποίο το ελληνικό νομοθετικό πλαίσιο προστατεύει τους χρήστες του Διαδικτύου από τις παράνομες ενέργειες.

3.2.2 Το Ελληνικό Νομοθετικό Πλαίσιο για το Ηλεκτρονικό Διαδικτυακό Έγκλημα

Η ραγδαία εξέλιξη της πληροφορικής και η ευρεία χρήση του Διαδικτύου έχουν οδηγήσει σε επαναστατικές αλλαγές σε κάθε είδους καθημερινές δραστηριότητες, όπως η εργασία, η κοινωνικοποίηση, η εκπαίδευση και η ψυχαγωγία. Αυτό το παγκόσμιο φαινόμενο συμβαίνει και στην Ελλάδα. Η αυξανόμενη χρήση του διαδικτύου στην Ελλάδα αποδεικνύεται από τα διαθέσιμα στατιστικά στοιχεία, που δείχνουν συνεχή αύξηση κάθε χρόνο σε όλους τους σημαντικούς δείκτες: πρόσβαση

στο διαδίκτυο, χρόνος σύνδεσης, αριθμός συνδεδεμένων συσκευών, συμμετοχή σε μέσα κοινωνικής δικτύωσης, ηλεκτρονικό εμπόριο και χρήση φορητών συσκευών. Ωστόσο, όλα αυτά φέρνουν και τα προβλήματα της εγκληματικότητας μέσω Διαδικτύου (Georgiou & Maspero, 2020).

Στατιστικά στοιχεία της Διεύθυνσης Ηλεκτρονικού Εγκλήματος σχετικά με το έγκλημα στον κυβερνοχώρο δείχνουν ότι ο συνολικός αριθμός σε νέες ποινικές υποθέσεις που διεκπεραιώθηκαν κατά το έτος 2020 αυξήθηκαν και έφτασαν τις 5.148. Όπως φαίνεται από το παρακάτω διάγραμμα, υπάρχει συνεχής αύξηση στον αριθμό των εγκλημάτων στον κυβερνοχώρο τα τελευταία χρόνια. Πιο συγκεκριμένα, η ετήσια αύξηση από το 2019 έως το 2020 έφτασε το 14% (Georgiou & Maspero, 2020).

Διάγραμμα 1: Η εγκληματικότητα μέσω Διαδικτύου στην Ελλάδα, 2018-2020



Πηγή: https://www.h2020-infinity.eu/sites/default/files/2022-02/pb_cybercrime_hellenicpolice_final.pdf

Η πλειοψηφία των περιστατικών που έχουν καταγραφεί μέσα Διαδικτύου αφορούν απάτη και τη δεύτερη θέση κατέχει η δημοσιοποίηση των προσωπικών δεδομένων. Πιο αναλυτικά, ένα μεγάλο ποσό, που φτάνει έως και το 40% των συνολικών εγκλημάτων, σχετίζεται με διαδικτυακή απάτη και οι περισσότερες περιπτώσεις αφορούσαν παράνομα χρήματα και μεταφορές μέσω τραπεζικών συστημάτων, δηλαδή γίνεται λόγος για απάτη που σχετίζεται με την αγορά προϊόντων (Georgiou & Maspero, 2020).

Στην Ελλάδα το Ίντερνετ έφτασε το 1990 και είναι αλήθεια ότι μέχρι το 1988 δεν υπήρχε καμία νομοθετική πρόβλεψη για προστασία από το ηλεκτρονικό έγκλημα. Αυτό οφειλόταν στο γεγονός ότι όταν ο νομοθέτης διαμόρφωνε τον Ποινικό Κώδικα δεν μπορούσε να έχει εικόνα των τεχνολογικών αλλαγών και των προβλημάτων που θα έφερνε το Διαδίκτυο. Η πρώτη απόπειρα θέσπισης νόμων για

την προστασία από το ηλεκτρονικό έγκλημα γίνεται μέσα από το νόμο 1805/ 1988 και τον Ποινικό κώδικα με τα άρθρα 13β, 13γ, 370 Β, Γ και 386 Α. Με το νόμο 1805/1988 που είναι εμπνευσμένος από το γερμανικό νόμο για την οικονομική εγκληματικότητα γίνεται η απόπειρα για την προσαρμογή στις τεχνολογικές εξελίξεις (Georgiou & Maspero, 2020).

Σήμερα όμως η νομική κατάσταση έχει εξελιχθεί κατά πολύ και η νομοθεσία του Ποινικού Κώδικα προσδιορίζεται μέσα από συγκεκριμένα άρθρα για την πάταξη της εγκληματικότητας μέσω Διαδικτύου.

3.2.3 Η Νομοθεσία του Ποινικού Κώδικα για την Πάταξη του Διαδικτυακού Εγκλήματος

Στο άρθρο 13 του Γενικού Ποινικού Κώδικα αναφέρεται ότι «έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή αναπαραγωγή στοιχείων που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία». Κάθε παρέμβαση σε αυτά με πρόθεση νόθευσης και μέσω του Διαδικτύου θεωρείται απόπειρα πλαστογραφίας.

Στο άρθρο 348 του Ποινικού Κώδικα θεσπίζεται η προστασία για την παιδική πορνογραφία με αποτέλεσμα να ορίζεται ότι «1. Όποιος κατ' επάγγελμα ή από κερδοσκοπία επιχειρεί να διευκολύνει, έστω και συγκαλυμμένα, με τη δημοσίευση αγγελίας ή εικόνας ή αριθμού τηλεφωνικής σύνδεσης ή με τη μετάδοση ηλεκτρονικών μηνυμάτων ή με οποιονδήποτε άλλο τρόπο τη γενετήσια πράξη με ανήλικο τιμωρείται με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή. [Παράλληλα,] 2. όποιος οργανώνει, χρηματοδοτεί, κατευθύνει, εποπτεύει, διαφημίζει ή μεσολαβεί με οποιονδήποτε τρόπο ή μέσο σε διενέργεια ταξιδιών με σκοπό από τους μετέχοντες σε αυτά την τέλεση γενετήσιων πράξεων σε βάρος ανηλίκου, τιμωρείται με κάθειρξη έως δέκα έτη. Όποιος με τον παραπάνω σκοπό μετέχει σε ταξίδια του προηγούμενου

εδαφίου τιμωρείται με φυλάκιση τουλάχιστον ενός έτους, ανεξάρτητα από την ευθύνη του για την τέλεση άλλων αξιόποινων πράξεων». Το έγκλημα αυτό με τη χρήση του Διαδικτύου έχει μεταλλαχθεί και έχει εξελιχθεί αρνητικά με την πάροδο των χρόνων.

Στη συνέχεια, στο ίδιο άρθρο στη Β παράγραφο φαίνεται ότι διώκεται και η προσέλευση ανηλίκων με στόχο γενετήσιους λόγους. Συγκεκριμένα, στο άρθρο θεοπίζεται ότι *«όποιος με πρόθεση, μέσω πληροφοριακών συστημάτων, προτείνει σε ανήλικο που δεν συμπλήρωσε τα δεκαπέντε έτη, να συναντήσει τον ίδιο ή τρίτο, με σκοπό τη διάπραξη σε βάρος του ανηλίκου των αδικημάτων των άρθρων 339 παράγραφοι 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή πενήντα χιλιάδων έως διακοσίων χιλιάδων ευρώ».*

Στα παραπάνω πρέπει να αναφερθεί ότι το άρθρο 362 του Ποινικού Κώδικα αναφέρεται στη δυσφήμιση και το άρθρο 363 του Ποινικού κώδικα αναφέρεται στη συκοφαντική δυσφήμιση που αποτελεί μια πολύ συνηθισμένη πρακτική που ασκείται μέσα από το Διαδίκτυο. Στο άρθρο 362 προβλέπεται ότι *«όποιος με οποιονδήποτε τρόπο ενώπιον τρίτου ισχυρίζεται ή διαδίδει για κάποιον άλλον γεγονός που μπορεί να βλάψει την τιμή ή την υπόληψή του τιμωρείται με φυλάκιση μέχρι δύο ετών ή με χρηματική ποινή. Η χρηματική ποινή μπορεί να επιβληθεί και μαζί με την ποινή της φυλάκισης».* Στο άρθρο 363 του Ποινικού Κώδικα ορίζεται ότι *«αν στην περίπτωση του άρθρου 362, το γεγονός είναι ψευδές και ο υπαίτιος γνώριζε ότι αυτό είναι ψευδές τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών · μαζί με τη φυλάκιση μπορεί να επιβληθεί και χρηματική ποινή. Μπορεί επίσης να επιβληθεί και στέρηση των πολιτικών δικαιωμάτων κατά το άρθρο 63».* Αυτό ισχύει και για το Διαδίκτυο όπου το φωτογραφικό υλικό και οι αναρτήσεις μπορούν να αποτελέσουν υλικό που θα βλάπτει την τιμή και την υπόληψη άλλων προσώπων.

Σε όλα αυτά πρέπει να συνεκτιμηθεί και το γεγονός ότι η απάτη μέσω Διαδικτύου διώκεται ποινικά και αυτό φαίνεται στο άρθρο 386 του Ποινικού Κώδικα. Ειδικότερα, *«όποιος με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με σκοπό από τη βλάβη αυτής της περιουσίας να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος*

τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των εκατόν είκοσι χιλιάδων (120.000) ευρώ επιβάλλεται κάθειρξη έως δέκα (10) έτη και χρηματική ποινή».

Επιπλέον, διευκρινίζεται η απάτη μέσω υπολογιστών και πιο αναλυτικά «όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων υπολογιστή:

- α) με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή,*
- β) με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα,*
- γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών ψηφιακών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας,*
- δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή, μετάδοση ή εξάλειψη ορθών ψηφιακών δεδομένων υπολογιστή, ιδίως ψηφιακών δεδομένων αναγνώρισης της ταυτότητας, ή*
- ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων ή νομισματικής αξίας τιμωρείται με φυλάκιση, και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον τριών (3) μηνών και χρηματική ποινή»*

Επομένως, εύκολα συμπεραίνεται ότι και στη χώρα μας η εγκληματικότητα μέσω Διαδικτύου ανθεί.

ΚΕΦΑΛΑΙΟ 4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ

4.1 Κυβερνοεπιθέσεις σε Ευρωπαϊκές Πετρελαϊκές Εγκαταστάσεις

Το Φεβρουάριο του 2022 οι διαδικτυακές επιθέσεις στις ευρωπαϊκές πετρελαϊκές εγκαταστάσεις ήταν πραγματικότητα. Αυτή η μαζική επίθεση κατέστρεψε τα συστήματα πληροφορικής, επηρεάζοντας δεκάδες τερματικούς σταθμούς, την αποθήκευση και μεταφορά πετρελαίου σε όλο τον κόσμο, συμπεριλαμβανομένων των Oiltanking στη Γερμανία, SEA-Invest στο Βέλγιο και Enos στην Ολλανδία. Η κυβερνοεπίθεση είχε επίσης ως αποτέλεσμα τη δυσκολία φόρτωσης και εκφόρτωσης φορτίων διυλισμένων προϊόντων σε έξι τερματικούς σταθμούς αποθήκευσης πετρελαίου στον κόμβο διύλισης Άμστερνταμ-Ρότερνταμ-Αμβέρσα (Ventre & Loiseau, 2023).

Η τελευταία μεγάλη κλίμακας επίθεση ransomware έχει στοχεύσει το λογισμικό τερματικού σταθμού πετρελαίου σε τουλάχιστον 17 λιμάνια στη Δυτική Ευρώπη, επαναδρομολογώντας δεξαμενόπλοια και διακόπτοντας σημαντικά τις αλυσίδες εφοδιασμού. Οι 17 τερματικοί σταθμοί που επηρεάστηκαν περιλαμβάνουν εκείνους στο Αμβούργο, τη Γάνδη, την Αμβέρσα-Zeebrugge και το Ρότερνταμ. Η Baker Botts υποστηρίζει ότι η πλήρης έκταση των επιθέσεων δεν είναι ακόμη γνωστή. Οι αναφορές δείχνουν ότι επιθέσεις ransomware που στοχεύουν το λογισμικό των τερματικών λιμανιών τους εμπόδισαν να επεξεργαστούν φορτηγίδες, με αποτέλεσμα την αλλαγή δρομολόγησης και τη συμφόρηση, ενώ εμποδίζουν τα δεξαμενόπλοια από τη φόρτωση και εκφόρτωση (Ventre & Loiseau, 2023).

Με τις παγκόσμιες εντάσεις που επηρεάζουν την πρόσβαση και τη διαθεσιμότητα πετρελαίου και φυσικού αερίου μπορούμε να υποθέσουμε ότι αυτές οι πρόσφατες επιθέσεις σε προμηθευτές πετρελαίου σε όλη την Ευρώπη έχουν σχεδιαστεί για να πυροδοτήσουν τις υπάρχουσες εντάσεις μεταξύ ορισμένων εμπλεκόμενων χωρών ή αν ο στόχος είναι η παραδοσιακή κερδοσκοπία. Αυτό είναι ένα ισχυρό ενδεχόμενο, καθώς υπήρξε άφθονη κάλυψη από τα μέσα ενημέρωσης σχετικά με την αύξηση των τιμών του φυσικού αερίου και του πετρελαίου (Ventre & Loiseau, 2023).

Αυτή η τελευταία επίθεση θα πρέπει να είναι μια περαιτέρω υπενθύμιση της συνεχώς αυξανόμενης συχνότητας, της πολυπλοκότητας και της σοβαρότητας των κυβερνοεπιθέσεων που αντιμετωπίζουμε όλοι. Η σημασία όλων των επιχειρήσεων να διαχειρίζονται συνεχώς την κυβερνοασφάλειά τους δεν ήταν ποτέ πιο αναγκαία. Αυτό ισχύει για όλα τα κρίσιμα στοιχεία υποδομής και όλο αυτό αποτελεί ένα τέλειο παράδειγμα του πώς ο κίνδυνος λογισμικού εξισώνεται με τον επιχειρηματικό κίνδυνο. Ευτυχώς, σε αυτήν την περίπτωση, είτε λόγω άλλων αντισταθμιστικών ελέγχων, είτε λόγω του εύρους της επίθεσης (Ventre & Loiseau, 2023).

4.2 Η Κυβερνοεπίθεση στην Uber

Η παραβίαση δεδομένων της Uber ξεκίνησε με έναν χάκερ που αγόρασε κλεμμένα διαπιστευτήρια που ανήκουν σε υπάλληλο της Uber από μια αγορά σκοτεινού διαδικτύου (dark internet). Μια αρχική προσπάθεια σύνδεσης στο δίκτυο της Uber με αυτά τα διαπιστευτήρια απέτυχε, επειδή ο λογαριασμός προστατεύτηκε με MFA. Για να ξεπεράσει αυτό το εμπόδιο ασφαλείας, ο χάκερ επικοινωνήσε με έναν υπάλληλο της Uber μέσω What's App και, ενώ προσποιήθηκε ότι είναι μέλος της ασφάλειας της Uber, ζήτησε από τον υπάλληλο να εγκρίνει τις ειδοποιήσεις MFA που αποστέλλονται στο τηλέφωνό του. Στη συνέχεια, ο χάκερ έστειλε μια πλημμύρα ειδοποιήσεων MFA στο τηλέφωνο του υπαλλήλου για να τον πείσει να υποκύψει σε αυτό το αίτημα. Για να τερματιστεί τελικά αυτή η καταιγίδα ειδοποιήσεων, ο υπάλληλος της Uber ενέκρινε ένα αίτημα MFA παραχωρώντας πρόσβαση στο δίκτυο των χάκερ, το οποίο τελικά οδήγησε στην παραβίαση δεδομένων (Lukings & Lashkari, 2021).

Μετά την επιτυχή σύνδεση στο intranet της Uber, ο χάκερ απέκτησε πρόσβαση στο VPN της εταιρείας και ανακάλυψε σενάρια Microsoft Powershell που περιέχουν τα διαπιστευτήρια σύνδεσης ενός χρήστη διαχειριστή στο Thycotic - τη λύση Privileged Access Management (PAM) της εταιρείας. Αυτή η ενέργεια αύξησε σημαντικά τη σοβαρότητα της παραβίασης διευκολύνοντας την πλήρη πρόσβαση διαχειριστή σε όλες τις ευαίσθητες υπηρεσίες της Uber συμπεριλαμβανομένων των DA, DUO, Onelogin, Amazon Web Services (AWS) και GSuite (Lukings & Lashkari, 2021).

Παρά τη μεγάλη ζημιά που πέτυχε ο χάκερ δεν έχει ανακοινωθεί κανένα στοιχείο κλοπής δεδομένων πελατών. Αυτό είναι πιθανό επειδή ο χάκερ δεν είχε σκοπό να προκαλέσει βλάβη, αλλά κυνηγούσε τη συγκίνηση μιας επιτυχημένης κυβερνοεπίθεσης και το σεβασμό της κοινότητας των χάκερ. Αν ο χάκερ είχε κίνητρο το οικονομικό κέρδος, πιθανότατα θα είχε πουλήσει τις αναφορές ασφαμάτων της Uber σε μια αγορά σκοτεινού διαδικτύου. Δεδομένου του καταστροφικού αντίκτυπου της παραβίασης δεδομένων που είναι δυνατό με τα ευρήματα ενός προγράμματος bounty bug, ο χάκερ θα τα είχε πουλήσει σε πολύ υψηλή τιμή (Lukings & Lashkari, 2021).

Δεδομένης της φήμης της Uber για τον επιτυχή χειρισμό προσπαθειών εκβιασμού, ευτυχώς, αυτό δεν συνέβη. Όταν η Uber παραβιάστηκε το 2016, η εταιρεία πλήρωσε στους κυβερνοεγκληματίες τα λύτρα των 100.000 δολαρίων με αντάλλαγμα τη διαγραφή του αντιγράφου των κλεμμένων δεδομένων τους. Στη συνέχεια, σε μια προσπάθεια απόκρυψης του συμβάντος, η εταιρεία ανάγκασε τους χάκερ να υπογράψουν μια συμφωνία μη αποκάλυψης και έκανε να φαίνεται ότι η πληρωμή των λύτρων ήταν μια αβλαβής ανταμοιβή στο πλαίσιο του προγράμματος επιβράβευσης ασφαμάτων της εταιρείας (Lukings & Lashkari, 2021).

Το γεγονός ότι ο υπάλληλος της Uber ενέδωσε στον κατακλυσμό των αιτημάτων MFA στο αρχικό στάδιο της επίθεσης αποτελεί ένδειξη ανεπαρκούς επίγνωσης μιας κοινής τακτικής εκμετάλλευσης MFA, γνωστής ως MFA Fatigue. Αν ο υπάλληλος της Uber γνώριζε αυτήν την τακτική, πιθανότατα θα είχε αναφέρει την απειλή αντί να πέσει θύμα αυτής, κάτι που θα εμπόδιζε την παραβίαση. Ο χάκερ χρησιμοποίησε επίσης τεχνικές κοινωνικής μηχανικής για να ξεγελάσει τον υπάλληλο της Uber να πιστεύει ότι ήταν μέλος της ομάδας ασφαλείας της Uber, κάτι που είναι μια άλλη κοινή τακτική κυβερνοεπίθεσης (Lukings & Lashkari, 2021).

4.3 Η Κυβερνοεπίθεση στη NASA το 1999

Θα υποθέταμε ότι η Nasa, ως ένας από τους μεγαλύτερους οργανισμούς στις Ηνωμένες Πολιτείες, αν όχι στον κόσμο, θα είχε ανοσία σε κυβερνοεπιθέσεις. Στην πραγματικότητα, αυτό απέχει πολύ από την κατάσταση. Το αδιανόητο συνέβη το 1999 όταν ο Τζόνθαν Τζέιμς, ο οποίος χρησιμοποιούσε το διαδικτυακό χειριστήριο "c0mrade", κατάφερε να διεισδύσει στη Nasa και στο Υπουργείο Άμυνας,

καθιστώντας τον έναν από τους πιο γνωστούς χάκερ στον κόσμο. Ήταν ο πρώτος χάκερ που καταδικάστηκε σε κέντρο κράτησης ανηλίκων (Marcella, 2021).

Ειδικότερα, ο χάκερ μπόρεσε να μπει στο Marshall Space Flight Center στο Huntsville όπου έκλεψε και κατέβασε δεδομένα αξίας 1,7 εκατομμυρίων δολαρίων. Εξαιτίας αυτής της εισβολής, η Nasa αναγκάστηκε να κλείσει τους υπολογιστές της στις εγκαταστάσεις και να υποβληθεί σε επισκευές που εκτιμήθηκαν σε περίπου 44.000 \$. Στη συνέχεια έγινε έφοδος στο σπίτι του Τζέιμς στις 26 Ιανουαρίου 2000, όπου συνελήφθη και τελικά καταδικάστηκε σε επτά μήνες κατ' οίκον περιορισμό και αναστολή έως ότου έκλεισε τα 18. Όταν μίλησε με την Frontline για τη σύλληψή του, ο Τζέιμς έδειξε ότι πιστεύει ότι δεν έχει κάνει τίποτα κακό και ότι δεν έχει προκαλέσει καμία καταστροφή ή βλάβη. Επίσης, δήλωσε ότι τον έπιασαν επειδή δεν κάλυπτε τα ίχνη του, καθώς θεωρούσε ότι δεν έκανε τίποτα εγκληματικό (Marcella, 2021).

4.4 Η Κυβερνοεπίθεση στη Sony Playstation Network

Η διακοπή του PlayStation Network το 2011 (μερικές φορές αναφέρεται ως PSN Hack) ήταν το αποτέλεσμα μιας "εξωτερικής εισβολής" στις υπηρεσίες PlayStation Network και Qriocity της Sony, κατά την οποία προσωπικές πληροφορίες από περίπου 77 εκατομμύρια λογαριασμούς παραβιάστηκαν και εμπόδιζε τους χρήστες του PlayStation να έχουν πρόσβαση σε φορητές κονσόλες. Η επίθεση έλαβε χώρα μεταξύ 17 Απριλίου και 19 Απριλίου 2011 αναγκάζοντας τη Sony να απενεργοποιήσει τους διακομιστές του PlayStation Network στις 20 Απριλίου. Στις 4 Μαΐου, η Sony επιβεβαίωσε ότι είχαν εκτεθεί στοιχεία προσωπικής ταυτοποίησης από τους 77 εκατομμύρια λογαριασμούς. Η διακοπή διήρκεσε 23 ημέρες και κυβερνητικά στελέχη σε διάφορες χώρες εξέφρασαν ανησυχία για την κλοπή και την καθυστέρηση μιας εβδομάδας της Sony προτού προειδοποιήσουν τους χρήστες της(Rai, 2023).

Η Sony δήλωσε στις 26 Απριλίου ότι προσπαθούσε να ενεργοποιήσει τις διαδικτυακές υπηρεσίες "μέσα σε μια εβδομάδα". Στις 14 Μαΐου, η Sony κυκλοφόρησε την έκδοση υλικολογισμικού PlayStation 3.61 ως ενημερωμένη έκδοση κώδικα ασφαλείας. Το υλικό λογισμικό απαιτούσε από τους χρήστες να

αλλάζουν τον κωδικό πρόσβασης του λογαριασμού τους κατά την είσοδο, αλλά τη στιγμή που κυκλοφόρησε το λογισμικό, το δίκτυο ήταν ακόμα εκτός σύνδεσης. Η περιφερειακή αποκατάσταση ανακοινώθηκε από τον Kazuo Hirai σε ένα βίντεο από τη Sony(Rai, 2023).

Εκτός από την καθυστερημένη ενημέρωση που προσέφερε η Sony, η εταιρεία επικρίθηκε με τη δικαιολογία ότι τα δεδομένα της πιστωτικής κάρτας ήταν κρυπτογραφημένα, αλλά η Sony παραδέχτηκε ότι άλλες πληροφορίες χρήστη δεν ήταν κρυπτογραφημένες τη στιγμή της εισβολής. Η Daily Telegraph ανέφερε ότι αν ο πάροχος αποθηκεύει τους κωδικούς πρόσβασης χωρίς κρυπτογράφηση, τότε είναι πολύ εύκολο για κάποιον άλλο – όχι μόνο έναν εξωτερικό εισβολέα, αλλά μέλη του προσωπικού ή εργολάβους που εργάζονται στον ιστότοπο της Sony – να αποκτήσει πρόσβαση και να ανακαλύψει αυτούς τους κωδικούς πρόσβασης και πιθανώς να τους χρησιμοποιεί για κακόβουλα μέσα(Rai, 2023).

Όλα τα παραπάνω συνέβησαν διότι ενώ οι κωδικοί πρόσβασης που αποθηκεύτηκαν δεν ήταν «κρυπτογραφημένοι», μετασχηματίστηκαν χρησιμοποιώντας μια κρυπτογραφική συνάρτηση κατακερματισμού. Υπάρχει διαφορά μεταξύ αυτών των δύο τύπων μέτρων ασφαλείας, αλλά οι κωδικοί πρόσβασης δεν αποθηκεύτηκαν στη βάση δεδομένων μας σε μορφή καθαρού κειμένου (Rai, 2023).

4.5 Η Κυβερνοεπίθεση στην Ουκρανία στο Δίκτυο Ηλεκτρικής Ενέργειας

Στις 23 Δεκεμβρίου 2015, το ηλεκτρικό δίκτυο σε δύο δυτικές περιφέρειες της Ουκρανίας παραβιάστηκε, κάτι που είχε ως αποτέλεσμα διακοπές ρεύματος σε περίπου 230.000 καταναλωτές στην Ουκρανία για περίπου 6 ώρες. Η επίθεση έλαβε χώρα κατά τη διάρκεια του συνεχιζόμενου Ρώσο Ουκρανικού Πολέμου (2014-σήμερα) και αποδίδεται σε μια ρωσική προηγμένη ομάδα επίμονης απειλής γνωστή ως "Sandworm". Η ομάδα αυτή είναι η πρώτη δημοσίως αναγνωρισμένη επιτυχημένη κυβερνοεπίθεση σε ηλεκτρικό δίκτυο(Lukings & Lashkari, 2021).

Το 2019, υποστηρίχθηκε ότι η Ουκρανία ήταν μια ειδική περίπτωση, που περιελάμβανε ασυνήθιστα ερειπωμένες υποδομές, υψηλό επίπεδο διαφθοράς και

εξαιρετικές δυνατότητες για ρωσική διείσδυση λόγω των ιστορικών δεσμών μεταξύ των δύο χωρών. Το ουκρανικό δίκτυο ηλεκτρικής ενέργειας κατασκευάστηκε όταν ήταν μέρος της Σοβιετικής Ένωσης, έχει αναβαθμιστεί με ρωσικά εξαρτήματα και (από το 2022), δεν έχει ακόμη επισκευαστεί (Lukings & Lashkari, 2021).

Οι Ρώσοι εισβολείς ήταν εξοικειωμένοι με το λογισμικό όσο και οι χειριστές τους. Επιπλέον, ο χρόνος της επίθεσης ήταν κατά τη διάρκεια της εορταστικής περιόδου όταν εργαζόταν μόνο ένα πλήρωμα από Ουκρανούς χειριστές. Επομένως, οι χάκερ γνώριζαν ότι η Ουκρανία ήταν ευάλωτη το διάστημα εκείνο (Lukings & Lashkari, 2021).

4.6 Η Κυβερνοεπίθεση στην Ελληνική Τράπεζα Θεμάτων Εξετάσεων του Υπουργείου Παιδείας

Το Ελληνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΛΕΤ) ενισχύει τα συστήματά του για να αποτρέψει νέες επιθέσεις στον κυβερνοχώρο, όπως αυτή που προκάλεσε χάος στις σχολικές εξετάσεις το Μάιο του 2023. Η μαζική εισροή έως και 280.000 συνδέσεων ανά δευτερόλεπτο από άσχετες πηγές απέκλεισε την πρόσβαση στην πλατφόρμα των εξετάσεων. Στελέχη των υπουργείων Παιδείας και Ψηφιακής Διακυβέρνησης και του ΕΛΕΤ έσπευσαν να παράσχουν διαβεβαιώσεις στο ενδιαφερόμενο κοινό ότι η ασφάλεια των πανελλαδικών εισαγωγικών εξετάσεων στα πανεπιστήμια δε θα τεθεί σε κίνδυνο.

Η πλατφόρμα της τράπεζας εξετάσεων έλαβε 165 εκατομμύρια επισκέψεις από 114 χώρες. Είναι η πιο σημαντική επίθεση που έγινε ποτέ σε ελληνικό δημόσιο κρατικό οργανισμό και οι επιθέσεις ήταν ισχυρές, καθώς έδειχναν ισχυρό κίνητρο και υψηλή τεχνική τεχνογνωσία, αλλά εκτράπηκαν με επιτυχία.

Από όλα τα παραπάνω παραδείγματα φαίνεται ότι τα συστήματα υπολογιστών μπορούν να παραβιαστούν με ποικίλα μέσα, αλλά η επιδίωξη μας είναι να κατανοηθούν οι κακόβουλες ενέργειες και οι επιτιθέμενοι που τις πραγματοποιούν. Ο κίνδυνος για τις πληροφορίες και τα περιουσιακά στοιχεία υπολογιστών προέρχεται από ένα ευρύ φάσμα απειλών. Ο αντίκτυπος στην επιχείρησή και τον οργανισμό θα εξαρτηθεί από τις ευκαιρίες που παρουσιάζονται, διότι οι επιτιθέμενοι έχουν διάθεση να εκμεταλλευτούν και αυτό είναι το κίνητρό τους, άλλωστε.

Το συμπέρασμα που εξάγεται από αυτά εστιάζει στο γεγονός ότι χρειάζεται ένας εύκολος κωδικός πρόσβασης σε έναν διαδικτυακό λογαριασμό και πολύ μικρή τεχνική ικανότητα με στόχο την εκμετάλλευση. Με λίγο πιο τεχνική γνώση οι εισβολείς μπορούν επίσης να χρησιμοποιήσουν εργαλεία που είναι άμεσα διαθέσιμα στο διαδίκτυο. Ακόμη, δεν πρέπει να παραλείπεται ότι οι χάκερ μπορούν να φέρουν πόρους (ανθρώπους ή χρήματα) που αντέχουν για να ανακαλύψουν νέα τρωτά σημεία. Αυτοί οι εισβολείς θα συνεχίσουν να αναπτύσσουν ειδικά εργαλεία και τεχνικές για την αξιοποίησή τους. Τέτοια τρωτά σημεία τους επιτρέπουν να παρακάμψουν τους βασικούς ελέγχους που παρέχονται από προγράμματα, όπως το Cyber Essentials.

Επομένως, είναι μεγάλη ανάγκη να δοθεί έμφαση στις μεθόδους αντιμετώπισης.

ΚΕΦΑΛΑΙΟ 5 ΜΕΘΟΔΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

5.1 Προληπτικά Εργαλεία

Η ασφάλεια στο Διαδίκτυο περνά μέσα από τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Για να είναι τα αρχεία μας και τα δεδομένα μας ασφαλή είναι απαραίτητο να υπάρχει εγκατεστημένο σύστημα που εμποδίζει τους ιούς να προσβάλλουν τον υπολογιστή μας (antivirus λογισμικό), η δημιουργία πιστοποιητικών των χρηστών (user id- password) και η εφαρμογή τειχών προστασίας (firewall) είναι απαραίτητα εργαλεία για την αντιμετώπιση των κακόβουλων ενεργειών (Ilbiz & Kaunert, 2023).

Αρχικά, στην περίπτωση των λογισμικών που αποτρέπει τους ιούς να εισβάλουν στον υπολογιστή μας, το λογισμικό αυτό αφορά μια κατηγορία προγραμμάτων που έχει σχεδιαστεί για την πρόληψη, τον εντοπισμό και την αφαίρεση μολύνσεων από κακόβουλο λογισμικό σε μεμονωμένες υπολογιστικές συσκευές, δίκτυα και συστήματα πληροφορικής (Ilbiz & Kaunert, 2023).

Στη συνέχεια, η δημιουργία πιστοποιητικών χρηστών εξασφαλίζει την προστασία των δεδομένων μας μιας που οι κωδικοί που χρησιμοποιούνται είναι προσωπικές ημερομηνίες ή γεγονότα που οι χρήστες εύκολα θυμούνται και οι χάκερ δεν μπορούν να μαντέψουν. Για τη μεγαλύτερη ασφάλεια συστήνεται οι κωδικοί να περιέχουν γράμματα και αριθμούς, όπως επίσης κεφαλαία και πεζά γράμματα (Ilbiz & Kaunert, 2023).

Τέλος, τα τείχη προστασίας αποφασίζουν από ποια κίνηση δικτύου επιτρέπεται να διέρχονται δεδομένα και ποια κίνηση θεωρείται επικίνδυνη. Ουσιαστικά, τα τείχη προστασίας λειτουργούν φιλτράροντας το καλό από το κακό ή το έμπιστο από το μη αξιόπιστο. Με άλλα λόγια, ένα τείχος προστασίας θωρακίζει το δίκτυο επειδή λειτουργεί ως φίλτρο 24/7 σαρώνοντας τα δεδομένα που επιχειρούν να εισέλθουν στο δίκτυο και εμποδίζοντας οτιδήποτε φαίνεται ύποπτο να περάσει (Ilbiz & Kaunert, 2023).

Σε όλα αυτά πρέπει να προστεθεί και η κρυπτογραφία που δίνει μεγάλη ασφάλεια στην πλοήγηση μας στο Διαδίκτυο.

5.2 Κρυπτογραφία και Ασφάλεια

Η κρυπτογραφία είναι η διαδικασία απόκρυψης ή κωδικοποίησης πληροφοριών έτσι ώστε μόνο το άτομο για το οποίο προορίζεται ένα μήνυμα να μπορεί να τις διαβάσει. Η τέχνη της κρυπτογραφίας έχει χρησιμοποιηθεί για την κωδικοποίηση μηνυμάτων εδώ και χιλιάδες χρόνια και συνεχίζει να χρησιμοποιείται σε τραπεζικές κάρτες, κωδικούς πρόσβασης υπολογιστών και ηλεκτρονικό εμπόριο (Ventre & Loiseau, 2023).

Ειδικότερα, η κρυπτογραφία είναι η μελέτη της ασφάλειας των επικοινωνιών από εξωτερικούς παρατηρητές. Οι αλγόριθμοι κρυπτογράφησης λαμβάνουν το αρχικό μήνυμα ή το απλό κείμενο και το μετατρέπουν σε κρυπτογραφημένο κείμενο, κάτι που δεν είναι κατανοητό. Το κλειδί επιτρέπει στο χρήστη να αποκρυπτογραφήσει το μήνυμα διασφαλίζοντας έτσι ότι μπορεί να διαβάσει το μήνυμα. Η ισχύς της τυχαιότητας μιας κρυπτογράφησης μελετάται επίσης, γεγονός που καθιστά πιο δύσκολο για οποιονδήποτε να μαντέψει το κλειδί ή την είσοδο του αλγορίθμου (Ventre & Loiseau, 2023).

Η κρυπτογραφία είναι ο τρόπος με τον οποίο μπορούμε να επιτύχουμε πιο ασφαλείς και ισχυρές συνδέσεις για να αναβαθμίσουμε το απόρρητό μας. Οι εξελίξεις στην κρυπτογραφία καθιστούν δυσκολότερη την παραβίαση των κρυπτογραφήσεων, έτσι ώστε τα κρυπτογραφημένα αρχεία, φάκελοι ή συνδέσεις δικτύου να είναι προσβάσιμα μόνο σε εξουσιοδοτημένους χρήστες (Ventre & Loiseau, 2023).

Η κρυπτογραφία βασίζεται σε τέσσερα σημεία:

- **Εμπιστευτικότητα:** η εμπιστευτικότητα διασφαλίζει ότι μόνο ο προβλεπόμενος παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να διαβάσει το περιεχόμενό του
- **Μη αποκήρυξη:** η μη απόρριψη σημαίνει ότι ο αποστολέας του μηνύματος δεν μπορεί να κάνει πίσω στο μέλλον και να αρνηθεί τους λόγους για την αποστολή ή τη δημιουργία του μηνύματος
- **Ακεραιότητα:** η ακεραιότητα εστιάζει στην ικανότητα να είμαστε βέβαιοι ότι οι πληροφορίες που περιέχονται στο μήνυμα δεν μπορούν να τροποποιηθούν κατά την αποθήκευση ή τη μεταφορά

- Αυθεντικότητα: η αυθεντικότητα διασφαλίζει ότι ο αποστολέας και ο παραλήπτης μπορούν να επαληθεύσουν ο ένας την ταυτότητα του άλλου και τον προορισμό του μηνύματος (Ventre & Loiseau, 2023).

Γενικότερα, όμως, η προστασία στο Διαδίκτυο αποτελεί μέθοδο στην οποία που πρέπει όλοι μας να εκπαιδευτούμε και να εφαρμόζουμε.

5.3 Προστασία και Περιήγηση στο Διαδίκτυο

Η προστασία ξεκινά από την εκπαίδευση και για το λόγο αυτό οι γονείς και οι εκπαιδευτικοί οφείλουν να επιβλέπουν το παιδί κατά τη χρήση του Διαδικτύου, χωρίς όμως τα παιδιά να αισθάνονται ότι παρακολουθούνται. Για να επιτευχθεί αυτός ο στόχος είναι απαραίτητο να τοποθετείται ο υπολογιστής σε κεντρικό σημείο στο σπίτι, με αποτέλεσμα η χρήση του υπολογιστή να είναι οικογενειακή υπόθεση. Παράλληλα, η ενημέρωση των παιδιών για τους κινδύνους που κρύβονται όταν μιλούν με αγνώστους μέσα σε chatrooms και η μη αποκάλυψη προσωπικών δεδομένων είναι χρυσός κανόνας για την πλοήγηση των παιδιών μέσα στο Διαδίκτυο (Marcella, 2021).

Οι νέοι πρέπει να αναπτύξουν κριτική θεώρηση απέναντι στο Διαδίκτυο και να διακόπτουν όποια ηλεκτρονική επαφή τους κάνει να νιώθουν άβολα ή όταν τους ζητούν προσωπικά δεδομένα. Στο πλαίσιο της προστασίας των νέων από εγκληματικές πράξεις του Διαδικτύου, είναι απαραίτητο οι νέοι χρήστες να γνωρίζουν τις υπηρεσίες στις οποίες μπορούν να απευθύνονται με στόχο να προστατεύονται από κακόβουλα άτομα (Marcella, 2021).

Όσον αφορά την ασφάλεια όλων κατά τις οικονομικές συναλλαγές, κρίνεται απαραίτητο να μη γίνονται συναλλαγές μέσα από υπολογιστές κοινόχρηστους (δημοτικές βιβλιοθήκες, internet café κτλ.), διότι το επίπεδο ασφάλειας στα σημεία αυτά είναι αμφίβολο. Ακόμη, οι κωδικοί πρόσβασης πρέπει να αλλάζουν συχνά και να μη βρίσκονται σε σημεία που εύκολα μπορεί να τους ανακαλύψει κανείς. Επίσης, οι ημερομηνίες γέννησης και άλλα στοιχεία που είναι εύκολο να τα ανακαλύψει κανείς καλό είναι να μη χρησιμοποιούνται ως κωδικοί ασφάλειας. Επιπλέον, είναι απαραίτητο να απενεργοποιηθεί η επιλογή της 'αυτόματης καταχώρησης' που έχει ο υπολογιστής, γιατί η αποθήκευση των κωδικών μας αφήνει έκθετους. Όσον αφορά τα spam email, ως χρήστες είναι απαραίτητο να μην απαντάμε στα μηνύματα αυτά,

γιατί έτσι δίνουμε το πραγματικό μας mail και μπορεί ο κίνδυνος να είναι προ των πυλών ευκολότερα από όσο φανταζόμαστε. Κατά την περιήγηση μας στα κοινωνικά δίκτυα, είναι κρίσιμης σημασίας να μη δημοσιοποιούμε προσωπικά δεδομένα και φωτογραφίες, διότι αυτά αποτελούν πολλές φορές την αχίλλειο πτέρνα μας για να πέσουμε θύματα του κυβερνοεγκλήματος. Τέλος, τα προγράμματα για την προστασία από ιούς είναι απαραίτητο να ανανεώνονται, με στόχο το δίκτυ προστασίας να μας προφυλάσσει από περισσότερες απειλές (Marcella, 2021).

ΚΕΦΑΛΑΙΟ 6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το σοβαρό και οργανωμένο κυβερνοέγκλημα αποτελεί βασική απειλή για την ασφάλεια της Ευρωπαϊκής Ένωσης (ΕΕ). Είναι χαρακτηριστικό ότι εγκληματικές ομάδες και μεμονωμένοι χάκερ συνεχίζουν να εμφανίζουν κέρδη πολλών δισεκατομμυρίων ευρώ από τις δραστηριότητές τους στην ΕΕ κάθε χρόνο. Τα τελευταία χρόνια, η τεχνολογία έχει αξιοποιηθεί με τέτοιο τρόπο που έχει επιφέρει σημαντικές αλλαγές σε κάθε τομέα της καθημερινότητας των ανθρώπων. Αν και οι αλλαγές αυτές προσφέρουν μεγάλη ευκολία και πολλαπλά οφέλη στην κοινωνία γενικότερα, συχνά χρησιμοποιούνται με κακόβουλο τρόπο ή η τεχνολογία γίνεται αντικείμενο εκμετάλλευσης με εγκληματική πρόθεση. Επομένως, η τεχνολογία αποτελεί πλέον βασικό συστατικό των περισσότερων, αν όχι όλων, των εγκληματικών δραστηριοτήτων που πραγματοποιούνται από εγκληματικές ομάδες στην ΕΕ. Το γεγονός αυτό αναδεικνύει την ευελιξία που χαρακτηρίζει τους εγκληματίες, ως προς την προσαρμογή στις αλλαγές που συντελούνται στην κοινωνία, καθώς και ο τρόπος με τον οποίο δρα το οργανωμένο έγκλημα.

Στην εργασία αυτή διερευνήθηκε το ηλεκτρονικό έγκλημα και το ζήτημα της ηθικής στον κυβερνοχώρο. Αρχικά, αναλύθηκε η έννοια και η φύση της ηθικής στον κυβερνοχώρο και εκτέθηκε το ζήτημα του ηλεκτρονικού εγκλήματος μέσα από τις κυριότερες μορφές του, καθώς και τη νομοθεσία που το αφορά, ενώ παράλληλα δόθηκαν πολλά παραδείγματα ηλεκτρονικού εγκλήματος. Ακόμη, εκτέθηκαν οι μέθοδοι αντιμετώπισης του ηλεκτρονικού εγκλήματος, αποδεικνύοντας ότι οι πολίτες δεν είναι απόλυτα εκτεθειμένοι σε εγκληματικές πράξεις που διαπράττονται στο χώρο του Διαδικτύου.

Ένα βασικό συμπέρασμα που εξάγεται από την παρούσα έρευνα είναι ότι το Διαδίκτυο αποτελεί μια βασική πηγή πληροφοριών και ένα περιβάλλον, στο οποίο ομάδες ατόμων, που έχουν σκοπό να παρανομήσουν, μπορούν να βρεθούν και να λειτουργήσουν συλλογικά. Στο πλαίσιο αυτό, λοιπόν, γίνεται κατανοητό ότι οι ομάδες αυτές έχουν τη δυνατότητα να αποκτήσουν πρόσβαση σε μία πληθώρα πληροφοριών, όπως δορυφορικές όψεις, διαδρομές, χρονοδιαγράμματα, συμβουλές για επιχειρησιακή ασφάλεια, οδηγίες για κατασκευή εκρηκτικών και ό,τι άλλο θα μπορούσε να φανεί χρήσιμο για τη διάπραξη κάποιας εγκληματικής ενέργειας.

Μέσω του Διαδικτύου, υπάρχουν αρχεία δεδομένων, εκατομμύρια εικόνες και βίντεο και τρισεκατομμύρια μηνύματα τα οποία ρέουν καθημερινά και στηρίζουν την παγκόσμια οικονομία. Αυτή η τεράστια ηλεκτρονική υποδομή είναι αυτό από το οποίο εξαρτάται ο κόσμος. Η διάπραξη εγκλήματος μπορεί να γίνει σχετικά εύκολο, χρησιμοποιώντας έναν υπολογιστή και παραποιώντας την ταυτότητα ενός ατόμου. Ακόμη, μέσω της χρήσης κακόβουλων προγραμμάτων, ένας υπολογιστής μπορεί να χρησιμοποιηθεί ως αντικείμενο για το έγκλημα στον κυβερνοχώρο. Αυτό δείχνει ότι οι περισσότερες από τις διαδικτυακές δραστηριότητες είναι ευάλωτες σε εισβολή και μπορούν να θέσουν σε κίνδυνο την προσωπική ασφάλεια των χρηστών, εξίσου αποτελεσματικά με τα κοινά καθημερινά εγκλήματα.

Από τα δεδομένα που καταγράφηκαν στην έρευνα προκύπτει ότι η πρόληψη αποτελεί ένα βασικό μέτρο προστασίας που θα πρέπει να ληφθεί υπόψη από τους χρήστες. Η έλλειψη γνώσεων ή έλλειψη πληροφοριών σχετικά με πιθανές απειλές από διάφορες τεχνολογίες συχνά δημιουργούν πιθανά θύματα προς εγκληματίες που γνωρίζουν περισσότερο την τεχνολογία. Για αυτό το λόγο, είναι απαραίτητο να υπάρξει ευαισθητοποίηση και ενημέρωση για αυτές τις απειλές, ενώ παράλληλα, οι χρήστες του Διαδικτύου και της τεχνολογίας γενικότερα, να είναι ενημερωμένοι και εκπαιδευμένοι για την ορθή χρήση και την αποφυγή των κακόβουλων ενεργειών.

Σίγουρα, είναι απαραίτητη η υποστήριξη από πλευράς πολιτείας με τη θέσπιση του απαραίτητου νομοθετικού πλαισίου, το οποίο θα προστατεύει του χρήστες. Ωστόσο, η τεχνολογία θα συνεχίσει να προσαρμόζεται και να αναπτύσσεται, συχνά με ρυθμό μεγαλύτερο από κάθε νόμο και την επιβολή του νόμου και για αυτό το λόγο, αναδεικνύεται η σημασία της ενημέρωσης των χρηστών σχετικά με τους κινδύνους και τις ενδεχόμενες κυβερνοεπιθέσεις που μπορεί να προκύψουν. Συνεπώς, γίνεται αντιληπτό ότι ενώ οι εγκληματίες συνεχίζουν να καταχρώνται και να εκμεταλλεύονται νέες και υπάρχουσες τεχνολογίες προκειμένου να ενισχύσουν τις εγκληματικές τους δραστηριότητες είναι σημαντικό οι αρχές επιβολής του νόμου να συνεχίσουν να χρησιμοποιούν όλους τους πόρους, τα εργαλεία και τις ευκαιρίες που έχουν στη διάθεσή τους.

Στο πλαίσιο αυτό, και προκειμένου να επιτευχθεί η αντιμετώπιση των κυβερνοεπιθέσεων, είναι απαραίτητο να υλοποιηθούν συμπράξεις δημόσιου και ιδιωτικού τομέα, να αναπτυχθούν καινοτόμες τεχνικές λύσεις, να ληφθούν μέτρα

πρόληψης, καθώς επίσης, να θεωρηθεί ένα ευέλικτο και αποτελεσματικό νομικό πλαίσιο, με στόχο το νομικό έρεισμα να παραμείνει αποδοτικό μέτρο κατά του εγκλήματος στην εποχή της τεχνολογίας.

Στο άμεσο μέλλον οι τομείς που θα πρέπει να μελετηθούν επισταμένως είναι οι απειλές που είναι περισσότερες και πιο επίμονες, όπως επίσης και η φύση των εγκληματικών πράξεων που χαρακτηρίζονται από περισσότερη προσαρμοστικότητα στα μέτρα προφύλαξης. Ακόμη, το cloud computing είναι περισσότερο ευαίσθητο σε επιθέσεις κυβερνοεγκλήματος και για το λόγο αυτό είναι απαραίτητο να ερευνηθούν μέτρα προστασίας. Αυτό για να συμβεί είναι απαραίτητη η παγκόσμια συνεργασία για τον περιορισμό του διαδικτυακού εγκλήματος, λαμβάνοντας υπόψη ότι τα κοινωνικά μέσα δικτύωσης είναι περισσότερα ευαίσθητα στο κυβερνοέγκλημα.

Οι δραστηριότητες των εγκληματιών του κυβερνοχώρου, αναμφίβολα, έχουν οδηγήσει στην αστάθεια της κοινωνικής δομής, σε οικονομικά διλήμματα, καθώς και σε άλλες μορφές απειλών για τους χρήστες του Διαδικτύου και την κοινωνία γενικότερα. Επομένως, η κοινωνία σήμερα υφίσταται ταχέως σοβαρό ηθικό εκφυλισμό εξαιτίας του υψηλού ποσοστού με τον οποίο οι εγκληματίες του κυβερνοχώρου αισθάνονται άνετα με αυτές τις ανήθικες πράξεις, παρά τους καθιερωμένους νομικούς περιορισμούς ως τιμωρία και τους ηθικούς κώδικες, ως οδηγό ενάντια στις εγκληματικές δραστηριότητες στον κυβερνοχώρο.

Μία βασική παράμετρος που θα πρέπει να ληφθεί υπόψη από τους χρήστες είναι να συμμορφώνονται με τους ηθικούς κανόνες της κοινωνίας. Αυτό σημαίνει ότι οποιαδήποτε δραστηριότητα του ανθρώπου, θα ήταν αξιόπαινο να σέβεται τους ηθικούς κανόνες και να προάγει την ευτυχία στην κοινωνία γενικότερα. Γι' αυτό το λόγο, ο Καντ κάνει τις ακόλουθες σκέψεις: *«Αν ήμουν αποκλειστικά μέλος του νοητού κόσμου, τότε όλες οι ενέργειές μου θα συμμορφώνονταν απόλυτα με την αρχή της αυτονομίας μιας καθαρής βούλησης. Αν ήμουν αποκλειστικά μέρος του κόσμου της αίσθησης, οι ενέργειές μου θα έπρεπε να εκληφθούν ως σε πλήρη συμφωνία με τον φυσικό νόμο των επιθυμιών και των κλίσεων, δηλαδή με την ετερονομία της φύσης»* (Osawaru, 2020, σελ. 32).

Συνοψίζοντας, από τη βιβλιογραφική επισκόπηση στην παρούσα έρευνα, καθώς και από την αναφορά των ιστορικών παραδειγμάτων κυβερνοεπιθέσεων, θα πρέπει να αναφερθεί ότι πρόκειται για ένα πολύ σημαντικό ζήτημα, το οποίο βρίσκεται σε

εξέλιξη και χρειάζεται ιδιαίτερη προσοχή η αντιμετώπιση και η προστασία των καταναλωτών – χρηστών. Με δεδομένο το γεγονός ότι οι περισσότερες δραστηριότητες του ανθρώπου βασίζονται, πλέον, στην χρήση της τεχνολογίας και του Διαδικτύου, γίνεται αντιληπτό ότι ο κίνδυνος κυβερνοεπιθέσεων αυξάνεται σημαντικά. Στο πλαίσιο αυτό, είναι απαραίτητο να ληφθούν μέτρα προστασίας από την πολιτεία και από τους φορείς που παρέχουν υπηρεσίες τεχνολογίας και διαδικτύου. Ωστόσο, θα πρέπει και οι χρήστες να γνωρίζουν τους κινδύνους και, σε ακόμη μεγαλύτερο βαθμό, να γνωρίζουν με ποιον τρόπο μπορούν να προστατέψουν τον εαυτό τους, τα δεδομένα τους και την εργασία τους. Η τεχνολογία, λοιπόν, δημιουργεί μια νέα πραγματικότητα, στην οποία η κοινωνία, θα πρέπει να προσαρμοστεί και θα πρέπει να μάθει να ζει με τα οφέλη που προσφέρει, αλλά και τους πιθανούς κινδύνους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Akdeniz, Y. (2016). *Internet Child Pornography and the Law: National and International Responses*. London: Taylor & Francis
- Alhaboby, Z. A., Alhaboby, D., Al-Khateeb, H. M., Epiphanious, G., Ismail, D. K. B., Jahankhani, H., & Pillai, P. (2018). Understanding the cyber-victimisation of people with long term conditions and the need for collaborative forensics-enabled disease management programmes. *Cyber Criminology*, 227-250.
- Babadac, A. A. (2015). Book Review: General Politics: Intelligence in an Insecure World. *Political Studies Review*, Vol. 13(1), pp. 128–128.
- Berlatsky, N. (Ed.). (2013). *Cybercrime*. New York: Greenhaven Publishing LLC.
- Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. Bloomsbury Publishing USA.
- Chowbe, V. (2023). An introduction to cyber crime. Ανακτήθηκε στις 6/10/20 από https://www.researchgate.net/publication/368880137_AN_INTRODUCTION_TO_CYBER_CRIME
- Dover, R., Dylan, H., & Goodman, M. S. (Eds.). (2017). *The Palgrave handbook of security, risk and intelligence*. Palgrave Macmillan
- Edwards, G. (2019). *Cybercrime investigators handbook*. John Wiley & Sons.
- Ευρωπαϊκό Κοινοβούλιο (2023). Fighting cybercrime: new EU cybersecurity laws explained. Ανακτήθηκε στις 31/8/2023 από https://www.europarl.europa.eu/news/en/headlines/security/20221103STO480_02/fighting-cybercrime-new-eu-cybersecurity-laws-explained?gclid=Cj0KCQjw2qKmBhCfARIsAFy8buIFDAAEq49Uu9RIaCWCV6G3BycboQFMvvDV5gsAf-F9IoWCsYFzmRUaAtjvEALw_wcB
- Georgiou, N. & Maspero, A. (2020). Cybercrime Situation in Greece. Ανακτήθηκε στις 31/7/ 2023 από https://www.h2020-infinity.eu/sites/default/files/2022-02/pb_cybercrime_hellenicpolice_final.pdf Ανακτήθηκε στις 31/7/ 2023
- Hill, J. B., & Marion, N. E. (2016). *Introduction to cybercrime: computer crimes, laws, and policing in the 21st century*. Bloomsbury Publishing USA.
- Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge.

- Johnson, M. (2016). *Cyber crime, security and digital intelligence*. Routledge.
- Ilbiz, E., & Kaunert, C. (2023). *The Sharing Economy for Tackling Cybercrime*. Springer Nature.
- Krieger, D. & Belliger, A. (2021). *Hiking Digital Ethics*. London: Anthem Press
- Lavorgna, A. & Holt, Th. (2021). *Researching Cybercrimes*. Berlin: Springer
- Lukings, M., & Lashkari, A. H. (2021). *Understanding cybersecurity law and digital privacy: a common law perspective*. Springer Nature.
- Manjikian, M. (2019). *Introduction to Cyber Politics and Policy*. Berlin: Sage Publications
- Marcella, A. J. (Ed.). (2021). *Cyber Forensics: Examining Emerging and Hybrid Technologies*. CRC Press.
- Marcum, C. (2019). *Cyber Crime*. New Jeffererson: Aspen Publishing
- Matei, F. C., & Bruneau, T. (2011). Intelligence reform in new democracies: factors supporting or arresting progress. *Democratization*, 18(3), 602-630.
- Michael, A. (2020). *About cyber crime*. Berlin: GRIN Verlag
- Mishra, A. (2020). *An Overview on Cybercrime & Security*. New Delhi: Notion Press
- Osawaru, Cr. (2020). Cybercrime and its Moral Implications in the Light of Kantian Ethics. *Sapientia Journal of Philosophy*, Vol. 13, pp. 22- 33
- Rachels, J. & Rachels, S. (2012). *Στοιχεία ηθικής φιλοσοφίας*. Αθήνα: Οκτώ
- Rai, S. (2023). *Computer Forensic and Digital Crime Investigation*. New Jersey: Notion Press
- Roche, E. (2016). Playing to the Edge: American Intelligence in the Age of Terror. By Michael Vincent Hayden. New York: Penguin Press, 2016. *Journal of Strategic Security*, Vol. 9(3), pp. 106– 108.
- Severance, C. R. (2015). *Introduction to Networking*. Charles Severance.
- Schoenherr, J. R. (2022). *Ethical Artificial Intelligence from Popular to Cognitive Science: Trust in the Age of Entanglement*. Taylor & Francis.
- Σφακιανάκης, Ε. (2016). *Ο κώδικας του Διαδικτύου*.
- Troia, V. (2020). *Hunting cyber criminals: a hacker's guide to online intelligence gathering tools and techniques*. John Wiley & Sons.

- Vasiliu-Feltes, I., & Thomason, J. (Eds.). (2021). *Applied Ethics in a Digital World*. IGI Global.
- Ventre, D., & Loiseau, H. (Eds.). (2023). *Cybercrime During the SARS-CoV-2 Pandemic: Evolutions, Adaptations, Consequences*. John Wiley & Sons.
- Xie, C. (2020). (Im) politeness and moral order in online interactions. *(Im) politeness and Moral Order in Online Interactions*, 1-183.