ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΝΗΛΙΚΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ: ΚΙΝΔΥΝΟΙ ΚΑΙ ΝΟΜΙΚΗ ΠΡΟΣΤΑΣΙΑ»

ΜΟΣΧΟΝΑ ΜΑΡΙΟΛΕΝΗ

ΕΠΟΠΤΕΥΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: ΓΕΩΡΓΙΑΔΟΥ ΝΙΚΗ

ΠΑΤΡΑ, ΙΑΝΟΥΑΡΙΟΣ 2022

ΠΡΟΛΟΓΟΣ

Σκοπός του παρόντος επιστημονικού κειμένου είναι να αναδείξει του τρόπους με τους οποίους είναι ευάλωτοι οι ανήλικοι στο διαδίκτυο και τα εγκλήματα με τα οποία μπορεί να έρχονται αντιμέτωποι. Παράλληλα, αναδεικνύει και τα νομοθετικά κείμενα, τα οποία αποσκοπούν στην προστασία αυτής τη ευάλωτης κοινωνικής ομάδας, σε συνδυασμό με τα μέσα προστασίας των πληροφοριακών συστημάτων που αποτρέπουν εξ υπαρχής την εμφάνιση και την εξέλιξη των διαδικτυακών εγκλημάτων.

Εν συντομία, στο πρώτο κεφάλαιο παρουσιάζεται μία εισαγωγή στην έννοια του Διαδικτύου. Στο δεύτερο κεφάλαιο, παρουσιάζονται ακροθιγώς οι κίνδυνοι από το διαδίκτυο για τους ανηλίκους χρήστες. Στο τρίτο κεφάλαιο, αναλύεται η νομοθεσία και η νομική προστασία στις περιπτώσεις των ηλεκτρονικών εγκλημάτων. Στο τέταρτο κεφάλαιο αναλύεται η αντιμετώπιση των διαδικτυακών εγκληματών.

Επιστημονικό συμπέρασμα της διπλωματικής εργασίας αυτής είναι ότι το Διαδίκτυο αποτελεί έναν επικίνδυνο κόσμο για τους ανήλικους χρήστες του. Καθώς, όμως, η χρήση του παρέχει μεγάλη άνεση και ευκολία, είναι απαραίτητο να προλαμβάνονται κατά το δυνατόν τα προβλήματα που δημιουργούνται κυρίως λόγω της άγνοιας των μηχανισμών δράσης των διαδικτυακών εγκληματιών. Έτσι, η γνώση γύρω από τους κινδύνους του Ιντερνέτ μπορεί να προλάβει δυσάρεστες καταστάσεις και να επιτρέψει την απόλαυση των προνομίων του, χωρίς φόβο.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική αποσκοπεί στην παρουσίαση του ζητήματος της χρήσης του διαδικτύου και των κινδύνων που εντοπίζονται για τους ανήλικους χρήστες. Παράλληλα, έχει ως στόχο την ανάλυση της ποινικής προστασίας για τους ανηλίκους και τα μέτρα αντιμετώπισης για την αντιμετώπιση του φαινομένου.

Για τον σκοπό αυτό αξιοποιείται η μεθοδολογία της βιβλιογραφικής έρευνας και ανασκόπησης. Η έρευνα πραγματοποιήθηκε σε αρθρογραφία νομικών κειμένων και στη νομολογία, ενώ παράλληλα εξετάστηκαν τα συμπεράσματα των επιστημών της κοινωνιολογίας και της ψυχολογίας. Η έρευνα οδήγησε στο συμπέρασμα ότι το διαδίκτυο είναι ένα χρήσιμο εργαλείο, το οποίο, όμως θα πρέπει να αξιοποιείται με προσοχή. Επίσης, μέσω της ανασκόπηση της βιβλιογραφίας διαμορφώθηκε το συμπέρασμα ότι η νομοθετική ρύθμιση για το ηλεκτρονικό έγκλημα, λόγω της αχανούς έκτασης του διαδικτύου και της απουσίας χωροχρονικών περιορισμών, δυσκολεύεται να προλάβει και να αναχαιτίσει τη δράση των εγκληματιών και συνήθως έπεται των εξελίξεων.

Όσον αφορά τους περιορισμούς κατά την εκπόνηση του παρόντος πονήματος, αυτοί έγκεινται κυρίως στη δυσκολία προσέγγισης των βιβλιοθηκών λόγω της έξαρσης της πανδημίας του κορονοϊού και την έρευνα κυρίως σε διαδικτυακές πηγές και την προσωπική συλλογή της γράφουσας, οι οποίες όμως προσέφεραν πληθώρα βιβλιογραφικών αναφορών και πλούσια επιστημονική γνώση.

Λέξεις Κλειδιά: Ιντερνέτ, εθισμός, εξάρτηση, ανήλικοι, ηλεκτρονικά εγκλήματα, *grooming*, παιδική πορνογραφία, bullying, διαδικτυακός εκφοβισμός, διαδικτυακή αποπλάνηση, προσωπικά δεδομένα, ηλεκτρονικό εμπόριο.

ABSTRACT

This dissertation aims to present the issue of internet use and the risks identified for underage users. At the same time, it aims to analyse the criminal protection for minors and the measures to deal with the phenomenon.

For this purpose, the methodology of bibliographic research and review is utilized.

The research was carried out by using articles, legal texts and case laws. At the same time the conclusions of the sciences of sociology and psychology were examined in this paper. The research has concluded that the internet is a useful tool, but it should also be used with caution. In addition to the review of the law literature, this paper formed the conclusion that the legislation on cybercrime, due to the vastness of the internet and the absence of space-time constraints, finds it difficult to prevent and stop the activity of criminals and usually follows developments.

As for the limitations in the preparation of this paper, they are mainly due to the difficulty of approaching libraries due to the outbreak of the coronavirus pandemic and that the research was mainly limited to online sources and the author's personal collection of scientific law books, which, however, provided a wealth of bibliographic references and a rich knowledge on the subject.

Key Words: Internet, addiction, minors, cybercrime, grooming, child pornography, bullying, cyberbullying, personal data, e-commerce

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Το κεντρικό ζήτημα της διπλωματικής αποτελούν οι ανήλικοι χρήστες του διαδικτύου και οι τρόποι με τους οποίους αυτοί μπορούν να προστατευθούν νομοθετικά και κοινωνικά. Για τον σκοπό αυτό αναλύονται επιστημονικά δεδομένα που προκύπτουν από τη βιβλιογραφική ανασκόπηση σε έγκυρα περιοδικά, βιβλία και άρθρα.

Σκοπός της παρούσας βιβλιογραφικής έρευνας είναι να αναλυθεί η θέση των ανηλίκων στην σφαίρα του Διαδικτύου τόσο ως καταναλωτών όσο και ως χρηστών των μέσων κοινωνικής δικτύωσης. Επίσης, αποσκοπεί στην ανάδειξη των κινδύνων του Διαδικτύου για τους ανηλίκους και τους τρόπους προστασίας τους, με προληπτικά μέτρα.

Εν συντομία, στο πρώτο κεφάλαιο παρουσιάζεται μία εισαγωγή στην έννοια του Διαδικτύου. Πιο συγκεκριμένα, γίνεται αναφορά στην ιστορική αναδρομή της εμφάνισης του διαδικτύου και στην εξάπλωσή του στα παιδιά και τους εφήβους. Επίσης, παρουσιάζεται η χρήση του στην Ευρώπη και στην Ελλάδα, το φαινόμενο της εξάρτησης και του εθισμού από το διαδίκτυο και τα αίτια και οι συνέπειές του. τέλος, το κεφάλαιο ολοκληρώνεται με την ανάλυση του δικαιώματος της πρόσβασης των ανηλίκων στο διαδίκτυο στο εθνικό και υπερεθνικό δίκαιο.

Στο δεύτερο κεφάλαιο, παρουσιάζονται οι κίνδυνοι από το διαδίκτυο για τους ανηλίκους. Αρχικά ορίζεται και κατηγοριοποιείται η έννοια του ηλεκτρονικού εγκλήματος. Επίσης παρουσιάζονται τα είδη των θυμάτων και των θυτών των ηλεκτρονικών εγκλημάτων. Στην συνέχεια, αναλύονται τα πιο διαδεδομένα διαδικτυακά εγκλήματα με επίκεντρο τους ανηλίκους. Έτσι, παρουσιάζονται η παιδική πορνογραφία ως διαδικτυακό έγκλημα, η προσέλκυση παιδιών για γενετήσιους λόγους - η Διαδικτυακή αποπλάνηση (*grooming*), η διαδικτυακή προσβολή της γενετήσιας αξιοπρέπειας, ο διαδικτυακός εκφοβισμός (*cyber-bullying*), η προπαγάνδα μίσους στο διαδίκτυο (*hate speech*), η απάτη κατά ανηλίκων στο διαδίκτυο, οι κίνδυνοι για τους ανήλικους καταναλωτές ως χρήστες του διαδικτύου και τα προσωπικά δεδομένα των ανήλικων στο διαδίκτυο

Στο τρίτο κεφάλαιο, αναλύεται η νομοθεσία και η νομική προστασία σε περίπτωση ηλεκτρονικών εγκλημάτων. Αρχικά, παρουσιάζεται η ιδιάζουσα νομική περίπτωση των ηλεκτρονικών εγκλημάτων, σε συνδυασμό με τη νομική προστασία σε διεθνές επίπεδο και τη νομική προστασία στο ευρωπαϊκό δίκαιο. Τέλος, παρατίθεται αναλυτικά η νομική προστασία στο ελληνικό δίκαιο, παρουσιάζοντας τα εγκλήματα κατά της γενετήσιας ελευθερίας ανηλίκων, η απάτη και η απάτη μέσω υπολογιστή, ο διαδικτυακός εκφοβισμός και η εξύβριση και η δυσφήμιση

Στο τέταρτο κεφάλαιο αναλύεται η αντιμετώπιση των διαδικτυακών εγκλημάτων. Πιο συγκεκριμένα, γίνεται αναφορά στις δυσκολίες κατά τη διερεύνηση και την απονομή δικαιοσύνης για τα διαδικτυακά εγκλήματα. Επίσης, διαμορφώνονται προτάσεις για τη δημιουργία ασφαλών πληροφοριακών συστημάτων και αναφέρονται τα πιο αποτελεσματικά μέτρα πρόληψης και προστασίας των ανηλίκων κατά τη χρήση του Διαδικτύου.

Κεφάλαιο 1. Εισαγωγή στην έννοια του Διαδικτύου

1.1 Ιστορική αναδρομή στην εμφάνιση του διαδικτύου

Με τον όρο διαδίκτυο νοείται ένα τεράστιο πλέγμα από ψηφιακές γραμμές που κατορθώνει, με εντυπωσιακή ταχύτητα, να διασυνδέσει εκατομμύρια χρήστες και κατόχους ηλεκτρονικών συσκευών. Η σπουδαιότητα του έγκειται στο γεγονός ότι είναι σε θέση να ενώσει χιλιάδες δίκτυα, τα οποία κατανέμονται σε κάθε γωνιά του πλανήτη, συνδέοντας έτσι άτομα και βέλτιστες υπηρεσίες με το πάτημα ενός κουμπιού. Το πλήθος των εργαλείων που εκείνο διαθέτει αλλά και η πληθώρα των καινοτομιών που εισήγαγε στο δεύτερο μισό του 20ου αιώνα διαμόρφωσαν έναν εικονικό κόσμο, η πρόσβαση στον οποίο γίνεται εύκολα και είναι, στην κοινωνία πια της πληροφόρησης, ελεύθερη για τους χρήστες κάθε ηλικίας (Ryan, 2010).

Η διεθνής ονομασία του είναι το «*Internet*», και η τελευταία αναβαθμισμένη έκδοσή του ανήλθε στο προσκήνιο μόλις τις τελευταίες 3 δεκαετίες, θέτοντας τις βάσεις για μια συλλογική αλλαγή του τρόπου που οι άνθρωποι διεκπεραιώνουν τις καθημερινές τους δραστηριότητες και εργασίες. Η σημερινή τελειοποιημένη μορφή του έχει εισβάλει καθοριστικά στις ζωές των χρηστών, διαμορφώνοντας έτσι, μια νέα κοινωνία, αυτή της πληροφορίας και της γρήγορης πρόσβασης σε αυτή, μέσα από χιλιάδες διαφορετικές πηγές, η αξιοπιστία των οποίων τίθεται διαρκώς υπό το μικροσκόπιο της ερευνητικής αμφισβήτησης (Curran, 2012).

Παρόλο που οι υπολογιστές και το διαδίκτυο έκαναν την εμφάνισή τους σε παγκόσμιο επίπεδο πριν από 30 χρόνια, στον ελλαδικό χώρο, τότε θεωρούνταν ακόμα μορφή πολυτέλειας ή ακόμα και ως κάτι υπερβολικό για να διαθέτει το κάθε σπίτι. Παρόλο που τα οφέλη του είναι υπαρκτά και κατανοητά την σημερινή εποχή, στην αρχή της κυκλοφορίας τους, οι Έλληνες καταναλωτές εμπιστεύονταν και βασίζονταν περισσότερο στα παραδοσιακά μέσα, όπως ήταν η τηλεόραση, το ραδιόφωνο και οι εφημερίδες (Ryan, 2010). Οι διαδικτυακές υπηρεσίες αποτελούσαν, κυρίως μέρος της καθημερινότητας των ερευνητικών ακαδημαϊκών κέντρων, όπως ο Δημόκριτος. Οι πρώτοι πάροχοι επένδυσαν στο ελληνικό *Internet* ήταν *η Hellas On Line* και η *Forthnet* (Athanasiades et al, 2015).

Παράλληλα, στο πλαίσιο αυτής της νέας καθεστηκυίας τάξης, το διαδίκτυο, σε συνδυασμό με την πρόοδο των ηλεκτρονικών υπολογιστών, εντάσσεται πλέον στα αγαθά ζωτικής σημασίας για την καθημερινή ζωή και ευημερία των πολιτών. Αυτό συμβαίνει, μιας και μέσω αυτού, τα άτομα αντλούν δεδομένα για την ενημέρωση και την πνευματική τους ανάπτυξη, αλλά ταυτόχρονα, εκτελούν και πλήθος υποχρεώσεων που σχετίζονται με την επαγγελματική τους ζωή (ασύγχρονη μέθοδος της τηλεργασίας), είτε με τις υποχρεώσεις τους απέναντι στο κράτος (πληρωμή λογαριασμών και φορολογίας). Με αυτόν τον τρόπο, η επιθυμητή αυτή «εισβολή» του στη διευκόλυνση της καθημερινότητας τους, έχει συντελέσει, ώστε το διαδίκτυο να αναχθεί σε αυτόνομη υπεραξία και αναπόσπαστο αγαθό για τους πολίτες (Ryan, 2010).

Η σημασία του διαφαίνεται και από το πλήθος των ηλεκτρονικών πλεγμάτων που έχουν διαμορφωθεί, μόλις τα τελευταία 25 χρόνια από την άνοδό του και την εισαγωγή του στις ανθρώπινες δραστηριότητες. Υπολογίζεται ότι σε αυτό το διάστημα, οι χρήστες του έχουν εκτοξευθεί σε αριθμούς, αγγίζοντας πλέον το 1,5 δισεκατομμύριο, αποτελώντας, κατά προσέγγιση το ένα τέταρτο του παγκόσμιου πληθυσμού. Η μεγάλη απήχησή του, με βάση τα δεδομένα της σύντομης ιστορίας του, βασίζεται κυρίως στο γεγονός ότι η ταχύτητα που προσφέρει, η διαδικτυακή μορφή ορισμένων υπηρεσιών και οι τεράστιες δυνατότητες στην επικοινωνία και την πληροφόρηση δεν μπορούν να τα συναγωνιστούν τα παραδοσιακά μοντέλα επιτέλεσης εργασιών που απαιτούν την φυσική παρουσία και την πολύωρη ταλαιπωρία των πολιτών. Μέσω του διαδικτύου, λοιπόν, οι χρήστες μπορούν να πραγματοποιούν πολλαπλές και ταυτόχρονες εργασίες, γεγονός που μειώνει τον χρόνο αναμονής και ευνοεί την ευκολία και την μείωση της γραφειοκρατίας (Curran, 2012).

Πιο συγκεκριμένα, ο όγκος των δεδομένων που ανταλλάσσεται και μεταδίδεται καθημερινά είναι ανυπολόγιστος, μιας και πλέον εμπεριέχει δεδομένα και πληροφοριακό υλικό που καλύπτει κάθε τομέα της ατομικής και συλλογικής δραστηριοποίησης των ατόμων. Έτσι, οι χρήστες αποκτούν πρόσβαση στο διαδίκτυο για να ολοκληρώσουν ηλεκτρονικές αγορές, να προσφέρουν οι ίδιοι υπηρεσιών *OnLin*e (άνοδος του *e-commerce*), να ενημερωθούν για την παγκόσμια επικαιρότητα μέσα από τις μηχανές αναζήτησης εφημερίδων τοπικών, εθνικών και διεθνών, να πραγματοποιήσουν οικονομικές συναλλαγές (*e-banking*), αλλά και να γνωρίσουν και να επικοινωνήσουν με άτομα που ζουν μακριά, μέσω της ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου (*email, yahoo mail, Gmail*). Ως συνέπεια των ανωτέρω, ο κάθε χρήστης έχει ελεύθερη πρόσβαση σε δεδομένα πληροφοριών, αγαθών και

υπηρεσιών που διακινούνται εύκολα και ταχύτατα μέσω του διαδικτυακού πλέγματος, από την άνεση του υπολογιστή του, υπερνικώντας τις καθυστερήσεις του πραγματικού κόσμου και τα χιλιομετρικά εμπόδια (Kleinrock, 2010).

Βέβαια, σε όλα τα οφέλη που καταγράφηκαν προηγουμένως, δεν πρέπει να παραγνωρίζεται το γεγονός ότι το διαδίκτυο εγκυμονεί κινδύνους και είναι σε θέση να επηρεάσει αρνητικά την ζωή των χρηστών, όταν η πρόσβαση σε αυτό δεν γίνεται λελογισμένα. Ειδικότερα, οι συνέπειες του μπορούν να ανιχνευθούν και είναι ιδιαίτερα ανησυχητικές όταν οι χρήστες του είναι κυρίως τα ανήλικα παιδιά, που εισάγονται στην πληθώρα των διαδικτυακών δεδομένων, χωρίς την απαραίτητη επίβλεψη ενηλίκων και, κατ΄ επέκταση είναι, από μόνα τους πιο επιρρεπή στο γίνουν θύματα των θελγήτρων και της ανωνυμίας που αυτό προσφέρει (Ryan, 2010).

Είναι απαραίτητο να επισημανθεί, ότι, οι ενήλικοι, στην πλειοψηφία τους, με την κατάλληλη ωριμότητα νου και την εγγενή αμφισβήτησή τους για τα κίνητρα των υπόλοιπων χρηστών του διαδικτύου, είναι σε θέση να αυτό-προστατευθούν και να αποφύγουν τους παρόντες κινδύνους, οι οποίοι, ίσως στα μάτια των παιδιών να φαίνονται περισσότερο ως εμπειρίες, με μικρό ρίσκο. Εξαιτίας αυτής της διάκρισης στον βαθμό της ανεπτυγμένης κριτικής σκέψης που διαθέτουν οι ενήλικες σε σύγκριση με τους ανηλίκους, το διαδίκτυο έχει μετεξελιχθεί τα τελευταία χρόνια, στον τόπο τέλεσης και συντήρησης παραβατικών συμπεριφορών επίδοξων δραστών, με θύματα τους τελευταίους, εκσυγχρονίζοντας και οξύνοντας την επαναληπτικότητα διάπραξης των παραδοσιακών εγκλημάτων αλλά και την εμφάνιση νέων μορφών τους (Curran, 2012).

Καταληκτικά, το διαδίκτυο βέβαια, δεν αποτελεί μια αρνητικά φορτισμένη έννοια, που πρέπει να εξοβελιστεί από την ζωή των παιδιών, μιας και η πλήρης απαγόρευσή του, στην εποχή που πλέον έχει επιβληθεί, ως βασικό καθημερινό αγαθό, θα είχε τα αντίθετα από τα επιθυμητά, αποτελέσματα προστασίας τους. Το σημαντικό που οφείλει να πραγματοποιηθεί, είναι η κοινωνία των ενηλίκων να λειτουργήσει, ως προστατευτική ασπίδα για τους ανηλίκους, διαμορφώνοντας συνθήκες ασφάλειας, στο πλαίσιο των οποίων, οι τελευταίοι μπορούν να αξιοποιούν στο μέγιστο της δυνατότητες του διαδικτύου, χωρίς να είναι δέκτες και μάρτυρες των αρνητικών δεδομένων του (Kleinrock, 2010).

1.2 Η εξάπλωση της χρήσης του από τα παιδιά και τους εφήβους

Η είσοδος στη νέα χιλιετία συνοδεύτηκε με την εκτεταμένη χρήση του διαδικτύου σε κάθε τομέα της ανθρώπινης δραστηριοποίησης καθιστώντας δυστυχώς, ως ομάδα στόχου του (*target group*) ακόμα και τους ανήλικους χρήστες. Η γρήγορη εξάπλωσή του και η αυτόματη ένταξή του στα νοικοκυριά οδήγησε, ώστε τα παιδιά να εξοικειωθούν με το εργαλείο αυτό και ταυτόχρονα να το χρησιμοποιούν για μεγάλα χρονικά διαστήματα, ακόμα και χωρίς την αναγκαία γονική επίβλεψη. Αυτό συνέβη βαθμιαία μιας και, ως αναπόσπαστο εργαλείο της καθημερινότητας αξιοποιείται καθημερινά από εκείνα σε πλήθος δραστηριοτήτων τους, είτε για επικοινωνία με τους συνομήλικούς τους είτε για την εκτέλεση σχολικών καθηκόντων ή παρακολούθηση σχολικών μαθημάτων, όπως συνέβη τα τελευταία χρόνια με τη μορφή της σύγχρονης εκπαίδευσης, λόγω της έξαρσης του κορωνοϊού (Άντρη, 2013).

Είναι εύκολα αντιληπτό ότι, όπως αναφέρθηκε και ανωτέρω, ότι το *Internet*, είναι έννοια ουδέτερη, χωρίς θετικό ή αρνητικό πρόσημο. Αυτό διαφαίνεται από το γεγονός ότι στο πλαίσιο του, η καθημερινή ζωή και συνδιαλλαγή έχει διευκολυνθεί, οι εργασίες εκτελούνται με ταχύτητα και ακρίβεια και έχουν αποκατασταθεί πλέον τα χιλιομετρικά και διασυνοριακά εμπόδια που επέβαλε η αναγκαστική φυσική παρουσία κάποτε για την απλή επίτευξη επικοινωνίας με άτομα σε διαφορετικά σημεία του πλανήτη (Ryan, 2010).

Ταυτόχρονα όμως, στον αντίποδα, η παγκόσμια διαδικτυακή κοινότητα ελλοχεύει, λόγω της ανωνυμίας που προσφέρει πολλαπλούς κινδύνους για τους χρήστες που δεν είναι πεπαιδευμένοι πάνω σε τέτοια ζητήματα ασφάλειας και προστασίας. Δυστυχώς, αυτός είναι ένας από τους βασικούς παράγοντες που θυματοποιούνται ανήλικοι χρήστες του, μιας και είναι ιδιαίτερα προβληματική η άκριτη έκθεση προσωπικών δεδομένων και στιγμών τους σε πλήθος αγνώστων με αμφίβολες προθέσεις και εγκληματικά κίνητρα. Ο κυβερνοχώρος, λοιπόν, έχει διευκολύνει, σε μεγάλο βαθμό, τους επίδοξους θηρευτές, ώστε να διευρύνουν το πεδίο της δράσης τους και τον αριθμό των θυμάτων τους, μιας και πλέον, μπορούν να προσεγγίζουν πιο εύκολα ανυποψίαστα άτομα μικρής ηλικίας δημιουργώντας τους ένα υποτυπώδες περιβάλλον ασφάλειας (Curran, 2012).

Παράλληλα, ακριβώς επειδή για την επιτέλεση ορισμένων από τις υποχρεώσεις τους υπαγορεύεται η χρήση του διαδικτύου, τα παιδιά φαίνεται να αφιερώνουν μεγάλο

μέρος του χρόνου τους μέσα στα όρια μιας ηλεκτρονικής οθόνης, αυξάνοντας έτσι τις πιθανότητες να βρεθούν στο στόχαστρο δραστών που θέλουν να τους βλάψουν και να τους εκμεταλλευτούν (Κοκκέβη κ.α., 2010). Βέβαια, η ανισομερής κατανάλωση ωρών στο διαδίκτυο σε συσχετισμό με τις αντίστοιχες της αφιέρωσης για την πραγματική κοινωνική ζωή, έχει φέρει στο προσκήνιο και το ζήτημα του εθισμού των ανηλίκων σε ένα εικονικό περιβάλλον της ευκολίας και της αφθονίας. Στις παραμέτρους αυτές, έχει συμβάλει καθοριστικά το γεγονός ότι, από την στιγμή που το «Internet» κρίθηκε ως υπέρτατο αγαθό, η πρόσβαση σε αυτό διευκολύνθηκε και πλέον είναι εφικτή σε διάφορα σημεία που βρίσκονται τα παιδιά, όπως στις σχολικές μονάδες, στους υπολογιστές στο σπίτι και τις δημοτικές βιβλιοθήκες, αλλά και μέσω των νέων μοντέλων κινητών (*smartphones*) και άλλων ηλεκτρονικών συσκευών (Athanasiades et al, 2015).

Επιπρόσθετα, αξίζει να καταγραφεί ότι τα μικρά παιδιά και οι έφηβοι δεν είναι σε θέση, ακόμα, να διαμορφώσουν με κριτική σκέψη και πληρότητα, μια ασφαλή κοσμοθεωρία, καταλήγοντας έτσι να μετατρέπονται σε υποχείρια και φερέφωνο των όσων διαβάζουν σε ιστοσελίδες με μη φιλτραρισμένο περιεχόμενο. Ως απότοκο του μεγάλου όγκου πληροφοριών που το διαδίκτυο είναι σε θέση να τους προσφέρει αποτελεί, δυστυχώς, και η ύπαρξη ανεπιβεβαίωτων πληροφοριακών δεδομένων που σκοπό έχουν να φανατίσουν και να παραπληροφορήσουν τους αναγνώστες τους. Αυτό ακριβώς είναι που παρατηρείται με τους νεαρούς χρήστες, οι οποίοι, λόγω της μειωμένης γνωστικής και πολύπλευρης ανάπτυξής τους αδυνατούν να διακρίνουν, σε ικανοποιητικό βαθμό, το ασφαλές από το επιβλαβές και το μη επιστημονικά επιβεβαιωμένο πληροφοριακό υλικό, καταλήγοντας έτσι, στην πρόσληψη γνώσεων λαθεμένων και ανακριβών, που εμποδίζει την περαιτέρω πνευματική τους ανάταση (Κοκκέβη κ.α., 2010).

Καταλήγοντας, τα ανωτέρω αποδεικνύουν περίτρανα ότι, προκειμένου να επικρατήσει η θετική όψη του διαδικτύου και να περιορισθούν οι αρνητικές προεκτάσεις του, βασικό εργαλείο καθίσταται η επιφυλακή και η ετοιμότητα των ενηλίκων για την προστασία των παιδιών που πλέον αποτελούν ένα σημαντικό ποσοστό των χρηστών του. Είναι αναγκαίο οι ανήλικοι να αναχθούν σε προτεραιότητα και των κατασταλτικών νόμων της Πολιτείας, ως μια ευάλωτη κοινωνική ομάδα που χρειάζεται καθοδήγηση σε έναν νέο κόσμο που περιπλέκει τα όρια της πραγματικότητας με το εικονικό αποτύπωμα τους στον κυβερνοχώρο (Athanasiades et al, 2015).

1.3 Η χρήση του διαδικτύου στην Ευρώπη και στην Ελλάδα

Παράλληλα, προκειμένου να διασφαλιστεί η επιστημονική πληρότητα της παρούσας επιστημονικής εργασίας, είναι απαραίτητο να καταγραφούν και τα δεδομένα που αντλούνται από τις ευρωπαϊκές και εθνικές υπηρεσίες, αναφορικά με τα ημερήσια και εβδομαδιαία ποσοστά έκθεσης των ανήλικων χρηστών στο διαδίκτυο (Athanasiades et al, 2015).

Από την μία, πιο συγκεκριμένα, στην Ευρώπη, τα παιδιά, από την ηλικία των 9 μέχρι τα 14, φαίνεται να αφιερώνουν κατά προσέγγιση, μιάμιση ώρα καθημερινά στο διαδίκτυο ενώ από την ηλικία των δεκαπέντε, η έκθεση σε αυτό, οξύνεται κατά μισή ακόμα ώρα (συνολικά ένα δίωρο). Γίνεται εύκολα αντιληπτό ότι δεν είναι ανησυχητικές μόνο οι ώρες που σπαταλούνται και αφαιρούνται από τις διαπροσωπικές σχέσεις των παιδιών, αλλά και το γεγονός ότι σε ορισμένες από τις περιπτώσεις, οι πρώτες επαφές με το *Internet* πραγματοποιούνται ήδη από την προσχολική ηλικία. Τα στατιστικά δεδομένα είναι ιδιαίτερα προβληματικά, μιας και από τη στιγμή που το διαδίκτυο και η πληθώρα των επιλογών του έχουν καταστεί σε «σύντροφο - φίλο» των παιδιών, όταν οι γονείς δουλεύουν ή ασχολούνται με άλλες δραστηριότητες τους, οι ανήλικοι (9 έως 15) προτιμούν, σε ποσοστά άνω του 80% να εκτελέσουν τις σχολικές υποχρεώσεις τους, να διασκεδάσουν, να συνομιλήσουν με συμμαθητές και συνομήλικους αποκλειστικά, μέσω των ηλεκτρονικών υπολογιστών. Ταυτόχρονα, σε αυτές τις ηλικίες ένα ποσοστό που πλησιάζει το 50% φαίνεται ότι είναι χρήστες των κοινωνικών δικτύων, με τους μισούς περίπου να δηλώνουν πλαστά δεδομένα, ιδιαίτερα στο πεδίο της συμπλήρωσης της ηλικίας, δηλώνοντας μεγαλύτερη από την πραγματική. Παράλληλα, σε ποσοστό 87%, επιλέγουν να συνδεθούν στο διαδίκτυο από την ασφάλεια του δωματίου τους από τον υπολογιστή, την ψηφιακή ταμπλέτα είτε το κινητό τους, ενώ το 60% το χρησιμοποιεί και κατά το σχολικό ωράριο. Βέβαια, στα παρόντα δεδομένα εκείνο που χρήζει ιδιαίτερης προσοχής είναι το γεγονός ότι το 50% των ανήλικων χρηστών αισθάνεται ότι μπορεί να εκφραστεί με μεγαλύτερη ασφάλεια, μέσω του διαδικτύου σε σύγκριση, με το εάν πρέπει να το κάνει πρόσωπο με πρόσωπο. Η συγκεκριμένη ομολογία, δημιουργεί έντονο προβληματισμό για το εάν η επιτυχής και πλήρης κοινωνικοποίηση των παιδιών μπορεί να πραγματοποιηθεί πλέον με την τόσο εκτεταμένη παρουσία του διαδικτύου στη ζωή τους (ENISA, n.d.).

Τα δεδομένα αυτά από τον ευρωπαϊκό χώρο επαναφέρουν, επίσης, την προβληματική για το ψηφιακό χάσμα που συντελείται, λόγω της διαρκούς παρουσίας των ανήλικων στον εικονικό από ό,τι στον πραγματικό κόσμο. Πιο συγκεκριμένα, στο πλαίσιο της παγκόσμιας «οικονομικής ατροφίας», αλλά και στην κρίση ηθικών αξιών που χαρακτηρίζει, δυστυχώς την σύγχρονη κοινωνία των πολιτών, οι λιγότερο προστατευμένες ηλικιακές ομάδες, ανάμεσα τους και τα παιδιά, μπορεί να βιώσουν αρνητικές εμπειρίες μέσω του διαδικτύου, μιας και το νεαρό της ηλικίας τους και η απειρία τους πάνω σε ζητήματα του ενήλικου κόσμου τους καθιστά ευάλωτους και επίκεντρο ενδιαφέροντος εγκληματικών δραστηριοτήτων (Athanasiades et al, 2015).

Τα παραπάνω στατιστικά δεδομένα αλλά και το πλήθος των περιστατικών όπου το θύμα των κυβερνοεγκλημάτων ήταν ανήλικος, οδήγησε την Ευρωπαϊκή Ένωση να δημιουργήσει καμπάνιες προστασίας και ενημέρωσης γονέων και παιδιών σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο. Είναι ευτυχές το γεγονός ότι με τους νέους κανονισμούς της για την προστασία των προσωπικών δεδομένων επιχειρεί να πλαισιώσει με τα ρυθμιστικά και προστατευτικά μέτρα της την κυβερνοασφάλεια των ανήλικων χρηστών και να τους επιτρέψει να το αξιοποιούν προς όφελος τους, αμβλύνοντας τις περιπτώσεις παραπλανητικών και εγκληματικών συμβάντων σε βάρος τους. Τέλος, με την ίδρυση οργανισμών, όπως ο *ENISA:EUROPEAN UNION AGENCY FOR CYBERSECURITY*, διευκολύνει την παροχή συμβουλών προς τα κράτη και τους πολίτες για την ασφάλεια στο διαδίκτυο και την προαγωγή μεθόδων λύσης και διαχείρισης των κρίσεων, ενδυναμώνοντας έτσι την προσπάθεια ελέγχου και προστασίας των χρηστών από τους κινδύνους του (ENISA, n.d.).

Από την άλλη, σε εθνικό επίπεδο, τα ποσοστά της έκθεσης των παιδιών στο φαινόμενο της μόνιμης διαδικτυακής παρουσίας είναι υψηλά και φαίνεται να συναγωνίζονται εκείνα των άλλων χωρών της Ευρώπης. Η δημοτικότητα του, πιο συγκεκριμένα, είναι αντιληπτό ότι έχει εκτοξευθεί τα τελευταία χρόνια, ειδικά αν αναλογιστεί κανείς ότι πριν από 3 δεκαετίες, μόλις το 1% των πολιτών των αστικών κέντρων διέθετε πρόσβαση σε αυτό. Σύμφωνα με έρευνα του 2019 της *Devolo Hellas* σε συνεργασία με το *infokids.gr*, το 59% των παιδιών κάτω των 10 ετών έχει πρόσβαση στο *Internet*. Στον ελλαδικό χώρο, τα παιδιά αρχίζουν να ασχολούνται με τους ηλεκτρονικούς υπολογιστές στην ηλικία των 6-8 ετών, και να μονοπωλούν σε αυτές τις ηλικίες, σε ποσοστό 38% τις διαδικτυακές σελίδες, σε ποσοστό 31% τα παιδιά ηλικίας 11 με 13 έτη, ενώ η χρήση των καινούριων smartphone κινητών παρατηρείται ακόμα και από την βρεφική ηλικία με δικές τους συσκευές πλοήγησης. Σε αυτά τα ποσοστά,

με τα ανήλικα παιδιά να αποτελούν ένα μεγάλο μέρος των χρηστών του διαδικτύου στην Ελλάδα, έρχεται να προστεθεί και το γεγονός ότι ένα τεράστιο μέρος αυτών διαθέτει μέσα κοινωνικής δικτύωσης από την ηλικία των 11 ετών (Devolo Hellas & Infokids.gr, 2019).

Σε όλα τα παραπάνω προστίθεται και το γεγονός ότι σε αντίστοιχη έρευνα με αντικείμενο τους γονείς και την ασφάλεια που παρέχουν στα παιδιά τους ενόσω πλοηγούνται τα τελευταία στο διαδίκτυο, οι πρώτοι σε ποσοστό 49% δήλωσαν ότι έχουν εν μέρει την γενική εποπτεία των διαδικτυακών δραστηριοτήτων τους, ενώ το 11% φαίνεται ότι δεν επιβάλλει καμία μορφή ελέγχου σε αυτά. Ταυτόχρονα, έρευνες αποδεικνύουν ότι περίπου το 60% των γονέων επιτρέπουν την περιορισμένη χρήση του διαδικτύου στα παιδιά, ενώ σε ποσοστό 30% των τελευταίων, η πρόσβαση σε αυτό πραγματοποιείται από δικές τους ηλεκτρονικές συσκευές, με το 20% εξ αυτών να διαθέτει πλήρη αυτονομία, μακριά από τον προστατευτικό έλεγχο των γονέων. Τα ποσοστά αυτά αποδεικνύουν ότι το ένα πέμπτο των ανηλίκων στην Ελλάδα είναι απολύτως εκτεθειμένο στους επίδοξους εγκληματίες που παραμονεύουν στον κυβερνοχώρο, μιας και οι γονείς παραμελούν την θωράκιση και την προστασία τους από τους κινδύνους που αυτό ελλοχεύει (Devolo Hellas & Infokids.gr, 2019).

Συμπερασματικά, τα ανωτέρω στατιστικά δεδομένα δημιουργούν έναν έντονο προβληματισμό σχετικά με την ποιότητα και την ποσότητα των ασφαλιστικών δικλείδων που θέτουν και οι ίδιοι οι γονείς στα τέκνα τους, όταν τους επιτρέπουν την ελεύθερη και άνευ προϋποθέσεων προσβασιμότητα στον διαδικτυακό χώρο (Tsimtsiou et al, 2017). Η υπερέκθεση αυτή λειτουργεί σε συνδυασμό με την αδυναμία των ίδιων να αντιληφθούν σε βάθος τις δυσάρεστες παραμέτρους μιας φαινομενικά αθώας πλοήγησης στα κοινωνικά δίκτυα. Προς αυτήν την κατεύθυνση, λοιπόν, το 2008, συστάθηκε στην Ελλάδα, η «Ελληνική Εταιρία Μελέτης Διαταραχής Εθισμού στο Διαδίκτυο», μια μη κερδοσκοπική οργάνωση που έθεσε ως προτεραιότητά της την συνεχή ενημέρωση και ευαισθητοποίηση του κοινωνικού συνόλου για τις αρνητικές συνέπειες που το διαδίκτυο μπορεί να επιφέρει στην σωματική και κυρίως στην ψυχική υγεία των νέων χρηστών του. Είναι, λοιπόν, καθήκον, του συνόλου της κοινωνίας να διαμορφώσει ένα ασφαλές και προστατευμένο διαδικτυακό περιβάλλον για τους ανηλίκους, προκειμένου να τους δώσει τα απαραίτητα εφόδια για να αναγνωρίζουν από μόνοι τους τους ενδεχόμενους κινδύνους, θωρακίζοντας την παρουσία τους στο διαδίκτυο και την κυβερνοασφάλεια τους (Άντρη, 2013).

1.4 Η εξάρτηση και ο εθισμός από το διαδίκτυο

Το διαδίκτυο όπως προαναφέρθηκε, κατέχει πλέον σημαντική θέση στην καθημερινότητα των περισσότερων ανθρώπων. Τόσο οι γονείς όσο και οι εκπαιδευτικοί θα πρέπει να είναι σε θέση να αναγνωρίσουν τους κινδύνους και τα εγγενή προβλήματα, τα οποία δημιουργούνται από την υπερβολική έκθεση και χρήση του Διαδικτύου από τους ανήλικους. Οι ανήλικοι χρήστες του διαδικτύου πολύ συχνά αδυνατούν να εντοπίσουν τις πιθανές επιπτώσεις της λανθασμένης χρήσης του Ίντερνετ και για το λόγο αυτό είναι απαραίτητη η συμβολή των ενηλίκων προκειμένου να αναγνωρίσουν και να αναστείλουν το φαινόμενο. Επίσης, επειδή το διαδίκτυο αποτελεί εργαλείο και είναι απαραίτητο στην σύγχρονη, κατά βάση ψηφιακή, κοινωνία, είναι πολύ χρήσιμο τα παιδιά από μικρή ηλικία να διδαχθούν τους τρόπους αξιοποίησης του διαδικτύου προκειμένου δρέπουν τα οφέλη της τεχνολογίας χωρίς τις αρνητικές της συνέπειες (Athanasiades et al, 2015).

Ένας από τους βασικότερους κινδύνους στο Διαδίκτυο είναι ο εθισμός, ο οποίος αποτελεί μία πολύ πρόσφατη μορφή εξάρτησης. Πιο αναλυτικά, η εξάρτηση από το διαδίκτυο περιγράφει την περίπτωση εκείνη κατά την οποία το Ίντερνετ αποκτά στην ζωή του ατόμου και στην καθημερινότητά του πολύ πιο μεγάλη σημασία από τον οικογενειακό και τον φιλικό του περίγυρο, από τις δραστηριότητες και τα χόμπι του, από την εργασία ή τη μόρφωσή του και γενικά από τις κοινωνικές και εργασιακές επαφές του έξω από την διαδικτυακή σφαίρα (Κοκκέβη κ.α., 2010).

Όπως αναφέρθηκε και στις ανωτέρω ενότητες, το Διαδίκτυο έχει πλέον εξαπλωθεί σε όλη την υφήλιο και έχουν παρατηρηθεί περιπτώσεις παιδιών και εφήβων που σπαταλούν πολλές ώρες στον υπολογιστή τους, σε ηλεκτρονικά παιχνίδια, σε διαδικτυακά φόρουμ και μέσα κοινωνικής δικτύωσης (Άντρη, 2013). Αυτό φυσικά είναι χαρακτηριστικό μίας γενιάς που ανατράφηκε στην εποχή της άνθισης της τεχνολογίας. Αυτό που οδηγεί στον χαρακτηρισμό της συμπεριφοράς τους ως εξάρτησης είναι η παραμέληση όλων των κοινωνικών συναναστροφών και των καθημερινών δραστηριοτήτων τους για χάρη της διαδικτυακής ενασχόλησης. Βέβαια, αξίζει να αναφερθεί ότι κάποιοι επιστήμονες ακόμα αναγνωρίζουν τον όρο «εθισμός στο Διαδίκτυο» ως αδόκιμο και εξακολουθεί να θεωρείται από την επιστημονική κοινότητα ως μία αμφιλεγόμενη ορολογία (Athanasiades et al, 2015).

Αυτό που καθιστά ιδιαίτερα επικίνδυνη μία πιθανή εξάρτηση από το Διαδίκτυο ειδικά στους εφήβους είναι ότι, σε μία ταραγμένη από προβλήματα αυτοεικόνας και ψυχολογικές διακυμάνσεις περίοδο της ζωής τους, τους προσφέρει τη δυνατότητα να παρουσιάζουν την ζωή τους όπως ακριβώς επιθυμούν. Με άλλα λόγια, το Ίντερνετ καλύπτει τις ψυχολογικές ανάγκες του ανθρώπου για επίτευξη της αποδοχής και της ενσωμάτωσης σε συνδυασμό με την επίφαση αυτοπεποίθησης λόγω της εξιδανικευμένης εικόνας του εαυτού του που παρουσιάζεται χωρίς περιορισμούς και αρνητικές επιπτώσεις (Kuss & Lopez-Fernandez, 2016). Έτσι, στην σύγχρονη σκληρή πραγματικότητά, ο εθισμός των ανηλίκων στην «τέλεια» ζωή, με την «τέλεια» εικόνα για το εαυτό και την «τέλεια» καθημερινότητα μπορεί να οδηγήσει σε απομάκρυνση από τον πραγματικό κόσμο και την εισαγωγή στον φαντασιακό κόσμο του Διαδικτύου, όπου διαμορφώνεται μία νέα αλήθεια, πιο ελκυστική και εθιστική (Κοκκέβη κ.α., 2010).

Κάποιες από τις πρώτες προειδοποιητικές ενδείξεις για τον εθισμό στο διαδίκτυο είναι η αδυναμία και η άρνηση του ατόμου να διακόψει την ενασχόλησή του με το ίντερνετ κατά βούληση και οι ανεπιτυχείς απόπειρες μείωσης ή περιορισμού τους χρόνου χρήσης του. Οι συμπεριφορές αυτές ξεκινούν από μία αρχική επιθυμία για ολοένα και περισσότερη ενασχόληση με το ίντερνετ, ακόμα και με την χρήση δικαιολογιών και μπορεί να φτάνουν μέχρι την εμμονική σκέψη και την αναμονή για τις διαδικτυακές δραστηριότητες. Αυτή η στάση απέναντι στο Ιντερνέτ οδηγεί σε συνεχώς αυξανόμενες ώρες χρήσης του, προκειμένου να ικανοποιηθεί η επιθυμία (Kuss & Lopez-Fernandez, 2016).

Αυτό που έχει σημασία είναι η συμπεριφορά του ατόμου όταν απομακρύνεται από το Ίντερνετ και την χρήση του. Αν τελικά δεν ικανοποιηθεί η επιθυμία αυτή για χρήση του Διαδικτύου, το άτομο μπορεί να αισθάνεται ανία και συναισθηματική κενότητα, ενώ σε πιο ακραίες περιπτώσεις μπορεί να γίνει επιθετικό και ευέξαπτο. Από την άλλη, το άτομο αυτό παρουσιάζει αίσθηση χαράς, ευθυμίας και ευεξίας, όταν τελικά χρησιμοποιεί το ίντερνετ και ικανοποιεί την ανάγκη του. Παράλληλα, σε κάποιες περιπτώσεις το εθισμένο άτομο μπορεί να εμφανίσει και ενοχικά αισθήματα, να εκδηλώσει μία αμυντική στάση απέναντι σε όποιον αναφέρεται στον τρόπο που χρησιμοποιεί το Διαδίκτυο ή να ψεύδεται σχετικά με τις δραστηριότητές τους και τις ώρες χρήσης (Athanasiades et al, 2015).

1.5 Τα αίτια και οι συνέπειες της υπερβολικής χρήσης του διαδικτύου στους νέους

Όσον αφορά το αίτια του φαινομένου της εξάρτησης στο διαδίκτυο, αυτά μπορούν να τοποθετηθούν σε τρεις βασικές κατηγορίες: τα ψυχολογικά, τα οικογενειακά και τα κοινωνικά αίτια (Cash et al, 2012).

Αρχικά, όσον αφορά τα ψυχολογικά αίτια της υπερβολικής χρήσης του Διαδικτύου, τα νεαρά άτομα, παρουσιάζουν μία πιο εύθραυστη ψυχολογία και μία έντονη διακύμανση των συναισθημάτων, λόγω του ότι δεν έχουν ακόμα αναπτύξει πλήρως την προσωπικότητά τους. στην περίπτωση που ένας ανήλικος διαπιστώνει ότι δεν διαθέτει αρκετούς φίλους στους οποίους μπορεί να εμπιστευθεί τις ανησυχίες του ή δεν διαθέτει ένα ανοικτό και δεκτικό οικογενειακό περιβάλλον που να αφουγκράζεται τις ανησυχίες της ηλικίας του, μπορεί να απομονωθεί και να οδηγηθεί στην άνεση που προσφέρει η επίπλαστη εικόνα του Διαδικτύου. Επομένως, η απομόνωση και η απόρριψη που μπορεί να αντιμετωπίζει ένα παιδί στην καθημερινή ζωή του μπορεί να το οδηγήσει στο να αναζητήσει την ψυχολογική ικανοποίηση και τις απαντήσεις που χρειάζεται σε αγνώστους στο Διαδίκτυο (Kuss & Lopez-Fernandez, 2016).

Από την άλλη, επειδή, η ψυχολογική ανάπτυξη είναι καθοριστική για τη μετέπειτα εξέλιξη του παιδιού αυτή δεν θα πρέπει να αφήνεται σε αγνώστους στο Διαδίκτυο και για το λόγο αυτό οι γονείς θα πρέπει να είναι διαρκώς σε επιφυλακή και να βεβαιώνονται ότι το παιδί διαθέτει επαρκή χρόνο με τους φίλους του και μπορεί να τους εκμυστηρευτεί τους προβληματισμούς του χωρίς το φόβο μία πιθανής τιμωρίας (Kuss & Lopez-Fernandez, 2016). Όταν ένα παιδί δεν αισθάνεται ότι οι ψυχολογικές του ανάγκες για αποδοχή, ενότητα, απελευθέρωση και στοργή ικανοποιούνται από τον οικογενειακό και κοινωνικό του περίγυρο, είναι πολύ πιθανόν να αναζητήσει την ελευθερία που προσφέρει η ανωνυμία στο ίντερνετ, με καταστροφικές συνέπιες σε περίπτωση που κάνει λανθασμένες επιλογές και έρθει σε επαφή με επικίνδυνα άτομα. Μάλιστα, το αίσθημα πληρότητας που προσφέρει η χωρίς συνέπειες και επίκριση επαφή με το Διαδίκτυο, το οποίο δεν παρέχει η αληθινή ζωή του παιδιού, γίνεται εθιστική και μπορεί να οδηγήσει σε όλο και μεγαλύτερη εξάρτηση από αυτό, από τις γνώμες και τις απόψεις αγνώστων και την ψυχολογική καταρράκωση (Athanasiades et al, 2015).

Τα ψυχολογικά αίτια, επομένως, βρίσκονται σε άρρηκτη σχέση με τα οικογενειακά, δεδομένου ότι, όπως προαναφέρθηκε, ο ανήλικος αναζητά την υποστήριξη της οικογένειας του, ως ασφαλούς πεδίου ανάπτυξης της προσωπικότητάς του (Cash et al, 2012). Όταν, όμως, οι γονείς απουσιάζουν ή αδιαφορούν για την ψυχοκοινωνική ανάπτυξη του παιδιού τους, δεν είναι σε θέση να επιβλέψουν την χρήση του διαδικτύου και παρέχουν πρόσφορο έδαφος για μία πιθανή εξάρτηση του παιδιού τους από αυτό. Πέραν αυτού, όταν το παιδί δεν διαθέτει ένα ισχυρό πυρήνα για την επίλυση των προβληματισμών του, είναι πολύ πιθανό να αναζητήσει την επιβεβαίωση και τις λύσεις στο ίντερνετ με αρνητικές συνέπειες για τη δυναμική της σχέσης με τους γονείς, που θα το ταλανίζουν και στην ενήλικη ζωή του (Tsimtsiou et al, 2017).

Τέλος, σχετικά με τα κοινωνικά αίτια της εξάρτησης από το διαδίκτυο σχετίζονται με τις κοινωνικές δεξιότητες και την ανάπτυξη του ανηλίκου. Σε αρκετές περιπτώσεις ορισμένα παιδιά δεν παρουσιάζουν ευκολία στην ανάπτυξη κοινωνικών συναναστροφών και το ίντερνετ μπορεί να καλύψει την ανάγκη τους για κοινωνική επαφή έστω και αν αυτή είναι εικονική. Επίσης, είναι πιθανόν, όταν ένα παιδί δεν έχει εξωσχολικά ενδιαφέροντα και δεν συμμετέχει σε δραστηριότητες που να το φέρνουν σε επαφή με τους συνομηλίκους του, να προτιμά να συναναστρέφεται με τους άλλους μέσω του διαδικτύου και να σπαταλά ώρες σε αυτό, χωρίς ουσιαστικά να βιώνει την πληρότητα της «πραγματικής» συναναστροφής. Τέλος, κάποιες τραυματικές εμπειρίες κοινωνικών σχέσεων του παιδιού στο παρελθόν μπορεί να το οδηγήσουν να απομονωθεί και να προτιμά να αναπτύσσει διαδικτυακές φιλίες, οι οποίες μπορεί να μην έχουν το ίδιο συναισθηματικό υπόβαθρο με τις φιλίες έξω από το ίντερνετ και άρα η διάλυσή τους θα το πληγώσει λιγότερο (Kuss & Lopez-Fernandez, 2016).

Παράλληλα, οι συνέπειες της υπερβολικής χρήσης του Διαδικτύου είναι ποικίλες και εντοπίζονται σε όλους τους τομείς της ζωής του ατόμου. Πιο αναλυτικά, όταν ένας ανήλικος χρησιμοποιεί σε υπερβολικό βαθμό το Διαδίκτυο, υπάρχει σοβαρή πιθανότητα να εμφανίσει από ήπιες μέχρι και πιο σοβαρές ψυχοσωματικές αντιδράσεις και να παρατηρήσει αρνητικές επιπτώσεις την συναισθηματική και την κοινωνική ζωή (Cash et al, 2012).

Αρχικά, όταν ένα άτομο περνά πολύ μεγάλο μέρος της ημέρας του στο Διαδίκτυο, είναι πολύ πιθανόν να παραμελεί τις κοινωνικές, τις φιλικές και τις οικογενειακές του συναναστροφές, με αποτέλεσμα να διακινδυνεύει να χάσει σημαντικές σχέσεις στην ζωή του ή να μειώνονται οι σχολικές και εκπαιδευτικές του επιδόσεις. Παράλληλα, πιθανότατα παραμελεί και τις κοινωνικές του υποχρεώσεις

σχετικά με το σχολείο, την εργασία και επιβαρύνει τους οικείους του με τις δίκες του ευθύνες (Tsimtsiou et al, 2017).

Επίσης, οι καταστάσεις αυτές είναι πιθανόν να οδηγήσουν και σε σωματικά συμπτώματα. Έτσι, η υπερβολική χρήση μπορεί αρχικά να επηρεάσει την στάση του σώματος και να προκαλέσει προβλήματα και πόνους στη μέση, στον αυχένα και την σπονδυλική στήλη. Παράλληλα, μπορεί να οδηγήσει σε σύνδρομο καρπιαίου σωλήνα, ξηροφθαλμία, ημικρανίες και πονοκέφαλους. Επίσης, παρατηρούνται σε νέους με εθισμό στο διαδίκτυο παραμέληση της προσωπικής υγιεινής και σοβαρές διαταραχές του ύπνου, με έντονη κούραση και υπνηλία την ημέρα ή αυπνίες το βράδυ. Επιπλέον, τα παιδιά που χρησιμοποιούν υπερβολικά το Διαδίκτυο, παραλείπουν γεύματα ή παρουσιάζουν υπερφαγία, λόγω της ακανόνιστης πρόσληψης τροφής σε συνδυασμό με την ελλιπή άσκηση με αποτέλεσμα να εμφανίζουν παχυσαρκία (Cash et al, 2012).

Τέλος, είναι αναγκαία η μνεία και στις ψυχολογικές επιπτώσεις της υπέρμετρης χρήσης του Διαδικτύου. Όπως προαναφέρθηκε το διαδίκτυο επιδρά ψυχολογικά στον χρήστη και του προσφέρει άμεση ικανοποίηση των αναγκών του, επιτρέποντας του να αναπτύξει μία νέα ταυτότητα, πολλές φορές αντίθετη από αυτήν της αληθινής του ζωής, η οποία διαθέτει όλα τα επιθυμητά χαρακτηριστικά που δεν θεωρεί ότι διαθέτει στην πραγματικότητα (Bessière et al, 2010) . Επειδή όμως η καθημερινότητα δεν ταυτίζεται με την εικονική πραγματικότητα του ιντερνέτ το παιδί αισθάνεται μειονεκτικά, καθώς δεν διαθέτει τα στοιχεία αυτά και παρουσιάζει κατάθλιψη, διαταραχές προσωπικότητας και κοινωνική φοβία, κρίσεις θυμού και αγχώδεις διαταραχές (Yen et al, 2011).

1.6 Το δικαίωμα πρόσβασης των ανηλίκων στο διαδίκτυο στο εθνικό και υπερεθνικό δίκαιο

Τη δυνατότητα πρόσβασης του ανηλίκου στο διαδίκτυο περιλαμβάνει το δικαίωμα στην πληροφόρηση και την ελευθερία έκφρασης, το οποίο κατοχυρώνουν συνταγματικά τα άρθρα 2 παρ. 1, 5, 5Α παρ.1 και 2 και 14 παρ. 1 του ελληνικού

Συντάγματος. Από την άλλη στον ευρωπαϊκό χώρο, το δικαίωμα αυτό εξασφαλίζεται από το άρθρο 10 της Ευρωπαϊκής Σύμβασης για τα Δικαιώματα του Ανθρώπου (ΕΣΔΑ) και από το άρθρο 11 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Τέλος, σε διεθνές επίπεδο, το δικαίωμα προστατεύεται από τη Διεθνή Σύμβαση του ΟΗΕ για τα Δικαιώματα του Παιδιού και από το άρθρο 19 του Διεθνούς Συμφώνου για τα Ατομικά και Πολιτικά Δικαιώματα (άρθρο 19) (Χρυσόγονος, 2014).

Αρχικά, το ελληνικό σύνταγμα του 2001, πρωτοπόρο για την εποχή και το στάδιο εξέλιξης του ίντερνετ, πρώτο κατοχύρωσε ρητά σε διακριτή συνταγματική διάταξη το δικαίωμα πρόσβασης στο διαδίκτυά, με το άρθρο 5Α παρ. 2 Συντ. έτσι, το ελληνικό Σύνταγμα προβλέπει ότι «*καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά, καθώς και της παραγωγής, ανταλλαγής και διάδοσής τους αποτελεί υποχρέωση του Κράτους, τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9, 9Α και 19*» (5Α § 2 Σ).

Το δικαίωμα αυτό παρουσιάζει μία έντονη κοινωνική διάσταση και είναι ένα θεμελιώδες δικαίωμα, το οποίο επιβάλλει στο κράτος να πραγματοποιήσει θετικές ενέργειες προκειμένου να εξασφαλίσει ίση δυνατότητα πρόσβασης στο διαδίκτυο σε όλους τους σε όλη την εδαφική έκταση της ελληνικής επικράτειας. Επίσης, η πρόσβαση αυτή πρέπει κατά την συνταγματική επιταγή να είναι ίση για όλους και το κράτος έχει την υποχρέωση να υλοποιήσει νόμους, προγράμματα, δράσεις και πολιτικές εξίσωσης της πρόσβασης στο Διαδίκτυο ανεξαρτήτως της οικονομικής και κοινωνικής καταβολής των πολιτών (υποχρέωση ενέργειας) (Δαγτόγλου, 2012).

Από την άλλη, το δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας που εξασφαλίζει το Σύνταγμα, εξασφαλίζει και την υποχρέωση του κράτους να απέχει από ενέργειες που μπορεί να περιορίσουν ή να εξαφανίσουν την ακώλυτη πρόσβαση των ατόμων στο Διαδίκτυο και στα οφέλη και τις εφαρμογές της κοινωνίας της πληροφορίας (υποχρέωση αποχής). Έτσι, με βάση τη διττή αυτή υποχρέωση του κράτους, που προκύπτει συνταγματικά από το άρθρο $5^{Α}$, θεμελιώνεται αγώγιμη αξίωση των πολιτών απέναντι στο κράτος και στους παρόχους των υπηρεσιών ηλεκτρονικών επικοινωνιών, προκειμένου να εξασφαλιστεί η πρόσβαση στις υλικοτεχνικές υποδομές που υποστηρίζουν την ανάπτυξη του Διαδικτύου αλλά και στην ίδια την πληροφορία που διακινείται μέσω αυτού (Χρυσόγονος, 2014).

Το συνταγματικό αυτό δικαίωμα στην κοινωνία της πληροφορίας, όπως αναλύθηκε ανωτέρω, μπορεί να συναχθεί ότι στηρίζεται και έμμεσα και από

υπερνομοθετικής ισχύος συμβάσεις τις οποίες έχει κυρώσει η ελληνική έννομη τάξη. Πιο συγκεκριμένα, αναγνωρίζεται ως ανθρώπινο δικαίωμα από το άρθρο 10 της ΕΣΔΑ, από το άρθρο 19 παρ.2 του ΔΣΑΠΔ και από άρθρα 11 και 36 του ΧΘΔΕΕ (Δαγτόγλου, 2012).

Τα άρθρα αυτά έχουν εξειδικευτεί με το άρθρο 3 παρ. 2ζ του ν.4070/2012 , ο οποίος ενσωμάτωσε την Οδηγία 2009/140/ΕΕ στην Ελληνική έννομη τάξη. Το άρθρο αυτό συγκεκριμένα ορίζει ότι: «*τυχόν μέτρα από δημόσιες αρχές που αφορούν στην πρόσβαση των τελικών χρηστών σε υπηρεσίες και εφαρμογές ή στη χρήση από τους τελικούς χρήστες υπηρεσιών και εφαρμογών μέσω δικτύων ηλεκτρονικών επικοινωνιών πρέπει να τελούν σε αρμονία με τα θεμελιώδη ανθρώπινα δικαιώματα και τις γενικές αρχές του Κοινοτικού δικαίου και, ιδιαιτέρως, να : Είναι κατάλληλα, αναλογικά και αναγκαία σε μία δημοκρατική κοινωνία. Εξασφαλίζουν δίκαιη και αμερόληπτη προκαταρκτική διαδικασία, η οποία περιλαμβάνει το δικαίωμα ακροάσεως του ενδιαφερομένου ή των ενδιαφερομένων. Υπόκεινται στις λοιπές διαδικαστικές διασφαλίσεις που προβλέπονται από την νομολογία του ΕΔΔΑ και τις γενικές αρχές του Κοινοτικού δικαίου. Διασφαλίζουν το δικαίωμα των θιγόμενων σε αποτελεσματικό και έγκαιρο δικαστικό έλεγχο του λαμβανόμενου μέτρου*.» (άρθρο 3 παρ. 2ζ ν.4070/2012) . Επομένως, η πρόσβαση στο Διαδίκτυο δεν περιορίζεται από το κράτος και ο κάθε πολίτης θα πρέπει να έχει τη δυνατότητα να πληροφορείται απρόσκοπτα μέσω αυτού και να προστατεύεται δικαστικά από τυχόν προσβολές του δικαιώματός του (ν. 4070/2012).

Παράλληλα, υφίσταται και η «Δυναμική Συμμαχία για τον Χάρτη των Δικαιωμάτων του Διαδικτύου» ή «*Dynamic Coalition for an Internet Bill of Rights*», η οποία στο Ρίο το 2008 ανέκυψε στην προετοιμασία για την Παγκόσμια Σύνοδο Κορυφής για την Κοινωνία της Πληροφορίας (*WSIS*), στην οποία διακηρύχθηκε ότι στόχος της δεν αποτελεί μια καινούρια νομική διακήρυξη δικαιωμάτων, η εφαρμογή εν τοις πράγμασι το σύνολο των υπαρχόντων ανθρωπίνων δικαιωμάτων όσον αφορά τον τομέα του δικαιώματος στην διαδικτυακή πληροφόρηση και στην χρήση του ίντερνετ (Δαγτόγλου, 2012).

Επομένως, γίνεται κατανοητό ότι στην σύγχρονη κοινωνία της πληροφόρησης, το δικαίωμα στην πρόσβαση στην πληροφορία και στο Διαδίκτυο αποτελεί πανανθρώπινη απαίτηση και ένα δικαίωμα που θα έπρεπε να αναγνωρίζεται σε όλους, παρόλο που εξακολουθούν να υφίστανται διαδικτυακά εγκλήματα και ψηφιακοί εγκληματίες. Επίσης θεωρείται από τους περσότερους ότι το διαδίκτυο θα πρέπει να

είναι ελεύθερο από τις επιρροές από τις κυβερνήσεις και από την παρεμβολή των πολιτικών σχηματισμών σε αυτό. Άλλωστε σε έρευνα του *BBC World* και της εταιρείας δημοσκοπήσεων *GlobeScan*, το 78 τοις εκατό δήλωσε ότι το Διαδίκτυο τους προσφέρει μεγαλύτερη ελευθερία, ενώ το 79 τοις εκατό θεωρεί το ίντερνετ θεμελιώδες δικαίωμα των ανθρώπων (BBC News, 2010).

Κεφάλαιο 2. Οι κίνδυνοι από το διαδίκτυο για τους ανηλίκους

2.1 Το ηλεκτρονικό έγκλημα: ο ορισμός και η εννοιολογική προσέγγιση του ζητήματος

Το φαινόμενο της διαδικτυακής προσβολής των εννόμων αγαθών, με μέσο τέλεσης τους ανώνυμους ηλεκτρονικούς λαβυρίνθους του Ίντερνετ ενυπάρχει ήδη από την δεκαετία του 1970, γεγονός που οδήγησε άμεσα τις έννομες τάξεις στην κατασκευή νέων ποινικών διατάξεων που επιμήκυναν τα νομοθετικά κατασταλτικά όριά τους και στην προστασία κατά της νέας μορφής τέλεσης παραβατικών συμπεριφορών (Αλεξανδρίδου, 2010).

Πιο συγκεκριμένα, η καινή αυτή μέθοδος επιτέλεσης εγκλημάτων και η εμφάνισή τους στον κοινωνικό χώρο, οδήγησε την επιστημονική κοινότητα στην διαμόρφωση ενός πεδίου ορισμού της εγκληματικής αυτής δράσης. Έτσι, ως ηλεκτρονικό έγκλημα θεωρείται κάθε δραστηριότητα με παράνομο σκοπό- κίνητρο, για την τέλεση της οποίας είναι απαραίτητη η κατοχή τεχνολογικών γνώσεων και η εξοικείωσή των δραστών με τα ηλεκτρονικά μέσα. Οι τυποποιημένες αυτές μορφές παραβατικών συμπεριφορών, όταν πληρούνται τα στοιχεία της αντικειμενικής υπόστασης και της υποκειμενικής κάλυψής τους τιμωρούνται από την ελληνική νομοθεσία με συγκεκριμένες ποινές (Αλεξανδροπούλου – Αιγυπτιάδου, 2002).

Πριν αναλυθεί εκτενέστερα το ζήτημα του ηλεκτρονικού εγκλήματος με επίκεντρο, κυρίως τα ανήλικα θύματα που αποτελεί τον κεντρικό άξονα έρευνας της παρούσας εργασίας, κρίθηκε αναγκαίο να επισημανθεί ότι τα εγκλήματα που σχετίζονται με το διαδίκτυο δεν είναι, μόνον όσα απαιτούν την χρήση ηλεκτρονικού υπολογιστή αλλά μπορούν να εκμεταλλεύονται και κάθε μέσο της σύγχρονης τεχνολογίας, όπως την κινητή τηλεφωνία, που διευκολύνει την ανώνυμη και απαρατήρητη «κατασταλτικά» πρόσβαση στο διαδίκτυο. Ταυτόχρονα, αξίζει να επισημανθεί ότι στο ελληνικό δικαιικό σύστημα δεν προβλέπεται νόμος που αυτόνομα και αποκλειστικά επιλύει τα ζητήματα του Διαδικτύου και κανονικοποιεί την

νομιμόφρονα συμπεριφορά των ηλεκτρονικών χρηστών από τη σκοπιά του ποινικού κατασταλτικού δικαίου (Αλεξανδρίδου, 2010).

2.2 Το ηλεκτρονικό έγκλημα: και η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων

Εν συνεχεία, το ηλεκτρονικό έγκλημα μπορεί να κατατμηθεί σε δύο επιμέρους έννοιες, την στενή και την ευρεία. Από τη μία, το «στενό ηλεκτρονικό έγκλημα» νοείται ως η παραβατική συμπεριφορά δράστη, ο οποίος αξιοποιεί τον ηλεκτρονικό υπολογιστή ως το μοναδικό μέσο πραγμάτωσης του εγκληματικού του σχεδίου. Σε αυτήν την κατηγορία εμπίπτουν τα λεγόμενα «οικονομικά εγκλήματα», όπως είναι ενδεικτικά η κατασκοπεία, η πειρατεία, η απάτη μέσω ηλεκτρονικού υπολογιστή και η παραποίηση προσωπικών δεδομένων (Βλαχόπουλος, 2007).

Σε αντιδιαστολή, η ευρεία μορφή των ηλεκτρονικών εγκλημάτων εμπερικλείει τις παρατυπίες εκείνες στα οποία ο ηλεκτρονικός υπολογιστής εμφανίζεται ως συμπληρωματικό – βοηθητικό μέσο επιτέλεσης, όπως συμβαίνει με τα «κυβερνοεγκλήματα», την διασπορά πορνογραφικού υλικού, την διάδοση ρατσιστικών πληροφοριών και την παρότρυνση σε βιαιότητες (Ζάννη, 2005).

Ταυτόχρονα, τα εγκλήματα αυτά που διαπράττονται με την βοήθεια της ψηφιακής τεχνολογίας, μπορούν να τελεσθούν, πέρα από το ηλεκτρονικό περιβάλλον και στην φυσική πραγματικότητα, όπως συμβαίνει με την συκοφαντική δυσφήμηση, η οποία μπορεί να πραγματωθεί είτε, μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας είτε με την παρουσία δύο προσώπων στο ίδιο κοινωνικό περιβάλλον χωρίς την παρεμβολή διαδικτυακών μέσων (Παπακωνσταντίνου, 2010). Το εν λόγω έγκλημα κωδικοποιείται στο άρθρο 363 ΠΚ, όπου προβλέπεται και η επιβαρυντική περίσταση της ηλεκτρονικής μορφής του εγκλήματος. Έτσι, «*αν στην περίπτωση του προηγούμενου άρθρου, το γεγονός είναι ψευδές και ο υπαίτιος γνώριζε ότι αυτό είναι ψευδές τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και χρηματική ποινή και αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω του διαδικτύου, με φυλάκιση τουλάχιστον έξι μηνών και χρηματική ποινή*». Σημειώνεται ότι το άρθρο αυτό είναι μέρος του νέου Ποινικού Κώδικα, όπως αυτός κωδικοποιήθηκε με τον Ν. 4619/2019,

και άρχισε να ισχύει από την 1η Ιουλίου του 2019 (Ποινικός Κώδικας, Νόμος 4619/2019).

Στην κατηγορία αυτή, όταν ένα «κοινό- κλασικό» έγκλημα του Ποινικού κώδικα, διαπράττεται σε «έδαφος» του ηλεκτρονικού διαδικτυακού χώρου, δεν εντοπίζεται ένα επιπλέον στοιχείο στην αντικειμενική υπόσταση του αδικήματος, αλλά στην πραγματικότητα αυτό θεωρείται ως εναλλακτικός τρόπος επιτέλεσής του, το διαδίκτυο, δηλαδή λειτουργεί απλώς, ως το «*modus operandi*» της εν λόγω εγκληματικής συμπεριφοράς. Το ιδιόμορφο ηλεκτρονικό περιβάλλον είναι, στην προκειμένη περίπτωση, το μέσο διευκόλυνσης στην διάπραξη του εγκλήματος και όχι ο μοναδικός τρόπος εμφάνισής του (Παπακωνσταντίνου, 2010).

Στην εν λόγω κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων διαφαίνεται ότι η νομοθετική κατασταλτική πρόβλεψη αποδίδει ικανοποιητικά αποτελέσματα ως προς την εφαρμογή και την επιβολή ποινών, μιας και δεν υπάρχουν αμφιβολίες ως προς την ειδική υπόστασή τους, αφού είναι επαρκής η περιγραφή των αντικειμενικών και υποκειμενικών στοιχείων τους. Στις περιπτώσεις των εγκλημάτων αυτών, η ήδη θεσπισμένη νομοθεσία, καταρχάς, φαίνεται να είναι ικανοποιητική ως προς τη διατύπωση της ειδικής υπόστασής τους, αφού περιγράφονται σε αυτές επαρκώς τα αντικειμενικά και τα υποκειμενικά στοιχεία των ως άνω εγκλημάτων (Yar & Steinmetz, 2019).

Βέβαια, σε ορισμένες περιστάσεις, θεωρητικοί της νομικής επιστήμης έχουν διατυπώσει επιφυλάξεις ως προς την αναγκαιότητα αναγωγής του ηλεκτρονικού εγκλήματος σε ξεχωριστό έγκλημα και κατ΄ επέκταση σε διαφοροποίηση στην επιβολή ποινών όταν πληρούται το στοιχείο της ηλεκτρονικής τέλεσης του εγκλήματος. Στην ρητορική τους επισημάνουν ότι οι προεκτάσεις του ηλεκτρονικού περιβάλλοντος είναι πολύ πιο ευρείες σε σχέση με το κοινό, οδηγώντας έτσι σε μεγαλύτερο και πιο δύσκολα ελεγχόμενο πεδίο περιορισμού των αρνητικών συνεπειών για το θύμα (Παπακωνσταντίνου, 2010). Για το λόγο αυτό, διαφαίνεται η πρόβλεψη του νομοθέτη, σε μερικά εγκλήματα, ώστε να καταστέλλεται με πιο επιβαρυντικά μέτρα η «*sui generis*» παραβατική δράση της εκμετάλλευσης της τεχνολογίας με εγκληματικά κίνητρα (άρθρο 386 Α ΠΚ- 1. *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 στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή*

ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση και χρηματική ποινή. Αν η ζημία που προκλήθηκε υπερβαίνει συνολικά το ποσό των 120.000 ευρώ, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή. […]) (Ποινικός Κώδικας, Νόμος 4619/2019).

Επιπλέον, υφίστανται πλέον εγκλήματα τα οποία μπορούν να διαπραχθούν αποκλειστικά στο κυβερνο- περιβάλλον, χωρίς τη χρήση διαδικτύου, όπως συμβαίνει με την αντιγραφή προγραμμάτων σε ηλεκτρονικό υπολογιστή από κάποιο φορητό μέσο μεταφοράς πληροφοριών («CD, USB stick»), όπως αναλύεται στο άρθρο 370Γ ΠΚ. Αναλυτικότερα, στο άρθρο αυτό προβλέπεται, «*1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους. 2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους. 3. Οι πράξεις που προβλέπονται στο άρθρο αυτό διώκονται με έγκληση».* (Ποινικός Κώδικας, Νόμος 4619/2019).Ταυτόχρονα, εκτός από την ελληνική εθνική νομοθεσία, προβλέπεται και στην Σύμβαση του Συμβουλίου της Ευρώπης ως προς την καταπολέμηση και καταστολή των εγκλημάτων στον κυβερνοχώρο («Convention on Cyber-crime»), στο επιμέρους άρθρο 4 του 2ου Κεφαλαίου, η αθέμιτη τροποποίηση δεδομένων (Παπακωνσταντίνου, 2010).

2.3 Η ειδικότερη κατηγορία των γνήσιων ηλεκτρονικών εγκλημάτων

Ειδικότερα, ως ηλεκτρονικά εγκλήματα μπορούν να θεωρηθούν και εκείνα που ποινικοποιούν μια συμπεριφορά που συσχετίζεται αποκλειστικά με τον κυβερνοχώρο. Τα εγκλήματα αυτής της κατηγορίας χαρακτηρίζονται ως «γνήσια εγκλήματα» του

κυβερνοχώρου (τα λεγόμενα *cybercrimes*) και εμφανίζεται, ενδεικτικά, στον κοινωνικό χώρο ως η διάδοση πορνογραφικού υλικού με ανήλικα θύματα, η κυβερνο-παρενόχληση (*cyber-stalking*), αλλά και η διάδοση κακόβουλου κατασκοπικού λογισμικού ή ιών. Χαρακτηριστικό παράδειγμα αποτελεί, όπως θα αναλυθεί και σε μετέπειτα κεφάλαιο του παρόντος επιστημονικού πονήματος, το άρθρο 384Α ΠΚ, όπου αναλύεται η παιδική πορνογραφία, και ο νόμος αναφέρει ότι «*όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή* […]» (Ποινικός Κώδικας, Νόμος 4619/2019).

Κατά συνέπεια, εν προκειμένω, γίνεται λόγος για τα διαδικτυακά εγκλήματα που μπορούν να εκτελεστούν μόνο στο διαδικτυακό εγκληματικό περιβάλλον και για την πλήρωση της αντικειμενικής υπόστασης είναι αναγκαία συνθήκη η σύνδεση του δράστη στο διαδίκτυο μέσω του ηλεκτρονικού μέσου. Οι βασικότερες και πιο διαδεδομένες μορφές γνήσιων ηλεκτρονικών εγκλημάτων αποτελούν οι κακόβουλες εισβολές σε δίκτυα (*hacking & cracking*), η ανεπιθύμητη αλληλογραφία (*spamming*), το ηλεκτρονικό ψάρεμα (p*hissing*), η διασπορά κακόβουλου λογισμικού μέσω ιών, η πειρατεία, η απάτη με νηγιαριανές επιστολές (*nigerian scam*), το ξέπλυμα χρήματος, η παιδική πορνογραφία και η διαδικτυακή τρομοκρατία (Ιγγλεζάκης, 2019).

Καταλήγοντας, το ηλεκτρονικό έγκλημα, ανεξαρτήτως της θεωρητικής διακλάδωσης και κατηγοριοποίησής του, εμπερικλείει ορισμένα κοινά γνωρίσματα που το διαφοροποιούν έντονα από τα παραδοσιακά εγκλήματα, και σε μεγαλό βαθμό το καθιστά πιο επίφοβο για τα ανυποψίαστα θύματα. Κατ΄ αρχάς βασικό στοιχείο του αποτελεί το γεγονός ότι το κυβερνο-έγκλημα διαπράττεται ταχύτατα και σε πραγματικό χρόνο, είναι γρήγορο και σε ορισμένες περιπτώσεις δεν γίνεται αντιληπτό ούτε από το ίδιο το θύμα. Ταυτόχρονα, η εύκολη διάπραξή του μπορεί να πραγματωθεί χωρίς να αφήσει πραγματικά ίχνη αλλά μόνο ψηφιακά, που καλύπτονται από τους δράστες λόγω των εξειδικευμένων τεχνολογικών γνώσεων τους (Παπακωνσταντίνου, 2010).

Η αντιμετώπιση και καταστολή τους είναι πολύ δύσκολη, καθώς πάντα τα στοιχεία των κυβερνο-εγκληματιών είναι ψεύτικα και σκοπό έχουν την παραπλάνηση των επίδοξων θυμάτων. Ταυτόχρονα, η δυσκολία έγκειται και στο γεγονός ότι ο τόπος διάδρασης ενός ηλεκτρονικού παραβάτη είναι άγνωστος και, δυστυχώς, δεν είναι σε θέση να περιοριστεί εδαφικά μέσα στα όρια μιας επικράτειας, μια προέκταση που

δημιουργεί προβλήματα για τον καθορισμό της ποινικής δικαιοδοσίας μεταξύ κρατών. Έτσι, για την διαλεύκανσή τους απαιτείται τεχνολογικά εξειδικευμένο προσωπικό των διωκτικών αρχών, αστυνομικοί, δικαστές, και εισαγγελείς και ταυτόχρονα αξιώνεται η συνεργασία τουλάχιστον δύο κρατών Για την διερεύνησή του ηλεκτρονικού εγκλήματος απαιτείται, τις πλείστες των περιπτώσεων, συνεργασία τουλάχιστον δύο κρατών: του μέρους, στα όρια του οποίου εξωτερικεύεται το έγκλημα και εκείνου, στο οποίο εντοπίζονται τα αποδεικτικά στοιχεία (Ιγγλεζάκης, 2019).

Για τους ανωτέρω λόγους, κρίνεται αναγκαίο, προκειμένου να μην τροχοπεδείται η επιβολή της δικαιοσύνης, να χαραχθούν κοινές πολιτικές δράσεις μεταξύ των εμπλεκόμενων κρατών και των εφαρμοστέων διατάξεων για το εν λόγω τετελεσμένο έγκλημα. Στο εθνικό ελληνικό δικαιικό σύστημα φαίνεται ότι η Ελληνική Αστυνομία έχει διανοίξει διαύλους συνεργασίας με αρκετές συναρμόδιες υπερθνικές οργανώσεις όπως είναι η *Europol* και η *Interpol*, ρυθμίζοντας έτσι τα ζητήματα με πλήθος άλλων κρατών, όπως οι ΗΠΑ, το Ισραήλ, η Ολλανδία κ.α., αλλά και υπογεγραμμένες συνθήκες, όπως η Συνθήκη της Βουδαπέστης για τα κυβερνοεγκλήματα ή η Σύμβαση του Συμβουλίου της Ευρώπης για τα εγκλήματα στον Κυβερνοχώρο και το Πρόσθετο Πρωτόκολλο αυτής, εισαγόμενο στην εθνική έννομη τάξη με τον ν.4411/2016 (Ιγγλεζάκης, 2019).

Προκειμένου να θεωρηθεί εμπεριστατωμένη η μελέτη και η διαφοροποίηση των ηλεκτρονικών εγκλημάτων, κρίθηκε σκόπιμο να αναλυθούν σε αδρές γραμμές οι κυριότερες μορφές που παίρνει η παραβατική συμπεριφορά των δραστών στον διαδικτυακό χώρο. Αρχικά, συχνή εγκληματική δράση αποτελεί η άνευ εξουσιοδότησης είσοδος σε ηλεκτρονικό υπολογιστή κάποιου ατόμου. Το έγκλημα αυτό αποδίδεται με την έννοια του *hacking ή cracking*, και στο πλαίσιο του εκτελούνται πράξεις παράνομες που σχετίζονται με την χωρίς δικαίωμα αξίωση για πρόσβαση στα ηλεκτρονικά συστήματα και λογιστικά κάποιου και η εξαγωγή ευαίσθητων και προσωπικών δεδομένων από αυτά. Για αυτό το εγκληματικό σενάριο, ανάλογα με τα κίνητρα και την μέθοδο διείσδυσης στα πληροφοριακά στοιχεία του θύματος, οι δράστες διακρίνονται στους *hackers* , από τη μία και στους *crackers* (*criminal hackers*), από την άλλη (Παπακωνσταντίνου, 2010).

Οι πρώτοι συνιστούν την κατηγορία εκείνων των εγκληματιών του κυβερνοχώρου, οι οποίοι διαθέτουν τις εξειδικευμένες και αναβαθμισμένες γνώσεις των τεχνολογικών συστημάτων και κατανοούν και εφαρμόζουν τις πρακτικές του προγραμματισμού, εντοπίζοντας έτσι τις ηλεκτρονικές αδυναμίες και τα ελαττώματα

στα συστήματα ασφαλείας των υπολογιστικών συστημάτων (Αλεξανδροπούλου, 2007).

Ο δικός τους ρόλος είναι περισσότερο να επιλύουν τα ζητήματα που θα προκύψουν από την εφαρμογή των παραπάνω προχωρημένων γνώσεων τους σε πληροφοριακά ζητήματα και εξαντλείται στην επίλυση αυτών, χωρίς περαιτέρω κίνητρα για οικονομική βλάβη ή ζημία πληροφοριών από τα συστήματα που κλήθηκαν να επεξεργαστούν και να προασπίσουν. Η παρανομία που εκείνοι κάνουν δεν γίνεται με κάποιο ταπεινό κίνητρο αλλά στην πραγματικότητα θεωρούν ότι επιτελούν κοινωνικό έργο για να αποτρέψουν πιθανότητα μελλοντικής δολιοφθοράς, υποκλοπής ή κατασκοπείας από κακόβουλα άλλα λογισμικά (Ιγγλεζάκης, 2019).

Από την άλλη, οι *crackers* θεωρούνται όσοι επιδίδονται σε παράνομες δραστηριότητες εισβολής σε συστήματα ηλεκτρονικών υπολογιστών με μόνο μέλημα να προκαλέσουν κακόβουλη και ανεπανόρθωτη ζημία στα δεδομένα που αποθηκεύονται στους διακομιστές, ή να δημιουργήσουν συνθήκες παραβίασης των κωδικών ασφαλείας, ενεργοποιώντας τα πιο εξειδικευμένα πρωτόκολλα προστασίας. Με αυτόν τον τρόπο, επιχειρούν με παράνομα τεχνολογικά μέσα να χειραγωγήσουν τις ηλεκτρονικές εντολές των χρηστών και να μεταφορτώσουν στους δικούς τους τραπεζικούς λογαριασμούς τα χρήματα από τους αντίστοιχους των θυμάτων τους. Αυτή τους η παράνομη δράση διακρίνεται από εκείνη των *hackers,* μιας και οι πρώτοι λειτουργούν κακόβουλα και ύπουλα, προκειμένου να αποκομίσουν για τον εαυτό τους οικονομικά οφέλη, ανεξαρτήτως των προβλημάτων και των χειραγωγήσιμων τεχνικών απάτης που αξιοποιούν (Παπακωνσταντίνου, 2010).

Παράλληλα, και η διασπορά κακόβουλων προγραμμάτων συνιστά μία από τις πιο επικίνδυνες, ως προς τις προεκτάσεις της μορφή διαδικτυακής εγκληματικότητας. Η συγκεκριμένη πρακτική φαίνεται ότι θέτει ως σκοπό της την διαγραφή ή ακόμα και την αλλοίωση των ηλεκτρονικά κατοχυρωμένων δεδομένων με μη ανιχνεύσιμους, προς τον ανυποψίαστο χρήστη, ιούς. Αναλυτικότερα, οι ιοί συνιστούν προγράμματα κατασκευασμένο με τέτοιον τρόπο, ώστε όταν ενεργοποιούνται έχουν την δυνατότητα να διαδοθούν μεταξύ διαφορετικών υπολογιστικών δικτύων, δημιουργώντας αυτοδύναμα αντίγραφα του εαυτού τους σε κάθε νέα συσκευή που φαίνεται να μολύνουν. Για τους διαδικτυακούς παραβάτες τόσο οι ιοί των συστημάτων όσο και των προγραμμάτων συμβάλλουν στην δυσλειτουργία των πληροφοριακών συστημάτων και εν τέλει στην χειραγώγηση του ηλεκτρονικού συστήματος, προκειμένου να προβεί σε διαγραφή αρχείων αλλά και σε εκμηδένιση του συνόλου των δεδομένων που

φυλάσσονται σε σκληρούς δίσκους και εξωτερικές μονάδες αποθήκευσης πληροφοριών (Αλεξανδροπούλου, 2007).

Οι ιοί μπορούν να πάρουν διάφορες μορφές και να υποκλέψουν πλήθος πληροφοριών μεταφέροντας αυτά τα δεδομένα σε προαποφασισμένες μονάδες των δραστών, να διαμορφώσουν ένα μη φανερό υποεπίπεδο του υπολογιστή όπου εκεί να εκτελείται η εντολή που έδωσε ο δράστης, παράλληλα με τις βασικές εντολές που του δίνει ο χρήστης ή ακόμα και να χρεώσουν υψηλές τιμές για ψεύτικες τηλεφωνικές επικοινωνίες και να αποκομίσουν το οικονομικό όφελος. Έτσι, υπάρχουν οι ιοί σκουλήκια (τα λεγόμενα *worms*), οι Δούρειοι Ίπποι (*Trojan Horses*), και οι *dialers* (Ιγγλεζάκης, 2019).

Επιπρόσθετα, το διαδίκτυο οδήγησε και στην μεταβολή του τόπου τέλεσης ορισμένων παραδοσιακών εγκλημάτων, όπως είναι η απάτη μέσω ηλεκτρονικού υπολογιστή. Μια από τις πιο διαδεδομένες μορφές που τελείται τα τελευταία χρόνια στο παγκόσμιο διαδικτυακό χώρο είναι οι λεγόμενες νιγηριανές απάτες. Σε αυτήν την διακεκριμένη μορφή απάτης, οι επίδοξοι εγκληματίες αποστέλλουν σε πλήθος ατόμων ένα *e-mail,* στο οποίο ο δράστης ζητά από τα τελευταία να του μεταφέρει μερικά χρήματα στον δικό του τραπεζικό λογαριασμό, επικαλούμενος την υποτιθέμενη ιδιότητά του ως μέλος του διπλωματικού σώματος, γόνος πλούσιων οικογενειών που βρίσκονται σε ξένη χώρα και κατ΄ επέκταση είναι θύμα πολιτικών συγκρούσεων σε αυτήν. Τα θύματα, λοιπόν, εμπιστεύονται τα λεγόμενά τους και τους αποστέλλουν τα ίδια τα χρήματα είτε τους κωδικούς ασφαλείας για τους δικούς τους προσωπικούς λογαριασμούς με αποτέλεσμα, οι παραβάτες να τους αδειάζουν, κλέβοντας έτσι, χωρίς να αφήνουν ίχνη μεγάλα χρηματικά ποσά (Reep-van den Bergh & Junger, 2018).

Ταυτόχρονα, παραλλαγή της απάτης μέσω ηλεκτρονικού υπολογιστή συνιστά και η απάτη με το ηλεκτρονικό μήνυμα «ψαρέματος», το λεγόμενο *phishing mail*. Σε αυτή τη μορφή, εγκληματικός σκοπός του δράστη συνιστά το εγχείρημα της υποκλοπής μέσω μηνυμάτων των οικονομικών πληροφοριών του θύματος. Έτσι, προκειμένου να θεωρηθεί αξιόπιστη και έμπιστη η συνομιλία, οι παραβάτες διαμορφώνουν ένα ηλεκτρονικό περιβάλλον, που το άτομο το αναγνωρίζει ως την τράπεζα που εκείνο συναλλάσσεται και διατηρεί τραπεζικούς λογαριασμούς. (Αλεξανδροπούλου, 2007).

Από εκείνο το σημείο, οι δράστες ζητούν από το ανυποψίαστο θύμα να αποστείλει το όνομα χρήστη και τον κωδικό πρόσβασης, ώστε να επιβεβαιωθούν τα πρωτόκολλα ασφαλείας της τράπεζας. Με αυτόν τον τρόπο, υποκλέπτονται τα δεδομένα των χρηστών και εν συνεχεία οι δράστες μπορούν να μεταφέρουν τα χρήματα

που παρανόμως απέσπασαν από τους τραπεζικούς λογαριασμούς τους σε δικά τους προσωπικά και μη ανιχνεύσιμα μέρη (Reep-van den Bergh & Junger, 2018).

Επιπλέον, μια ακόμα μορφή ηλεκτρονικού εγκλήματος συνιστά και η πειρατεία λογισμικού, στην οποία οι παραβάτες επιχειρούν αν υποκλέψουν τα ηλεκτρονικά προγράμματα του υπολογιστή, προκειμένου να τα αξιοποιήσει για ιδιοτελείς σκοπούς, ή να τα εκμεταλλευτεί οικονομικά, πουλώντας τα σε τρίτους. Το μεγάλο ζήτημα που προκύπτει αποτελεί το γεγονός ότι κάθε ηλεκτρονικό σύστημα που νόμιμα κυκλοφορεί προς πώληση διαθέτει εξατομικευμένη άδεια χρήσης, η οποία λειτουργεί ως πιστοποιητικό του νόμιμου διανομέα και κατόχου κατά την έναρξη της διαδικασίας εγκατάστασής του στο υπολογιστικό σύστημα του αγοραστή. Σκοπός του δράστη αποτελεί η χειραγώγηση του κωδικού αυτού πιστοποίησης προκειμένου να αποκτήσει ο ίδιος την πλήρη πρόσβαση στο εμπορικά εκμεταλλεύσιμο δημιούργημα, προκαλώντας ανεπανόρθωτη ζημία στο θύμα, μιας και το τελευταίο χάνει τα οικονομικά οφέλη από τις αγορές του προϊόντος του (Αλεξανδροπούλου, 2007).

Κλείνοντας, με τον όρο *spamming* νοείται μια ακόμα μορφή διαδικτυακού εγκλήματος, στο πλαίσιο της οποίας ο δράστης αποστέλλει σε μεγάλο αριθμό ανυποψίαστων χρηστών, μηνύματα τα οποία λειτουργούν ως εμπορική, ανεπιθύμητη και απρόκλητη συρροή ηλεκτρονικών μηνυμάτων. Το πρόβλημα με τα συγκεκριμένα μηνύματα έγκειται στο γεγονός ότι τα θύματα δεν έχουν με κάποιον τρόπο ζητήσει την αποστολή των μηνυμάτων αυτών και δεν επιθυμούν να βρίσκονται σε επικοινωνία με τον αποστολέα τους. Το περιεχόμενό τους είναι συνήθως διαφημιστικού σκοπού ενημέρωσης των επίδοξων καταναλωτών, αλλά για προϊόντα και εταιρικές υπηρεσίες αμφίβολης ποιότητας και αξιοπιστίας. Το ζήτημα είναι ότι τα *spam mails* αποστέλλονται χωρίς την συγκατάθεση του καταναλωτή, με αποτέλεσμα να λειτουργούν ως έμμεση και κακόβουλη διαφήμιση προς όφελος των μεγάλων εταιριών που πληρώνουν υπέρογκα ποσά στις υπηρεσίες *spamming* για να βρίσκονται πάντα στο ηλεκτρονικό ταχυδρομείο των χρηστών (Reep-van den Bergh & Junger, 2018).

Καταλήγοντας, γίνεται εύκολα αντιληπτό ότι το διαδίκτυο έφερε στην επιφάνεια νέες μορφές επιτέλεσης παραδοσιακών εγκλημάτων αλλά οδήγησε και στην διαμόρφωση της αντικειμενικής υπόστασης νέων αυτοτελών παραβατικών συμπεριφορών, γεγονός που καθιστά τους χρήστες ευάλωτους σε πλήθος κακόβουλων δραστών, που είναι σε θέση με τις τεχνολογικές γνώσεις που κατέχουν να τον παραπλανήσουν και να τον καταστήσουν αντικείμενο οικονομικής, κυρίως, εκμετάλλευσης. Το ζήτημα είναι ιδιαίτερα ακανθώδες και χρήζει άμεσης επέμβασης

των διωκτικών αρχών του ηλεκτρονικού εγκλήματος, προκειμένου οι πολίτες να χρησιμοποιούν με ασφάλεια τα τεχνολογικά επιτεύγματα, χωρίς τον κίνδυνο που επισείει η ταπεινή δράση των εγκληματιών του κυβερνοχώρο (Αλεξανδροπούλου, 2007).

2.4 Το προφίλ εγκληματιών και τύποι ανηλίκων που βρίσκονται σε κίνδυνο

Το ζήτημα της ηλεκτρονικής τέλεσης εγκλημάτων είναι μια ακανθώδης προέκταση της προόδου της τεχνολογίας, μιας και ο νέος ψηφιακός κόσμος αποτέλεσε το έρεισμα για την δημιουργία και την κοινωνική διάγνωση νέων εγκληματικών μοντέλων, που είναι σε θέση να διαπράττουν τα αδικήματα με μικρότερο ρίσκο και μεγαλύτερη ανωνυμία (Grispos, 2019).

Πιο συγκεκριμένα, η τέλεση ενός διαδικτυακού εγκλήματος εμπεριέχει γνωρίσματα που το διαφοροποιούν από τα κοινά παραδοσιακά αδικήματα, γεγονός που γίνεται αντιληπτό τόσο από την ευκολία διάπραξής του όσο και από την διεύρυνση των πιθανών δραστών της ήδη εκτεταμένης «εγκληματικής σκακιέρας». Με άλλα λόγια, είναι εύκολα αντιληπτό ότι στα ψηφιακά εγκλήματα, οι δράστες δεν χρειάζεται να διαθέτουν ορισμένα τυπικά προσόντα, πέρα από την εξειδίκευση στην μεταχείριση και την ανώνυμη εκμετάλλευση του διαδικτυακού χώρου, γεγονός που δεν επιτρέπει στις διωκτικές αρχές να περιορίσουν σημαντικά τον κύκλο των υπόπτων και των εμπλεκόμενων προσώπων, αφήνοντας ανοιχτό το πεδίο για δράση ατόμων υπεράνω πάσης υποψίας (Reep-van den Bergh & Junger, 2018).

Παρόλα αυτά, το θέμα του κινήτρου των επίδοξων δραστών παραμένει ως ζήτημα, που λειτουργεί διευκολυντικά προς την δράση των αστυνομικών αρχών, προκειμένου να εξακριβώσουν τον γενεσιουργό παράγοντα της εγκληματικής έκρηξης των διαδικτυακών παραβατών. Είναι φυσικό, λοιπόν, επακόλουθο της δικαστικής και αστυνομικής ψυχολογίας, το γεγονός ότι η διαμόρφωση ενός εγκληματικού προφίλ και η σκιαγράφηση των εσωτερικών κινήτρων του δράστη είναι σε θέση να συμβάλλουν ώστε να κατανοηθεί ο τρόπος δράσης του και εν τέλει να αναζητηθούν τα κατασταλτικά μέτρα για την σύλληψή του και την διάνοιξη των δρόμων για την ποινική δικαιοσύνη (Grispos, 2019).

Αναλυτικότερα, οι δράστες των ηλεκτρονικών εγκλημάτων τείνουν να είναι ενεργοί στο πεδίο του διαδικτύου με βασικό κίνητρο την εκμετάλλευση της ανωνυμίας που προσφέρει ο κυβερνοχώρος προς το προσωπικό παραβατικό τους όφελος. Η ψηφιακή τεχνολογία για τους ίδιους αποτελεί το αναγκαίο μέγεθος προκειμένου να θέσουν σε λειτουργία τον εγκληματικό μηχανισμό και να προκαλέσουν τα μέγιστα δυνατά καταστροφικά αποτελέσματα σε όσο το δυνατόν μεγαλύτερο αριθμό θυμάτων (Reep-van den Bergh & Junger, 2018).

Οι δράστες αυτοί μπορούν να κατατμηθούν σε περαιτέρω κατηγορίες εγκληματικών προσωπικοτήτων ανάλογα με τις δικές τους προσωπικές δεξιότητες, τεχνολογικές γνώσεις και οικονομικούς πόρους. Με βάση, λοιπόν, αυτήν την κοινωνική και επιστημονική αλληλεπίδρασή τους με άτομα του εγκληματικού διαδικτυακού χώρου και εγκληματικές ηλεκτρονικές δράσεις, οι ψηφιακοί εγκληματίες μπορούν αν διακριθούν σε τρεις επιμέρους κατηγορίες (Grispos, 2019). Έτσι, μπορούν να αναγνωρισθούν ως δράστες μιας περίπλοκης παραβατικής πράξης, τα άτομα εκείνα που κατασκευάζουν τα εργαλεία που εγκυμονούν τους κινδύνους για τα θύματα, οι χρήστες αυτών, που εκμεταλλεύονται τα επεμβατικά συστήματα των κακόβουλων λογισμικών, και τέλος παρατηρείται και η κατηγορία των διαμορφωτών των προγραμμάτων που επιτρέπουν την αδικοπραξία σε βάρος ανυποψίαστων ατόμων (Ramdinmawii et al, 2014).

Οι λόγοι που ωθούνται σε τέτοιες παραβατικές συμπεριφορές πρέπει να αναζητηθούν στο χώρο των εσωτερικών κινήτρων τους και στην προσωπική τους κατανόηση για την κοινωνική πραγματικότητα. Πιο συγκεκριμένα, δεν είναι σπάνιες οι περιπτώσεις που οι ηλεκτρονικοί παραβάτες διακατέχονται από το «σύνδρομο του Ρομπέν των Δασών» (Robin Hood syndrome), όπου θέτουν τον εαυτό τους στο επίκεντρο των «καλών Σαμαρειτών» για τους λιγότερο προνομιούχους, και οραματίζονται ότι εκείνοι με τη δράση τους μπορούν να διαλευκάνουν τις κοινωνικές ανισότητες και την γενικότερη κοινωνική σήψη. Έτσι, στο δικό τους αξιακό σύστημα, τα αδικήματα που διαπράττουν είναι δικαιολογημένα και λειτουργούν ως αντίβαρο στην προσπάθεια των μεγάλων εταιρειών να συγκεντρώσουν ολιγαρχικά και μονοπωλιακά τα πλούτη. Με αυτόν τον τρόπο, ο δικός τους ρόλος, από την δική τους προοπτική, θεωρείται πολύ σημαντικός και οφείλουν να συνεχίσουν να διαπράττουν τα εγκλήματα μιας και με αυτόν τον τρόπο ανατρέπουν την καθεστηκυία τάξη των πραγμάτων (Ramdinmawii et al, 2014).

Ταυτόχρονα, τα κίνητρα επίσης πρέπει να αναζητηθούν και στα λιγότερα αλτρουιστικά ηθικά αντανακλαστικά τους. Η πλεονεξία και η φιλοκέρδεια είναι βασικοί λόγοι που τους ωθούν στην παραβατική συμπεριφορά μιας και καταστρώνουν το σχέδιο τους με βάση το τι μπορούν να αποκομίσουν οι ίδιοι από την περιουσιακή κατάσταση των θυμάτων τους. Με αυτόν τον τρόπο, αντικειμενικοποιούν τα θύματά τους ανάγοντάς τα σε αναγκαίο κακό για να πετύχουν τους ιδιοτελείς στόχους τους. Αυτό φαίνεται από το γεγονός ότι ο ανθρώπινος παράγοντας δεν υφίσταται, αλλά στην πραγματικότητα όταν βρίσκονται πίσω από την οθόνη των ηλεκτρονικών λογισμικών τους, το μόνο που αντιλαμβάνονται είναι αριθμητικές ακολουθίες αποδεσμευμένες από συναισθήματα και πραγματικά πρόσωπα. Εξαιτίας αυτής της κατάστασης, τα κίνητρά τους, όταν τρέφονται από την φιλοχρηματία τους, μπορούν να εξελιχθούν σε επικίνδυνα εργαλεία αποκτήνωσης και εξαγοράς των ηθικών τους αναστολών (Hargreaves & Prince, 2013).

Παράλληλα, το εγκληματικό προφίλ ορισμένων δραστών στοιχειοθετείται και από την αδυναμία τους να αντιληφθούν ότι οι πράξεις στις οποίες προβαίνουν, έχουν υπαρκτό αντίκτυπο στη ζωή άλλων ατόμων και ότι αυτές είναι σε θέση να επισείουν ευθύνες προς το πρόσωπό τους. Πιο αναλυτικά, οι ίδιοι, στην ψηφιακή πραγματικότητα που έχουν διαμορφώσει, όπου η αδρεναλίνη της εγκληματικής τους δράσης εντείνει την ανάγκη τους για συνέχιση του παραβατικού τους μοτίβου- σχεδίου, φτάνουν στο σημείο να αγνοούν την ζημία που προξενούν στα θύματά τους, και απεναντίας βάζουν ως προτεραιότητα την προσωπική οικονομική ωφέλειά τους (Grispos, 2019).

Ταυτόχρονα, όμως, η εγκληματική τους δράση μπορεί να οφείλεται και στην διαστρεβλωμένη εικόνα που έχουν διαμορφώσει για τον ίδιο τους τον εαυτό και τον ρόλο που διαδραματίζουν στην κοινωνία, ως προς την τεχνολογική τους επαγρύπνηση αλλά και την θεοποίηση των ηλεκτρονικών συστημάτων. Ειδικότερα, οι δράστες μπορεί να διακατέχονται από ένα αίσθημα υπεροχής σε σχέση με τον κοινό νομιμόφρονα πολίτη, αντιλαμβανόμενοι τον εαυτό τους και το έργο που επιτελούν, ως μια αβλαβή και αθώα ασχολία με την οποία εκείνοι καταπιάνονται (Hargreaves & Prince, 2013).

Στο εγκληματικό παρασκήνιο, φαίνεται ότι το προφίλ των εν λόγω διαδικτυακών δραστών στρέφεται περισσότερο στην ανάγκη τους να ηρωοποιήσουν τον εαυτό τους, διαστρεβλώνοντας τον κοινωνικό αντίκτυπο των εγκλημάτων τους. Έτσι, για τους ίδιους, λόγου χάριν, η εισβολή σε πληροφοριακά συστήματα επεξεργασίας προσωπικών δεδομένων δεν συνιστά μια ποινικά κολάσιμη πράξη, που επισύρει ποινές,

αλλά με βάση τη δική τους κατανόηση λειτουργεί ως θετικό το γεγονός ότι αποδεικνύουν στα θύματα ότι πρέπει να αυξήσουν τα επίπεδα της ασφάλειας που προστατεύουν τα ηλεκτρονικά τους δεδομένα (Ramdinmawii et al, 2014).

Δεν είναι βέβαια, σπάνιες οι περιπτώσεις που οι δράστες αναπτύσσουν εχθρικά και εκδικητικά συναισθήματα προς τα θύματα, κατηγορώντας τα για το γεγονός ότι δεν προστατεύουν πιο αποτελεσματικά τα προσωπικά τους στοιχεία και με αυτόν τον τρόπο τείνουν να δικαιολογούν ηθικά τις παραβατικές πράξεις της εισβολής στα πληροφοριακά συστήματα, και κατόπιν στον βανδαλισμό και την παραβίαση της εμπιστευτικότητας που τα τελευταία αξιώνουν. Τέλος, συχνά παρατηρείται το γεγονός ότι η τέλεση τέτοιων εγκλημάτων, στο πλαίσιό των οποίων, οι δράστες διατηρούν την ανωνυμία τους, μπορεί να προκύπτει και ως αντίδραση τους σε κοινωνικές και πολιτικές καταστάσεις και κακώς κείμενα της εποχής. Με αυτόν τον τρόπο, εκείνοι θεωρούν ότι εκφράζουν τον θυμό και την αγανάκτησή τους, αγνοώντας ότι στο ενδιάμεσο στάδιο βλάπτονται άτομα ή ακόμα και αδιαφορώντας για τον αρνητικό αντίκτυπο σε αυτά. Στην δική τους κατανόηση τα κίνητρά τους είναι αγωνιστικά και μπορούν να αιτιολογήσουν την προσβολή ορισμένων εννόμων αγαθών συμπολιτών τους (Grispos, 2019).

Από όλα τα παραπάνω προκύπτει αβίαστα το συμπέρασμα ότι τα κίνητρα των διαδικτυακών δραστών ποικίλουν και η αναζήτηση και ο προσδιορισμός τους είναι αναγκαία συνιστώσα για την ευκολότερη αναζήτηση και περιορισμό του κύκλου των υπόπτων τέλεσης αδικημάτων. Επιγραμματικά, αυτά φαίνεται να εξαντλούνται στον χώρο των μειωμένων ηθικών αναστολών και στην γενικότερη λαθεμένη αντίληψη του κοινωνικού περιγύρου και του εαυτού τους (Ramdinmawii et al, 2014).

Δεν μπορεί, βέβαια, να παραβλέψει κανείς το γεγονός ότι ο βαθμός της επικινδυνότητας της δράσης των ανώνυμων ηλεκτρονικών εγκληματιών και η πιθανότητα κλιμάκωσης των παραβατικών συμπεριφορών τους βρίσκονται σε άμεση συσχέτιση με τα κίνητρά τους (Hargreaves & Prince, 2013). Αν η ενασχόλησή τους με την αρνητική όψη του διαδικτύου οφείλεται κυρίως στο νεαρό της ηλικίας τους και στην ανάγκη τους να «διασκεδάσουν» ή να αναγνωρισθούν ως αυθεντίες των ηλεκτρονικών υπολογιστών, η παράνομη πρόσβασή τους στα έννομα αγαθά τρίτων μπορεί να τερματιστεί πιο ομαλά, χωρίς να δημιουργούνται περαιτέρω επίφοβες προεκτάσεις, διασώζοντάς τα από φανερή και ανεπανόρθωτη βλάβη (Grispos, 2019).

Από την άλλη, όμως όταν η κοινωνική υπόσταση των εννόμων αγαθών θυσιάζεται στο βωμό των προσωπικών οικονομικών και εκδικητικών κινήτρων, η

ωφέλεια που αποκομίζουν οι παραβάτες από την παραβίαση των προσωπικών δεδομένων των θυμάτων, πουλώντας τα σε τρίτους ή αξιοποιώντας τα αρνητικά οι ίδιοι, δημιουργεί ένα περιβάλλον αμφιβολίας και ανασφάλειας προς τους πολίτες, με ανυπολόγιστες συνέπειες για την κοινωνική συνοχή και ευημερία (Hargreaves & Prince, 2013).

Στον αντίποδα της εγκληματικής ψυχολογικής σκιαγράφησης των δραστών, έρχεται να προστεθεί το ζήτημα των ατόμων που πλήττονται κυρίως από την παραβατική συμπεριφορά. Στο πλαίσιο των εγκλημάτων που τελούνται μέσω διαδικτύου, τα άτομα που στοχοποιούνται, σε μεγαλύτερο βαθμό, ανήκουν στις ομάδες που κοινωνικά χαρακτηρίζονται ως ευπαθείς και χαίρουν μεγαλύτερο βαθμό προστασίας (Martellozzo & Jane, 2017).

Πιο συγκεκριμένα, θύματα επίδοξων δραστών καταλήγουν να είναι άτομα σε νεαρές ηλικίες. Οι ανήλικοι, λοιπόν, θεωρούνται συχνά ως αδύναμοι να υπερασπιστούν, αυτοτελώς, τον εαυτό τους, με αποτέλεσμα να κάνουν λάθος επιλογές και να αποτελούν εύκολη λεία των διαδικτυακών εγκληματιών. Ακριβώς επειδή, διανύουν μια περίοδο της ζωής τους που αναζητούν ακόμα στοιχεία της προσωπικότητάς τους, και η ωριμότητά τους προκύπτει εκ των υστέρων από εμπειρίες και λάθη που έχουν διαπράξει, οι παραβάτες θεωρούν ότι είναι οι ιδανικοί για εκμετάλλευση και για επιτέλεση σε βάρος τους των ηθικά ισχνών εγκληματικών τους δράσεων (Oksanen & Keipi, 2013).

Παράλληλα, ακόμα και στην συνειδητή εξερεύνηση ζητημάτων της σεξουαλικής τους ταυτότητας από τους νέους, οι ανώνυμοι δράστες του διαδικτύου είναι πιθανόν να δράξουν της εγκληματικής ευκαιρίας να παραβιάσουν και να σπιλώσουν την αγνότητα της σωματικής και ψυχικής ακεραιότητας των παιδιών, εκμεταλλευόμενοι την αθωότητα και την πνευματική ανωριμότητά τους (Näsi et al, 2015). Έτσι, ακριβώς επειδή το στάδιο της εφηβείας είναι ο χρόνος κατά τον οποίο τα παιδιά αρχίζουν να απομακρύνονται από τις συμβουλές και τις παραινέσεις των γονέων, επιχειρούν να ξεγλιστρήσουν από την κηδεμονική τους μέριμνα και να αναζητήσουν νέες εμπειρίες, χωρίς να αντιλαμβάνονται τον κίνδυνο που εγκυμονεί η απρόσεχτη αυτή στάση τους για τους ίδιους. Κατά συνέπεια, λοιπόν, η παιδική σκέψη τους και το αίσθημα της περιέργειας είναι σε θέση να τους ωθήσει σε λάθος επιλογές και ανθρώπους που μπορούν να επιδράσουν στο σώμα και στον ψυχισμό τους με βάση τα δικά τους ταπεινά και παραβατικά κίνητρα (Martellozzo & Jane, 2017).

Ταυτόχρονα, τα θύματα μπορεί να μην αντιληφθούν το γεγονός ότι θυματοποιούνται, ειδικά μάλιστα αν λάβει κανείς υπόψη ότι τα ανήλικα άτομα δεν διαθέτουν την ίδια κριτική σκέψη των ενηλίκων, απότοκο της κατανόησης ότι ο κόσμος δεν είναι ιδανικός και ότι υπάρχουν και άνθρωποι των οποίων η συμπεριφορά μπορεί αν είναι ύποπτη και ποινικά μεμπτή. Έτσι, άτομα μοναχικά ή συναισθηματικά ευάλωτα μπορούν να στοιχειοθετήσουν το προφίλ θύματος που κάποιος επίδοξος εγκληματίας θα στοχοποιήσει προκειμένου να επωφεληθεί, παρασέρνοντας με κενές υποσχέσεις και ψευδείς ελπίδες (Oksanen & Keipi, 2013).

Σε καμία περίπτωση, οι παραπάνω εφηβικές συμπεριφορές δεν μπορούν να λειτουργήσουν ως επιχείρημα υπέρ των δραστών, μιας και οι τελευταίοι είναι ο μόνος δεκτός λόγος που τα παιδιά δεν μπορούν να κάνουν «υπολογισμένα και ασφαλή λάθη», που θα τους δώσουν χρήσιμα μαθήματα για το μέλλον και δεν θα τραυματιστούν ανεπανόρθωτα από την παραβατική τους δράση. Κατά συνέπεια, λοιπόν, οι δράστες αναζητούν μονίμως τα άτομα εκείνα που λειτουργούν ως ο αδύναμος κρίκος και θα είναι πιο εύκολο να χειραγωγηθούν από τους ίδιους για να πραγματοποιήσουν τους ανήθικους σκοπούς τους. Δυστυχώς, στις πλείστες των περιπτώσεων, οι ανήλικοι εμπίπτουν στην ανωτέρω περιγραφή, καθιστώντας τους ευάλωτα θύματα για τους εγκληματίες και ειδικότερα εκείνους του διαδικτυακού χώρου, όπου η ανωνυμία τους καλύπτει τα ποταπά κίνητρά τους (Näsi et al, 2015).

2.5 Τα είδη διαδικτυακού εγκλήματος με επίκεντρο τα εγκλήματα κατά ανηλίκων

Σε συνέχεια της ανωτέρω ανάλυσης των ηλεκτρονικών εγκλημάτων, είναι αναγκαίο να αναφερθεί ότι τα διαδικτυακά εγκλήματα κατά των ανηλίκων θα πρέπει να αποτελούν ένα διακριτό κεφάλαιο μελέτης και χρήζουν ειδικής ανάλυσης.

Όπως προαναφέρθηκε οι ανήλικοι έχουν δικαίωμα στην πρόσβαση στο διαδίκτυο, γεγονός που τους αναγνωρίζεται και συνταγματικά, μέσω του δικαιώματός τους στην πληροφόρηση και την ελευθερία έκφρασης των άρθρων 2§1, 5, 5Α §1 και 2 και 14§1 του Συντάγματος. Επίσης, το δικαίωμά τους αυτό κατοχυρώνεται και σε ευρωπαϊκό επίπεδο από την Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του Ανθρώπου και από τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Σε διεθνές επίπεδο, το δικαίωμα

νομοθετείται μέσω της Διεθνούς Σύμβασης του ΟΗΕ για τα Δικαιώματα του Παιδιού και στο Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (Καϊάφα-Γκμπάντι, 2012).

Είναι χαρακτηριστικό ότι τα διαδικτυακά εγκλήματα κατά των ανηλίκων, μπορεί να αφορούν εγκλήματα κατά της γενετήσιας ελευθερίας τους, της περιουσίας και της τιμής τους. Τα τρία πιο διαδεδομένα εγκλήματα που τελούνται σε βάρος των ανηλίκων μέσω του Διαδικτύου, είναι εκείνα κατά της γενετήσιας ελευθερίας και πιο συγκεκριμένα, το έγκλημα της παιδικής πορνογραφίας, της διαδικτυακής προσέγγισης - άγρας ανηλίκων για γενετήσιους λόγους – grooming και της διαδικτυακής προσβολής της γενετήσιας αξιοπρέπειας. Είναι χαρακτηριστικό ότι τα περισσότερα εγκλήματα κατά των ανηλίκων αφορούν την γενετήσια ελευθερία και αξιοπρέπειας τους, δεδομένου ότι το Διαδίκτυο παρέχει πλέον στους παιδόφιλους εγκληματίες μεγαλύτερη ελευθερία κινήσεων στην εγκληματική τους δράση (Saini et al, 2012).

Παράλληλα, υπάρχουν και άλλα εγκλήματα που στρέφονται κατά των ανηλίκων, με κορωνίδα τους τον διαδικτυακό εκφοβισμό – cyber-bullying. Στην σύγχρονη εποχή, ο εκφοβισμός που παρατηρούνταν μεταξύ ανηλίκων στους σχολικούς χώρους, πλέον έχει μεταφερθεί στο Διαδίκτυο, όπου η ανωνυμία παρέχει μεγαλύτερη αποκτήνωση και γίνεται ευκολότερη η προσέγγιση των θυμάτων των εκφοβιστών (Καϊάφα- Γκμπάντι, 2012).

Τέλος, υφίστανται και διαδικτυακά εγκλήματα κατά της περιουσίας, όπως η απάτη κατά ανηλίκων, ενώ είναι διάχυτοι και οι κίνδυνοι λόγω της έλλειψη ασφάλειας στις καταναλωτικές τους συναλλαγές και της διαρροής των προσωπικών δεδομένων των ανηλίκων. Επίσης, είναι χαρακτηριστικός και η προσηλυτισμός σε προπαγανδιστικές απόψεις μίσους με ρατσιστικά, ομοφοβικά και σεξιστικά κίνητρα (*hate speech*) (Saini et al, 2012).

Είναι αναγκαίο να αναφερθεί ότι ο ποινικός νομοθέτης, σε όλα σχεδόν τα δίκαια ανά την υφήλιο, έχει προβλέψει ειδικές διατάξεις για την προστασία των ανηλίκων. Στο ελληνικό ποινικό δίκαιο, ο νομοθέτης δεν στηρίζεται στον ορισμό της ανηλικότητας κατά το αστικό δίκαιο, που ορίζεται μετά το πέρας των 18 χρόνων και που σχετίζεται περισσότερο με την ενηλικίωση και το πέρας της σχολικής ζωής, αλλά ασπάζεται τα διδάγματα της ψυχολογίας και την σεξουαλική εξέλιξη των παιδιών. Έτσι, στα ποινικά εγκλήματα κατά των ανηλίκων στο πεδίο της γενετήσιας ζωής τους, κάνει λόγο για ανηλίκους κάτω των 15 ετών (Καϊάφα- Γκμπάντι, 2012).

Στη συνέχεια θα αναλυθούν τα σημαντικότερα εγκλήματα κατά των ανηλίκων, τα οποία έχουν ως μέσο τέλεσης το Διαδίκτυο.

2. 6 Η παιδική πορνογραφία ως διαδικτυακό έγκλημα

Αρχικά, ο όρος «πορνογραφία» εμφανίστηκε και ορίστηκε κατά το 1857 από το λεξικό της Οξφόρδης, ακολουθώντας τις προτάσεις της γαλλικής κουλτούρας και αναφέρεται συνολικά στην πορνεία σε συνδυασμό με την αισχρολογία και τις άσεμνες εικόνες. Η πορνογραφία ενηλίκων διακρίνεται από εκείνη των ανηλίκων δεδομένου ότι η δεύτερη αποτελεί ποινικά κολάσιμο αδίκημα, λόγω της σεξουαλικής εκμετάλλευσης ή της σεξουαλικής κακοποίησης παιδιών, όπως θα αναλυθεί και στο οικείο κεφάλαιο.

Κατά το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελλάδος και από τον ελληνικό ποινικό κώδικα, η παιδική πορνογραφία ορίζεται ως *«η αποτύπωση με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς»* (Δίωξη Ηλεκτρονικού εγκλήματος, χ.χ.).

Έτσι, κατά το άρθρο 348^{A} στην παρ.3 «*Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων συνιστά η αναπαράσταση ή η πραγματική ή η εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής γενετήσιας πράξης που διενεργείται από ή με ανήλικο.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Παράλληλα, σύμφωνα με το άρθρο 121 του ποινικού κώδικα, «*1. Στο κεφάλαιο αυτό με τον όρο ανήλικοι νοούνται αυτοί που κατά τον χρόνο τέλεσης της πράξης έχουν ηλικία μεταξύ του δωδέκατου και του δέκατου όγδοου έτους της ηλικίας τους συμπληρωμένων.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Το έγκλημα αυτό τυποποιείται στον ποινικό κώδικα λόγω του ότι τα παιδιά πρέπει να προστατεύονται από κακόβουλες σεξουαλικές ενέργειες εναντίον του, λόγω της αδυναμίας τους να παρέχουν συναίνεση. Τα παιδιά βρίσκονται σε ηλικία που δεν γνωρίζουν ή δεν κατανοούν τους κινδύνους των πράξεων αυτών, δεν διαθέτουν την κατάλληλη εκπαίδευση και δεν είναι σε θέση να συμμετέχουν ισότιμα. Άλλωστε τα

παιδιά στις ηλικίες αυτές δεν διαθέτουν πλήρη δικαιοπρακτική ικανότητα, που οδηγεί στο συμπέρασμα ότι και για το νομοθέτη του Αστικού Κώδικα, δεν είναι σε θέση να συμμετέχουν πλήρως στις συναλλαγές, λόγω της ηλικίας και της πνευματικής τους ανάπτυξης. Έτσι, ένα άτομο που δεν έχει δικαιοπρακτική ικανότητα και δεν είναι σε θέση να ψηφίζει σε εκλογικές διαδικασίες, να είναι δυνατόν να μπορεί να συγκαταθέσει σε σεξουαλική πράξη και κυρίως στην καταγραφή και τη διανομή της (Καϊάφα-Γκμπάντι, 2012).

Σύμφωνα με τη Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, η παιδική πορνογραφία μπορεί να λάβει τις εξής μορφές: πρώτον, να συμμετέχει ένας ανήλικος σε σεξουαλική δραστηριότητα. Δεύτερον, όταν ένα άτομο που συμμετέχει σε σεξουαλική δραστηριότητα και προσποιείται ότι είναι ανήλικο. Τέλος, όταν αποδίδονται αληθοφανείς εικόνες αναπαράστασης ανηλίκου που συμμετέχει σε σεξουαλικές δραστηριότητες (Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης, χ.χ.).

Τα κυκλώματα παιδοφιλίας λόγω της αυστηρής νομοθετικής ρύθμισης για την παιδική πορνογραφία σε όλες σχεδόν τις έννομες τάξεις, έχουν βρει πρόσφορο έδαφος στην ανωνυμία του διαδικτύου. Έτσι, μέσω Διαδικτύου μπορούν να εργάζονται σε διαφορετικές χώρες με διαφορετικές νομοθεσίες, με σκοπό τη συλλογή και διανομή πορνογραφικού υλικού προς δικό τους κέρδος ή ακόμα και για δική τους ικανοποίηση (Δίωξη Ηλεκτρονικού εγκλήματος, χ.χ.).

Παράλληλα, υπάρχουν διαδικτυακά *fora* με συμβουλές για την αποφυγή ανίχνευσης και για την καλύτερη ενορχήστρωση των εγκλημάτων κατά των ανηλίκων. Τέλος, στην σύγχρονη εποχή με την ταχύτατη εξάπλωση του διαδικτύου και στις νεαρότερες ηλικίες, πολλά παιδιά μπορεί να γίνουν θύματα παιδόφιλων μέσω του Διαδικτύου, ενώ αυτό αποτελεί πρόσφορο έδαφος και για τους εγκληματίες, καθώς η ανωνυμία του δίνει τη δυνατότητα να συνομιλήσουν και να παρασύρουν μικρά παιδά με μεγαλύτερη ευκολία. Μάλιστα, συνήθως αναπτύσσουν φιλικές σχέσεις με τα παιδιά και παρουσιάζονται ως ακίνδυνοι, προκειμένου να τα πείσουν να μοιραστούν πιο προσωπικές φυτογραφίες τους, τις οποίες είτε αξιοποιούν οι ίδιοι είτε διανέμουν μέσω του Διαδικτύου. Επομένως, στην σύγχρονη εποχή, η εύκολη πρόσβαση των ανηλίκων στο Διαδίκτυο τους καθιστά εύκολα θύματα της διαδικτυακής παιδικής πορνογραφίας (Δίωξη Ηλεκτρονικού εγκλήματος, χ.χ.).

2.7 Η Προσέλκυση παιδιών για γενετήσιους λόγους - Η Διαδικτυακή αποπλάνηση *(grooming)*

Όπως αναλύθηκε και ανωτέρω, τα παιδιά στο Διαδίκτυο είναι πιο εύκολα θύματα σεξουαλικών εγκλημάτων. Ένα ακόμη έγκλημα στο οποίο είναι αρκετά ευάλωτα μέσω του Διαδικτύου είναι και η προσέλκυση παιδιών για γενετήσιους λόγους ή διαδικτυακή αποπλάνηση – *grooming* (Ngejane et al, 2018).

Στο ελληνικό ποινικό δίκαιο, στο άρθρο 348Β για την «Προσέλκυση παιδιών για γενετήσιους λόγους» *«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 παρ. 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Το φαινόμενο του *grooming* έχει διαπιστωθεί ότι ασκεί επιρροή τόσο σε σωματικό, όσο και σε ψυχολογικό επίπεδο στο ανήλικο θύμα, την οποία ίσως δεν είναι σε θέση να αντιληφθεί κατά την στιγμή τέλεσης του εγκλήματος αλλά υποσυνείδητα το επηρεάζει για την υπόλοιπη ζωή του. Βασικός στόχος του θύτη είναι η «απευαισθητοποίηση» του παιδιού ή *desensitation,* όπως είναι γνωστή στη διεθνή βιβλιογραφία, ώστε να το πείσει ότι είναι σε θέση σωματικά και ψυχολογικά να μετέχει σε μία σεξουαλική πράξη. Με άλλα λόγια, η διαδικασία του *grooming* έχει ως στόχο τη μείωση των φυσικών αναστολών του ανήλικου θύματος, με την αξιοποίηση ψυχολογικών τεχνικών επιβολής ελέγχου και άσκησης εξουσίας, με την χρήση μεθόδων ανάπτυξης συναισθηματικού δεσμού με το δράστη και χειραγώγησης του θύματος (Καϊάφα- Γκμπάντι, 2012).

Στο σύγχρονο διαδίκτυο, η κυρίαρχη μέθοδος προσέγγισης των παιδιών είναι η περιήγηση και η δημιουργία προφίλ των επίδοξων δραστών στα διάφορα μέσα κοινωνικής δικτύωσης ή και σε σελίδες διαδικτυακών παιχνιδιών, λόγω της πληθώρας ανηλίκων σε αυτά. Στα μέσα αυτά, οι θύτες *groomers* εντοπίζουν τα θύματά τους, και εκμεταλλεύονται την ανάγκη των παιδιών να εμφανίζονται ως δημοφιλή στους συνομηλίκους τους, με την αύξηση των «φίλων» *friends*, των «ακολούθων» *followers* και την επικοινωνία με πολλούς ανθρώπους μέσω μηνυμάτων «*direct messages*». Επίσης, οι φωτογραφίες των ανηλίκων ανεβαίνουν πλέον στα προσωπικά τους προφίλ

από τους ίδιους και χωρίς έλεγχο των γονέων, οπότε είναι πλέον πιο εύκολος ο εντοπισμός των θυμάτων από τους θύτες. Έτσι, στην σύγχρονη εποχή οι *groomers* δεν συχνάζουν πλέον σε προαύλια σχολείων και σε παιδικές χαρές, όπου ήταν και ευκολότερος ο εντοπισμός τους από τις αρχές και τους γονείς, αλλά μέσα στο σπίτι του κάθε παιδιού μέσω του Διαδικτύου (Ngejane et al, 2018).

Το πρώτο πράγμα που θα κάνει ένας *groomer* είναι η δημιουργία κλίματος εμπιστοσύνης και συνεργασίας με το παιδί, με σκοπό να το πείσει για τον τελικό σκοπό του, που είναι η συνάντηση και η τελική σεξουαλική κακοποίηση του παιδιού. Παρουσιάζεται δηλαδή ως κοινό μυστικό, που μπορούν να μοιράζονται μόνο οι δύο τους, και καθώς αναπτύσσεται η σχέση αυτή το παιδί επιθυμεί να είναι αρεστό στον θύτη και να ικανοποιεί τις απαιτήσεις του. Ωστόσο, όπως θα καταδειχθεί και στη συνέχεια, στο πλαίσιο της διαδικασίας του *grooming*, πολλοί θύτες αξιοποιούν τα δώρα και διάφορα ωφελήματα, με σκοπό να εξασφαλίσουν την σιωπή και την υπακοή του θύματος, ενώ σε πιο ακραίες περιπτώσεις μπορεί να αξιοποιήσουν απειλές εναντίον του ίδιου του παιδιού ή της οικογένειάς του. Σε κάθε περίπτωση, στο έγκλημα αυτό, ο δράστης έχει ως σκοπό να δημιουργήσει μία σχέση εξουσίαση με το παιδί, ενώ το θύμα αισθάνεται φόβο, σύγχυση και αμηχανία, μέχρι να φτάσει στον τελικό σκοπό του που είναι η σεξουαλική κακοποίηση (O'Connell, 2003).

Κατά τον O'Connell, (2003), ο οποίος κωδικοποίησε τον τρόπο δράσης ενός τέτοιου εγκληματία, τα στάδια του εγκλήματος αυτού είναι τα εξής: Πρώτο στάδιο είναι η «Ανάπτυξη φιλικής σχέσης ή *Friendship Forming*», κατά το οποίο ο *groomer* προσπαθεί να δημιουργήσει μία φιλική σχέση με το παιδί, ανταλλάσσοντας και συλλέγοντας προσωπικές πληροφορίες και καθοδηγώντας το να μοιράζεται μόνο μαζί του εμπειρίες και φωτογραφίες της καθημερινότητάς του (Ngejane et al, 2018). Το στάδιο αυτό είναι αρκετά επικίνδυνο γιατί το παιδί δεν υποψιάζεται τις προθέσεις του θύτη, καθώς οι φωτογραφίες και τα θέματα που συζητούνται στο στάδιο αυτό δεν είναι σε καμία περίπτωση σεξουαλικής φύσης (O'Connell, 2003).

Κατά το δεύτερο στάδιο, που ορίζεται ως «Διαμόρφωση σχέσης ή *Relationship Forming*», ο θύτης προσπαθεί να προχωρήσει την σχέση που είχε ήδη διαμορφώσει στο προηγούμενο στάδιο με το παιδί, δημιουργώντας του την πεποίθηση ότι αυτός είναι ο καλύτερος του φίλος (Speed, 2021). Προκειμένου να το επιτύχει αυτό, ο *groomer* συλλέγει μέσα από τις συζητήσεις πληροφορίες που αφορούν στο οικογενειακό περιβάλλον του παιδιού, την καθημερινότητα του, στο σχολείο, τους φίλους και τις δραστηριότητές του (O'Connell, 2003).

Κατά το τρίτο στάδιο, που ονομάζεται «Εκτίμηση Κινδύνου - *Risk Assessment*», το οποίο είναι από τα σημαντικότερα της διαδικασίας, ο *groomer* εξετάζει τις πιθανότητες αποκάλυψης της δράσης του, ελέγχοντας το περιβάλλον του παιδιού, την οικογένεια και τους φίλους του και την ασφάλεια του υπολογιστή που χρησιμοποιεί το θύμα, προκειμένου να ελέγξει τις πιθανότητες ανακάλυψης της δράσης του από τους γονείς του ανηλίκου. Με άλλα λόγια, εξετάζει με προσοχή τις κινήσεις του θύματος και υπολογίζει τη δράση του προκειμένου να ελαχιστοποιήσει κατά το δυνατό τις πιθανότητες σύλληψης του από την οικογένεια του ανηλίκου και τελικά από τις αρχές (O'Connell, 2003).

Επίσης, στο τέταρτο στάδιο, στην «Αποκλειστικότητα - *Exclusivity*», ο θύτης έχει διαμορφώσει μία πολύ δυνατή σχέση εμπιστοσύνης με το παιδί, πείθοντάς το ότι τους συνδέουν ισχυροί δεσμοί και ότι μόνο αυτός είναι σε θέση να το κατανοήσει σε βάθος, απομακρύνοντας το ψυχολογικά από τους γονείς και το υπόλοιπο φιλικό περιβάλλον του (Speed, 2021). Έτσι, το θύμα καταλήγει να τον εμπιστεύεται τυφλά και να μοιράζεται τους φόβους και τις ανησυχίες του μόνο με αυτόν, με αποτέλεσμα ο θύτης να το έχει εγκλωβίσει με μαεστρία στην σχέση αυτή και να το απομακρύνει από τους οικείους του, οι οποίοι πιθανότατα να μπορούσαν να το βοηθήσουν (O'Connell, 2003).

Καθώς προχωρά η εγκληματική δράση, φτάνει πλέον στο «Σεξουαλικό Στάδιο - *Sexual Stage*», κατά το οποίο ο *groomer* αρχίζει να εισφέρει σταδιακά πλέον στην συζήτηση σεξουαλικές συνομιλίες και σεξουαλικού περιεχομένου λεξιλόγιο, προκειμένου να εισαγάγει το παιδί ομαλά στο επόμενο και τελευταίο στάδιο, που είναι η «Υλοποίηση των Φαντασιώσεων - *Fantasy Enactment»*. Στο τελικό αυτό στάδιο ο δράστης του *grooming* πλέον εισαγάγει τις καθαρά σεξουαλικής φύσεως δραστηριότητες, είτε διαδικτυακά είτε με συνάντηση πρόσωπο με πρόσωπο, είτε με πειθώ είτε με εξαναγκασμό και απειλή. Επομένως, στο στάδιο αυτό, πλέον, περιγράφονται στο παιδί και υλοποιούνται, χωρίς περιστροφές, οι σεξουαλικές φαντασιώσεις του *groomer* (O'Connell, 2003).

Είναι χαρακτηριστικό ότι και ο νομοθέτης, έχει διακρίνει την ευαλωτότητα των ανηλίκων, η οποία στο Διαδίκτυο είναι διπλή. Από τη μία, οι παιδόφιλοι εγκληματίες και από την άλλη το Διαδίκτυο, το οποίο προσέφερε στην ήδη δυσεπίλυτη δράση τους το προκάλυμμα της ανωνυμίας (Speed, 2021). Έτσι, τα παιδιά παλαιότερα θα αντιμετώπιζαν παλαιότερα κινδύνους από ενήλικους παραβάτες στο πλαίσιο της σχολικής αυλής ή ενός πάρκου, στο οποίο θα μπορούσαν να επέμβουν οι γονείς ή οι δάσκαλοί τους. πλέον στο αχανές περιβάλλον του διαδικτύου, είναι ιδιαίτερα δύσκολο

ακόμα και για τη Δίωξη Ηλεκτρονικού Εγκλήματος να εντοπίσει τους εγκληματίες κατά των ανηλίκων ή να ανακόψει τη ροή των δεδομένων που αυτοί διακινούν, δεδομένου ότι ισχύει ο κανόνας ότι στο Διαδίκτυο κανένα δεδομένο δεν σβήνεται ποτέ οριστικά (Καϊάφα- Γκμπάντι, 2012).

2.8 Η Διαδικτυακή προσβολή της γενετήσιας αξιοπρέπειας

Κατά το άρθρο 337 ΠΚ «*3. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλων μέσων ή τεχνολογιών πληροφορικής αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δέκα πέντε έτη και με χειρονομίες ή προτάσεις, προσβάλλει την τιμή του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν επακολούθησε συνάντηση ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.*» (Ποινικός Κώδικας, Νόμος 4619/2019).

Πρόκειται για την ποινική κωδικοποίηση της ηπιότερης μορφής σεξουαλικής προσβολής κατά του ανηλίκου, το οποίο εξελίχθηκε προκειμένου να συμπεριλάβει και τις νεότερες μορφές της, οι οποίες πραγματοποιούνται μέσω του διαδικτύου. Η διαδικτυακή αυτή προσβολή του ανηλίκου τελείται μόνο από ενήλικο, που έχει δηλαδή συμπληρώσει το 18^{ο} έτος της ηλικίας του και αφορά θύματα που είναι νεαρότερα των 15 ετών. Είναι μία σύνθετη εγκληματική συμπεριφορά στην οποία ο θύτης αποκτά επαφή μέσω του διαδικτύου ή άλλου μέσου επικοινωνίας με το θύμα και να έχει προβεί σε ασελγείς χειρονομίες ή προτάσεις, οι οποίες προσβάλλουν την τιμή του ανηλίκου στο πεδίο της γενετήσιας ζωής του (Καϊάφα- Γκμπάντι,2012).

Έτσι, για να θεωρηθεί ότι υπάρχει το διαδικτυακό αυτό έγκλημα δεν μπορεί να τελείται μέσω συμβατικών μεθόδων επικοινωνίας όπως το τηλέφωνο ή η αλληλογραφία, και σχετίζεται κυρίως με το γεγονός ότι η σχέση που δημιουργείται ανάμεσα στα δύο μέρη είναι τέτοιου βαθμού ώστε ο θύτης να είναι σε θέση να επηρεάσει το ανήλικο θύμα και να του απευθύνει τις ασελγείς χειρονομίες ή τις προτάσεις που απαιτούνται ή ακόμα και να το πείσει να συναντηθούν, το οποίο συνιστά νομικά μία επιβαρυντική περίσταση (Speed, 2021).

Δεδομένου ότι το έγκλημα τελείται διαδικτυακά, το περιεχόμενο των ασελγών χειρονομιών και προτάσεων θα πρέπει να γίνεται μέσω του διαδικτύου και δεν περιλαμβάνει σωματική επαφή .Έτσι, ως ασελγείς χειρονομίες νοούνται κυριολεκτικά

οι κινήσεις των χεριών του θύτη σχετικά με ασελγείς πράξεις, ενώ οι ασελγείς προτάσεις είναι προτάσεις που αφορούν στην τέλεση ασελγών πράξεων (Συμεωνίδου-Καστανίδου, 2020).

Αυτό που συνιστά κατά το νόμο επαυξημένο αξιόποινο για τον δράστη είναι η τελική συνάντηση με τον ανήλικο, δεδομένου ότι η επαφή από κοντά συνιστά μεγαλύτερο κίνδυνο για το θύμα. Πιο συγκεκριμένα, η συνάντηση μεταξύ του δράστη και του θύματος θα πρέπει να βρίσκεται σε αιτιώδη σχέση με τη διαδικτυακή επαφή και προσβολή της γενετήσιας αξιοπρέπειας και να έχει προκληθεί από αυτήν. Η συνάντηση αυτή θα πρέπει να είναι προσυμφωνημένη και να έχει καθοριστεί μία συγκεκριμένη ώρα και ένα ορισμένο μέρος συνεύρεσης, στο οποίο θα είναι δυνατή η επικοινωνία μεταξύ του δράστη και του θύματος. Επομένως, το έγκλημα αυτό κατά των ανηλίκων είναι ηπιότερο και συνήθως αποτελεί προστάδιο και προθάλαμο για τα δύο προηγούμενα εγκλήματα της παιδικής πορνογραφίας και της προσέλκυσης παιδιών για γενετήσιους λόγους (Καϊάφα- Γκμπάντι,2012).

2.9 Ο Διαδικτυακός εκφοβισμός (*cyber-bullying*): ερμηνεία της έννοιας και είδη εκφοβισμού

Το φαινόμενο του «Διαδικτυακού εκφοβισμού ή *Cyber bullying*» θεωρείται ως μία εξελιγμένη και πιο σύγχρονη μορφή του εκφοβισμού, η οποία έχει λάβει ποικίλες μορφές μέσω των εξελιγμένων τεχνολογιών επικοινωνίας, δηλαδή μέσω του διαδικτύου και των κινητών τηλεφώνων. Είναι ιδιαίτερα διαδεδομένο φαινόμενο στις μαθητικές κοινότητες και αφορά κυρίως τους ανήλικους χρήστες του Ιντερνέτ χωρίς να σημαίνει ότι αποκλείεται να ασκείται και σε ενηλίκους. Το φαινόμενο αυτό σχετίζεται κυρίως με την παρενόχληση και τον εκφοβισμό, με την ταπείνωση και τις απειλές σε βάρος των ατόμων κυρίως νεαρής ηλικίας. Αφορά δηλαδή κυρίως την ψυχολογική βία με την χρήση του Διαδικτύου, των κινητών τηλεφώνων και άλλων ψηφιακών τεχνολογιών. Η μορφή διαδικτυακής επίθεσης ασκείται συνήθως από ανηλίκους σε βάρος συνομηλίκων τους, δεδομένου ότι όταν στο φαινόμενο μετέχουν ενήλικοι, τότε παίρνει τη μορφή της διαδικτυακής παρενόχλησης και όχι του εκφοβισμού (King, 2010).

Πιο αναλυτικά, οι κυριότερες μορφές διαδικτυακού εκφοβισμού είναι οι εξής: Αρχικά, η «Παρενόχληση» είναι η πλέον χαρακτηριστική και αφορά την συνεχόμενη

αποστολή προσβλητικών ή ακόμα και απειλητικών μηνυμάτων μέσω του Διαδικτύου, με την χρήση μηνυμάτων στα μέσα κοινωνικής δικτύωσης, μέσω *e-mail*, ή σε διαδικτυακά «fora» ή παιχνίδια. Όπως είναι λογικό, το σύνολο αυτών των επιθέσεων μπορεί να επηρεάσει αρνητικά την ψυχική κατάσταση κάθε ανηλίκου, σε μία φάση της ψυχοκοινωνικής τους ανάπτυξης ή οποία είναι ήδη ταραχώδης με έντονες διακυμάνσεις συναισθημάτων (Kowalski et al, 2012).

Η πιο σοβαρή μορφή της παρενόχλησης είναι το λεγόμενο *Cyber stalking* ή αλλιώς Διαδικτυακή καταδίωξη. Στην περίπτωση αυτή ο θύτης εξαπολύει κατά του θύματος του επίμονες απειλές και παρουσιάζει καταδιωκτικές συμπεριφορές χρησιμοποιώντας το Διαδίκτυο. Πρόκειται για έντονες επιθετικές συμπεριφορές, όπως η βία και ο εκφοβισμός ή η παρακολούθηση (Mishna et al, 2012).

Παράλληλα, μία μορφή εκφοβισμού που ανθεί μέσω του Διαδικτύου λόγω της ανωνυμίας και του μηδαμινού ελέγχου των χρηστών του είναι η πλαστοπροσωπία. Το έγκλημα αυτό πραγματώνεται με την χρήση μιας πλαστής ταυτότητας, όπως το όνομα ενός γνωστού προσώπου, ώστε είτε να αξιοποιήσει το όνομα αυτό ως προσωπείο για να εξαπολύσει απειλές και ύβρεις σε βάρος ενός άλλου προσώπου ή να εκμαιεύσει πληροφορίες, είτε, αν έχει υποκλέψει τους κωδικούς και το όνομα του θύματος, να αποστέλλει σε άλλους, γνωστούς του θύματος, μηνύματα προσποιούμενος ότι είναι το θύμα, διαλύοντας έτσι τις φιλικές και οικογενειακές σχέσεις του θύματος. Τέλος, σε ακραίες μορφές του εγκλήματος αυτού, ο θύτης μπορεί να έχει αλλάξει εντελώς τον κωδικό του θύματος και να το εμποδίζει εντελώς από το να αποκτήσει πρόσβαση στο λογαριασμούς του (Kowalski et al, 2012).

Παράλληλα, ο εκφοβισμός μπορεί να λάβει τη μορφή της δυσφήμισης του θύματος μέσω του διαδικτύου. Στη μορφή αυτή, ο θύτης αποστέλλει σε άλλους χρήστες προσωπικά δεδομένα με τη μορφή βίντεο και φωτογραφιών, τις οποίες έχει μοιραστεί το θύμα με το θύτη χωρίς να έχει δώσει άδεια για τη διανομή τους σε τρίτους. Στη πιο ακραία περίπτωση, αυτή η μορφή εκφοβισμού αφορά υλικό σεξουαλικού περιεχομένου, το οποίο διανέμεται χωρίς την συγκατάθεση του θύματος (Mishna et al, 2012).

Τέλος, μία σημαντική μορφή εκφοβισμού είναι και ο αποκλεισμός του θύματος από διαδικτυακές ομάδες συνομιλίας με φίλους ή από τα διαδικτυακά δωμάτια επικοινωνίας στα παιχνίδια. Ο διαδικτυακός αποκλεισμός όπως και αυτός στην πραγματική ζωή αποτελεί ένα βαρύ πλήγμα για τους ανηλίκους, δεδομένου ότι

επιθυμούν να είναι μέρος της ευρύτερης ομάδας και να μην περιθωριοποιούνται (Kowalski et al, 2012).

Είναι χρήσιμο πριν ολοκληρωθεί η ανάλυση του εκφοβισμού μέσω Διαδικτύου να αναφερθούν τα γενικότερα χαρακτηριστικά ενός θύτη. Αρχικά, οι θύτες παρουσιάζουν αυτοπεποίθηση και έντονα κυριαρχική προσωπικότητα, κάτω από την οποία όμως κρύβεται ένα άτομο με ανασφάλειες και προβλήματα, τα οποία εκδηλώνει με τον εκφοβισμό όσων θεωρεί ως κατώτερους. Παράλληλα, σε αρκετές περιπτώσεις, τα άτομα αυτά παρουσιάζουν και βιαιότητα και εκρήξεις θυμού. Στις περισσότερες περιπτώσεις η διαδικτυακή επίθεση σε άλλους ανηλίκους αντικατοπτρίζεται και σε επιθετικότητα και εκφοβισμό και στην πραγματική ζωή. Επίσης, τα άτομα αυτά αδυνατούν να υπακούσουν σε κανόνες και καταφέρονται επιθετικά και κατά των ενηλίκων, που προσπαθούν να τους εφαρμόσουν. Σε κάθε περίπτωση, όμως, έχουν τη δυνατότητα να ξεφεύγουν από τέτοιες καταστάσεις λόγω της ευγλωττίας τους. πρόκειται συνήθως για άτομα με έντονα προβληματικό οικογενειακό περίγυρο, με θυμό για την ζωή τους, τον οποίο εκδηλώνουν σε άλλους (Mishna et al, 2012).

2.10 Η προπαγάνδα μίσους στο διαδίκτυο (*hate speech*)

Το διαδίκτυο αποτελεί έναν κυκεώνα πληροφοριών, όπου ο κάθε χρήστης έχει την ευκαιρία να εκφράσει την γνώμη του με μηδαμινό ή πολλές φορές ανύπαρκτο έλεγχο. Όπως είναι λογικό, στο περιβάλλον αυτό έχει ανθίσει κατά τις τελευταίες δεκαετίες η λεγόμενη ρητορική μίσους ή *hate speech*. Η ρητορική αυτή στο διαδίκτυο είναι κοινωνικοπολιτικό φαινόμενο, του οποίου τα αίτια μπορούν να αναζητηθούν σε ποικίλους παράγοντες. Ορίζεται ως ο λόγος εκείνος, ο οποίος αναπαράγει με επιθετικό τρόπο στερεοτυπικές απόψεις σε βάρος ομάδων ανθρώπων που καταπιέζονται κοινωνικά λόγω του φύλου τους, της καταγωγής τους, της θρησκείας τους ή του σεξουαλικού τους προσανατολισμού (Waldron, 2012).

Η ρητορική μίσους θα πρέπει να διακρίνεται από τον εκφοβισμό – *bullying*, δεδομένου ότι η μεν πρώτη απευθύνεται σε βάρος μία ομάδας ανθρώπων και στα άτομα που την αποτελούν, ενώ ο δεύτερος έχει ως στόχο ένα συγκεκριμένο άτομο. Βέβαια, σε αρκετές περιπτώσεις η στοχοποίηση του ατόμου στον ατομικό εκφοβισμό βασίζεται στα γενικότερα αίτια απαξίωσης της ευάλωτης κοινωνικής ομάδας στην οποία ανήκει το άτομο αυτό (Bakalis, 2015).

Επειδή, επομένως, το Διαδίκτυο επιτρέπει την ελεύθερη διακίνηση των ιδεών κάθε ανθρώπου, ο λόγος που υποκινεί βία και μίσος εναντίον μίας κοινωνικής ομάδας ανθεί στην εποχή μας. Όσον αφορά του ανηλίκους, αυτοί μπορεί να πληγούν από το φαινόμενο αυτό σε ένα διττό σχήμα: Από τη μία, μπορεί ο ανήλικος να ενταχθεί σε ομάδα που διακινεί αυτές τις ιδέες μίσους σε βάρος άλλων ανθρώπων. Έτσι, σε μία τρυφερή ηλικία, ο ανήλικος μπορεί να δηλητηριαστεί μέσω του Διαδικτύου από τη μισαλλοδοξία και να επεκταθεί και σε πράξεις βίας στην πραγματική ζωή. Είναι χαρακτηριστικές οι επιθέσεις σε βάρος ευάλωτων κοινωνικών ομάδων που οργανώνονται μέσω του Διαδικτύου και μπορεί να οδηγήσουν σε τραυματισμούς ακόμη και θάνατο ανθρώπων. Συνεπώς, ένας ανήλικος χωρίς κριτική σκέψη μπορεί να επηρεαστεί εύκολα από ρητορικές με ρατσιστικό, ομοφοβικό ή σεξιστικό περιεχόμενο, οδηγώντας τον να μισεί κάτι που τυχαία δεν είναι και ο ίδιος (Waldron, 2012).

Από την άλλη, η ρητορική μίσους μπορεί να επηρεάσει τους ανηλίκους και ως θύματά της. Με άλλα λόγια, η ρητορική μίσους μπορεί να απευθύνεται κατά των ανηλίκων, οι οποίοι υπάγονται στις κατηγορίες και στα χαρακτηριστικά που έχουν θέσει οι θύτες και κατά των οποίων στρέφουν το μίσος τους. έτσι, οι ανήλικοι μπορεί να έρθουν αντιμέτωποι με επιθέσεις φραστικές στα προσωπικά τους μέσα κοινωνικής δικτύωσης ή στις πιο ακραίες περιπτώσεις να βρεθούν αντιμέτωποι με επιθέσεις κατά της σωματικής τους ακεραιότητας, λόγω της εξάπλωσης της ρητορικής μίσους (Bakalis, 2015).

2.11 Η απάτη κατά ανηλίκων στο διαδίκτυο

Επίσης, ο νομοθέτης έχει διαμορφώσει ένα ειδικό έγκλημα απάτης μέσω διαδικτύου, με το άρθρο 386Α για την απάτη με υπολογιστή *«1. 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 στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με*

τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση και χρηματική ποινή» (Ποινικός Κώδικας, Νόμος 4619/2019).

Τα παιδιά, όπως είναι λογικό, αποτελούν μία από τις πιο ευπαθείς ομάδες στις απάτες μέσω του υπολογιστή, χωρίς αυτό να σημαίνει ότι αποκλείονται οι ενήλικες ως θύματα. Σε κάθε περίπτωση τόσο για ανηλίκους, όσο και για ενήλικες, η απάτη μέσω υπολογιστή έχει κοινό παρονομαστή την χρήση του διαδικτύου ως μέσο για την τέλεση της κοινής απάτης. Από την άλλη, υπάρχουν στο έγκλημα αυτό και τρόποι δράσης, όπου το οικονομικό όφελος ή η ζημιά είναι αποτέλεσμα της ίδιας της παρέμβασης στο πρόγραμμα και τα δεδομένα του υπολογιστή (Δίωξη Ηλεκτρονικού εγκλήματος, χ.χ.).

Οι πιο χαρακτηριστικές μορφές διαδικτυακής απάτης είναι οι ακόλουθες: Πρώτον, η απάτη με την αποστολή ηλεκτρονικού μηνύματος «ψαρέματος». Στην περίπτωση αυτής της απάτης, ο θύτης αποστέλλει μηνύματα στα θύματά του με σκοπό την αποκόμιση των προσωπικών δεδομένων του, των κωδικών των τραπεζικών του λογαριασμών και των οικονομικών του στοιχείων. Αρχικά, το θύμα βρίσκει στο ηλεκτρονικό του ταχυδρομείο ένα μήνυμα, το οποίο παρουσιάζεται ως μήνυμα εκ μέρους της τράπεζας του θύματος. Συνήθως στο μήνυμα εμφανίζεται μία επιβεβαιωτική καρτέλα, που ζητά από τον χρήστη να επιβεβαιώσει το *username* και το *password* του τραπεζικού του λογαριασμού στο *Web Banking*. Συνήθως, οι τράπεζες προειδοποιούν στην τραπεζική σύμβαση τους πελάτες τους ότι η τράπεζα δεν ζητά ποτέ τέτοιες πληροφορίες. Παρόλα αυτά, τα μηνύματα αυτά είναι τόσο ρεαλιστικά, που κάποιος ανυποψίαστος χρήστης μπορεί όντως να παρασυρθεί (Σφακιανάκης, 2016).

Μία άλλη μορφή απάτης που συχνά παρουσιάζεται στο διαδίκτυο είναι και η εμφάνιση ενός παραθύρου κατά την περιήγηση στο διαδίκτυο, στο οποίο υπάρχει μία υπόσχεση για μεγάλα δώρα και χρηματικά ποσά, που κέρδισε ο χρήστης σε κάποια κλήρωση. Αυτό που συνιστά την απάτη, όμως είναι ότι για να λάβει το δώρο, θα πρέπει να πληρώσει ένα χρηματικό ποσό. Μόλις το καταβάλουν, δεν λαμβάνουν κανένα άλλο μήνυμα που να τους ενημερώνει για το δώρο, που υποτίθεται ότι κέρδισαν.

2.12 Οι κίνδυνοι για τους ανήλικους καταναλωτές ως χρήστες του διαδικτύου

Στην σύγχρονη εποχή, μεγάλο ποσοστό του πληθυσμού πραγματοποιεί τις αγορές του διαδικτυακά. Είναι λογικό, λοιπόν, οι ανήλικοι να αποτελούν σημαντικό μέρος του καταναλωτικού κοινού που πραγματοποιεί διαδικτυακές αγορές. Άλλωστε και στο νόμο 2251/1994 περί προστασίας του καταναλωτή, ως διαδικτυακός καταναλωτής ή καταναλωτής εξ αποστάσεως, μπορεί να είναι κάθε φυσικό πρόσωπο, το οποίο, καταναλώνει αγαθά και υπηρεσίες εκτός εμπορικού καταστήματος, δηλαδή μέσω του Διαδικτύου. από την άλλη, από τον Αστικό Κώδικα ορίζεται ότι «*οι ανήλικοι μέχρι την ηλικία των 18 χρόνων μπορούν να συνάπτουν δικαιοπραξίες από τις οποίες θα αποκτούν μόνο όφελος χωρίς να γεννώνται για αυτούς υποχρεώσεις*» (Σφακιανάκης, 2016).

Για να συγκεράσει αυτές τις δύο τάσεις, ο νόμος 2251/1994 και με σκοπό την προστασία της ψυχικής υγείας του ανήλικου καταναλωτή, έχει διαμορφώσει κάποιες νομοθετικές απαγορεύσεις ως προς τη διάθεση συγκεκριμένων προϊόντων από τους προμηθευτές. Αναλυτικότερα, στο άρθρο 7α του νόμου αυτού ορίζεται η υποχρέωση των προμηθευτών να διαθέτουν μόνο προϊόντα τα οποία, από τη φύση και τον προορισμό τους δεν συνιστούν κίνδυνο για την ψυχική, πνευματική και ηθική ανάπτυξη των ανηλίκων (Lawspot, 2020).

Στην πραγματικότητα, όμως, παρόλη την νομοθετική ρύθμιση της κατάστασης, εξακολουθούν να υπάρχουν κίνδυνοι για τον ανήλικο καταναλωτή. Μερικά τέτοια περιστατικά, στα οποία ο ανήλικος καταναλωτής μπορεί να βρεθεί σε κίνδυνο είναι αρχικά η πιθανότητα διαδικτυακών καταστημάτων, τα οποία δεν διασφαλίζουν την ασφάλεια των καταναλωτών τους, οπότε μπορεί να υπάρξει υποκλοπή των δεδομένων τραπεζικών συναλλαγών μέσω της συναλλαγής που πραγματοποιεί ο ανήλικος (Σφακιανάκης, 2016).

Παράλληλα, υπάρχει η πιθανότητα, το διαδικτυακό κατάστημα να μην υφίσταται στην πραγματικότητα και να αποσπάσει τα χρήματα του ανηλίκου, χωρίς να προσφέρει το αντάλλαγμα της αγοράς του. Έτσι, ένας προμηθευτής μπορεί να εκμεταλλευτεί την απειρία και ευπείθεια του ανήλικου καταναλωτή προκειμένου να του αποσπάσει κάποιο χρηματικό ποσό (Συνήγορος του καταναλωτή, 2011).

Επίσης, δεδομένου ότι στις περισσότερες ιστοσελίδες τα φίλτρα προστασίας των ανηλίκων είναι παρωχημένα και κάθε ανήλικος γνωρίζει πως να τα απενεργοποιήσει, ο ανήλικος καταναλωτής μπορεί να βρεθεί αντιμέτωπος με σελίδες που απευθύνονται μόνο σε ενηλίκους, όπως είναι εκείνες με περιεχόμενο σεξουαλικής φύσεως, το οποίο μπορεί να τραυματίσει ένα παιδί ψυχικά (Σφακιανάκης, 2016).

Επίσης, ένα σημαντικό στοιχείο που θα πρέπει να παρατηρηθεί για τον ανήλικο καταναλωτή, ο οποίος χρησιμοποιεί μία κοινή συσκευή με τους ενηλίκους, που έχουν την εποπτεία του είναι τα λεγόμενα *big data* των ενηλίκων. Πιο αναλυτικά, ως *Big data* ορίζονται τα σύνολα των δεδομένων προσωποποίησης και προσαρμογής που διαμορφώνονται από την παρατήρηση της παρουσίας ενός χρήστη στο Διαδίκτυο. Τα δεδομένα αυτά σχετίζονται με τις διαφημίσεις που του προβάλλονται, οι οποίες είναι προσαρμοσμένες στις προτιμήσεις του. Έτσι, όταν ο ανήλικος χρησιμοποιεί συσκευές με λογαριασμούς ενηλίκων, στους οποίους παρουσιάζονται διαφημίσεις και προτάσεις που απευθύνονταν στο ενήλικο, γεγονός που μπορεί να φέρει τον ανήλικο σε επαφή με μηνύματα που δεν ταιριάζουν στην ηλικία και την ψυχική τους ανάπτυξη (Συνήγορος του καταναλωτή, 2011).

2.13 Τα προσωπικά δεδομένα των ανήλικων στο διαδίκτυο

Οι ανήλικοι της σύγχρονης εποχής χαρακτηρίζονται ως ψηφιακοί ιθαγενείς του Διαδικτύου, με την έννοια ότι μεγάλωσαν και γαλουχήθηκαν κατά την περίοδο ανάπτυξης των διαδικτυακών εφαρμογών και για το λόγο αυτό καθολη τη διάρκεια της ζωής τους βρίσκονται σε επαφή με το Ιντερνέτ. Για το λόγο αυτό, από πολύ νεαρή ηλικία διαθέτουν λογαριασμούς σε πλατφόρμες κοινωνικής δικτύωσης, όπως το Facebook, το Twitter, το Google-, το TikTok, το Instagram και άλλα, στις οποίες διαβιβάζονται και κοινοποιούνται προσωπικά δεδομένα ανηλίκων, με μηδαμινό έλεγχο (Ιγγλεζάκης, 2020).

Άλλωστε, όπως και σε όλα τα προηγούμενα εγκλήματα, έτσι και σε αυτά κατά των προσωπικών δεδομένων, οι ανήλικοι είναι περισσότερο ευάλωτοι λόγω του βαθμού ψυχικής και διανοητικής ανάπτυξής τους. Έτσι, οι ανήλικοι δημοσιεύουν περιεχόμενο στις σελίδες αυτές, κάποιοι ακόμα και επαγγελματικά, χωρίς επίβλεψη από τους γονείς τους, οι οποίοι στις περισσότερες περιπτώσεις δεν γνωρίζουν πώς ακριβώς να προστατεύσουν τα παιδιά τους (Αλεξανδροπούλου, 2007).

Έτσι, σε πολλές περιπτώσεις η ιδιωτικότητα και τα προσωπικά δεδομένα των ανηλίκων χρηστών των διαδικτυακών εφαρμογών μπορεί να βρίσκονται σε κίνδυνο λόγω της ελλιπούς προστασίας από το κράτος και τους γονείς τους. Οι νέοι έχουν μία ιδιαίτερη σχέση με το διαδίκτυο, σχεδόν παρορμητική, και είναι δύσκολο να ελεγχθεί από τους φορείς τις εξουσίας. Αυτό μπορεί να έχει πολύ σοβαρές συνέπειες όμως, οι οποίες μπορεί να σχετίζονται με το σύνολο των προηγούμενων εγκλημάτων (Ιγγλεζάκης, 2020).

Η αυτοέκθεση των ανηλίκων στα μέσα κοινωνικής δικτύωσης δίνει πληθώρα πληροφοριών σε ένα ευρύ φάσμα εγκληματιών, οι οποίοι είναι σε θέση να συγκεντρώσουν πληροφορίες για την ζωή και την εικόνα των ανηλίκων σε δευτερόλεπτα. Έτσι, τα προσωπικά δεδομένα που προσφέρουν απλόχερα οι ανήλικοι μπορεί στο μέλλον να χρησιμοποιηθούν για εγκληματικές δράσεις εναντίον τους (Αλεξανδροπούλου, 2007).

Παράλληλα, πέραν της δημοσίευσης των προσωπικών δεδομένων τους από τους ίδιους τους ανηλίκους, αυτοί είναι επιρρεπείς και στη δημοσιοποίηση των προσωπικών πληροφοριών τους και από τρίτους. Προσωπικές φωτογραφίες που μοιράζεται ένας ανήλικος χρήστης με κάποιον άλλον μπορεί εύκολα να δημοσιοποιηθούν σε όλα τα μέσα κοινωνικής δικτύωσης. Επίσης, λόγω της πληθώρας πληροφοριών που μοιράζεται καθημερινά ένας ανήλικος στο ίντερνετ είναι εφικτή η ταυτοποίηση του από οποιονδήποτε, γεγονός που μπορεί να οδηγήσει σε δημοσιοποίησή της διεύθυνσής του, του σχολείου του και της οικογένειάς του, της προσωπικής του κατάσταση και των ενδιαφερόντων του, δια μέσου της κοινοποίησης προσωπικών φωτογραφιών και της επισήμανσης σε αυτές των φίλων του, καθώς και με την κοινοποίηση της τοποθεσίας του (Ιγγλεζάκης, 2020).

Πέραν των κακόβουλων χρηστών, οι πληροφορίες αυτές συλλέγονται και από τα λογισμικά των κοινωνικών δικτύων, με αποτέλεσμα να παρουσιάζονται στον χρήστη προσαρμοσμένες διαφημίσεις ανάλογα με τις προτιμήσεις του. με τον τρόπο αυτό ο ανήλικος χρήστης θα μετατραπεί σε άβουλο καταναλωτή, δεδομένου ότι ο αλγόριθμος γνωρίζει ποιες σελίδες να τους παρουσιάσει και πώς να καταστήσει ελκυστικό το προϊόν ανάλογα με τις προτιμήσεις που έχει δηλώσει ήδη από την πρώτη μέρα εγγραφής του στις κοινωνικές πλατφόρμες (Ιγγλεζάκης, 2020).

Κεφάλαιο 3. Η νομοθεσία και η νομική προστασία σε περίπτωση ηλεκτρονικών εγκλημάτων

3.1 Η ιδιάζουσα νομική περίπτωση των ηλεκτρονικών εγκλημάτων

Τα ζητήματα νομικής προστασίας των ανηλίκων και εν γένει των χρηστών του διαδικτύου είναι πολυσχιδή. Πιο συγκεκριμένα, επειδή ακριβώς το διαδίκτυο διαθέτει μία ολόκληρη γκάμα τεχνικών θεμάτων σχετικά με τη λειτουργία του, η νομική διάρθρωση των προστατευτικών κανόνων, συμπλέκεται αναπόφευκτα με τις τεχνικές έννοιες, καθιστώντας τη μελέτη της ιδιαίτερα ενδιαφέρουσα και περίπλοκη. Παράλληλα, η βιβλιογραφία και η αρθρογραφία γύρω από τα θέματα των ηλεκτρονικών εγκλημάτων είναι πιο περιορισμένη συγκριτικά με άλλα θέματα, καθώς εγκλήματα του διαδικτύου αποτελούν μία πρόσφατη νομοθετική προσθήκη που δεν έχει μελετηθεί ακόμα εκτενώς (Δαλακούρας, 2019).

Επίσης, όσον αφορά τα αποδεικτικά μέσα σχετικά με τα ηλεκτρονικά εγκλήματα, αυτά διαφέρουν σημαντικά συγκριτικά με εκείνα των παραδοσιακών εγκλημάτων. Τα αποδεικτικά μέσα των ηλεκτρονικών εγκλημάτων δεν έχουν υλική ύπαρξη και υπόσταση στον φυσικό κόσμο και γι’ αυτό δεν ταυτίζονται με τα παραδοσιακά, καθώς στα ηλεκτρονικά εγκλήματα, οι αποδείξεις είναι δυνατόν να κατευθυνθούν και να ελεγχθούν από απόσταση, αλλάζοντας τη μορφή και το περιεχόμενο τους ή εξαφανίζοντάς τα με μεγαλύτερη ευκολία σε σχέση με τα άλλα εγκλήματα (Αγγελής, 2005).

Έτσι, ενώ τα αποδεικτικά μέσα ενός εγκλήματος που έχει φυσική υπόσταση και αφήνει χειροπιαστές αποδείξεις στον φυσικό κόσμο είναι απτά και μπορούν να συλλεγούν στον τόπο του εγκλήματος, στα ηλεκτρονικά εγκλήματα ο τόπος του εγκλήματος σε ένα ηλεκτρονικό έγκλημα μπορεί να είναι όλο το διαδίκτυο και οι αποδείξεις μπορεί να βρίσκονται σε όλη την υφήλιο, να μεταβάλλονται και να είναι δυσπρόσιτες. Επομένως, τα ηλεκτρονικά εγκλήματα δεν περιορίζονται χωροχρονικά και αντίστοιχα οι αποδείξεις τους μπορεί να βρίσκονται σε όλο το φάσμα του Διαδικτύου (Βλαχόπουλος, 2013).

Έτσι, αξίζει να αναφερθεί ότι η νομοθεσία για τα ηλεκτρονικά εγκλήματα συνήθως έπεται των εξελίξεων, καθώς δεν προλαβαίνει τον τρόπο δράσης των διαδικτυακών εγκληματιών. Έτσι, συχνά τίθεται το ερώτημα του κατά πόσο η ποινική νομοθεσία είναι σε θέση να ελέγξει και να προλάβει την εξέλιξη των εγκλημάτων στο διαδίκτυο. Υπάρχει δηλαδή αμφιβολία για το κατά πόσο τα διαδικτυακά εγκλήματα μπορούν να αποτελέσουν μέρος της ποινικής νομοθεσίας, κυρίως λόγω της πιθανής αποτελεσματικότητας στη διερεύνηση και εξιχνίασή τους (Δαλακούρας, 2019).

Για την αντιμετώπιση του εγκλήματος στο διαδίκτυο απαιτούνται εξειδικευμένες γνώσεις τόσο σε νομικό όσο και τεχνικό επίπεδο, κάτι που αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε κράτους, καθώς ελάχιστοι νομικοί τις διαθέτουν (Αγγελής, 2005).

Είναι χαρακτηριστικό ότι οι άνθρωποι της ελληνικής και διεθνούς αστυνομίας, οι οποίοι ασχολούνται με το ηλεκτρονικό έγκλημα, θέτουν συχνά στο προσκήνιο την αδυναμία της ποινικής νομοθεσίας να προλάβει και να ελέγξει τις εξελίξεις. Πιο συγκεκριμένα, όπως παρατηρείται συχνά η νομοθετική ρύθμιση των θεμάτων ηλεκτρονικού εγκλήματος απαιτεί έναν συνδυασμό της τεχνολογικής και της νομικής γνώσης. Οι εγκληματίες είναι τόσο εξελιγμένοι τεχνολογικά, ώστε είναι σχεδόν αδύνατον να προληφθούν οι ενέργειές τους από τη νομοθετική ρύθμιση ή από τη δράση των διωκτικών αρχών. Επιπλέον, οι νομοθέτες αναγκάζονται να παρακολουθούν συνεχώς τις εξελίξεις στο ηλεκτρονικό έγκλημα, προκειμένου να κατορθώσουν να συμβαδίσουν κατά το δυνατόν με τους εγκληματίες (Βλαχόπουλος, 2013).

3.2 Η νομική προστασία σε διεθνές επίπεδο

Όσον αφορά τις διεθνείς συμβάσεις για το κυβερνοέγκλημα, η βασική δυσκολία που εμφανίζεται είναι η δικαιοδοσία. Πιο αναλυτικά, καθώς όπως προαναφέρθηκε τα εγκλήματα που τελούνται στο Διαδίκτυο, δεν έχουν συγκεκριμένο τόπο τέλεσης, όπως τα κοινά εγκλήματα, είναι ιδιαιτέρως δυσχερές να προσδιοριστεί το κράτος δράσης και η νομοθεσία που θα εφαρμοστεί για την καταπολέμησή του. η πρώτη διεθνής προσπάθεια έγινε από την *Interpol*, η οποία ήταν ο πρώτος διεθνής οργανισμός, ο οποίος προσπάθησε να παρουσιάσει και να κανονικοποιήσει το ηλεκτρονικό έγκλημα.

Αυτό πραγματοποιήθηκε κατά το 1979 κατά τη διάρκεια του Τρίτου Διεθνούς Συμποσίου για την απάτη που πραγματοποιήθηκε στο Παρίσι (Schjolberg,2020).

Παράλληλα, ο Οργανισμός Ηνωμένων Εθνών (Ο.Η.Ε.) πρότεινε στο «*8ο Συνέδριο για την Πρόληψη του Εγκλήματος και τη Μεταχείριση των Παραβατών»* ένα ψήφισμα αναφορικά με την εφαρμογή νομοθεσίας σχετικά με το ηλεκτρονικό έγκλημα. Αυτό το ψήφισμα μετουσιώθηκε στο *«Εγχειρίδιο για την πρόληψη και τον έλεγχο του ηλεκτρονικού εγκλήματος»* του 1994. Το συγκεκριμένο κείμενο έχει ιδιαίτερη σημασία δεδομένου ότι αποτελεί το πρώτο βιβλίο σχετικά με την ηλεκτρονική εγκληματικότητα και τη νομοθεσία των κρατών. Επίσης παρατίθενται προτάσεις σχετικά με την αντιμετώπιση και τις προσθήκες στα διεθνή και εθνικά νομοθετικά κείμενα και αναλύεται το φαινόμενο της ηλεκτρονικής εγκληματικότητας, οι βασικότερες μορφές του και η σχετική νομοθεσία διαφόρων χωρών. Αναπτύσσονται προτάσεις για την πληρέστερη και αποτελεσματικότερη αντιμετώπιση. Αποτελεί την πρώτη μεθοδική διεθνή προσπάθεια προσέγγισης νομοθετικού πλαισίου για το ηλεκτρονικό έγκλημα και έτσι θεωρείται βάση πάνω στην οποία μπορούν να γίνουν περεταίρω αναθεωρήσεις και τροποποιήσεις ανάλογα με τις τρέχουσες κάθε φορά τεχνολογικές αλλά και νομικές εξελίξεις (Δαλακούρας, 2019).

Παράλληλα, ο πρώτος νόμος σχετικά με το κυβερνοέγκλημα θεσπίστηκε το 1984 στις Η.Π.Α. με το όνομα *«Computer Fraud and Abuse Act».* Αν και αποτέλεσε την πρώτη παγκόσμια νομοθετική προσπάθεια για ποινικό κολασμό των ηλεκτρονικών εγκλημάτων, είχε αρκετά μειονεκτήματα που σχετίζονταν με την αδυναμία του προσδιορισμού της δικαιοδοσίας των δικαστηρίων και την περιορισμένη ορολογία σχετικά με τα ηλεκτρονικά εγκλήματα, δεδομένου ότι κατά το χρόνο θέσπισής του νόμου δεν είχε αναπτυχθεί ακόμα η τεχνολογία των ηλεκτρονικών υπολογιστών ούτε το Διαδίκτυο. Καθώς εξελίσσεται η τεχνολογία και προχωρά και η νομοθετική αντιμετώπιση, το 1996, το νόμο αυτό συμπληρώνει το *«National Information Infrastructure Protection Act»* (Βλαχόπουλος, 2013).

Η πιο σημαντική διεθνής σύμβαση για το Κυβερνοέγκλημα είναι η *«Διεθνής Σύμβαση για το έγκλημα στον Κυβερνοχώρο»* του 2001 που υπογράφηκε στη Βουδαπέστη. Η Σύμβαση αυτή έχει διεθνή αποδοχή, καθώς σε αυτήν μέχρι σήμερα έχουν προσχωρήσει σχεδόν όλα τα μέλη του Ευρωπαϊκού Συμβουλίου, η Ιαπωνία, οι Η.Π.Α., ο Καναδάς και η Νότια Αφρική. Κατά κύριο λόγο η *«Σύμβαση για το Έγκλημα στον κυβερνοχώρο»* αποσκοπούσε στην εναρμόνιση των εθνικών νομοθεσιών των συμβαλλόμενων κρατών-μελών αναφορικά με την εγκληματικότητα στο διαδίκτυο.

Μία πολύ σημαντική και προοδευτική προσθήκη της Σύμβασης είναι ότι παρέχει το απαραίτητο νομοθετικό πλαίσιο απαραίτητο σχετικά με την έρευνα και τη δίωξη των ηλεκτρονικών εγκλημάτων, με αποτέλεσμα να γίνεται πιο αποτελεσματική η αντιμετώπιση των εγκλημάτων αυτών. Επίσης, καθώς ένα σημαντικό κομμάτι της αντιμετώπισης του ηλεκτρονικού εγκλήματος έγκειται στη διεθνή συνεργασία, η σύμβαση αυτή καθορίζει τη δικαστική συνεργασία των κρατών, όσον αφορά την έκδοση, την αμοιβαία συνδρομή για την παροχή των πληροφοριών και την αποθήκευση των δεδομένων (Δαλακούρας, 2019).

3.3 Η νομική προστασία στο ευρωπαϊκό δίκαιο

Όσον αφορά το ευρωπαϊκό νομικό πλαίσιο, το πρώτο νομοθετικό κείμενο έγινε το 1976 από το Συμβούλιο της Ευρώπης στο Στρασβούργο. Το 1996 το Συμβούλιο της Ευρώπης εξέδωσε τρεις συστάσεις την «Σύσταση No R» (1989), την «Σύσταση No R» (1995) και την «Σύσταση No R» (2001). Αυτές έδωσαν στα κράτη- μέλη υποδείξεις και κατευθυντήριες γραμμές. Σε αυτές τις συστάσεις για πρώτη φορά καθιερώθηκε σε διεθνές νομικό κείμενο μία γενική δικονομία σχετικά με την έρευνα στα κυβερνοεγκλήματα. Αυτές οι συστάσεις αποτέλεσαν τον προθάλαμο για την εξαιρετικά σημαντική «*Σύμβαση για το έγκλημα στον Κυβερνοχώρο»,* οι οποία αναλύθηκε ανωτέρω (Δαλακούρας, 2019).

Επίσης, στο ευρωπαϊκό επίπεδο θεσπίστηκε η Οδηγία 2013/40/ΕΕ, η οποία αντικατέστησε την απόφαση-πλαίσιο 2005/222/ΔΕΥ του Συμβουλίου και μεταφέρθηκε στο ελληνικό δίκαιο με τον νόμο 4411/2016 και έθεσε κανόνες σχετικά με τις επιθέσεις κατά των συστημάτων πληροφοριών. Αρχικά, ορίστηκαν συγκεκριμένα τα ποινικά αδικήματα και οι ποινές των ηλεκτρονικών εγκλημάτων στα πληροφοριακά συστήματα. Όπως, όλες οι ευρωπαϊκές οδηγίες, έτσι και αυτή εναρμονίζει την ποινική δικαιοσύνη στα κράτη μέλη και ενισχύει την συνεργασία μεταξύ τους (Γέρμανος & Γεωργίου, 2021).

Στην οδηγία αυτή, τα εγκλήματα αυτά τελούνται μόνο εκ δόλου και με πρόθεση και εξ αντιδιαστολής δεν τιμωρούνται από αμέλεια. Επίσης, ποινικοποιείται και η ηθική αυτουργία, η συνέργεια και η απόπειρα του εγκλήματος. Τέλος, όσον αφορά τις

ποινές για τα εγκλήματα αυτά, αυτές είναι ανάλογες της προσβολής, καθώς έχει πραγματοποιηθεί στάθμιση της προσβολής (Δαλακούρας, 2019).

Όσον αφορά την αντιμετώπιση του κυβερνοεγκλήματος στην Ευρωπαϊκή Ένωση, έχει διαμορφωθεί από το 2013 το Ευρωπαϊκό Κέντρο για το Έγκλημα στον κυβερνοχώρο (EC3), το οποίο αποσκοπεί στην αντιμετώπιση των ηλεκτρονικών εγκλημάτων στην Ένωση και στην προστασία των κυβερνήσεων και των πολιτών σχετικά από τα εγκλήματα αυτά. Ο οργανισμός αυτός έχει επιδείξει από την ίδρυσή του σημαντικές επιτυχίες, μέσω επιχειρήσεων υψηλής ποιότητας οι οποίες οδήγησαν σε συλλήψεις και κατάσχεση κακόβουλου λογισμικού (Γέρμανος & Γεωργίου, 2021).

3.4 Η νομική προστασία στο ελληνικό δίκαιο: Τα σημαντικότερα ηλεκτρονικά εγκλήματα και η ανάλυσή τους

Η ελληνική έννομη τάξη δεν έχει διαμορφώσει ένα εξειδικευμένο πλαίσιο νομοθεσίας για τα ηλεκτρονικά εγκλήματα. Η ειδικότερη αυτή ενότητα των εγκλημάτων ρυθμίζεται από τις επιμέρους ενότητες του ποινικού κώδικα, οι οποίες προβλέπουν τα εγκλήματα, ενώ σε κάποιες περιπτώσεις η τέλεση μέσω διαδικτύου αποτελεί ειδικότερο διακεκριμένο τρόπο τέλεσης του εγκλήματος με βαρύτερη ποινή. Χαρακτηριστικό παράδειγμα είναι το 337 παρ. 3 ΠΚ, ο οποίος ορίζει ότι «*Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλων μέσων ή τεχνολογιών πληροφορικής αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δέκα πέντε έτη και με χειρονομίες ή προτάσεις, προσβάλλει την τιμή του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν επακολούθησε συνάντηση ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.*» (Βλαχόπουλος, 2013).

Ο ισχύων Ποινικός Κώδικας είναι ο Νόμος 4619/2019 έχει διαμορφώσει το συγκεκριμένο νομικό πλαίσιο της προστασία των ανηλίκων στον τομέα της γενετήσιας ελευθερίας τους στα άρθρα του Κεφαλαίου 19, από το άρθρο 336 μέχρι 353ΠΚ. Επίσης στον ισχύοντα ποινικό κώδικα υφίσταται και γενική ρύθμιση για την προστασία από την απάτη και την απάτη μέσω υπολογιστή, το διαδικτυακό εκφοβισμός και την εξύβριση. Τα εγκλήματα αυτά διαφοροποιούνται από εκείνα της πρώτης περίπτωσης, καθώς δεν αφορούν μόνο ανηλίκους (Βλαχόπουλος, 2013).

Από την άλλη, η νομοθετική προστασία δεν έγκειται μόνο στην ποινική όψη του ζητήματος. Πιο αναλυτικά, υπάρχουν προστατευτικοί νόμοι σχετικά με τις τηλεπικοινωνίες, οι οποίοι επεκτείνονται και στην χρήση του διαδικτύου. Ο πιο πρόσφατος είναι ο νόμος 4070/2012 σχετικά με τις «*Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις*», ο οποίος είναι τροποποιητικός του προγενέστερου νόμου 3431/2006 περί ηλεκτρονικών επικοινωνιών. Επίσης, υπάρχει και ο νόμος 2225/20.7.94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας, καθώς και ο νόμος 3471/2006, ο οποίος αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Επομένως, γίνεται κατανοητό ότι υπάρχει ένα σοβαρό πλέγμα νομοθετικών διατάξεων, πέραν του ποινικού κώδικα, καθώς τα ηλεκτρονικά εγκλήματα είναι πολυεπίπεδα και η αντίστοιχη προστασία θα πρέπει να είναι πολύμορφη (Δαλακούρας, 2019).

Επίσης στον ελληνικό χώρο έχουν διαμορφωθεί και τρείς ανεξάρτητες αρχές, οι οποίες έχουν ως σκοπό την προστασία απέναντι σε θέματα ασφάλειας στις επικοινωνίες και πιο συγκεκριμένα στο διαδίκτυο. Αυτές οι αρχές είναι η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.). Οι αρχές αυτές ελέγχουν τους όρους του απορρήτου των τηλεπικοινωνιών καθώς και του διαδικτύου (Βλαχόπουλος, 2013).

3.4.1 Τα εγκλήματα κατά της γενετήσιας ελευθερίας ανηλίκων

Από την άλλη, όσον αφορά το ποινικό σκέλος της νομοθετικής προστασίας, το οποίο αναμφίβολα είναι το πιο σημαντικό, τα εγκλήματα κατά της γενετήσιας ελευθερίας ανηλίκων είναι τα πλέον διαδεδομένα και αποτελούν τα πιο συχνά σε βάρος των ανηλίκων (Συμεωνίδου- Καστανίδου, 2020).

Πιο συγκεκριμένα, το άρθρο 337, το οποίο τιτλοφορείται «Προσβολή της γενετήσιας αξιοπρέπειας»

«*1. Όποιος με χειρονομίες γενετήσιου χαρακτήρα, με προτάσεις που αφορούν γενετήσιες πράξεις, με γενετήσιες πράξεις που τελούνται ενώπιον άλλου ή με επίδειξη των γεννητικών του οργάνων, προσβάλλει βάναυσα την τιμή άλλου, τιμωρείται με φυλάκιση έως ένα έτος ή χρηματική ποινή. Για την ποινική δίωξη απαιτείται έγκληση*.

2. Με φυλάκιση έως δύο έτη ή χρηματική ποινή τιμωρείται η πράξη της προηγουμένης παραγράφου, αν ο παθών είναι νεότερος των δώδεκα ετών.

3. Ενήλικος, ο οποίος μέσω διαδικτύου ή άλλων μέσων ή τεχνολογιών πληροφορικής αποκτά επαφή με πρόσωπο που δεν συμπλήρωσε τα δέκα πέντε έτη και με χειρονομίες ή προτάσεις, προσβάλλει την τιμή του ανηλίκου στο πεδίο της γενετήσιας ζωής του, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών. Αν επακολούθησε συνάντηση ο ενήλικος τιμωρείται με φυλάκιση τουλάχιστον τριών ετών.

4. Όποιος προβαίνει σε χειρονομίες γενετήσιου χαρακτήρα ή διατυπώνει προτάσεις για τέλεση γενετήσιων πράξεων σε πρόσωπο που εξαρτάται εργασιακά από αυτόν ή εκμεταλλευόμενος την ανάγκη ενός προσώπου να εργαστεί, τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή. Για την ποινική δίωξη απαιτείται έγκληση.» (Ποινικός Κώδικας, Νόμος 4619/2019).

Το έγκλημα αυτό έχει ιδιαίτερη σημασία για τα διαδικτυακά εγκλήματα κυρίως σε σχέση με την παράγραφο τρία. Το έγκλημα τελείται μόνο από ενήλικο, ο οποίος μέσω του διαδικτύου ή άλλων μέσων ή τεχνολογιών πληροφορικής, έρχεται σε επαφή με ανήλικο. Οι ανήλικοι, για να είναι ποινικά κολάσιμη η πράξη πρέπει να είναι κάτω των δέκα πέντε ετών (Συμεωνίδου- Καστανίδου, 2020).

Επίσης το έγκλημα τελείται μόνο και με χειρονομίες ή προτάσεις, οι οποίες θα πρέπει να προσβάλλουν την τιμή του ανηλίκου στο πεδίο της γενετήσιας ζωής του. η διακεκριμένη περίπτωση του εγκλήματος τελείται όταν επέρχεται συνάντηση του ανηλίκου με τον ενήλικο. Επομένως, το έγκλημα αυτό αφορά τον ενήλικο ο οποίος μέσω του Ιντερνέτ γνωρίζει ανηλίκους και απευθύνει σε αυτούς είτε χειρονομίες, είτε προτάσεις με γενετήσιο περιεχόμενο. Ως «χειρονομίες γενετήσιου χαρακτήρα» νοούνται οι γενετήσιες πράξεις που είναι ήσσονος βαρύτητας, οι οποίες προσβάλλουν την γενετήσια αξιοπρέπεια, όπως είναι για παράδειγμα οι χειρονομίες, οι θωπείες ή οι ψαύσεις του σώματος, όταν δεν καταλήγουν σε γενετήσια πράξη (ΑΠ 930/2020) (Συμεωνίδου- Καστανίδου, 2020).

Το άρθρο 337 συνήθως αποτελεί προπαρασκευαστική πράξη των βαρύτερων εγκλημάτων του κεφαλαίου και απορροφάται μέσω της φαινομενικής συρροής. Επίσης παρατηρείται ότι στον ποινικό κώδικα προστατεύεται συγκεκριμένα η ανηλικότητα, όταν οι προσβολές γίνονται μέσω Διαδικτύου, προκειμένου να προσαρμοστεί ο νόμος προς τις απαιτήσεις της σύγχρονης διαδικτυακής κοινωνίας (Μαργαρίτη & Μαργαρίτη, 2020).

Εν συνεχεία, το άρθρο 339 με τίτλο «Γενετήσιες πράξεις με ανηλίκους ή ενώπιόν τους» ορίζει ότι *«1. Όποιος ενεργεί γενετήσια πράξη με πρόσωπο νεότερο των δεκαπέντε ετών ή το παραπλανά με αποτέλεσμα να ενεργήσει ή να υποστεί τέτοια πράξη τιμωρείται, αν δεν υπάρχει περίπτωση να τιμωρηθεί βαρύτερα με το άρθρο 351Α, ως εξής: α) αν ο παθών δεν συμπλήρωσε τα δώδεκα έτη, με κάθειρξη, β) αν ο παθών συμπλήρωσε τα δώδεκα αλλά όχι τα δεκατέσσερα έτη, με κάθειρξη έως δέκα έτη και γ) αν συμπλήρωσε τα δεκατέσσερα έτη, με φυλάκιση τουλάχιστον δύο ετών.*

2. Οι γενετήσιες πράξεις μεταξύ ανηλίκων κάτω των δεκαπέντε ετών δεν τιμωρούνται, εκτός αν η μεταξύ τους διαφορά ηλικίας είναι μεγαλύτερη των τριών ετών, οπότε μπορούν να επιβληθούν μόνο αναμορφωτικά ή θεραπευτικά μέτρα.

3. Όποιος εξωθεί ή παρασύρει ανήλικο, που δεν συμπλήρωσε τα δεκαπέντε έτη, να παρίσταται σε γενετήσια πράξη μεταξύ άλλων, χωρίς να συμμετέχει σε αυτήν, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή αν ο ανήλικος είναι μικρότερος των δεκατεσσάρων ετών και με φυλάκιση έως τρία έτη ή χρηματική ποινή αν έχει συμπληρώσει το δέκατο τέταρτο έτος της ηλικίας του.» (Ποινικός Κώδικας, Νόμος 4619/2019).

Το άρθρο αυτό έχει προστατευτική ισχύ για τον ανήλικο, όταν το διαδίκτυο χρησιμοποιείται ως μέσον προς σκοπό και έχει ως αποτέλεσμα των βιασμό του ανηλίκου. Αρχικά, αξίζει να αναφερθεί ότι υπό τον προϊσχύσαντα ΠΚ, η πράξη κατά του ανηλίκου θα έπρεπε να είναι ασελγής, με την έννοια ότι θα έπρεπε να προσβάλει αντικειμενικά το κοινό αίσθημα αιδούς και την περί των ηθών κοινή αντίληψη. Από την άλλη προβλεπόταν και υποκειμενικό στοιχείο, το οποίο αφορούσε και την ικανοποίηση ή τη διέγερση της γενετήσιας ορμής του δράστη. Με την έννοια αυτή, αποτελούσαν ασελγείς πράξεις, η συνουσία και η παρά φύση ασέλγεια, οι θωπείες στα γεννητικά οργάνου του ανηλίκου, η επαφή με τα γεννητικά όργανα του δράστη στα γεννητικά όργανα του ανήλικου, ο εναγκαλισμός και ο ασπασμός στο πρόσωπο και το σώμα του παιδιού, μόνο όταν ακολουθούνται από τη διέγερση ή την ικανοποίηση της επιθυμίας του δράστη, που προσβάλλουν την αγνότητα της παιδικής ηλικίας του ανηλίκου. Πλέον αξιοποιείται ο όρος γενετήσια πράξη, η οποία περιγράφει με σύγχρονους όρους τις πράξεις βιασμού κατά ανηλίκων (Μαργαρίτη & Μαργαρίτη, 2020).

Όσον αφορά την προστασία κατά των ηλεκτρονικών εγκλημάτων του 339, σημασία έχει η παράγραφος 3, η οποία αφορά την τέλεση του εγκλήματος ενώπιον των ανηλίκων που δεν συμπλήρωσαν τα δεκαπέντε έτη, καθώς εξωθούνται, να παρίστανται

σε γενετήσια πράξη μεταξύ άλλων, χωρίς να συμμετέχουν σ' αυτήν. Η παράγραφος αυτή έχει προβλεφθεί για την πιο ολοκληρωμένη προστασία του ανηλίκου, καθώς ακόμα και η παρουσία σε μία τέτοια πράξη μπορεί να τραυματίσει ανεπανόρθωτα τον ανήλικο, ακόμα και αν δεν συμμετέχει σε αυτή. Η παρουσία του ανηλίκου δεν είναι ανάγκη να είναι φυσική, καθώς μπορεί να γίνεται και μέσω υπηρεσιών διαδικτύου, που περιλαμβάνου ζωντανή βιντεοκλήση. Έτσι, το άρθρο αυτό έχει ιδιαίτερη αξία, καθώς μπορεί ο δράστης να μεταδίδει σε ανήλικο γενετήσια πράξη μέσω διαδικτύου και να προσβάλλει με τον τρόπο αυτό την ανηλικότητα και την γενετήσια αξιοπρέπειά του (Συμεωνίδου- Καστανίδου, 2020).

Τέλος, ένα πολύ διαδεδομένο έγκλημα του κυβερνοχώρου είναι αναμφίβολα η παιδική πορνογραφία. Πρόκειται για το πλέον σύνηθες έγκλημα κατά των ανηλίκων και με την ανάπτυξη του Διαδικτύου η διανομή και η θέαση παιδική πορνογραφίας έχει εκτοξευθεί, γίνεται με μεγαλύτερη ταχύτητα και το υλικό της δεν διαγράφεται ουσιαστικά ποτέ από τον Παγκόσμιο ιστό παρά τις προσπάθειες των διωκτικών αρχών (Μαργαρίτη & Μαργαρίτη, 2020).

Στον ελληνικό ποινικό κώδικα, η ποινικοποίηση της παιδικής πορνογραφίας γίνεται στο άρθρο 348Α «Πορνογραφία ανηλίκων». «*1. Όποιος με πρόθεση παράγει, διανέμει, δημοσιεύει, επιδεικνύει, εισάγει στην Επικράτεια ή εξάγει από αυτήν, μεταφέρει, προσφέρει, πωλεί ή με άλλον τρόπο διαθέτει, αγοράζει, προμηθεύεται, αποκτά ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει ή μεταδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Στην παράγραφο ένα παρατηρείται ότι το έγκλημα μπορεί να τελεστεί με διάφορους τρόπους, οι οποίοι περιοριστικά αναφέρονται στο νόμο. Σκοπός είναι να καλύψει την ευρεία γκάμα μεθόδων δημιουργίας και κυκλοφορίας του πορνογραφικού υλικού, προκειμένου οι ανήλικοι να προστατεύονται ολικά σε σχέση με την πορνογραφία. Επίσης, περιλαμβάνει και την διασυνοριακή παιδική πορνογραφία, η οποία περιλαμβάνει την εισαγωγή και την εξαγωγή του πορνογραφικού υλικού (Συμεωνίδου- Καστανίδου, 2020).

Στην παρ. 2. Ορίζεται ότι «*Όποιος με πρόθεση παράγει, προσφέρει, πωλεί ή με οποιονδήποτε τρόπο διαθέτει, διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας ή διαδίδει πληροφορίες σχετικά με την τέλεση των παραπάνω πράξεων, μέσω πληροφοριακών συστημάτων, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Η παράγραφος αυτή αφορά την πορνογραφία ανηλίκων που τελείται μέσω του Διαδικτύου. Αυτή είναι η κατεξοχήν παράγραφος τιμώρησης του κυβερνοεγκλήματος της παιδικής πορνογραφίας. Πρόκειται για ειδικότερη μορφή του εγκλήματος της παραγράφου 1 που εξειδικεύεται ως προς το μέσον τέλεσης τους εγκλήματος (Συμεωνίδου- Καστανίδου, 2020).

Οι ορισμοί της παραγράφου 3 έχουν ιδιαίτερη σημασία για τον προσδιορισμό της έννοιας της πορνογραφίας. Έτσι, *«3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων συνιστά η αναπαράσταση ή η πραγματική ή η εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα των γεννητικών οργάνων ή του σώματος εν γένει του ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και της πραγματικής ή εικονικής γενετήσιας πράξης που διενεργείται από ή με ανήλικο.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Στην παράγραφο 4 προβλέπονται οι διακεκριμένες μορφές του εγκλήματος κατά των ανηλίκων. Πιο αναλυτικά, *«4. Οι πράξεις των παραγράφων 1 και 2 τιμωρούνται με κάθειρξη έως δέκα έτη και χρηματική ποινή: α. αν τελέσθηκαν κατ' επάγγελμα, β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή της σωματικής δυσλειτουργίας, λόγω οργανικής νόσου ανηλίκου ή με την άσκηση ή απειλή χρήσης βίας ανηλίκου ή με τη χρησιμοποίηση ανηλίκου που δεν έχει συμπληρώσει το δέκατο πέμπτο έτος ή αν η παραγωγή του υλικού της παιδικής πορνογραφίας εξέθεσε τη ζωή του ανηλίκου σε σοβαρό κίνδυνο και γ. αν δράστης της παραγωγής του υλικού παιδικής πορνογραφίας είναι πρόσωπο στο οποίο έχουν εμπιστευθεί ανήλικο για να τον επιβλέπει ή να τον φυλάσσει, έστω και προσωρινά.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Ενώ, λοιπόν, ο ανήλικος αποτελεί πάντα το θύμα του εγκλήματος αυτού, στην παράγραφο αυτή προβλέπονται ειδικότερες μορφές εκμετάλλευσης των ανηλίκων. Έτσι, όταν ο ανήλικος εμφανίζει ψυχική η διανοητική ασθένεια και σωματική δυσλειτουργία, έχει ανάγκη, ή βρίσκεται υπό το καθεστώς βίας, ο δράστης τιμωρείται με την αυξημένη ποινή της παραγράφου αυτής. Το ίδιο ισχύει και όταν ο ανήλικος είναι κάτω των 15 ετών ή τον έχουν εμπιστευτεί στο δράστη για να τον επιβλέπει ή να τον φυλάσσει, έστω και προσωρινά. Στην προκειμένη περίπτωση, ο δράστης εκμεταλλεύεται την σχέση εμπιστοσύνης λόγω της οποίας του εμπιστευθήκαν τον ανήλικο (Συμεωνίδου- Καστανίδου, 2020).

Τέλος, στην παράγραφο 6 προβλέπεται ότι «*Όποιος εν γνώσει αποκτά πρόσβαση σε υλικό παιδικής πορνογραφίας μέσω πληροφοριακών συστημάτων, τιμωρείται με*

φυλάκιση έως τρία έτη ή χρηματική ποινή.» (Ποινικός Κώδικας, Νόμος 4619/2019). Η παράγραφος αυτή είναι ένα πλημμέλημα και αφορά όσους παρακολουθούν μέσω του Διαδικτύου παιδική πορνογραφία. Η δράση αυτών των ατόμων προσβάλλει εμμέσως τους ανηλίκους, καθώς δημιουργεί μία πρόσφορη αγορά για την όλο και μεγαλύτερη παραγωγή παιδική πορνογραφίας, η οποία προσβάλλει άμεσα τους ανηλίκους (Συμεωνίδου- Καστανίδου, 2020).

Παρατηρείται, επομένως, ότι το σύνολο του κεφαλαίου 19 του ποινικού κώδικα για την προσβολή της γενετήσιας αξιοπρέπειας των ανηλίκων δημιουργεί ένα προστατευτικό πλαίσιο, το οποίο επεκτείνεται στις περιπτώσεις που τα εγκλήματα τελούνται μέσω διαδικτύου. Η προσβολή της γενετήσιας αξιοπρέπειας (337), ο βιασμός (339) και η παιδική πορνογραφία (348^{A}) είναι τα κυριότερα εγκλήματα που τελούνται μέσω διαδικτύου και αφορούν τους ανηλίκους. Η πρόβλεψη των εγκλημάτων αυτών είναι ένα θετικό βήμα προς την σωστή κατεύθυνση. Παρόλα αυτά, εξακολουθεί να υφίσταται η δυσκολία σχετικά με τη δίωξη και την εξαφάνιση του υλικού από το διαδίκτυο, καθώς ό,τι ανεβαίνει στο Διαδίκτυο, δύσκολα μπορεί να διαγραφεί μόνιμα (Συμεωνίδου- Καστανίδου, 2020).

Τέλος, σημαντικό βήμα στην ποινικοποίηση των διαδικτυακών εγκλημάτων είναι και το άρθρο 348Β για το grooming, που ορίζει 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 παρ. 1 και 2 ή 348Α, όταν η πρόταση αυτή ακολουθείται από περαιτέρω πράξεις που οδηγούν σε μία τέτοια συνάντηση, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Η διαδικασία της προσέγγισης παιδιών για γενετήσιους λόγους αποτελεί μία από τις πιο χαρακτηριστικές ποινικά κολάσιμες πράξεις σε βάρος ανηλίκων στο διαδίκτυο. Ο ποινικός νομοθέτης ποινικοποίησε την πράξη αυτή και αφορά ανηλίκους κάτω των 15 ετών που προσεγγίζονται μέσω των πληροφοριακών συστημάτων. Ο σκοπός της προσέγγισης είναι συγκεκριμένος και τμήμα της νομοτυπικής μορφής, και αφορά τα αδικήματα των δύο προαναφερθέντων άρθρων 339 (βιασμός) και 348^{A} (πορνογραφία). Τέλος, η πράξη πρέπει να συνοδεύεται από πράξεις που οδηγούν σε συνάντηση με τον ανήλικο. Πρόκειται για ένα πλημμέλημα, το οποίο προστατεύει τον ανήλικο από επιτήδειους, οι οποίοι εκμεταλλεύονται την ευπιστία των ανηλίκων στο διαδίκτυο και χρησιμοποιούν τα μέσα κοινωνικής δικτύωσης για να επιτύχουν ένα

ραντεβού για την τέλεση άλλων γενετήσιων αδικημάτων (Συμεωνίδου- Καστανίδου, 2020).

3.4.2 Η απάτη και η απάτη μέσω υπολογιστή

Ο ποινικός κώδικας περιλαμβάνει δύο άρθρα για την απάτη. Η πρώτη, το άρθρο 386: *«1. 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 χρηματική ποινή.» και η δεύτερη το άρθρο 386^{A}: «Απάτη με υπολογιστή 1. 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 στη λειτουργία προγράμματος ή συστήματος υπολογιστή, γ) με τη χρησιμοποίηση μη ορθών ή ελλιπών δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, δ) με τη χωρίς δικαίωμα εισαγωγή, αλλοίωση, διαγραφή ή εξάλειψη δεδομένων υπολογιστή, ιδίως δεδομένων αναγνώρισης της ταυτότητας, ή ε) με τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων τιμωρείται με φυλάκιση και χρηματική ποινή.»* (Ποινικός Κώδικας, Νόμος 4619/2019).

Το δεύτερο άρθρο για την απάτη μέσω υπολογιστή προστέθηκε προκειμένου να τιμωρείται κάθε απάτη που γίνεται με την χρήση του διαδικτύου και των υπολογιστών. Το άρθρο για την απάτη μέσω ηλεκτρονικού υπολογιστή δεν αφορά αποκλειστικά τους ανηλίκους, αλλά μπορεί να επεκταθεί και σε εκείνους. Όπως προαναφέρθηκε, οι ανήλικοι είναι ιδιαίτερα επιρρεπείς στη διαδικτυακή απάτη και άρα χρήζουν προστασίας από το νόμο (Παπαδαμάκης, 2020).

Το άρθρο αυτό προστέθηκε λόγω της συμμόρφωσης του Έλληνα νομοθέτη στις επιταγές της Σύμβασης της Βουδαπέστης για το έγκλημα στον κυβερνοχώρο, με το νόμο 4411/2016. Το άρθρο 13 περ. στ' και ζ ΠΚ ορίζει ότι «*Πληροφοριακό σύστημα είναι συσκευή ή ομάδα διασυνδεδεμένων ή σχετικών μεταξύ τους συσκευών, εκ των οποίων μία ή περισσότερες εκτελούν, σύμφωνα με ένα πρόγραμμα, αυτόματη*

επεξεργασία ψηφιακών δεδομένων, καθώς και τα ψηφιακά δεδομένα που αποθηκεύονται, αποτελούν αντικείμενο επεξεργασίας, ανακτώνται ή διαβιβάζονται από την εν λόγω συσκευή ή την ομάδα συσκευών με σκοπό τη λειτουργία, τη χρήση, την προστασία και τη συντήρηση των συσκευών αυτών.

ζ) Ψηφιακά δεδομένα είναι η παρουσίαση γεγονότων, πληροφοριών ή εννοιών σε μορφή κατάλληλη προς επεξεργασία από πληροφοριακό σύστημα, συμπεριλαμβανομένου προγράμματος που παρέχει τη δυνατότητα στο πληροφοριακό σύστημα να εκτελέσει μια λειτουργία. » (Ποινικός Κώδικας - Νόμος 4619/2019).

Το έγκλημα αυτό περιλαμβάνει πέντε διαφορετικούς τρόπους τέλεσης, οι οποίες περιοριστικά αναφέρονται στο άρθρο. Οι πιο σημαντικοί για το παρόν πόνημα τρόποι τέλεσης είναι οι δύο τελευταίοι, οι οποίοι προστέθηκαν με την τελευταία τροποποίηση του κώδικα το 2019. Αυτοί διεύρυναν το αξιόποινο και περιλαμβάνουν πλέον την κατοχή προγράμματος ή συστήματος υπολογιστή, το οποίο έχει ως σκοπό να τελέσει έγκλημα απάτης με υπολογιστή, όπως για παράδειγμα είναι τα προγράμματα Hacking για διείσδυση σε ξένους υπολογιστές με σκοπό την αποκόμιση περιουσιακού οφέλους(Παπαδαμάκης, 2020).

Η επόμενη προσθήκη αφορά τη χωρίς δικαίωμα αξιοποίηση λογισμικού προορισμένου για τη μετακίνηση χρημάτων, η οποία αφορά την προστασία απέναντι στα ηλεκτρονικά εγκλήματα «κλοπής» ψηφιακού χρήματος. Από την στιγμή που ψηφιοποιήθηκε το χρήμα και οι τραπεζικές συναλλαγές γίνονται μέσω του διαδικτύου, πολλές φορές παρατηρήθηκαν υποκλοπές τραπεζικών δεδομένων και οι απάτες δεν αφορούν πλέον φυσικό χρήμα αλλά ψηφιακά είδη χρημάτων (Παπαδαμάκης, 2020).

Παράλληλα, πλέον, καθώς οι συναλλαγές και οι αγορές γίνονται μέσω Διαδικτύου και μπορεί να πραγματοποιούνται και από ανηλίκους, αυξάνονται σημαντικά οι πιθανότητες από τρίτο ιστότοπο να εισαχθεί κακόβουλο λογισμικό στον υπολογιστή και να υποκλαπούν δεδομένα τραπεζικής φύσεως. Επομένως, γίνεται κατανοητό ότι η επέκταση του αξιοποίνου και στις περιπτώσεις αυτές των ηλεκτρονικών απατών μέσω προγραμμάτων υπολογιστή ήταν αναγκαία προσθήκη του νέου νόμου και μπορεί να αντιμετωπίσει πιο αποτελεσματικά το φαινόμενο (Παπαδαμάκης, 2020).

3.4.3 Ο διαδικτυακός εκφοβισμός

Όσον αφορά το *cyber bullying*, ο νομοθέτης έχει θεσπίσει με τον προηγούμενο ποινικό νόμο το άρθρο 312 ΠΚ με τον τίτλο «Πρόκληση βλάβης με συνεχή σκληρή συμπεριφορά», το οποίο ανέφερε ότι: «*1.Αν δεν συντρέχει περίπτωση βαρύτερης αξιόποινης πράξης, τιμωρείται με φυλάκιση, όποιος με συνεχή σκληρή συμπεριφορά προξενεί σε τρίτον σωματική κάκωση ή άλλη βλάβη της σωματικής ή ψυχικής υγείας. Αν η πράξη τελείται μεταξύ ανηλίκων δεν τιμωρείται εκτός αν η μεταξύ τους διαφορά ηλικίας είναι μεγαλύτερη από τρία (3) έτη, οπότε επιβάλλονται μόνο αναμορφωτικά ή θεραπευτικά μέτρα.*

2. Αν το θύμα δεν συμπλήρωσε ακόμη το δέκατο όγδοο (18ο) έτος της ηλικίας του ή δεν μπορεί να υπερασπίσει τον εαυτό του και ο δράστης το έχει στην επιμέλεια ή στην προστασία του ή ανήκει στο σπίτι του δράστη ή έχει μαζί του σχέση εργασίας ή υπηρεσίας ή το έχει αφήσει στην εξουσία του ο υπόχρεος για την επιμέλεια του ή του το έχουν εμπιστευθεί για ανατροφή, διδασκαλία, επίβλεψη ή φύλαξη έστω προσωρινή, αν δεν συντρέχει περίπτωση βαρύτερης αξιόποινης πράξης, επιβάλλεται φυλάκιση τουλάχιστον έξι (6) μηνών. Με την ίδια ποινή τιμωρείται όποιος με συστηματική παραμέληση των υποχρεώσεων του προς τα προαναφερόμενα πρόσωπα γίνεται υπαίτιος να πάθουν σωματική κάκωση ή βλάβη της σωματικής ή ψυχικής τους υγείας.» (Ποινικός Κώδικας-Νόμος 4322/2015).

Το άρθρο αυτό προστέθηκε με το νόμο 4322/2015 τροποποιήθηκε το άρθρο 312 ΠΚ. Στην παράγραφο 1 φαίνεται ότι ποινικοποιείται το bullying με τη νομοτυπική μορφή να αποτελείται από μία σταθερή και συνεχιζόμενη σκληρή συμπεριφορά προς ένα άλλο άτομο, η οποία μπορεί να προκαλέσει σε τρίτον σωματική κάκωση ή κάποια άλλη βλάβη της σωματικής ή της ψυχικής υγείας του. Η έννοια του συνεχούς της επίθεσης ορίζεται ως η διαρκής κατάσταση, η οποία έχει τέτοια χρονική διάρκεια, ώστε δεν φαίνεται να διακόπτεται (Σπυρόπουλος, 2011).

Βέβαια τίθεται μία ρήτρα επικουρικότητας του άρθρου αυτού αναφορικά με το αν τιμωρείται βαρύτερα από άλλη πράξη, όπως οι διατάξεις για τις σωματικές βλάβες. Με βάση τις ερμηνευτικές προσθήκες του ανώτατου Δικαστηρίου, του Αρείου Πάγου, η έννοια της σκληρής συμπεριφοράς εμφανίζεται να στερείται συναισθήματος απέναντι σε ένα άλλο πρόσωπο, που εμφανίζεται πιο αδύναμο, ενώ η συμπεριφορά αυτή εκφράζεται με την πρόκληση πόνων, βασάνων και οδυνών σε σωματικό και ψυχικό επίπεδο (Συμεωνίδου – Καστανίδου, 2001).

Επίσης πρόκειται για κοινό και γνήσιο πολύτροπο έγκλημα και ως εκ τούτου μπορεί αν τελεστεί με οποιονδήποτε από τους περισσότερους τρόπους τέλεσης, που περιγράφονται στη νομοτυπική μορφή. Επίσης, στην περίπτωση που το θύμα είναι ανήλικο, ο νομοθέτης στην παρ. 2 όρισε μία διακεκριμένη μορφή του εγκλήματος. Επιπλέον, όπως παρατηρείται από το άρθρο, η πρόκληση της βλάβης ρητά αφορά είτε την σωματική είτε την ψυχική υγεία του θύματος (Σπυρόπουλος, 2011).

Από την άλλη τέθηκε συχνά το ζήτημα ότι λόγω της προαναφερθείσας ρήτρας επικουρικότητας σε σχέση με βαρύτερη πράξη, δεν έμενε μεγάλο πεδίο εφαρμογής για το άρθρο αυτό. Στο νέο ποινικό κώδικα του 2019 το άρθρο αυτό μετετράπη σε «σωματική βλάβη αδυνάμων ατόμων» δηλώνοντας άμεσα πως η διάταξη πλέον καταλαμβάνει όλες τις σωματικές βλάβες σε βάρος των αδυνάμων ατόμων, ακόμη και αν είναι μεμονωμένες. Πλέον το 312 ΠΚ για να τύχει εφαρμογής, θα πρέπει τα αδύναμα άτομα να βρίσκονται υπό την επιμέλεια ή υπό την προστασία του δράστη, να συνοικούν μαζί του ή να έχουν σχέση εργασίας ή υπηρεσίας με αυτόν (Συμεωνίδου- Καστανίδου, 2020).

3.4.4 Η εξύβριση και η δυσφήμιση

Όσον αφορά την εξύβριση, στον ποινικό κώδικα αυτή ορίζεται από το άρθρο 361 και συγκεκριμένα *«1. Όποιος, εκτός από τις περιπτώσεις της δυσφήμησης (άρθρα 362 και 363), προσβάλλει την τιμή άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλο τρόπο τιμωρείται με φυλάκιση έως έξι μήνες ή χρηματική ποινή. Αν τελεί την πράξη δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως ένα έτος ή χρηματική ποινή. Από την άλλη η δυσφήμιση θεσμοθετείται στο άρθρο 362 «1. 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 έως ένα έτος ή χρηματική ποινή. Αν η πράξη τελέστηκε δημόσια με οποιονδήποτε τρόπο ή μέσω διαδικτύου, επιβάλλεται φυλάκιση έως τρία έτη ή χρηματική ποινή.»* (Ποινικός Κώδικας- Νόμος 4619/2019).

Όπως παρατηρείται ήδη από την ανάγνωση των δύο άρθρων, η εξύβριση και δυσφήμιση είναι δύο αμοιβαία αποκλειόμενα εγκλήματα, όπως φαίνεται και από την ρήτρα του 361 ΠΚ. Η μεν εξύβριση αφορά την γενικότερη προσβολή της τιμής του

άλλου με λόγο ή με έργο ή με οποιονδήποτε άλλο τρόπο. Η δε δυσφήμιση αφορά ισχυρισμούς ή διαδόσεις γεγονότος (δηλαδή περιστατικού που έχει συμβεί στο παρελθόν ή συμβαίνει στο παρόν), ενώπιον τρίτου, το οποίο μπορεί να προσβάλλει την τιμή ή την υπόληψη του. Επομένως, οι δύο αυτές εγκληματικές πράξεις διαφέρουν αν και αποτελούν και οι δύο προσβολές της τιμής. Η εξύβριση είναι ηπιότερη μορφή, ενώ η δυσφήμιση, δεδομένου ότι αποτελεί διάδοση γεγονότος προσβλητικού της τιμής, τιμωρείται βαρύτερα (Συμεωνίδου- Καστανίδου, 2020).

Και στις δύο περιπτώσεις, όπως παρατηρείται, προβλέπεται διακεκριμένη μορφή των εγκλημάτων, όταν η πράξη τελείται μέσω του Διαδικτύου. Επειδή, λοιπόν, τα εγκλήματα αυτά, όταν τελούνται μέσω του ίντερνετ, προκαλούν μεγαλύτερη βλάβη του εννόμου αγαθού της τιμής, λόγω του ευρύτερου κοινού στο οποίο δημοσιοποιείται η προσβολή. Επομένως, υφίσταται ποινική πρόβλεψη για την προστασία της τιμής των χρηστών του διαδικτύου, οι οποίοι βιώνουν υβριστικές ή δυσφημιστικές επιθέσεις κυρίως μέσω των κοινωνικών δικτύων(Συμεωνίδου- Καστανίδου, 2020).

Κεφάλαιο 4. Η αντιμετώπιση των διαδικτυακών εγκλημάτων

4.1 Οι δυσκολίες κατά τη διερεύνηση και την απονομή δικαιοσύνης για τα διαδικτυακά εγκλήματα

Λόγω της ταχέως οξύνσεως του ηλεκτρονικού εγκληματικού παρασκηνίου, κρίθηκε αναγκαίο τα εθνικά ποινικά δικαστήρια να βρίσκονται σε επιφυλακή για την πάταξή τους. Το δυστυχές έγκειται στο γεγονός ότι οι ανακριτικοί υπάλληλοι της ελληνικής αστυνομίας έρχονται καθημερινά αντιμέτωποι με εγκληματίες στο στόχαστρο των οποίων βρίσκονται ανήλικοι, και που επιδίδονται σε παραβατικές δραστηριότητες με θύματα τους ανωτέρω. Ενδεικτικά παραδείγματα εγκληματικών παρατυπιών είναι ο διαδικτυακός εκφοβισμός (*cyber-bullying*), η παρακίνηση ανηλίκων για συμμετοχή σε παράνομα παίγνια αλλά και η διανομή πορνογραφικού υλικού (Minnaar, 2014).

Βέβαια, είναι απαραίτητο να επισημανθεί ότι το ζήτημα με τα ηλεκτρονικά εγκλήματα εντοπίζεται όχι μόνο στην σύλληψη του δράστη, αλλά παρουσιάζει προβλήματα ο ακριβής εντοπισμός και περιορισμός της παθογόνου αυτής εξάπλωσης κυρίως, εξαιτίας των ιδιαίτερων χαρακτηριστικών του. Πιο συγκεκριμένα, η ακριβής απονομή της ποινικής δικαιοσύνης πρέπει να γίνεται προς ένα ορισμένο πρόσωπο, που αναγνωρίζεται ως ο δράστης (Αγγελής, 2005).

Ωστόσο, στην περίπτωση της διερεύνησης των διαδικτυακών παραβιάσεων, ο εντοπισμός του είναι πολύ δύσκολος, μιας και το Ίντερνετ λειτουργεί ως ένας αχανής χώρος πληροφοριών που διακινούνται σε ελάχιστο χρόνο, με αποτέλεσμα η ακριβής τοποθεσία και το ίδιο το πρόσωπο του εγκληματία να παραμένει κεκαλυμμένη και προστατευμένη (Ajayi, 2016).

Ταυτόχρονα, οι διάφοροι ιστότοποι, που επιτρέπουν την διάδοση και συντήρηση των εγκληματικών δραστηριοτήτων, είναι σε θέση, πέρα από την απόκρυψη της πραγματικής ταυτότητας των εγκληματιών, να συμβάλλουν, ώστε η προσβολή των εννόμων αγαθών των ανηλίκων να παραμείνει ενεργή ακόμα και μετά την σύλληψη των δραστών. Αυτό οφείλεται στο γεγονός ότι η μεγάλη επισκεψιμότητα των ιστοσελίδων αυτών δημιουργεί τις προϋποθέσεις ώστε πολλοί χρήστες του διαδικτύου

να έχουν πρόσβαση σε αυτό σε διαδικτυακούς χώρους με προστατευμένες *IP address* («διεύθυνση IP»), στις οποίες η δίωξη του ηλεκτρονικού εγκλήματος να μην είναι σε θέση να υπεισέλθει για να τις κλείσει (*shutting down websites with malicious content*) (Minnaar, 2014).

Για να γίνει πιο απτή η εγκληματική δράση, μέσω του διαδικτύου, το παράδειγμα της διανομής πορνογραφικού υλικού με θύματα ανηλίκους, μπορεί να δώσει σαφείς απαντήσεις στις δυσχέρειες που καλείται να αποσοβήσει καθημερινά το τμήμα της «ηλεκτρονικής αστυνομίας». Έτσι, οι δράστες, αρχικά μπορούν να ανεβάσουν το πορνογραφικό υλικό σε διακεκριμένες παράνομες ιστοσελίδες, όπου έχει ελεύθερη πρόσβαση ένας ακαθόριστος αριθμός χρηστών (Ajayi, 2016).

Οι τελευταίοι, με τη σειρά τους, με την είσοδο και την παρακολούθηση του συγκεκριμένου παραβατικού υλικού, συντηρούν μια μεγάλη επισκεψιμότητα στις ιστοσελίδες αυτές (*website traffic*), μετουσιώνοντας και τους εαυτούς τους σε δυνητικούς δράστες του εν λόγω εγκλήματος, μιας και μπορούν να το κατεβάσουν στους δικούς τους υπολογιστές και στην συνέχεια να το διανείμουν οι ίδιοι. Με αυτόν τον τρόπο, αυξάνεται ο αριθμός των πιθανών δραστών, ενώ ταυτόχρονα μειώνονται οι πιθανότητες η δίωξη του ηλεκτρονικού εγκλήματος να μπορέσει να σβήσει κάθε διαδικτυακό ίχνος της παραβατικής δραστηριοποίησης (Saini et al, 2012).

Στα ανωτέρω προστίθεται και το γεγονός ότι στις πλείστες των περιπτώσεων, η επίλυση της διαδικτυακής παθογένειες αξιώνει την συνεργασία περισσότερων κρατών, στα τοπικά όρια των οποίων ανιχνεύονται οι δράστες αλλά και το πεδίο δράσης τους. Πιο αναλυτικά, με δεδομένο ότι το διαδικτυακό έγκλημα δεν μπορεί να περιοριστεί σε στενά εδαφικά και χρονικά όρια, όπως συμβαίνει συχνά στα παραδοσιακά κοινά εγκλήματα, όπου ο χωροχρόνος είναι εύκολα προσδιορίσιμος, η διακρατική συνεργασία είναι απαραίτητη, μιας και μπορεί να αποκλίνει ο χρόνος και ο τόπος που γίνεται αντιληπτή η εγκληματική δραστηριοποίηση, με εκείνον που συνελήφθη ο δράστης (Minnaar, 2014).

Ταυτόχρονα, στο παραπάνω πρόβλημα του τοπικού και χρονικού προσδιορισμού του εγκλήματος προστίθεται και το ζήτημα της δικανικής δικαιοδοσίας. Ειδικότερα, ακριβώς επειδή υπάρχει μια διασυνοριακή διερεύνηση του εγκλήματος, μιας και απαιτείται η ενεργοποίηση των ανακριτικών υπαλλήλων περισσότερων κρατών, εμμένει το ζήτημα του κατά πόσο και με ποια κριτήρια θα προσδιοριστεί η κατά τόπον και καθ’ ύλην αρμοδιότητα των δικαστηρίων. Με άλλα λόγια, ακριβώς επειδή δεν υφίσταται ένα δικαστήριο ευρωπαϊκό που να εκδικάζει τις περιπτώσεις των

ηλεκτρονικών εγκλημάτων, όταν συμπλέκονται περισσότερα κράτη, ο βαθμός δικαιοδοσίας αλλά και το εφαρμοστέο δίκαιο δεν μπορούν να προσδιοριστούν εκ των προτέρων, μιας και ο τόπος τέλεσης του αδικήματος, αλλά και ο τόπος επέλευσης των συνεπειών του ενδέχεται να μην ταυτίζονται, εμποδίζοντας έτσι την έρευνα σε έναν μοναδικό εδαφικό χώρο (Αγγελής, 2005).

Επιπλέον, δυσχέρειες παρουσιάζει στο σύστημα απονομής της δικαιοσύνης και η ελλιπής εκπαίδευση των ανακριτικών αρχών για την καταστολή των ηλεκτρονικών εγκλημάτων (Saini et al, 2012). Στις ικανότητες των αστυνομικών της δίωξης ηλεκτρονικού εγκλήματος, προστίθεται, πέρα από την σωματική εκπαίδευση, η αναγκαιότητα ύπαρξης τεχνικών γνώσεων για τους ηλεκτρονικούς υπολογιστές. Αν ελλείπει η ανωτέρω συνιστώσα, γίνεται εύκολα αντιληπτό ότι οι αστυνομικές αρχές δεν διαθέτουν επαρκές και με την κατάλληλη τεχνογνωσία προσωπικό, προκειμένου να αποκατασταθεί η προσβολή των εννόμων αγαθών των ανηλίκων (Αγγελής, 2005).

Βέβαια, η παραπάνω αξίωση για κατάκτηση της αναγκαίας τεχνογνωσίας για ζητήματα ηλεκτρονικών υπολογιστών απευθύνεται και στους υπόλοιπους παράγοντες της δικανικής διαδικασίας. Έτσι, οι Έλληνες νομικοί, δικηγόροι, δικαστές και εισαγγελείς οφείλουν να συμβαδίσουν με τις εξελίξεις που επιβάλλει η διεύρυνση των εγκληματικών τύπων και παραβατικών δράσεων, διαφορετικά η απονομή της δικαιοσύνης δεν θα είναι αποτελεσματική. Κατά συνέπεια, η τεχνική ορολογία των νέων μορφών εγκλημάτων είναι απαραίτητο να ενσωματωθεί στην νομική εκπαίδευση των παραγόντων της δίκης, μιας και από αυτή εξαρτάται κατά κύριο λόγο η ορθή δικονομική κρίση (Garfinkel, 2010).

Κλείνοντας, στις δυσκολίες που φέρνουν στον νομικό κόσμο, η τέλεση των ηλεκτρονικών εγκλημάτων μπορεί να προστεθεί και το ζήτημα ότι οι ορολογίες είναι διατυπωμένες αποκλειστικά στην αγγλική γλώσσα, χωρίς, μέχρι στιγμής να έχει υπάρξει προσπάθεια απόδοσής τους στην ελληνική. Το γεγονός αυτό, συμβάλλει περαιτέρω στην διαιώνιση του προβλήματος απονομής της δικαιοσύνης, μιας και αναγκάζει το δικαστήριο να υπεισέλθει σε ζητήματα που δεν είναι δόκιμα στα ελληνικά και μπορούν να αποδοθούν μόνο περιγραφικά (Αγγελής, 2005).

Σε όλα αυτά, τέλος, προστίθεται και το πρόβλημα της δυσχερούς συλλογής αποδεικτικών μέσων για την επίρρωση των δικονομικών λεγομένων. Έτσι, στο πλαίσιο της κύριας ποινικής διαδικασίας, η απόδειξη των πραγματικών περιστατικών για εγκλήματα που αναφύονται στην διαδικτυακή ανωνυμία είναι ιδιαίτερα δύσκολη και συχνά πρέπει να στηρίζεται αποκλειστικά σε εκθέσεις πραγματογνωμόνων ή σε

μαρτυρικές καταθέσεις, γεγονός που δεν διασφαλίζει πάντα την ακεραιότητα των δικονομικών αποφάσεων (Ajayi, 2016).

Παρόλα τα ζητήματα που αναφύονται, είναι έντονα επιβεβλημένο από τον χαρακτήρα των ατόμων που θυματοποιούνται να επιλυθούν τα ανωτέρω προβλήματα, για να επιτευχθεί η αποκαταστατική όψη της ποινικής δικαιοσύνης. Η ανηλικότητα που προστατεύεται από το ελληνικό δίκαιο ως κοινωνικό αγαθό απαιτεί την λήψη αποφασιστικών προληπτικών και κατασταλτικών μέτρων, που να είναι σε θέση να προστατεύσουν τα παιδιά από την εγκληματική δραστηριοποίηση των διαδικτυακών παραβατών. Στο πλαίσιο της ανωτέρω προσπάθειας, είναι ιδιαίτερα ενθαρρυντική η δράση της ελληνικής δίωξης ηλεκτρονικού εγκλήματος (Saini et al, 2012).

Πιο συγκεκριμένα, ο κρατικός αυτός φορέας έχει αντιληφθεί την σπουδαιότητα της αντιμετώπισης των νέων αυτών διακεκριμένων εγκλημάτων ιδίως μάλιστα όταν τα θύματα είναι οι ανήλικοι, οι οποίοι χρειάζονται την ενήλικη και πιο υποψιασμένη για τους κινδύνους που ελλοχεύουν στον διαδικτυακό χώρο, θωράκιση. Στο εγχείρημα αυτό, το πρώτο μέλημα, στο οποίο εστιάζει η αστυνομία είναι η παρατήρηση των αλλαγών που επιφέρει στον τρόπο που κατανοείται το έγκλημα, η διαδικτυακή τέλεσή του. Μέσα από την κατανόηση των διαφοροποιήσεων που έχει από τα κοινά-παραδοσιακά εγκλήματα, η ελληνική αστυνομία έχει την δυνατότητα να καταλήξει σε ορισμένα επαρκή συμπεράσματα και να σκιαγραφήσει τον τρόπο ηλεκτρονικής δράσης των παραβατών (Ajayi, 2016).

Με αυτόν τον τρόπο, το προσωπικό της μπορεί να επιμορφωθεί πιο άρτια και αποτελεσματικά για τα ζητήματα τεχνικής φύσεως, μια νέα οπτική στην διευκόλυνση των διαδικτυακών παραβατικών δραστηριοτήτων. Η συνεχής εκπαίδευση και ο εφοδιασμός των αστυνομικών αρχών με την απαραίτητη τεχνογνωσία για τους ηλεκτρονικούς υπολογιστές μπορούν να συμβάλλουν, ώστε το αστυνομικό προσωπικό που ασχολείται με τα ηλεκτρονικά εγκλήματα να βρίσκεται σε διαρκή επιφυλακή και να μπορέσει να επέμβει αποφασιστικά ανακόπτοντας το πλήθος των συνεπειών της έξαρσης τους επιτρέποντας την περαιτέρω καταστολή τους (Αγγελής, 2005).

Στον ελλαδικό χώρο, η δράση της ηλεκτρονικής δίωξης είναι ιδιαίτερα ενθαρρυντική, μιας και διαθέτει προσωπικό που κατέχει τις γνώσεις για την κατασταλτική επέμβαση στον διαδικτυακό χώρο και την άρση της ανωνυμίας των δραστών, όπου αυτοί αφήνουν ηλεκτρονικά ίχνη, που οι διωκτικές αρχές «ακολουθούν». Η υπηρεσία, ωστόσο της δίωξης του ηλεκτρονικού εγκλήματος εφιστά την προσοχή των πολιτών σε οτιδήποτε τους κινήσει την υποψία κατά την περιαγωγή

τους στους διαδικτυακούς χώρους, μιας και η χωρίς χρονοτριβή επέμβασή της αυξάνει τις πιθανότητες να βρεθούν ίχνη που θα οδηγήσουν στην εύρεση των δραστών και στην καταδίκη τους για τα διαπραττόμενα εγκλήματά τους. Έτσι, είναι ενθαρρυντικό το γεγονός ότι υπάρχει διακριτό τμήμα της ελληνικής αστυνομίας που στελεχώνεται, κυρίως από νέους αστυνομικούς που κατέχουν την τεχνογνωσία των ηλεκτρονικών υπολογιστών και είναι σε θέση να κινούνται στους διαδικτυακούς χώρους, αναζητώντας παράνομες ιστοσελίδες ή ύποπτο διακινούμενο υλικό (Αγγελής, 2005).

4.2 Ασφαλή πληροφοριακά συστήματα

Είναι εύκολα αντιληπτό ότι η ανάπτυξη του διαδικτύου τις τρεις τελευταίες δεκαετίες ήταν αλματώδης, δημιουργώντας τις προϋποθέσεις για την διαμόρφωση μιας διακεκριμένης μορφής κοινωνικού χώρου, με εξατομικευμένα γνωρίσματα και νέους διακριτούς ρόλους. Βέβαια, εκτός από τα θετικά που έχει προσφέρει η κοινωνία της πληροφορίας, τα οποία φυσικά δεν μπορούν να παραβλεφθούν, οι επιπτώσεις αυτής της νέας τεχνολογίας, έφερε αντιμέτωπο το σύνολο των πολιτών που μετεξελίχθηκαν σε χρήστες του, με νέες προκλήσεις (Αγγελής, 2005).

Πιο συγκεκριμένα, το παραδοσιακό μη εικονικό περιβάλλον διακατέχεται από πλήθος κανόνων που οι άνθρωποι επέλεξαν για την κοινωνική συναναστροφή τους για την διατήρηση της ευπρέπειας των διαπροσωπικών σχέσεων. Στον αντίποδα, αυτός ο μεστός τεχνολογικός πολιτισμός μετεξέλιξε την σκακιέρα των επικοινωνιακών πρακτικών και των κανόνων της κοινωνικής πραγματικότητας, ωθώντας τους χρήστες του στην υιοθέτηση των νεοεισαχθέντων συμπεριφορικών συμβάσεων και δεδομένων (Sammons & Cross, 2016).

Ο ψηφιακός κόσμος συμβιώνει σε παράλληλο χωροχρόνο με τη μη εικονική πραγματικότητα, διαθέτοντας ουσιαστικά ένα καινό καθεστώς από κανόνες που στις περισσότερες περιπτώσεις δεν συμβαδίζει πλήρως με την καθεστηκυία καθημερινότητα, επιτρέποντας παρεκκλίσεις από τις κοινωνικές νόρμες. Αυτό βέβαια, μπορεί να έχει ανυπολόγιστες συνέπειες, μιας και η ανωνυμία που προσφέρει το διαδίκτυο στους χρήστες του είναι σε θέση να υποθάλπει παραβατικές στάσεις και συμπεριφορές που στον πραγματικό κόσμο αποτυπώνονται ως εγκληματικές δράσεις και είναι ποινικά κολάσιμες (Αγγελής, 2005).

Στο πλαίσιο της εξέτασης του φαινομένου των ηλεκτρονικών εγκλημάτων με θύματα κυρίως ανήλικα άτομα, είναι απαραίτητο να επισημανθεί ότι η αποσόβηση των αρνητικών συνεπειών του διαδικτύου συνιστά πρώτιστο μέλημα της κοινωνίας της τεχνολογίας, μιας και ο νόμος των πολιτειών (έστω και των νεοοικοδομηθέντων, όπως αυτός του διαδικτυακού χώρου) οφείλει να προστατεύει τις υπεραξίες της ανθρώπινης αξιοπρέπειας και της προσωπικής ζωής των αδυνάμων και πιο επιρρεπών, σε ζητήματα ευπιστίας και αδυναμίας πρόβλεψης των προβλημάτων, κοινωνικών ομάδων (Sammons & Cross, 2016).

Ειδικότερα, είναι απαραίτητο η πρόσβαση και η αξιοποίηση των δυνατοτήτων που προσφέρει το Ίντερνετ να γίνεται με σεβασμό σε θεμελιώδη δικαιώματα και αγαθά που το σύνολο των ανθρώπινων κοινοτήτων έχει αποδεχθεί ως απαραβίαστο πυρήνα για την κοινωνική συναναστροφή και συνεργασία. Αυτό οδηγεί, ώστε τα συστήματα που παράγονται και λειτουργούν στο διαδίκτυο και οφείλουν να διευκολύνουν τις ανθρώπινες επαφές, να γίνονται με γνώμονα τον σεβασμό των προσωπικών δεδομένων αλλά και του απορρήτου των συνομιλιών και της αλληλογραφίας και κατά συνέπεια να προστατεύονται τα στοιχεία εκείνα που συναπαρτίζουν την έννοια της ανθρώπινης οντολογικής κοινωνικής παρουσίας και της εκτίμησης που αξιώνει η ατομικότητα του κάθε ανθρώπου (Αγγελής, 2005).

Με δεδομένο, λοιπόν, ότι το διαδίκτυο πλέον έχει μετουσιωθεί σε αναπόσπαστο εργαλείο της καθημερινότητας των πολιτών, αφού μέσω αυτού, εκείνοι διαπλάθονται εκπαιδευτικά αλλά και κοινωνικά, ψυχαγωγούνται ή επικοινωνούν με τους υπόλοιπους χρήστες, αξιώνεται η κατάστρωση μιας πολιτικής που να διαμορφώνει ένα ασφαλές περιβάλλον περιαγωγής στις ιστοσελίδες και τους διαδικτυακούς τόπους. Κατά συνέπεια, ένα πληροφοριακό σύστημα, προκειμένου να διαθέτει επίπεδο ασφαλείας και προστασίας του συνόλου των χρηστών του και να μην υποσκάπτει ή διαιωνίζει την τέλεση εγκλημάτων οφείλει να διακρίνεται από εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Sammons & Cross, 2016).

Αναλυτικότερα, η έννοια της εμπιστευτικότητας (*confidentiality*) αφορά, κατά κύριο λόγο την διακίνηση προϊόντων και ηλεκτρονικών δεδομένων μόνο μέσα από εξουσιοδοτημένα άτομα και φορείς. Κάτι τέτοιο, αποκαθιστά την εγγενή αμφισβήτηση και δυσπιστία των χρηστών για την φερεγγυότητα των διαδικτυακών διανομέων, επιτρέποντας την ελεύθερη διακίνηση των αγαθών, με μέτρα ασφαλείας και αξιοπιστίας (Maindonald & Stott, 2014).

Παράλληλα, η ακεραιότητα (*data integrity*), αποτελεί στοιχείο που πρέπει να διακρίνει κάθε πληροφοριακό σύστημα, μιας και οι μηχανισμοί της είναι σε θέση να προλαμβάνουν την κακοήθη δράση των μη εξουσιοδοτημένων εγγραφών ή δημιουργίας δεδομένων, με σκοπούς παράνομους. Έτσι, η ηλεκτρονική πληροφορία προστατεύεται από κάθε προσπάθεια τροποποίησής ή μεταβολής της, εξασφαλίζοντας την ορθότητά της (Garg et al, 2020).

Τέλος, με την έννοια της διαθεσιμότητας (*availability*) νοείται το σύνολο των παραμέτρων που λαμβάνονται, προκειμένου οι χρήστες που είναι εξουσιοδοτημένοι να έχουν προσπελάσιμη είσοδο στο πληροφοριακό σύστημα, χωρίς να παρεμποδίζεται η εξυπηρέτησή τους, όταν χρειάζεται να προσπελάσουν τους υπάρχοντες πόρους του. Με αυτόν τον τρόπο, διαφυλάσσεται και η ίδια η προστασία των αρχών της εμπιστευτικότητας και της ακεραιότητας, καθώς η εξουσιοδοτημένη πρόσβαση στην πληροφορίας για την αποκάλυψη ή τη μεταβολή της γίνεται ανεμπόδιστα και χωρίς χρονοτριβή (Trivedi et al, 2012).

Με βάση τα παραπάνω, γίνεται αντιληπτό ότι στο πιθανό σενάριο της απουσίας ή παραβίασης των ιδιοτήτων αυτών, ένα πληροφοριακό σύστημα παύει να θεωρείται ασφαλές, λειτουργώντας ως μέσο προς σκοπό για τις εγκληματικές δράσεις παραβατών. Η ανασφάλεια αυτή αποτρέπει την προστασία των χρηστών και ειδικότερα των ανήλικων ατόμων, που είναι πιο ευάλωτα και λιγότερο υποψιασμένα για τις κακόβουλες προθέσεις των αγνώστων του διαδικτύου. Η επίθεση στα πληροφοριακά συστήματα γίνεται, κατά συνέπεια, για να καταστεθούν ανασφαλή, αδυνατώντας να διαφυλάξουν τους πόρους και την προστασία των διακινούμενων δεδομένων. Έτσι, διαρρηγνύεται η ασφάλεια των πληροφοριών και οι χρήστες είναι εκτεθειμένοι σε κάθε κακόβουλη πρακτική (Sammons & Cross, 2016).

Όπως προαναφέρθηκε, η ανθρώπινη αξιοπρέπεια αξιώνει την λήψη μέτρων, προληπτικών και κατασταλτικών σε κάθε περιστατικό παραβίασης των αρχών της προστασίας των ατομικών δεδομένων που συμβαίνει στον χωροχρόνο του διαδικτύου. Απότοκο και ιδιαίτερη έκφανση της προστασίας και προαγωγής της ατομικής ελευθερίας, συνιστά το ότι στον κάθε άνθρωπο, στην νέα εικονική πραγματικότητα, επιτρέπεται η άνευ εμποδίων διακίνηση και διατύπωση των προσωπικών του ιδεών, η ελεύθερη ανάπτυξη της προσωπικότητας, αλλά και η επικάλυψη των επικοινωνιών του με πρωτόκολλα απαραβίαστου (Garg et al, 2020).

Οι παραπάνω θεμελιακές βάσεις της ανθρώπινης αξιοπρέπειας, οδηγούν στην συνειδητοποίηση ότι τα θετά δικαιώματα των ατόμων αξιώνουν την αναγκαιότητα

εφαρμογής μέτρων που να διασφαλίζουν την μη διαρροή και κοινοποίηση των πληροφοριών τους σε τρίτα, άγνωστα προς τους ίδιους, πρόσωπα και απαιτούν την διακίνησή τους με μυστικότητα και ασφάλεια. Ωστόσο, παρόλο που σε θεωρητικό επίπεδο η εφαρμογή των ανωτέρω αρχών θεωρείται τυπικά εύκολα πραγματοποιήσιμη, εντούτοις, τόσο από νομικής όσο και από τεχνικής απόψεως το ζήτημα είναι δυσεπίλυτο. Αυτό συμβαίνει γιατί ενώ, ο τεχνικός των πληροφοριακών συστημάτων σκοπεύει να εξασφαλίσει την προστασία των χρηστών του, εν τέλει κάποιος που επιδίδεται σε εγκληματικές δραστηριότητες μπορεί, με τη σειρά του να παραγάγει ένα σύστημα «αντασφάλειας» που εξουδετερώνει τους προστατευτικους μηχανισμούς του πρώτου, προκειμένου να διευκολυνθεί η παραβίαση και η διαρροή των ανασφαλών πλέον δεδομένων (Sammons & Cross, 2016).

Τέλος, αν το ζήτημα ιδωθεί από την νομική σκοπιά, εξακολουθεί να είναι ακανθώδες, μιας και τα εθνικά νομοθετικά αντανακλαστικά για την παρακολούθηση των τεχνολογικών εξελίξεων και κατανόηση των επιπτώσεων που αυτές επιφέρουν κοινωνικά είναι μειωμένα, διευκολύνοντας την ελεύθερη και ατιμώρητη περιδιάβαση των διαδικτυακών δραστών. Αυτό βέβαια, συμπλέκεται και με το γεγονός ότι δεν υφίσταται ορισμένη τεχνική δομή στον κυβερνοχώρο, με αποτέλεσμα η μη σταθεροποίηση αυτού να εμποδίζει την ουσιαστική και δικονομική διαλεύκανση των παραβατικών συμπεριφορών (Shinder & Cross, 2008).

4.3 Μέτρα πρόληψης και προστασίας των ανηλίκων

Με βάση όλα τα παραπάνω γίνεται εύκολα αντιληπτό ότι ο διαδικτυακός χώρος ελλοχεύει πολλαπλούς κινδύνους για τους χρήστες του. Βέβαια, αυτό εντείνεται όταν το θύμα είναι ένα ανήλικο άτομα, καθώς το νεαρό της ηλικίας του δεν του επιτρέπει να μπορεί να σταθμίζει, με λογική και σύνεση το πλήθος των αρνητικών συνεπειών που δύναται να δρομολογηθούν από μία λαθεμένη επιλογή. Οι παραβάτες του διαδικτύου, γνωρίζουν, δυστυχώς αυτή την αφέλεια που χαρακτηρίζει τα παιδιά, επιλέγοντας συνειδητά να στοχοποιήσουν τέτοια άτομα για την επιτέλεση των εγκληματικών τους κινήτρων (Smith et al, 2014).

Προκειμένου, λοιπόν, να προστατευτούν τα παιδιά από την εγγενή αδυναμία δράσης τους και την τάση τους προς την αναζήτηση της διασκέδασης, αγνοώντας τις

επιπτώσεις που επισείονται, είναι απαραίτητο οι γονείς, σε συνεργασία με εκείνα να εκπαιδευτούν πάνω σε ζητήματα ασφαλούς πλοήγησης στο διαδίκτυο. Ο λόγος που η ευθύνη προστασίας δεν εναπόκειται μόνο στους ενηλίκους είναι γιατί και τα ίδια τα παιδιά οφείλουν να πληροφορούνται ότι οι κίνδυνοι είναι υπαρκτοί, καλώντας τα να οξύνουν την κριτική τους σκέψη και να αντιμετωπίζουν τον χώρο του διαδικτύου με γόνιμη αμφισβήτηση και την λήψη όσο το δυνατόν περισσότερων προφυλάξεων, θέτοντας την ασφάλεια ως προτεραιότητα (Ahmad et al, 2019).

Πιο συγκεκριμένα, η περιαγωγή στο διαδίκτυο απαιτεί την εφαρμογή ορισμένων μέτρων ασφαλείας, ώστε οι επίδοξοι δράστες ηλεκτρονικών εγκλημάτων να μην μπορούν να θυματοποιήσουν εύκολα τα ανυποψίαστα ανήλικα άτομα. Από την πλευρά των παιδιών, η πρόσβασή τους στο διαδίκτυο οφείλει να γίνεται μετά από κάποια ηλικία, όταν εκείνο είναι πλέον ώριμο και έτοιμο να καταλάβει τους πιθανούς κινδύνους (Smith et al, 2014).

Βασικό θέμα της συζήτησης αυτής με τους γονείς είναι αναγκαίο να αποτελέσει η υπενθύμιση ότι το παιδί δεν πρέπει να μοιράζεται προσωπικές του πληροφορίες με τρίτους. Ακόμα και αν το ίδιο θεωρεί ότι συνομιλεί με άτομο που γνωρίζει, οι γονείς πρέπει να βρίσκονται σε επιφυλακή για να ελέγξουν την πραγματική ταυτότητα του χρήστη, προκειμένου να είναι σίγουροι ότι το παιδί δεν βρίσκεται εκτεθειμένο σε αγνώστους που επιδιώκουν την διαρροή ευαίσθητων δεδομένων και στοιχείων του ανηλίκου (Edwards et al, 2018).

Επιπλέον, ακόμα και για τις αγοραστικές συναλλαγές που πραγματοποιούνται ηλεκτρονικά, πρέπει να λαμβάνονται μέτρα προφύλαξης, μιας και τις περισσότερες φορές, οι διαδικτυακοί παραβάτες, επιλέγουν τρόπους εξαπάτησης που δεν θα κινήσουν τις υποψίες ή θα προλάβουν εξαπίνης το άτομο, που θα αντιληφθεί πολύ αργά τις παραβιάσεις των προσωπικών του δεδομένων. Έτσι, είναι χρήσιμο να αποφεύγονται ιστοσελίδες που δεν είναι κρυπτογραφημένες και κατά συνέπεια, μη αξιόπιστες για ηλεκτρονικές αγορές (Leena, 2011).

Είναι επιθυμητό τα διαδικτυακά καταστήματα που επιλέγουν να διαθέτουν τα εχέγγυα ανεξάρτητων φορέων ή αρχών πιστοποίησης, προκειμένου να μειώνονται οι πιθανότητες καταστρατήγησης των μηχανισμών ασφαλείας τους, ενώ παράλληλα να αποδεικνύουν την αξιοπιστία τους με κρυπτογραφημένες επικοινωνίες αξιοποιώντας το πρωτόκολλο *SSL* (*Secure Socket Layer*) (Leena, 2011). Έτσι, προχωρώντας στη διαδικασία ολοκλήρωσης των συναλλαγών, καλό είναι να επιλέγεται η χρήση χρεωστικών καρτών ή ακόμα και προπληρωμένων πιστωτικών καρτών, προκειμένου

να διασφαλίζεται ότι δεν θα αποσπαστούν χρηματικά ποσά μεγαλύτερα από εκείνα των ηλεκτρονικών αγορών (Edwards et al, 2018).

Για να θεωρηθεί πλήρης η έρευνα των ασφαλών πληροφοριακών συστημάτων κρίθηκε αναγκαίο να αναλυθεί αδρομερώς η έννοια της κρυπτογραφίας, που όπως αναφέρθηκε και παραπάνω αποτελεί ένα από τα μέτρα που περιχαρακώνουν τα πληροφοριακά συστήματα για να εξοπλιστούν με τα πρωτόκολλα προστασίας και ασφάλειας. Μέσω της κρυπτογραφίας (*cryptography*), επιτυγχάνεται η αξιόπιστη και με κάθε προστατευτικό εχέγγυο επικοινωνία και μετάδοση της πληροφορίας, εμποδίζοντας τους κακόβουλους δράστες από την διαρροή της (Katz & Lindell, 2020).

Η κρυπτογράφηση των πληροφοριών συναπαρτίζεται από το αρχικό μήνυμα (*plaintext*), το σύστημα της κρυπτογράφησης (*cryptosystem*), το κείμενο που παράγεται από την διαδικασία αυτή (κρυπτογραφημένο κείμενο - *ciphertext*) , και το κλειδί (*key*), που επιτρέπει την κρυπτογράφηση και την αποκρυπτογράφηση του μηνύματος. Με αυτόν τον τρόπο, τα απόρρητα δεδομένα μπορούν να προφυλάσσονται από τις κυβερνοεπιθέσεις, διευκολύνοντας ταυτόχρονα την διακίνησή τους στα ασφαλή κανάλια επικοινωνίας και εμποδίζοντας την πιθανότητα αλλοίωσής τους (Katz & Lindell, 2020).

Παράλληλα, στα μέτρα ασφαλείας που χρειάζεται να εφαρμόζονται σε τακτά χρονικά διαστήματα περιλαμβάνονται και οι αλλαγές των κωδικών πρόσβασης των χρηστών. Στα συστήματα, λοιπόν, που για την είσοδο σε αυτά απαιτείται η εισαγωγή ενός εξατομικευμένου ονόματος χρήστη (*user ID*) και ενός κωδικού πρόσβασης (*password*), γίνεται έλεγχος για την (αν)αλήθεια των στοιχείων, σύμφωνα με τα στοιχεία που είναι καταχωρημένα στη δική τους βάση δεδομένων των κωδικών. Εφόσον, η διασταύρωση των πληροφοριών είναι επιτυχής διευκολύνεται η πρόσβαση στο σύστημα και τις υπηρεσίες του (Edwards et al, 2018).

Ωστόσο, παρόλο που το συγκεκριμένο μέτρο ασφαλείας είναι ικανό να προφυλάξει, σε ένα πρωταρχικό στάδιο τα δεδομένα, είναι απαραίτητο να επισημανθεί ότι δυστυχώς στις κυβερνοεπιθέσεις, αυτές οι βάσεις δεδομένων μπορούν να υποκλαπούν ή να εκτεθούν στο εγκληματικό προσκήνιο. Από την πλευρά των εταιριών που διαθέτουν τα συστήματα αυτά, χρειάζεται να επενδυθούν χρήματα για τον εξοπλισμό τους με εργαλεία λογισμικού που μπορούν να πιστοποιηθούν ότι οι κωδικοί θα παραμείνουν μυστικοί και ασφαλείς, και δεν θα υπάρξει διαρροή πληροφοριών των χρηστών τους (Smith et al, 2014).

Προκειμένου να είναι προστατευμένοι οι χρήστες, χρειάζεται να τροποποιούν συχνά τον κωδικό πρόσβασής τους ειδικότερα σε λειτουργικά πληροφοριακά συστήματα που αποθηκεύουν ευαίσθητα προσωπικά ή ακόμα και οικονομικά δεδομένα. Η επιλογή των κωδικών πρόσβασης και η αλλαγή τους πρέπει να γίνεται συνειδητά και να πραγματοποιείται κατανοώντας τους κινδύνους μιας πιθανής υποκλοπής. Για αυτό το λόγο, πρέπει να τροποποιούνται και να εισάγονται κωδικοί που να είναι δυσχερές να προβλεφθούν από τους δράστες και να αποφεύγεται η χρήση ονομάτων, ημερομηνιών και γενικότερα στοιχείων που μπορεί εν τέλει να προεικάσει ο δράστης (Edwards et al, 2018).

Επιπρόσθετα, αναφέρθηκε προηγουμένως ότι οι εταιρίες και οι φορείς μπορούν, για να διασφαλίσουν την προστασία των δεδομένων που μεταχειρίζονται να αξιοποιήσουν πακέτα λογισμικών, τα οποία προστίθενται στα πληροφοριακά συστήματα κατά τον σχεδιασμό της ασφάλειάς τους και μειώνουν τον κίνδυνο κυβερνοεπιθέσεων (Smith et al, 2014).

Υπάρχουν δύο εφαρμογές που χρησιμοποιούνται κατά κύριο λόγο. Από την μία επιλέγονται τα λογισμικά antivirus, που στοχεύουν στην απώθηση κακόβουλων ιών. Πιο συγκεκριμένα, οι κυβερνοεπιθέσεις στην πλειοψηφία τους επιχειρούνται με την επιθετική τακτική της διασποράς ιών σε ένα λογισμικό προκειμένου αυτό να προσβληθεί και να μειωθούν τα πρωτόκολλα ασφαλείας του. Ωστόσο, με τη χρήση των αντιβιοτικών προγραμμάτων ενεργοποιείται η τριπλή δράση αυτών για την θωράκιση των υπολογιστικών συστημάτων (Zare et al, 2018).

Το λογισμικό αυτό της αντιμετώπισης των ιών ξεκινά με το στάδιο της ανίχνευσης των ιών, προκειμένου να διαπιστωθεί αν το σύστημα έχει μολυνθεί από κάποιον ιό. Αυτή η διαδικασία εκκινείται είτε χειροκίνητα από τον ίδιο τον χρήστη με μια σειρά εντολών ελέγχου του σκληρού δίσκου είτε αυτοματοποιημένα, με το antivirus λογισμικό να φορτώνεται στη μνήμη του υπολογιστικού συστήματος και να ελέγχει παράλληλα όλες τις εκτελούμενες εφαρμογές. Μετά το πέρας της ανίχνευσης, το λογισμικό προσδιορίζει την ταυτότητα και το είδος των ιών, για να εκτιμηθεί το εύρος της ζημιάς που προκλήθηκε, να επιδιορθωθεί και κατ’ επέκταση να επιστρέψει το σύστημα στην ομαλή του λειτουργία. Στο τρίτο τμήμα της δράσης των αντιβιοτικών προγραμμάτων, ολοκληρώνεται η δράση τους με τον καθαρισμό των ιών, αφαιρώντας τους και απομακρύνοντάς τους από τα αρχεία στα οποία είναι πιθανόν να επιτίθεται, με αποτέλεσμα να προστατεύεται το σύστημα από τη διαρροή των δεδομένων του (Arneja & Sachdev, 2015).

Από την άλλη, υπάρχει και η εφαρμογή των *firewalls*, ένα διακριτό εργαλείο λογισμικού που λειτουργεί ως φίλτρο (*packet filtering*) για τα όσα πακέτα ζητούν πρόσβαση σε ένα προστατευμένο δίκτυο, ξεχωρίζοντας την ύπαρξη ενός ασφαλούς δικτύου από ένα εξωτερικό, επιτρέποντας έτσι, ή απαγορεύοντας την κίνηση προς το δεδομένο αξιόπιστο δίκτυο (*permit or deny*). Με αυτόν τον τρόπο, τα ίδια τα υπολογιστικά συστήματα και οι χρήστες τους θέτουν όρια στα κακοήθη λογισμικά των κυβερνοεπιθέσεων προστατεύοντας τα δεδομένα και διευκολύνοντας την ασφαλή πρόσβαση στο διαδίκτυο (Zare et al, 2018).

Είναι απαραίτητο, βέβαια, να επισημανθεί ότι για να ληφθούν τα παραπάνω μέτρα ασφαλείας, απαιτείται όλοι οι εμπλεκόμενοι φορείς αγωγής και κοινωνικοποίησης να έχουν την κατάλληλη επιμόρφωση σχετικά με τις συνέπειες της αρνητικής όψης του διαδικτύου για τα ανήλικα άτομα. Στην Ελλάδα, στο πλαίσιο της Ευρωπαϊκής Επιτροπής ενεργοποιήθηκε το πρόγραμμα *Safer Internet*, για την πρόληψη του διαδικτυακού εκφοβισμού, μια δράση που επιχειρεί να προστατεύσει τους ανηλίκους από την έκθεσή τους σε επιβλαβή σχόλια και ακατάλληλη μεταχείριση από άλλους χρήστες, ευαισθητοποιώντας τους εμπλεκόμενους για τα ζητήματα ασφάλειας και διαχείρισης τέτοιων κρίσεων (Arneja & Sachdev, 2015).

Τέλος, από το 2008, λειτουργούν τρία συστήματα δραστηριοποίησης που συναπαρτίζουν το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου. Έτσι, υπάρχει η ανοιχτή γραμμή καταγγελιών (*Safe Line*), η δράση ενημέρωσης και επαγρύπνησης («*saferinternet4kids.gr*») και η γραμμή βοήθειας («*Help – Line.gr*»), που διαχειρίζονται τις παθογένειες που γίνονται μέσω του διαδικτύου. Κλείνοντας, θα ήταν παράλειψη να μην αναφερθεί ότι με τον ν. 4512/2018, τροποποιήθηκε ο νόμος για την προστασία του καταναλωτή, θέτοντας τον ανήλικο καταναλωτή και την ψυχική του υγεία ως προτεραιότητα του. Αυτή η πρακτική καταδεικνύει την σπουδαιότητα που κατέχει η διατήρηση της ψυχικής ευημερίας των ανηλίκων και η διαμόρφωση προσωπικοτήτων που δεν έχουν σπιλωθεί από την αρνητική επενέργεια του διαδικτύου και των ατόμων που υποκρύπτουν μέσω της ανωνυμίας αυτού της προθέσεις τους (Δαλακούρας, 2019).

Κατά συνέπεια, τα μέτρα ασφαλείας που λαμβάνονται οφείλουν να είναι ανάλογα του κινδύνου που υφίστανται τα ανήλικα άτομα από τους επιτήδειους του διαδικτύου. Τόσο οι γονείς, όσο και οι εταιρείες που διαχειρίζονται προσωπικά δεδομένα αλλά και το ίδιο το κράτος είναι απαραίτητο να ενεργοποιηθούν προκειμένου να διαμορφωθεί ένας διαδικτυακός χώρος προσιτός και κατάλληλος για την ανάπτυξη των παιδιών στο

νέο μοντέλο κοινωνίας, αυτό της τεχνολογικής προόδου και της επίφοβης ανωνυμίας, που συχνά καταχρώνται οι διαδικτυακοί εγκληματίες (Shinder & Cross, 2008).

ΕΠΙΛΟΓΟΣ

Από όλα τα παραπάνω προκύπτει αβίαστα το συμπέρασμα ότι στην εποχή της τεχνολογικής ανάτασης, οι νέοι πρωτοστατούν, ως χρήστες των νέων διαδικτυακών επιλογών. Στην γενιά αυτή, η πληροφορία και η ταχεία διάδοσή της εξυψώθηκε σε υπεραξία και ένα αγαθό που δεν μπορεί να περιοριστεί στα στενά τοπικά όρια μιας επικράτειας. Για τα ανήλικα άτομα, η ενασχόληση με το Ίντερνετ δεν νοείται ως μια απλή συμπληρωματική δραστηριότητά τους, αλλά ως η κύρια καθημερινή τους ενασχόληση. Απότοκο της ανωτέρω πρακτικής αποτελεί το γεγονός ότι καταναλώνουν πολλές ώρες στα διαδικτυακά κανάλια και τις ιστοσελίδες, ερχόμενοι σε επαφή με μεγάλο αριθμό ανεπιβεβαίωτων προσώπων, αυξάνοντας έτσι την πιθανότητα να θυματοποιηθούν λόγω κακόβουλων προθέσεων.

Αυτό επιβεβαιώνει ότι δεν είναι μόνο η πληροφορία που δεν περιορίζεται τοπικά και χρονικά λόγω του διαδικτύου, αλλά και τα εγκλήματα που διευκολύνονται μέσω των ιδιαίτερων χαρακτηριστικών που αυτό το είδος επικοινωνίας και συνδιαλλαγής διαθέτει. Πιο συγκεκριμένα, στο διαδίκτυο έχουν πρόσβαση εκατομμύρια χρήστες που δεν ελέγχονται προσωπικά για την παρουσία τους σε αυτό, επιτρέποντάς τους να διατηρήσουν την ανωνυμία τους και να επιδοθούν σε εγκληματικές δράσεις χωρίς να αφήσουν κανένα ίχνος. Την ίδια στιγμή, οι ανυποψίαστοι χρήστες που θυματοποιούνται από εκείνους είναι πολύ δύσκολο να προλάβουν τις εγκληματικές συνέπειες που προελαύνουν, μιας και τις περισσότερες φορές η επίτευξη του εγκληματικού σχεδίου δεν ακολουθεί τον παραδοσιακό τρόπο επιτέλεσης εγκλημάτων αλλά βασίζεται στο λαθεμένο αίσθημα ασφάλειας που περιβάλλει τα άτομα, όταν περιάγονται στις διαδικτυακές ιστοσελίδες.

Στην γεωμετρική αύξηση των ηλεκτρονικών εγκλημάτων με διευκολυντικό μέσο την διαδικτυακή ανωνυμία και την ταχύτητα κάλυψης των ηλεκτρονικών ιχνών συμβάλει και το γεγονός ότι τα ανήλικα άτομα έχουν ελεύθερη είσοδο σε αυτό, χωρίς ωστόσο αυτά να είναι εφοδιασμένα με τα κριτικά εργαλεία για την γόνιμη αμφισβήτηση των όσων εκτίθενται στις διαδικτυακές σελίδες. Ταυτόχρονα, συχνά οι επιτήδειοι χρησιμοποιούν ως μέσο πίεσης και εντυπωσιασμού την παιδική ψυχολογική αφέλεια και αθωότητα εξαναγκάζοντας τα σε πράξεις που προσβάλλουν την προσωπικότητά τους και καταστρατηγούν την ανθρώπινη αξιοπρέπεια. Η μη

συμβατική αυτή εκδοχή των εγκληματιών των διαδικτυακών εγκλημάτων είναι ιδιαίτερα επίφοβη μιας και στοχοποιούν κατά κύριο λόγο την ευάλωτη αυτή κοινωνική ομάδα, επιδρώντας έντονα στον ψυχισμό τους και καταπατώντας κάθε αίσθημα ασφάλειας που αυτή βιώνει.

Προκειμένου το ζήτημα να επιλυθεί, οφείλει ως αντίβαρο της υψηλούς τεχνογνωσίας που κατέχουν οι εγκληματικές προσωπικότητες να υπάρξει παρόμοια εκπαίδευση των διωκτικών αρχών για την ελαχιστοποίηση αυτής της ακραιφνούς έξαρσης των ηλεκτρονικών εγκλημάτων. Από μέρους τους οι έλεγχοι στους διαδικτυακούς τόπους αλλά και σε ύποπτες ιστοσελίδες οφείλουν να εντατικοποιηθούν, προκειμένου να προλαμβάνονται περιπτώσεις δραστών που δεν έχουν κατορθώσει ακόμα να εκδηλώσουν το εγκληματικό τους σχέδιο.

Ταυτόχρονα, η άμβλυνση της εμφάνισής τους μπορεί να γίνει πραγματικότητα μόνο αν όλοι οι εμπλεκόμενοι φορείς που λειτουργούν προστατευτικά απέναντι στα ανήλικα άτομα βρίσκονται σε ετοιμότητα και επιφυλακή, σε περίπτωση που υπάρξει η υποψία ότι το παιδί θυματοποιείται διαδικτυακά προκειμένου να ενεργοποιηθεί και ο προληπτικός και ο κατασταλτικός μηχανισμός εξασφάλισης της θωράκισης της ανηλικότητά τους και της προσωπικότητάς τους. Το ίδιο το κράτος, τέλος, κρίνεται επιτακτικό να διαμορφώσει νομοθετικά προστατευτικό περιβάλλον, συγκεράζοντας τις τεχνολογικές γνώσεις και συμπεράσματα τεχνογνωσίας που προκύπτουν από την εξέταση του τρόπου τέλεσης των ηλεκτρονικών εγκλημάτων με την διαμόρφωση μιας υπερεθνικής πρακτικής για την αποσόβηση και διαχείριση τέτοιων διαδικτυακών κρίσεων που ξεπερνούν τα τοπικά όρια και εκμαυλίζουν την έννοια της κοινωνικής συνοχής και του απαραβίαστου της ανθρώπινης προσωπικότητας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνόγλωσση:

Αγγελής, Ι. (2005). Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης. *Ποινική Δικαιοσύνη,* 23-40.

Αλεξανδρίδου, Ε. (2010). *Το Δίκαιο του Ηλεκτρονικού Εμπορίου*. Αθήνα: Εκδόσεις Σάκκουλα.

Αλεξανδροπούλου – Αιγυπτιάδου, Ε. (2002). *Ζητήματα από το Δίκαιο της Πληροφορικής*. Αθήνα – Κομοτηνή: Εκδόσεις Σάκκουλα.

Αλεξανδροπούλου- Αιγυπτιάδου, Ε. (2007). Η πλοήγηση των ανηλίκων στο διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων. *Αρμενόπουλος ΞΑ,*12-35.

Άντρη, Ε. (2013). Το φαινόμενο τον διαδικτυακού εθισμού στο σύγχρονο άνθρωπο. *Cyprus Nursing Chronicles, 14*(3). Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://cncjournal.cyna.org/wp-content/uploads/2019/07/CNC-14-3.6-11.pdf

Γέρμανος, Γ. Αθ. & Γεωργίου, Ν. Χ. (2021). *Κυβερνοέγκλημα: Πρόληψη, Διερεύνηση, Αντιμετώπιση.* Ιδιωτική Έκδοση

Βλαχόπουλος, Κ. (2007). *Ηλεκτρονικό Έγκλημα*. Αθήνα: Νομική Βιβλιοθήκη.

Βλαχόπουλος, Κ. (2013). *Ηλεκτρονικό έγκλημα: Μορφές, πρόληψη, αντιμετώπιση.* Αθήνα: Νομική Βιβλιοθήκη

Δαγτόγλου, Π. (2012). *Συνταγματικό Δίκαιο - Ατομικά Δικαιώματα*. Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Δαλακούρας, Θ. (2019). *Ηλεκτρονικό Έγκλημα.* Αθήνα: Νομική Βιβλιοθήκη.

Ζάννη, Α. (2005). *Το διαδικτυακό έγκλημα*. Αθήνα: Εκδόσεις Σάκκουλα

Ιγγλεζάκης, Ι. (2018). *Δίκαιο πληροφορικής*. Αθήνα: Εκδόσεις Σάκκουλα

Παναγοπούλου-Κουτνατζή, Φ. (2010). *Οι ιστότοποι Κοινωνικής Δικτυώσεως ως Εθνική, Ευρωπαϊκή και Διεθνής Πρόκλησης της Προστασίας της Ιδιωτικότητας*. Αθήνα-Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Ιγγλεζάκης, Ι. (2020). *Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (Κανονισμός 2016/679) και ο Εφαρμοστικός Νόμος (Ν. 4624/2019)*. Αθήνα: Interactive Books

Καϊάφα- Γκμπάντι, Μ. (2012). Διαδικτυακές προσβολές της ανηλικότητας. *ΠοινΧρ.,* 171.

Κοκκέβη, Α., Ξανθάκη, Μ., Φωτίου, Α., & Καναβού, Ε. (2010). Χρήση Η/Υ και ίντερνετ από τους εφήβους. *Ερευνητικό Πανεπιστημιακό Ινστιτούτο Ψυχικής Υγιεινής*. Ανακτήθηκε 16 Νοεμβρίου, 2021 από http://2dim-filyr.thess.sch.gr/wp-content/uploads/1326624038-08_HBSC_2010_EPIPSI_20121.pdf

Μαργαρίτη, Μ. & Μαργαρίτη, Ά. (2020). *Ποινικός Κώδικας, Ερμηνεία Εφαρμογή*. Αθήνα: Εκδόσεις Σάκκουλας.

Παπαδαμάκης, Α. (2020). *Τα περιουσιακά εγκλήματα.* Αθήνα: Εκδόσεις Σάκκουλα.

Παπακωνσταντίνου, Ε. (2010). *Δίκαιο Πληροφορικής*. Αθήνα: Εκδόσεις Σάκκουλα.

Σπυρόπουλος, Φ. (2011). *Σχολικός τραμπουκισμός.* Αθήνα – Κομοτηνή : Εκδόσεις Σάκκουλα.

Συμεωνίδου – Καστανίδου, Ε. (2001). *Εγκλήματα κατά της ζωής*. Αθήνα – Θεσσαλονίκη: Εκδόσεις Σάκκουλα

Συμεωνίδου- Καστανίδου, Ε. (2020). *Εγκλήματα κατά προσωπικών αγαθών* . Αθήνα: Νομική Βιβλιοθήκη.

Σφακιανάκης Ε. (2016). *Ο κώδικας του διαδικτύου*. Αθήνα: Εκδόσεις Πολιτεία.

Χρυσόγονος, Κ. (2014). *Συνταγματικό Δίκαιο Θεσσαλονίκη*. Αθήνα: Εκδόσεις Σάκκουλας.

<u>Ξενόγλωσση</u>

Ahmad, N., Arifin, A., Asma'Mokhtar, U., Hood, Z., Tiun, S. & Jambari, D. I. (2019). Parental awareness on cyber threats using social media. *Jurnal Komunikasi: Malaysian Journal of Communication*, *35*(2). Retrieved November 14, 2021, from https://ejournal.ukm.my/mjc/article/view/33515

Arneja, P. S. & Sachdev, S. (2015). Detailed Analysis of Antivirus based Firewall and Concept of Private Cloud Antivirus based Firewall. *International Journal of Computer Applications*, *111*(4).

Athanasiades, C., Kamariotis, H., Psalti, A., Baldry, A. C. & Sorrentino, A. (2015). Internet use and cyberbullying among adolescent students in Greece: the "Tabby" project. *Hellenic Journal of Psychology*, *12*(1), 14-39. Retrieved November 14, 2021, from https://pseve.org/wp-content/uploads/2018/03/Volume12_Issue1_Athanasiades.pdf

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1-12. DOI : https://doi.org/10.5897/JIIS2015.0089

Bessière, K., Pressman, S., Kiesler, S. & Kraut, R. (2010). Effects of internet use on health and depression: a longitudinal study. *Journal of medical Internet research*, *12*(1), e1149. DOI: 10.2196/jmir.1149

Bakalis, C. (2015). Cyberhate: an issue of continued concern for the Council of Europe's Anti-Racism Commission. *Council of Europe.* Retrieved November 14, 2021, from https://rm.coe.int/cyberhate-an-issue-of-continued-concern-for-the-council-of-europe-s-an/16808c6d9f

Cash, H., D Rae, C., H Steel, A. & Winkler, A. (2012). Internet addiction: A brief summary of research and practice. *Current psychiatry reviews*, *8*(4), 292-298. DOI : https://doi.org/10.2174/157340012803520513

Curran, J. (2012). Rethinking internet history: James Curran. In *Misunderstanding the internet*. [eBook version] England: Routledge. Retrieved November 14, 2021, from https://courses.helsinki.fi/sites/default/files/course-material/4511752/CURRAN%20ET%20AL_Misunderstanding%20the%20internet.pdf

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L. & Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British journal of educational technology*, *49*(1), 45-55. DOI: https://doi.org/10.1111/bjet.12529

DeNardis, L. (2010). The emerging field of Internet governance. *Yale Information Society Project Working Paper Series*. DOI: http://dx.doi.org/10.2139/ssrn.1678343

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital investigation*, *7*, 64-S73. DOI: https://doi.org/10.1016/j.diin.2010.05.009

Garg, N., Bawa, S. & Kumar, N. (2020). An efficient data integrity auditing protocol for cloud computing. *Future Generation Computer Systems*, *109*, 306-316. DOI: https://doi.org/10.1016/j.future.2020.03.032

Grispos, G. (2019). Criminals: Cybercriminals. *Encyclopedia of Security and Emergency Management*, 1-7. Retrieved November 14, 2021, from https://www.researchgate.net/profile/George-Grispos-2/publication/337011271_Criminals_Cybercriminals/links/5dc04fcf299bf1a47b130c56/Criminals-Cybercriminals.pdf

Hargreaves, C. & Prince, D. (2013). *Understanding cyber criminals and measuring their future activity*. [eBook version] Security Lancaster: Lancaster University. Retrieved November 14, 2021, from https://eprints.lancs.ac.uk/id/eprint/65477/1/Final_version_Understanding_cyber_criminals_and_measuring_their_activity.pdf

Katz, J. & Lindell, Y. (2020). *Introduction to modern cryptography*. [eBook version] Florida: CRC press. Retrieved November 14, 2021, from https://eclass.uniwa.gr/modules/document/file.php/CSCYB105/Reading%20Material/%5BJonathan_Katz%2C_Yehuda_Lindell%5D_Introduction_to_Mo%282nd%29.pdf

King, A. V. (2010). Constitutionality of cyberbullying laws: Keeping the online playground safe for both teens and free speech. *Vanderbilt Law Review*, *63*, 845. Retrieved November 14, 2021, from https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1425&context=vlr

Kleinrock, L. (2010). An early history of the internet [History of Communications]. *IEEE Communications Magazine*, *48*(8), 26-36. Retrieved November 14, 2021, from https://www.researchgate.net/publication/262316090_An_early_history_of_the_internet_History_of_Communications

Kowalski, R. M., Limber, S. P. & Agatston, P. W. (2012). Cyberbullying: Bullying in the digital age. [eBook version] New York City: John Wiley & Sons. Retrieved November 14, 2021, from https://books.google.gr/books?hl=en&lr=&id=ARKbrXsdOmYC&oi=fnd&pg=PR6&dq=info:1_SzzEVl83IJ:scholar.google.com&ots=RRoGDZSmLU&sig=lUgpyF1zuvelfxgtYM6ajMaAkik&redir_esc=y#v=onepage&q&f=false

Kuss, D. J. & Lopez-Fernandez, O. (2016). Internet addiction and problematic Internet use: A systematic review of clinical research. *World journal of psychiatry*, *6*(1), 143. Retrieved November 14, 2021, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4804263/

Leena, N. (2011). Cybercrime effecting e-commerce technology. *Oriental Journal of Computer Science & Technology*, *4*(1), 209-212. Retrieved November 14, 2021, from http://www.computerscijournal.org/dnload/N.%20Leena/OJCSV04I01P209-212.pdf

Maindonald, J. H. & Stott, H. P. (2014). Confidentiality and Computers. *Wiley Statistics Reference Online*. DOI: https://doi.org/10.1002/9781118445112.stat05014

Martellozzo, E., & Jane, E. A. (2017). *Cybercrime and its victims*. [eBook version] England: Routledge. Retrieved November 14, 2021, from https://lib.cmb.ac.lk/wp-content/uploads/2019/03/Routledge-Studies-in-Crime-and-Society-Elena-Martellozzo_-Emma-A-Jane_-eds.-Cybercrime-and-Its-Victims-Routledge-2017.pdf

Minnaar, A. (2014). 'Crackers', cyberattacks and cybersecurity vulnerabilities: the difficulties in combatting the 'new' cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*, 127-144. Retrieved November 14, 2021, from https://journals.co.za/doi/abs/10.10520/EJC171548

Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims. *Children and Youth Services Review*, *34*(1), 63-70. DOI: 10.1016/j.childyouth.2011.08.032

Näsi, M., Oksanen, A., Keipi, T. & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210. Retrieved November 14, 2021, from https://www.tandfonline.com/doi/abs/10.1080/14043858.2015.1046640

Ngejane, C. H., Mabuza-Hocquet, G., Eloff, J. H. & Lefophane, S. (2018). Mitigating online sexual grooming cybercrime on social media using machine learning: A desktop survey. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* Retrieved November 14, 2021, from https://ieeexplore.ieee.org/abstract/document/8465413

O'Connell, R. (2003). A typology of child cybersexploitation and online grooming practices. *Cyberspace Research Unit, University of Central Lancashire*. Retrieved November 14, 2021, from http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf

Oksanen, A. & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309. Retrieved November 14, 2021, from https://www.tandfonline.com/doi/abs/10.1080/17450128.2012.752119

Ramdinmawii, E., Ghisingh, S. & Sharma, U. M. (2014). A study on the cyber-crime and cyber criminals: A global problem. *International Journal of Web Technology, 3,*

172-179. Retrieved November 14, 2021, from http://www.ijwebt.com/documents/%20IIR_IJWT_042.pdf

Reep-van den Bergh, C. M. & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science, 7*(1), 1-15. Retrieved November 14, 2021, from https://link.springer.com/article/10.1186/s40163-018-0079-3

Ryan, J. (2010). *A History of the Internet and the Digital Future*. [eBook version] London: Reaktion Books. Retrieved November 14, 2021, from https://books.google.gr/books?hl=en&lr=&id=l0OYhHefumoC&oi=fnd&pg=PP1&ots=GTf5V9NF-P&sig=msUlxIDxSpKt1qt8iUOXzTOzdHM&redir_esc=y#v=onepage&q&f=false

Saini, H., Rao, Y. S. & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications, 2*(2), 202-209. Retrieved November 14, 2021, from https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review

Sammons, J. & Cross, M. (2016). *The basics of cyber safety: Computer and mobile device safety made easy*. [eBook version] Amsterdam: Elsevier. Retrieved November 14, 2021, from https://books.google.gr/books?hl=el&lr=&id=vLNZAwAAQBAJ&oi=fnd&pg=PP1&dq=cyber+crimes+and+safety&ots=2dvqm8ydH4&sig=tEJTUaIE6bjgXo3KIIVEdYdqbHE&redir_esc=y#v=onepage&q=cyber%20crimes%20and%20safety&f=false

Schjolberg, S. (2020). *The History of Cybercrime*. [eBook version] Retrieved November 14, 2021, from https://www.researchgate.net/publication/313662110_The_History_of_Cybercrime_1976-2016

Shinder, D. L., & Cross, M. (2008). [eBook version] *Scene of the Cybercrime*. Amsterdam: Elsevier. Retrieved November 14, 2021, from https://books.google.gr/books?hl=el&lr=&id=fJVcgl8IJs4C&oi=fnd&pg=PP1&dq=cyber+crime+security+features&ots=eAAztaSDnZ&sig=0R6CrOnyLIBr8eYgQ_HjN_h-f8A&redir_esc=y#v=onepage&q=cyber%20crime%20security%20features&f=false

Smith, P. K., Thompson, F., & Davidson, J. (2014). Cyber safety for adolescent girls: Bullying, harassment, sexting, pornography, and solicitation. *Current opinion in obstetrics and gynecology*, *26*(5), 360-365.

Speed, F. C. (2021). Online Grooming: An Exploration into the Genetic-Social Variables Which Enable Victimisation. In *Rethinking Cybercrime*, 237-258. [eBook version] London: Palgrave Macmillan. Retrieved November 14, 2021, from https://books.google.gr/books?id=d7wIEAAAQBAJ&pg=PA237&lpg=PA237&dq=Speed,+F.+C.+(2021).+Online+Grooming:+An+Exploration+into+the+Genetic-Social+Variables+Which+Enable+Victimisation&source=bl&ots=YeYtxu3fDv&sig=ACfU3U2NEj1aemuSe_FS81hkHkVy687skg&hl=el&sa=X&ved=2ahUKEwiAqYiatZz0AhVxhP0HHdZqBngQ6AF6BAgCEAM#v=onepage&q=Speed%2C%20F.%20C.%20(2021).%20Online%20Grooming%3A%20An%20Exploration%20into%20the%20Genetic-Social%20Variables%20Which%20Enable%20Victimisation&f=false

Trivedi, K., Andrade, E. & Machida, F. (2012). *Advances in Computers* [eBook version]. Amsterdam: Elsevier. Retrieved November 14, 2021, from https://www.sciencedirect.com/science/article/abs/pii/B9780123965257000010

Tsimtsiou, Z., Dantsi, F., Sekeri, Z., Trikoilis, N. & Nanos, P. (2017). Internet Usage in Primary and Secondary School Children: A Multi-Center, School-Based, Cross-Sectional Study in Greece. *International Journal of High-Risk Behaviors and Addiction*, *6*(2). Retrieved November 14, 2021, fromhttps://sites.kowsarpub.com/ijhrba/articles/14971.html

Waldron, J. (2012). *The harm in hate speech*. [eBook version] Harvard University Press. Retrieved November 14, 2021, from https://www.researchgate.net/publication/235697997_Jeremy_Waldron_The_Harm_in_Hate_Speech_Cambridge_Mass_Harvard_University_Press_2012_I-CONnect_25_February_2013_httpwwwiconnectblogcom201302book-review-jeremy-waldrons-the-harm-in-hate-speech

Yen, J. Y., Yen, C. F., Wu, H. Y., Huang, C. J. & Ko, C. H. (2011). Hostility in the real world and online: the effect of internet addiction, depression, and online activity. *Cyberpsychology, Behavior, and Social Networking*, *14*(11), 649-655. DOI: 10.1089/cyber.2010.0393

Yar, M. & Steinmetz, K. F. (2019).[eBook version] *Cybercrime and society*. New York: Sage. Retrieved November 14, 2021, from

https://books.google.gr/books?hl=el&lr=&id=gpuHDwAAQBAJ&oi=fnd&pg=PP1&dq=Cybercrime+and+society.&ots=fmsYnaAxIV&sig=OXVW0Wexfvi-wZBF_eRqoF6qPJg&redir_esc=y#v=onepage&q=Cybercrime%20and%20society.&f=false

Zare, H., Olsen, P., Zare, M. J. & Azadi, M. (2018). Operating system security management and ease of implementation (passwords, firewalls, and antivirus). In *Information Technology-New Generations* (pp. 749-755). Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-77028-4_98

Ιστοσελίδες

Δίωξη Ηλεκτρονικού εγκλήματος. (χ.χ.). *Απάτες μέσω διαδικτύου*. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://cyberalert.gr/apates-meso-diadiktiou/

Νόμος 4070/2012. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.taxheaven.gr/law/4070/2012

Ποινικός Κώδικας - Νόμος 4619/2019. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.lawspot.gr/nomikes-plirofories/nomothesia/poinikos-kodikas-nomos-4619-2019

Ποινικός Κώδικας- Νόμος 4322/2015. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.e-nomothesia.gr/kat-dikasteria-dikaiosune/n-4322-2015.html

Σύμβαση για τα Διαδικτυακά Εγκλήματα του Συμβουλίου της Ευρώπης. (χ.χ.). Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.europarl.europa.eu/doceo/document/TA-8-2019-0032_EL.html

Συνήγορος του καταναλωτή. (2011). *Ανήλικος καταναλωτής: Ευκαιρίες, κίνδυνοι και μέσα προστασίας*. Ανακτήθηκε 16 Νοεμβρίου, 2021 από http://www.synigoroskatanaloti.gr/docs/studies/2011-11-30.%CE%9F%CE%BC%CE%B9%CE%BB%CE%AF%CE%B1%20%CE%A3%CF%84%CE%9A-%CE%9A%CE%BF%CE%BB%CE%AD%CE%B3%CE%B9%CE%BF%20%CE%91%CE%B8%CE%B7%CE%BD%CF%8E%CE%BD.pdf

Σύνταγμα της Ελλάδας. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/

BBC News. (2010). *Four in Five Regard Internet Access as a Fundamental Right: Global Poll* . Retrieved November 16, 2021, from http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf

Devolo Hellas & Infokids.gr. (2019). *Έρευνα devolo Hellas: 6 στα 10 ελληνόπουλα έως δέκα ετών έχουν πρόσβαση στο Internet.* Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.devolo.gr/schetika-me-tin-devolo/deltia-typoy/ereyna-devolo-hellas-6-sta-10-ellinopoyla-eos-deka-eton-echoyn-prosbasi-sto-internet

Enisa: European Union Agency for Cybersecurity (n.d.). Retrieved November 16, 2021, from https://www.enisa.europa.eu/publications#c3=2011&c3=2021&c3=false&c5=publicationDate&reversed=on&b_start=0

Lawspot (2020). *Προστασία καταναλωτών κατά τις ηλεκτρονικές αγορές: Οδηγίες από τον Συνήγορο του Καταναλωτή*. Ανακτήθηκε 16 Νοεμβρίου, 2021 από https://www.lawspot.gr/nomika-nea/prostasia-katanaloton-kata-tis-ilektronikes-agores-odigies-apo-ton-synigoro-toy