ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ Δ.Ο.Ε.Π.&Τ.Μ.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Η ΝΟΜΟΘΕΣΙΑ ΓΙΑ ΤΗΝ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΠΑΠΑΖΩΗ ΠΑΝΑΓΙΩΤΑ

ΠΑΓΟΥΛΑΤΟΥ ΠΑΝΑΓΙΩΤΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:ΣΩΤΗΡΗΣ ΤΡΙΑΝΤΑΦΥΛΛΟΥ

ΠΥΡΓΟΣ, 2018

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΜΗ ΛΟΓΟΚΛΟΠΗΣ

Βεβαιώνω/ουμε ότι είμαι/είμαστε ο/οι συγγραφέας/εις αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα/είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία.

Επίσης, έχω/έχουμε αναφέρει τις πηγές από τις οποίες έκανα /κάναμε χρήση δεδομένων, ιδεών η λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες.

Ακόμη δηλώνω/ουμε ότι αυτή η γραπτή εργασία προετοιμάστηκε από εμένα/εμάς προσωπικά και αποκλειστικά και ειδικά για την συγκεκριμένη πτυχιακή εργασία ότι θα αναλάβω/ουμε πλήρως τις συνέπειες εάν η εργασία αυτή αποδειχτεί ότι δεν μου/μας ανήκει.

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ 1	ΥΠΟΓΡΑΦΗ
Παναγιώτου Παναγιώτα	
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ 2	ΥΠΟΓΡΑΦΗ
Παναγιώτα Παναγίν	
ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΦΟΙΤΗΤΗ 3	ΥΠΟΓΡΑΦΗ

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Στην σημερινή εποχή της πληροφορίας και των τεχνολογικών εξελίξεων παρατηρείται η ολοένα αυξανόμενη διείσδυση των ευρυζωνικών τεχνολογιών στην κοινωνία και διαφαίνεται η τάση για σύγκλιση των τηλεπικοινωνιακών δικτύων παροχής υπηρεσιών καθώς και για πρόσβαση <οποτεδήποτε>, <από οπουδήποτε>, και <με οτιδήποτε>. Σε αυτό το συνεχώς μεταβαλλόμενο περιβάλλον ,η έννοια του ηλεκτρονικού εγκλήματος αποκτά μία καινούργια διάσταση. Παραδοσιακές ηλεκτρονικές απειλές όπως: Κακόβουλο λογισμικό, μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές και συστήματα, ενοχλητικά ηλεκτρονικά μηνύματα, επιθέσεις κλοπής ηλεκτρονικής ταυτότητας και τα λοιπά, αναμένεται να βρουν νέα, εξίσου γόνιμα, εδάφη για την εξάπλωσή τους. Επιπλέον, η κακόβουλη χρήση των τεχνολογιών δικτύωσης μπορεί να διευκολύνει την τέλεση συμβατικών εγκλημάτων ή να ενισχύσει επιπλέον το καταστρεπτικό τους έργο.

ΠΕΡΙΛΗΨΗ

Η ανεξέλεγκτη κούρσα της τεχνολογικής προόδου, ο διαρκώς αυξανόμενος αριθμός των χρηστών του Διαδικτύου σε παγκόσμιο επίπεδο και η οικονομική κρίση των τελευταίων ετών- με τα συνακόλουθά της- αποτελούν ένα εκρηκτικό μείγμα, το οποίο έχει οδηγήσει στην ενίσχυση των υφιστάμενων φαινομένων ψηφιακής εγκληματικότητας, αλλά παράλληλα αποτελεί τη βάση για τη γέννηση νέων μορφών Κυβερνο-εγκλημάτων.

Στην παρούσα εργασία θα αναπτυχθούν συνοπτικά οι παραπάνω έννοιες και θα παρουσιαστούν, με τρόπο εμπεριστατωμένο αλλά και κατανοητό στο ευρύ κοινό, παραβατικές συμπεριφορές στον Κυβερνοχώρο, όπου θύματα των εγκληματιών είναι πλέον οι μεμονωμένοι, καθημερινοί χρήστες και όχι τόσο οργανισμοί ή άλλοι φορείς, όπου οι τεχνολογικές εξελίξεις (ψηφιακά <πορτοφόλια>, αποθήκευση <cloud>, κρυπτογράφηση και τα λοιπά) δυσχεραίνουν το έργο των διωκτικών Αρχών και όπου ο νομοθέτης- με δεδομένο το μη χωρικό περιορισμό του ψηφιακού εγκλήματος στα όρια ενός κράτους και δεδομένη τη <διαμάχη> μεταξύ της προστασίας του απορρήτου των επικοινωνιών και της διαφύλαξης των προσωπικών δεδομένων των χρηστών- βρίσκεται αντιμέτωπος με μια δυσεπίλυτη εξίσωση.

ΕΙΣΑΓΩΓΗ

Η τεχνολογική έκρηξη την τελευταία δεκαετία μας έφερε όλους πιο κοντά στον παγκόσμιο ιστό και στην χρήση του υπολογιστή ως εργαλείο που ικανοποιεί τις περισσότερες ανάγκες μας. Αναμφισβήτητα την τελευταία δεκαετία οι ηλεκτρονικοί υπολογιστές και το Διαδίκτυο (internet) παίζουν σημαντικό ρόλο στις ζωές των ανθρώπων.

Σήμερα σε κάθε νοικοκυριό υπάρχει τουλάχιστον ένας ηλεκτρονικός υπολογιστής και μία σύνδεση προς το παγκόσμιο Διαδίκτυο μέσω του οποίου άνθρωποι από όλο τον κόσμο επικοινωνούν μεταξύ τους, ανταλλάσουν μηνύματα, προβαίνουν σε αγοροπωλησίες, εκτελούν τραπεζικές συναλλαγές και άλλα.

Μάλιστα, λόγω της οικονομικής κρίσης, πολλά δεδομένα έχουν αλλάξει. Οι απλοί χρήστες τείνουν να περνούν όλο και περισσότερη ώρα μπροστά σε μία οθόνη. Πολλοί είναι εκείνοι οι οποίοι εργάζονται εξ αποστάσεως- δηλαδή χωρίς την ανάγκη αυτοπρόσωπης παρουσίας τους σε ένα συγκεκριμένο χώρο εργασίας. Ακόμα περισσότεροι είναι εκείνοι που για λόγους οικονομίας αποφεύγουν, παραδείγματος χάρη, τις νυχτερινές εξόδους και προτιμούν να μείνουν σπίτι για να διασκεδάσουν παρακολουθώντας μια ταινία online. Εξάλλου, η επικοινωνία μεταξύ των χρηστών γίνεται πλέον σε μεγάλο βαθμό μέσω Διαδικτύου, με τη χρήση κατάλληλου λογισμικού και φυσικά το μοναδικό κόστος σε αυτή την περίπτωση είναι τα σταθερά τέλη προς την εταιρεία παροχής υπηρεσιών Διαδικτύου.

Εξαιτίας της κρίσης, όμως, έχει αλλάξει και η φιλοσοφία από την πλευρά των επιχειρήσεων. Μεγάλος αριθμός αυτών- για να μειώσει το κόστος λειτουργίας τους- έχει στραφεί στην πώληση προϊόντων και παροχή υπηρεσιών μέσω ηλεκτρονικών καταστημάτων. Σημαντική μείωση στο κόστος μπορεί να επιτευχθεί, επίσης, με τη χρήση online αποθηκευτικού χώρου για τα δεδομένα της εταιρείας ή online δωρεάν λογισμικού (παραδείγματος χάρη αντί του Microsoft Office πολλές εταιρείες επιλέγουν το δωρεάν Open Office).

Δυστυχώς αυτή την τεχνολογική επανάσταση των τελευταίων χρόνων και την αλλαγή στις συνήθειες χρηστών και επιχειρήσεων δεν άργησαν να την αντιληφθούν και οι εγκληματίες, οι οποίοι άρχισαν να χρησιμοποιούν το διαδίκτυο και τις υπηρεσίες που αυτό προσφέρει με απώτερο στόχο τη διευκόλυνση των εγκληματικών πράξεών τους.

Πολλά από τα εγκλήματα που διαπράττονται μέσα από τον Κυβερνοχώρο έχουν παραμείνει ίδια, με τη μόνη διαφορά ότι ο τόπος του εγκλήματος αλλάζει από έναν τόπο του πραγματικού κόσμου σε έναν διαδικτυακό.

Επιπλέον έχουν αναπτυχθεί και νέου είδους εγκλήματα που δεν υπήρχαν στο παρελθόν, παραδείγματος χάρη η κλοπή διαδικτυακής ταυτότητας (identity theft), online κλοπή κωδικών πιστωτικών καρτών, επιθέσεις άρνησης υπηρεσιών και τα λοιπά.

Επί του παρόντος, μάλιστα περίπου 2,5 δισεκατομμύρια άτομα σε όλο τον κόσμο έχουν πρόσβαση στο Διαδίκτυο και οι εκτιμήσεις δείχνουν ότι σχεδόν 1,5 δισεκατομμύριο θα διαθέτουν πρόσβαση στα επόμενα τέσσερα χρόνια. Καθώς η σχέση μας με το Διαδίκτυο θα γίνεται συνεχώς στενότερη, λόγω των τεράστιων πλεονεκτημάτων του, θα είμαστε όλο και περισσότερο εκτεθειμένοι στο κυβερνοέγκλημα (cybercrime).

Έτσι, λοιπόν, με την ανάπτυξη του Διαδικτύου και της τεχνολογίας, έχουμε και άνθιση ενός νέου είδους εγκληματικότητας που αναπτύσσεται με τη χρήση της ψηφιακής τεχνολογίας και των ηλεκτρονικών υπολογιστών.

Είναι αναμφισβήτητο γεγονός ότι το ηλεκτρονικό και διαδικτυακό έγκλημα συνιστά μία μορφή εγκληματικότητας, η οποία βαίνει διαρκώς αυξανόμενη, τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο, μεταλλάσσεται δε διαρκώς με την εμφάνιση ολοένα και πιο εξελιγμένων μεθόδων διάπραξης αδικημάτων. Αυτό οφείλεται κυρίως στη ραγδαία ανάπτυξη των τεχνολογικών συστημάτων, στη χρησιμοποίηση –ενασχόληση με το Διαδίκτυο μεγαλύτερου αριθμού χρηστών, στη δυσχέρεια ανίχνευσης- απόδειξης αλλά και στην ανωνυμία που αυτό δυνητικά παρέχει στους χρήστες του.

ΚΕΦΑΛΑΙΟ 1

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ - ΧΡΗΣΤΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΓΕΝΙΚΩΣ - ΧΡΗΣΤΕΣ ΤΟΥ ΔΙΑΔΙΚΤΟΥ ΣΤΗΝ ΕΛΛΑΔΑ - ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ, ΤΙ ΕΙΝΑΙ?

1.1 ΤΟ ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο αποτελεί το μεγαλύτερο υπολογιστικό σύστημα στον κόσμο. Μπορούμε να το φανταστούμε ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, που διασύνδεει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα διασκορπισμένα αν τον κόσμο, παρέχοντας στους χρήστες τους μια τεράστια ποικιλία εργαλείων και υπηρεσιών.

Η πληροφορική, οι υπολογιστές, το διαδίκτυο και γενικότερα η σύγχρονη τεχνολογία έχουν εισβάλει στην καθημερινότητα του ανθρώπου, καθώς παρέχουν μια σειρά δυνατοτήτων που βελτιώνουν την ποιότητα της ζωής του. Η απλοποίηση κάποιων εργασιών, η οργάνωση των πληροφοριών, η επιτάχυνση διαδικασιών όπως και ο ακριβής, άμεσος υπολογισμός και διαχείριση μεγάλου όγκου δεδομένων είναι λίγες μόνο από τις ωφέλειες που μπορεί να καρπωθεί ο σύγχρονος άνθρωπος από τη ραγδαίως αναπτυσσόμενη πληροφορική τεχνολογία. Από την άλλη, ένα από τα πλέον αρνητικά στοιχεία τη πληροφορικής τεχνολογίας, είναι και η δημιουργία πρόσφορων συνθηκών για την ανάπτυξη και διάδοση νέων μορφών εγκλημάτων. Το ηλεκτρονικό έγκλημα είναι ένα φαινόμενο εξελισσόμενο με ταχύτατους ρυθμούς, καθώς συμβαδίζει με αυτούς της ανάπτυξης της τεχνολογίας. Υπάρχει επομένως κάθε κίνδυνος κάθε απάτης, από καλούς γνώστες της τεχνολογίας, οι οποίοι προσπαθούν να πραγματοποιήσουν παράνομες πράξεις, μετατρέποντας την τεχνολογία κατά αυτό τον τρόπο σε ένα καταστροφικό όπλο. Οι δυνατότητες δίωξης από τις αρμόδιες αρχές είναι περιορισμένες, καθώς υπάρχει έλλειψη εμπειρίας αλλά και εκπαίδευσης σε επαρκή βαθμό όπως επίσης και ασάφεια όσον αφορά τη νομοθεσία. Το διαδίκτυο είναι παγκόσμιο σύστημα διασυνδεδεμένων δικτύων υπολογιστών, οι οποίοι χρησιμοποιούν καθιερωμένη ομάδα πρωτοκόλλων, η οποία συχνά αποκαλείται "TCP/IP" (αν και αυτή δεν χρησιμοποιείται από όλες τις υπηρεσίες του Διαδικτύου) για να εξυπηρετεί εκατομμύρια χρήστες καθημερινά σε ολόκληρο τον κόσμο. Οι διασυνδεδεμένοι ηλεκτρονικοί υπολογιστές ανά τον κόσμο, οι οποίοι βρίσκονται σε ένα κοινό δίκτυο επικοινωνίας, ανταλλάσσουν μηνύματα (πακέτα) με τη χρήση διαφόρων πρωτοκόλλων (τυποποιημένοι κανόνες επικοινωνίας), τα οποία υλοποιούνται σε επίπεδο υλικού και λογισμικού. Το κοινό αυτό δίκτυο καλείται διαδίκτυο. Το διαδίκτυο (ιντερνέτ) μπορεί να περιγράφει ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, το οποίο διασύνδεει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων[1]. Είναι ένας απέραντος, εικονικός κόσμος στον οποίο μπορούν εύκολα να έχουν πρόσβαση χρήστες κάθε ηλικίας. Με τη σημερινή του μορφή (World Wide Web- www), εισέβαλε στη ζωή μας πριν από είκοσι περίπου χρόνια , αλλάζοντας ριζικά την πλειοψηφία των ανθρώπινων δραστηριοτήτων. Το διαδίκτυο και κατ' επέκταση οι ηλεκτρονικοί υπολογιστές, έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητας μας, είτε ως μέσα ψυχαγωγίας, ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων[2].

[1] Ζάννη Αναστασία, <Το διαδικτυακό έγκλημα>, σελ. 23
[2] Ελαφρός Γιάννης, <Το διαδίκτυο αλλάζει άρδην την ζωή μας>, σελ.31

Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών – δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Υπολογίζεται ότι 1,5 δισεκατομμύριο χρήστες, περίπου το 24% του παγκόσμιου πληθυσμού, συνδέονται με το ιντερνέτ, για κάθε είδος δραστηριότητα, όπως για παράδειγμα αγορές προϊόντων, παροχή υπηρεσιών on line (e-commerce, e-banking κλπ), για αναζήτηση πληροφοριών, ειδήσεων (μηχανές αναζήτησης όπως Google, Yahoo, blogs, portals εφημερίδων), για επικοινωνία μέσω ανταλλαγής ηλεκτρονικού ταχυδρομείου (e-mail). Στις μέρες μας, γίνεται σε μεγάλο βαθμό και η χρήση εφαρμογών κοινωνικής δικτύωσης (facebook, twitter, chat rooms). Το σύνολο των δικτυακών τύπων στο ιντερνέτ εκτιμάται ότι έχει ανέλθει στα 156 πλέον εκατομμύρια. Αυτό σημαίνει ότι κάθε χρήστης έχει δυνατότητα πρόσβασης σε τεράστιες ποσότητες πληροφοριών, υπηρεσιών και άλλων αγαθών που διακινούνται μέσω διαδικτύου.

1.2 Η ΕΞΑΠΛΩΣΗ ΚΑΙ ΕΠΙΚΡΑΤΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ.

Οι εξελίξεις στην τεχνολογία των ηλεκτρονικών υπολογιστών ήταν ραγδαίες και διαδέχονταν η μία την άλλη, με διαρκεί ανάπτυξη της τεχνολογίας, όταν στις αρχές της δεκαετίας του 1990, κάνει την εμφάνιση του το Διαδίκτυο όπως το γνωρίζουμε σήμερα και αρχίζει να εξαπλώνεται και να αναπτύσσεται με ραγδαίο ρυθμό.

Το διαδίκτυο είναι το μεγαλύτερο είναι το μεγαλύτερο υπολογιστικό σύστημα στον κόσμο. Η δομή του είναι πλήρως ανοιχτή σε κάθε χρήστη ηλεκτρονικού υπολογιστή, είναι απόλυτα αποκεντρωμένο και αυτοδιαχειριζόμενο καθώς δεν είναι ιδιοκτησία κανενός και δεν ελέγχεται από κανέναν. Οι υπηρεσίες του Διαδικτύου παρέχουν στους χρήστες του μια πληθώρα εφαρμογών που σχετίζονται με την πρόσβαση σε μια πληθώρα πληροφοριών, την κοινωνική δικτύωση, την εκπαίδευση, την ανάπτυξη νέων τύπων εργασίας (τηλε-εργασία) κι εμπορίου (ηλεκτρονικό εμπόριο), ην ψυχαγωγία και την επικοινωνία.

Θα μπορούσαμε να ορίσουμε το διαδίκτυο ως την τεχνική εκείνη μέσω της οποίας διάφορα δίκτυα ηλεκτρονικών υπολογιστών συνδέονται μεταξύ τους. Μέσω αυτής της σύνδεσης δίδεται στους χρήστες η δυνατότητα να έχουν πρόσβαση στο υλικό, τις πληροφορίες και το περιεχόμενο όλων αυτών των δικτύων. Για να επιτευχθεί η σύνδεση στο διαδίκτυο χρειάζεται ένας ηλεκτρονικός υπολογιστής και ένα modem το οποίο να συνδέεται με το τηλέφωνο.
Το διαδίκτυο περιλαμβάνει πολύ μικρά εμπόδια στην είσοδο, επικοινωνία και μετάδοση πληροφοριών. Τα εμπόδια είναι ταυτόσημα και για τον ομιλητή και για τον ακροατή. Επειδή δε, υπάρχουν τόσα αδύναμα εμπόδια, υπάρχει ένα εκπληκτικά διαφορετικό περιεχόμενο διαθέσιμο στο διαδίκτυο. Η σχετικά ανοιχτή πρόσβαση δημιουργεί μια σχετική ισότητα μεταξύ των ομιλητών.

Οι επιστήμονες ακολούθως ανέπτυξαν τεχνολογία η οποία επιτρέπει σε απεριόριστο αριθμό βασικών δεδομένων να αλληλοσυνδέονται ηλεκτρονικά και έτσι οι υπάρχουσες σε μια από αυτές, πληροφορίες να μπορούν να κυκλοφορούν και στις υπόλοιπες. Έτσι όποιο δεδομένο και αν υπάρχει σε ένα συνδεδεμένο ηλεκτρονικό υπολογιστή είναι εξίσου προσβάσιμο από άλλο δικτυωμένο ηλεκτρονικό υπολογιστή.

1.3 ΤΙ ΕΙΝΑΙ ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΠΩΣ ΕΞΕΛΙΧΘΗΚΕ;

Το διαδίκτυο είναι ένα πλέγμα ψηφιακών γραμμών, το οποίο συνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα ανά τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων.

Υπάρχουν δύο απόψεις σχετικά με την ακριβή τόπο και χρόνο που σχεδιάστηκε αρχικά το διαδίκτυο. Η πρώτη άποψη λέει ότι το διαδίκτυο άρχισε να σχεδιάζεται το 1963 από το Lawrence Roberts, ο οποίος έφτιαξε με μια ομάδα συνεργατών ένα δίκτυο, στόχος του οποίου ήταν η ενδοεπικοινωνία, απαλλαγμένη από οποιαδήποτε εξωτερική παρεμβολή. Σύμφωνα με τη δεύτερη και πιο διαδεδομένη, το διαδίκτυο δημιούργησε το 1954 ο Paul Baran, ερευνητής σε αμερικάνικη εταιρεία, ο οποίος πρότεινε ένα σχέδιο τηλεπικοινωνιακού δικτύου, εντελώς διαφορετικού από τα ήδη υπάρχοντα.

Στις αρχές του 1950, το Υπουργείο Εθνικής Άμυνας των ΗΠΑ αποφάσισε να υιοθετήσει ένα δίκτυο πληροφοριών μεγάλου εύρους, προκειμένου να ανταποκριθεί τεχνολογικά στην εκτόξευση του Sputnik[3] από τη Ρωσία. Για αυτό το σκοπό ιδρύθηκε η υπηρεσία ARPA [4](Advanced Research Project Agency) γνωστή ως DARPA (Defense Advanced Research Projects Agency). Αποστολή της συγκεκριμένης υπηρεσίας ήταν να βοηθήσει τις στρατιωτικές δυνάμεις των ΗΠΑ να αναπτυχθούν τεχνολογικά και να δημιουργηθεί ένα δίκτυο επικοινωνίας το οποίο θα μπορούσε να επιβιώσει σε μια ενδεχόμενη πυρηνική επίθεση. Για να έχει αυξημένη αξιοπιστία το δίκτυο, κάθε σταθμός του υποδικτύου θα έπρεπε να συνδέεται με τουλάχιστον άλλους δύο σταθμούς. Το δίκτυο[5] αυτό άρχισε να γίνεται πραγματικότητα το 1968 όταν ανατέθηκε στην εταιρία BBN να σχεδιάσει λογισμικό για το υποδίκτυο, ενώ το λογισμικό για τους τερματικούς κόμβους ανατέθηκε σε ερευνητές μεγάλων πανεπιστημίων. Στο τέλους του 1972 το δίκτυο, που ονομάστηκε ARPANET αριθμούσε 32 τερματικούς σταθμούς.

Παράλληλα δημιουργήθηκαν και άλλα δίκτυα, τα οποία χρησιμοποιούσαν διαφορετικά πρωτόκολλα(όπως το x.25 και το UUCP) τα οποία συνδέονταν με το ARPANET. Το πρωτόκολλο που χρησιμοποιούσε το ARPANET ήταν το NCP (Network Control Protocol), το οποίο, όμως, είχε το μειονέκτημα ότι λειτουργούσε μόνο με συγκεκριμένους τύπους υπολογιστών. Έτσι, δημιουργήθηκε η ανάγκη στις αρχές του 1970 για ένα πρωτόκολλο που θα ένωνε όλα τα δίκτυα που είχαν δημιουργηθεί μέχρι τότε. Το 1974 λοιπόν, δημοσιεύεται η μελέτη των Βιντ Σερφ (Vint Cerf) και Μπομπ Κάαν (Bob Kahn) από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol) που αργότερα το 1978 έγινε TCP/IP, προσετέθη δηλαδή το Internet Protocol (IP), ώσπου το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET. Το 1984 υλοποιείται το πρώτο DNS (Domain Name System) σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών. Ένα ακόμα σημαντικό βήμα στην ανάπτυξη του διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation, NSF) των ΗΠΑ, το οποίο δημιούργησε την πρώτη διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet.

---

[3] Sputnik. Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα. Σελ.59

[4] Η λέξη Arpanet προκύπτει από τα αρχικά της υπηρεσίας του αμερικανικού στρατού

[5] Δίκτυο είναι ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους ασύρματα ή ασύρματα που δίνει την δυνατότητα να διαμοιράζονται πληροφορίες ταυτόχρονα σε ένα μεγάλο σύνολο ανθρώπων.

Ο όρος διαδίκτυο ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το ARPANET με το NSFNet και Internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε TCP/IP[6]. Η μεγάλη άνθιση του διαδικτύου όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Τιμ Μπέρνερς- Λι στο ερευνητικό ίδρυμα CERN το 1989, ο οποίος είναι στην ουσία, η ¨πλατφόρμα¨, η οποία κάνει εύκολη την πρόσβαση στο Ιντερνέτ, ακόμα και στη μορφή που είναι γνωστό σήμερα.

1.4 ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ Η ΕΠΙΚΟΙΝΩΝΙΑ.

Με την εμφάνιση οποιουδήποτε νέου μέσου, ο τομέας της επικοινωνίας αναμφισβήτητα επηρεάζεται. Η επίδραση αυτή πηγάζει κυρίως από την τεχνολογία του νέου μέσου. Σε τι επίπεδο μπορεί η τεχνολογία του διαδικτύου να αλλάξει τον τρόπο με τον οποίο επικοινωνούν και πληροφορούνται μαζικά οι άνθρωποι. Υπάρχουν διαφορετικές και αντικρουόμενες προσεγγίσεις πάνω στο θέμα.

Σύμφωνα με την προσέγγιση της ¨ιντερνετοφιλίας¨, το διαδίκτυο, αλλά και η ψηφιακή τεχνολογία γενικότερα, έχουν την ικανότητα να δημιουργούν ¨¨εικονικούς χώρους¨, ¨εικονικές κοινότητες¨, όπου παύουν να υφίστανται οι κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν εύκολα. Η επικοινωνία μέσω του διαδικτύου καθίσταται άμεση και αμφίδρομη. Δίνεται η δυνατότητα σε κάθε χρήστη ηλεκτρονικού υπολογιστή συνδεδεμένου στο διαδίκτυο, να πληροφορηθεί αλλά και να πληροφορήσει ανταλλάσσοντας απόψεις μέσω ενός πιο συμμετοχικού και λιγότερο ελεγχόμενου διαύλου επικοινωνίας. Οι χρήστες αποκτούν ολοένα και περισσότερο την ιδιότητα του παγκοσμίου πολίτη. Υπάρχει έντονη τάση, ήδη από την αρχή της εμφάνισης του διαδικτύου, να θεωρείται ένα άκρως δημοκρατικό μέσο μαζικής επικοινωνίας, το οποίο αποδιαμεσολαβεί την επικοινωνία και καθιστά ισχυρότερο τον μέσο άνθρωπο, καθώς δίνει στον τελευταίο τη δυνατότητα πρόσβασης σε μεγάλο όγκο πληροφοριών συγκεντρωμένων σε ένα ¨χώρο¨ και τη δυνατότητα της προσωπικής επιλογής των πληροφοριών αυτών. Συνεπώς, η βασική θέση της προσέγγισης αυτής είναι ότι το Διαδίκτυο θα εκδημοκρατίσει την κοινωνία με το να βελτιώσει την επικοινωνία καταργώντας την ανάγκη για διαμεσολάβηση.

1.5 ΝΟΜΙΚΑ ΚΑΙ ΗΘΙΚΑ ΖΗΤΗΜΑΤΑ.

Η παραβίαση πνευματικών δικαιωμάτων, η πορνογραφία, η πλαστοπροσωπία και η προσφορά παρανόμων προϊόντων είναι φαινόμενα υπαρκτά στο Ιντερνέτ και ο περιορισμός τους είναι ιδιαίτερα δύσκολος. Για παράδειγμα, η λέξη "sex" παραμένει μία από τις πλέον δημοφιλείς στις μηχανές αναζήτησης. Συχνά, η ανησυχία αυτή, που θεωρείται από κάποιους αβάσιμη, μπορεί να υποστηριχθεί από κάποια εγκλήματα ή αποτρόπαιες καταστάσεις (συνήθως περιπτώσεις παιδεραστίας κ.ά.). Το Διαδίκτυο έχει κατηγορηθεί ως παράγοντας που έπαιξε ρόλο σε θανάτους[7]. Ο Μπράντον Βέντας (Brandon Vedas) πέθανε από υπερβολική δόση ενός μείγματος νομίμων και παρανόμων ναρκωτικών παρακινούμενος από συνομιλητές του στο IRC. Ο Σων Γούλεϊ (Shawn Woolley) αυτοκτόνησε με πιστόλι για λόγους που σχετίζονται με τον εθισμό του με το EverQuest, ένα Μαζικά Πολυχρηστικό

[6] Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 63

[7] Παναγιωτοπούλου, Ρ. (2003. Η ΨΗΦΙΑΚΗ ΠΡΟΚΛΗΣΗ: ΜΜΕ ΚΑΙ ΔΗΜΟΚΡΑΤΙΑ. ΤΥΠΟΘΗΤΩ

Διαδικτυακό Παιχνίδι Ρόλων (MMORPG), όπως ισχυρίστηκε η μητέρα του. Ο Άρμιν Μάιβες (Armin Meiwes) μαχαίρωσε μέχρι θανάτου και έφαγε μέρος του σώματος του Μπερντ-Γιούργκεν Μπράντες (Bernd Jürgen Brandes) όταν ο τελευταίος απάντησε στην αγγελία του πρώτου που ζητούσε έναν «μεγαλόσωμο άνδρα έτοιμο να σφαγιαστεί και μετά να καταβροχθιστεί».

Επιπλέον, το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αντίστοιχη αρχή, η οποία θα ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί -σύμφωνα με πολλούς χρήστες αυτό θα αποτελούσε λογοκρισία. Όπως χαρακτηριστικά λέγεται "το Διαδίκτυο ελέγχεται από τους χρήστες του". Βεβαίως, οι κρατικές υπηρεσίες και αστυνομίες σε κάθε χώρα, καθώς και οι αντίστοιχες νομοθετικές ρυθμίσεις, παρεμβαίνουν για την αναστολή των αξιόποινων πράξεων που διαπράττονται μέσω Διαδικτύου.

Επίσης, ένα ακόμη ηθικό ζήτημα είναι ο συγκεντρωτισμός των Μ.Μ.Ε. και αναφέρεται στο ολιγοπώλιο μικρού σχετικά αριθμού εταιριών που κατέχουν τα μέσα και ελέγχουν όλη την αλυσίδα διανομής του προϊόντος. Στα πλαίσια του Διαδικτύου τίθεται το ερώτημα του κατά πόσο οι οικονομικές διαδικασίες στο παρόν καπιταλιστικό γίγνεσθαι περιορίζουν τη δημόσια σφαίρα και το αν είναι αποδεκτή ή κατακριτέα η πρωτοφανής ισοτιμία στην παρουσία και διαχείριση της πληροφορίας και του εμπορεύματος στο χώρο του Ίντερνετ. Επίσης παρά το γεγονός ότι το Ίντερνετ συχνά περιγράφεται ως αποκεντρωμένο, με απροσπέλαστο όγκο πληροφοριών και, συνεπώς, χωρίς κεντρικό έλεγχο, είναι εμφανής η εκτενής ιεράρχηση του περιεχομένου από μηχανές αναζήτησης και η γενικότερη διαιώνιση των ισοτόπων με την υψηλότερη επισκεψιμότητα.

1.6 ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ.[8]

Το δικαίωμα των Ευρωπαίων πολιτών για ελεύθερη πρόσβαση στο Διαδίκτυο κατοχυρώνεται στο άρθρο 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης. Πρόσφατα στο Ευρωπαϊκό Κοινοβούλιο ψηφίστηκε τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση... εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη». Ακόμη όμως και με την εν λόγω τροπολογία η πρόσβαση στο Διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας. Συγκεκριμένα, η τροπολογία αναφέρει επίσης «…η πρόσβαση στο Διαδίκτυο δεν μπορεί να περιοριστεί χωρίς να προηγηθεί δικαστική απόφαση. Εξαιρούνται οι περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών.» Χαρακτηριστικό παράδειγμα αποτελεί η Βρετανία, στην οποία οι πάροχοι απαγόρευσαν την πρόσβαση σε μια λίστα ιστοσελίδων στην οποία μέχρι τώρα βρίσκονταν σελίδες παιδικής πορνογραφίας, όμως πρόσφατα προστέθηκαν και άλλες, όπως αυτή που αφορά το χάκινγκ (hacking). Στους χρήστες που θα επιχειρούν να εισέλθουν σε κάποια από αυτές τις σελίδες θα απαγορεύεται η είσοδος, ενώ τα ηλεκτρονικά τους ίχνη θα καταγράφονται. Έτσι, παρά την εν λόγω τροπολογία, εξακολουθεί να μην λαμβάνεται υπ’ όψη ότι το αδιάσειστο δικαίωμα της πρόσβασης των πολιτών στο Διαδίκτυο αποτελεί προαπαιτούμενο για την προάσπιση και άλλων θεμελιωδών δικαιωμάτων όπως η γνώση, η παιδεία η ελευθερία έκφρασης και πολιτικής δράσης.

[8] https://el.wikipedia.org/wiki/Διαδίκτυο

Είναι σημαντικό, επίσης, να κατανοηθεί πως οι χρήστες του Διαδικτύου δεν είναι πελάτες αλλά πολίτες και ως τέτοιοι θα πρέπει να λογίζονται σε θέματα που αφορούν αφενός την υποδομή του διαδικτύου και αφετέρου το δικαίωμα πρόσβασης σε αυτό. Σχετικά με την υποδομή οφείλει η εκάστοτε εθνική αρχή να μεριμνά για την επέκταση του δικτύου, ακόμα και σε περιοχές που η ιδιωτική πρωτοβουλία αρνείται να προβεί στην απαιτούμενη επένδυση, όταν τη θεωρεί οικονομικά ασύμφορη. Έτσι θα διασφαλιστεί το δικαίωμα των πολιτών για ενημέρωση και ελευθερία έκφρασης. Όσον αφορά την πρόσβαση πρέπει να κατοχυρώνεται το δικαίωμα των πολιτών για ελεύθερη και ισότιμη πρόσβαση όπως αναφέρθηκε και με τα παραπάνω.

1.7 ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ ΚΑΙ ΠΡΟΣΤΑΣΙΑ.

Η πρόσβαση στο διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών, τόσο στο επίπεδο του χρησιμοποιούμενου υλικού, όσο και σε προσωπικό επίπεδο.

1.7.1 Πρόκληση ζημιών στο υπολογιστικό σύστημα

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο φαινομενικά αθώο αρχείο όπως ένα κείμενο ή μια φωτογραφία και όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο το δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου. Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη. Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

1.7.2 Πρόκληση Ζημιών Σε Προσωπικό Επίπεδο

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνον είναι δυνατό να υφαρπάζουν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών τραπέζης κτλ. Ανάλογη μέθοδος ακολουθείται και από ορισμένους ιστοτόπους, στους οποίους ο ανυπόμονος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλνοντας ένα προϊόν, το οποίο όχι μόνο δε θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστοτόπου για να πραγματοποιήσουν οι ίδιοι αγορές, χρεώνοντας τον ¨πελάτη¨ τους. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται ¨Phishing¨ (παραφθορά της λέξης fishing = ψάρεμα). Αρκετά προγράμματα περιήγησης αναγνωρίζουν τους ιστοτόπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα, ωστόσο αυτό δεν συμβαίνει σε ποσοστό 100%. Οι χρήστες είναι καλό να γνωρίζουν κανείς χρηματοπιστωτικός φορέας δεν χρησιμοποιεί το διαδίκτυο για να

ανανεώσει προσωπικές πληροφορίες, ενώ ένας προστατευόμενος ιστότοπος αρχίζει πάντα με το πρόθεμα https (secure, ασφαλής).

1.7.3 Παραπλάνηση

Αρκετές φορές οι χρήστες του διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε η αποκομιδή ιδίου οφέλους είτε, απλά, η χαρά της παραπλάνησης των (αγνώστων) χρηστών.

1.7.4 Προστασία

Υπάρχουν τρεις τρόποι προστασίας, οι οποίοι θα πρέπει να χρησιμοποιούνται σε συνδυασμό:
* Χρήση τείχους προστασίας (firewall)
* Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (spyware).
* Συνεχής ενημέρωση των χρηστών.

1.8 ΧΡΗΣΤΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ.

Σταθερή ανοδική ήταν η πορεία της διείσδυσης της χρήσης του Διαδικτύου στην Ελλάδα με τα ποσοστά να έχουν φθάσει πλέον πολύ κοντά στο ζενίθ τους, δεδομένου ότι στα μεγάλα αστικά κέντρα είναι ελάχιστοι εκείνοι που δεν μπορούν να χρησιμοποιούν έστω και μια φορά την εβδομάδα το ιντερνέτ, ενώ πλέον ακόμη και στις πιο απομακρυσμένες περιφέρειες το διαδίκτυο τα ποσοστά διείσδυσης κινούνται σε πολύ υψηλά επίπεδα.

Σύμφωνα με τα τελευταία στοιχεία της Focus Bari και της έρευνας Web ID της τελευταίας, η διείσδυση του διαδικτύου στην Ελλάδα φθάνει στο 82% του πληθυσμού ηλικίας 13 – 70 ετών, ποσοστό που μοιάζει εντυπωσιακά υψηλό για μία χώρα που θεωρείται ότι έχει μείνει πίσω σε σχέση με την υπόλοιπη Ευρώπη αναφορικά με την αξιοποίηση του ιντερνέτ[9]. Μάλιστα, το ποσοστό διείσδυσης στα αστικά κέντρα ανέρχεται πλέον στο 92% καθώς το διαδίκτυο αποτελεί βασικό κομμάτι της καθημερινότητας σχεδόν όλων των Ελλήνων, οι μισοί εκ των οποίων έχουν λογαριασμό στο facebook. Η πορεία της διείσδυσης ήταν σταθερά ανοδική την τελευταία 20ετία. Το διαδίκτυο έκανε την εμφάνιση του στις αρχές της δεκαετίας του ΄90 και αρχικά περιοριζόταν σε χρήστες που είχαν πρόσβαση μέσω ερευνητικών και ακαδημαϊκών κέντρων (Δημόκριτος, ΙΤΕ) για να κάνουν στη συνέχεια την εμφάνιση τους οι πρώτοι πάροχοι υπηρεσιών πρόσβασης (ISPs) όπως ήταν η Hellas On Line, η Forthnet κ.ά. Το 1995 που ξεκινά η Focus Bari να παρακολουθεί τη διείσδυση του Διαδικτύου, μόλις το 1% των κατοίκων στα μεγάλα αστικά κέντρα (πληθυσμός πάνω από 50.000 κάτοικοι) είχε πρόσβαση.

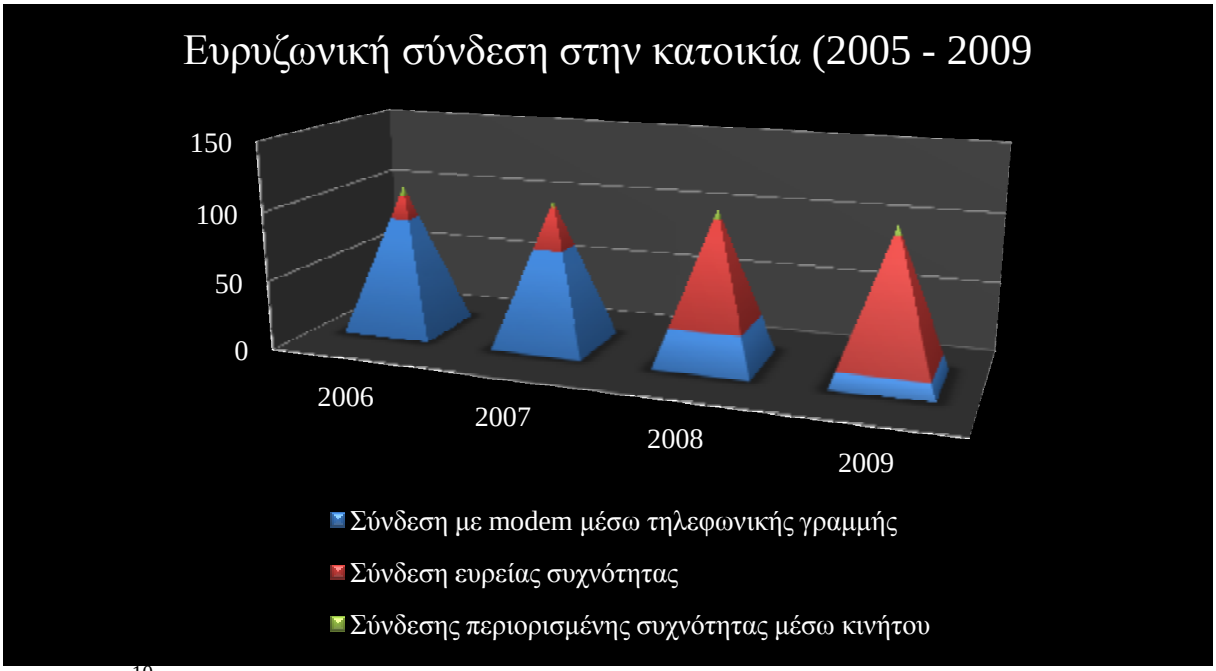
Το ποσοστό αυτό στα μεγάλα αστικά κέντρα είχε φθάσει στο 21% στις αρχές της δεκαετίας του 2000 οπότε η Focus Bari επεκτείνει το δείγμα της προκειμένου να περιλάβει και τις ημιαστικές περιοχές. Όμως η ταχεία επέκταση της χρήσης των προσωπικών υπολογιστών έχει

[9] https://www.cnn.gr

ως αποτέλεσμα να αρχίσει να αυξάνεται και η διείσδυση του διαδικτύου. Ειδικά μετά το 2005, εμφανίζονται στην Ελλάδα οι πρώτες ADSL συνδέσεις, που σημαίνει ότι δεν χρειάζεται να απασχολείς την τηλεφωνική γραμμή του σπιτιού και οι ταχύτητες είναι αρκετά καλύτερες, η διείσδυση κινείται με εντυπωσιακά γρήγορους ρυθμούς. . Από το 31% του 2004 φθάνουμε στο 56% του 2010, με τα νούμερα να συνεχίζουν να αφορούν τα αστικά κέντρα και τις ημιαστικές περιοχές.

Την τρέχουσα δεκαετία, η άνοδος συνεχίζεται περαιτέρω με την επικρατούσα άποψη να είναι πως το Facebook και η αυξημένη δημοτικότητα των social media σε συνδυασμό με την εμφάνιση των smartphones βοήθησαν σημαντικά ώστε η διείσδυση του Διαδικτύου να ενισχυθεί σημαντικά. Το αποτέλεσμα είναι το 2016 να κλείσει με τη διείσδυση πανελλαδικά να φθάνει στο 79% σε πανελλαδικό επίπεδο (ηλικίες 13-70 ετών) και στο 90% στα αστικά κέντρα, ενώ τα πιο πρόσφατα στοιχεία (Οκτώβριος 2017) κάνουν λόγο για ποσοστά της τάξεως του 92% και του 82%. Και θα πρέπει να σημειωθεί ότι στα παιδιά ηλικίας 10-12 ετών τα ποσοστά χρήσης κυμαίνονται σε επίπεδα της τάξεως του 90%. Κάτι που σημαίνει ότι τα επόμενα χρόνια, είναι πολύ πιθανό τα ποσοστά χρήσης να ενισχυθούν ακόμη περισσότερο, γεγονός που ενδέχεται να επηρεάσει ακόμη περισσότερο την καθημερινότητα μας, αν σκεφτεί κανείς την αύξηση που παρατηρείται στη χρήση του Διαδικτύου για την αγορά προϊόντων και υπηρεσιών ή την ενημέρωση και την ψυχαγωγία. Απ' ότι φαίνεται η ψηφιακή επανάσταση έφθασε και στην Ελλάδα.

Σύμφωνα με τα τελευταία στοιχεία (9/12/2009) της Εθνικής Στατιστικής Υπηρεσίας Ελλάδος ένα στα τρία νοικοκυριά διαθέτει ευρυζωνική σύνδεση. Συγκεκριμένα αυξήθηκε η χρήση ηλεκτρονικών υπολογιστών κατά 6,5% και η πρόσβαση στο διαδίκτυο κατά 11%, σε σύγκριση με το προηγούμενο έτος. Η αύξηση αυτή ενισχύει την απόφαση σε επένδυση στις νέες τεχνολογίες για την εξέλιξη των επιχειρήσεων.



Πίνακας 1[10]

[10] Στατιστικά στοιχεία, Ελληνική Στατιστική Υπηρεσία (ΕΣΥΕ)

Αναλυτικά η εν λόγο έρευνα έδειξε ότι τι προφίλ των χρηστών μπορεί να συνοψιστεί σε: απόφοιτους δευτεροβάθμιας εκπαίδευσης και ΙΕΚ, ανήκει στην ηλικιακή ομάδα 25 – 34 και είναι μισθωτός.

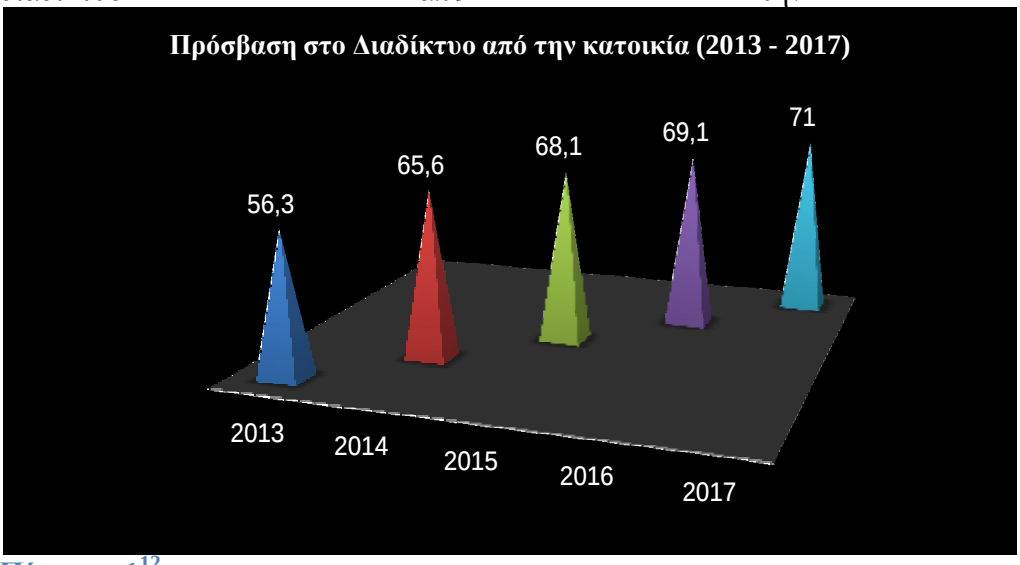
Επίσης οι κυριότεροι λόγοι πλοήγησης είναι:
* Αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες. (77,8%)
* Αναζήτηση ή λήψη ηλεκτρονικών μηνυμάτων. (72,9%)
* Αναζήτηση πληροφοριών για ταξίδια και καταλύματα.(58,1%)
* Ανάγνωση πάσης φύσεως πληροφοριών με σκοπό τη γνώση.(54,9%)
* Ανάγνωση εφημερίδων και περιοδικών.(50,0%)
* Αποστολή μηνυμάτων σε chat site, blogs, σε ομάδες συζήτησης (My Space, facebook), συμμετοχή σε forums, ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο (Messenger, Skype κ.α.). (42,3%)

Σημαντικό γεγονός αποτελεί ότι η ηλικιακή ομάδα 18 – 24 ετών επέλεξε σε ποσοστό 44% τον τελευταίο λόγο.

Το Ευρωβαρόμετρο[11] διαπιστώνει αύξηση της διείσδυσης των Η/Υ και του ιντερνέτ στα ελληνικά νοικοκυριά, αλλά η αύξηση αυτή δεν είναι αρκετή για να κλείσει το χάσμα μεταξύ Ελλάδας και Ε.Ε. Αντίστοιχα βήματα κάνουν οι άλλες, λιγότερο ανεπτυγμένες χώρες της Ε.Ε. Αξίζει να σημειωθεί ότι η Ελλάδα είναι η δεύτερη χώρα, μετά τη Ρουμανία, με τη μεγαλύτερη αναλογία Η/Υ που διαθέτουν σύνδεση στο ιντερνέτ.

Σημειώνεται ότι τα στοιχεία του Ευρωβαρομέτρου αφορούν μετρήσεις που έγιναν στο τέλος του 2009. Από την Ελλάδα αξιοποιήθηκε δείγμα 1.000 επικριθέντων, σε σύνολο 26.700 ατόμων σε ολόκληρη την Ε.Ε.

Την τελευταία πενταετία (2013 – 2017) καταγράφεται αύξηση 26,1% στην πρόσβαση στο διαδίκτυο από την κατοικία



Πίνακας 1[12]

[11] Το Ευρωβαρόμετρο αποτελεί μια σειρά ερευνών που λαμβάνουν χώρα ανά τακτικά χρονικά διαστήματα για λογαριασμό της Ευρωπαϊκής Επιτροπής από το 1973.
[12] Στατιστικά στοιχεία, Ελληνική Στατιστική Υπηρεσία (ΕΣΥΕ)

1.9 ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΩΝ ΜΕΣΩΝ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

Τα social media εμφανίστηκαν για πρώτη φορά στο χώρο του διαδικτύου ήδη από το 1994. Στόχος των πρώτων υβριδικών σελίδων Κοινωνικής Δικτύωσης ήταν η υποστήριξη διάδρασης των χρηστών τους μέσω chat rooms και ατομικών ιστοσελίδων στις οποίες μπορούσαν να δημοσιεύσουν και να μοιραστούν προσωπικές σκέψεις, ιδέες και πληροφορίες.

Οι καταχωρήσεις σε αυτές τις ατομικές ιστοσελίδες βασίζονταν σε χρήση εργαλείων δημοσίευσης στον Παγκόσμιο Ιστό, γεγονός που αποτέλεσε τον προάγγελο των Ιστολογίων.

Σε μια επέκταση των μέχρι τότε πρακτικών, νέοι Ιστότοποι Κοινωνικής Δικτύωσης (Classmates.com, SixDegrees.com), έδωσαν μεγαλύτερη έμφαση στη δικτύωση των χρηστών τους, χρησιμοποιώντας τις διευθύνσεις του ηλεκτρονικού ταχυδρομείου τους. Πλέον, ο κάθε συμμετέχοντας στην υπηρεσία είχε την δυνατότητα να καθορίσει ένα προσωπικό «προφίλ» καθώς και μια «λίστα φίλων» με τους οποίους μπορούσε να ανταλλάσει άμεσα μηνύματα. Οι υπηρεσίες αυτές για πρώτη φορά συγκεντρώθηκαν στον καινοτομικό ιστότοπο SixDegrees.com το 1997, οποίος όμως δεν κατάφερε να επιζήσει και τρία χρόνια αργότερα διέκοψε τη δραστηριότητά του[13].

Παράλληλα, με την πρώτη ενοποιημένη προσπάθεια Υπηρεσίας Κοινωνικής Δικτύωσης και μεταξύ του 1999 και 2001, αναπτύχθηκαν δυο διαφοροποιημένες υπηρεσίες που βασίζονταν σε δεσμούς εμπιστοσύνης: α) μεταξύ καταναλωτών σχετικά με προϊόντα (Epinions.com) και β) μεταξύ φίλων(Friendster.com) αντίστοιχα.

Οι καινοτομίες που προσέφεραν συμπεριελάμβαναν μεταξύ άλλων την προβολή των δεσμών φιλίας μεταξύ των χρηστών, ενώ παράλληλα υποστήριζαν λειτουργίες διαχείρισης περιεχομένου και διασυνδέσεων με τρίτους χρήστες.

Λίγα χρόνια αργότερα μεταξύ 2002 και 2004, εμφανίστηκαν τρείς Ιστότοποι Κοινωνικής Δικτύωσης (Friendster.com, MySpace, Bebo) που έκτοτε αποτέλεσαν τη δημοφιλέστερη περίπτωση τέτοιου είδους υπηρεσιών. Αυτά στάθηκαν και αφορμή να καταστούν προσφιλείς οι υπηρεσίες Κοινωνικής Δικτύωσης στη μαζική πλειοψηφία των διαδικτυακών χρηστών, σε βαθμό που κατάφεραν να ξεπεράσουν σε επισκεψιμότητα (MySpace) ακόμα και την Ιστοσελίδα της μηχανής αναζήτησης της Google[14].

Το 2004 δημιουργήθηκε το Facebook, που υπήρξε πολύ καλός ανταγωνιστής, και η ανάπτυξή του ήταν το ίδιο γρήγορη. Το 2006 ήταν η χρόνια που το Facebook σταμάτησε να απευθύνεται μόνο στην κοινότητα των αμερικανικών κολλεγίων, και απευθύνθηκε στο σύνολο των διαδικτυακών χρηστών ελεύθερα, δίνοντας παράλληλα τη δυνατότητα ενσωμάτωσης add-on εφαρμογών που είχαν αναπτυχθεί από τρίτους εκτός υπηρεσίας. Παράλληλα η υπηρεσία παρείχε τη δυνατότητα σχηματισμού ατομικών κοινωνικών δικτύων, διασυνδέονταν έτσι πέρα από χρήστες και Κοινωνικά Δίκτυα μεταξύ τους. Από το σημείο αυτό και έπειτα, οι Ιστότοποι Κοινωνικής Δικτύωσης καθίστανται οι ταχύτερα και μαζικότερα αναπτυσσόμενες ιστοσελίδες στον Παγκόσμιο Ιστό, χωρίς να γνωρίζουν γεωγραφικά σύνορα.

---

[13] Tuten Tracy, (2016), ***Social Media Marketing***, Εκδόσεις Δίαυλος, σελ. 23-27

[14] Tuten Tracy, (2016), ***Social Media Marketing***, Εκδόσεις Δίαυλος, σελ. 23-27

1.10 Ο ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ

1.10.1 Τύποι Εθισμού Στο Διαδίκτυο

Υπάρχουν πέντε διαφορετικοί τύποι εθισμού στο διαδίκτυο:
1) ο εθισμός του υπολογιστή, δηλαδή, ο εθισμός στο παιχνίδι στον υπολογιστή.
2) η υπερφόρτωση πληροφοριών δηλαδή, web surfing εθισμός.
3) οι διαδικτυακοί καταναγκασμοί, δηλαδή τα online τυχερά παιχνίδια σε απευθείας σύνδεση ή εθισμός στα online ψώνια.
4) ο cybersexual εθισμός δηλαδή, σε απευθείας σύνδεση πορνογραφία ή εξάρτηση από το σεξ.
5) ο εθισμός στις διαδικτυακές σχέσεις δηλαδή, ένας εθισμός σε απευθείας σύνδεση σχέσεις.
Υπάρχουν επίσης και κάποιοι τύποι συμπεριφορών που αφορούν τους εθισμένους στο διαδίκτυο.

- Ο πρώτος τύπος αφορά στην υπερβολική χρήση ιστοσελίδων που απευθύνονται σε ενηλίκους για διαδικτυακό σεξ (cyber sex) και διαδικτυακό πορνογραφικό υλικό (cyber porn).[15]
- Ο δεύτερος τύπος αφορά στις διαδικτυακές σχέσεις. Υπερβολική δηλαδή, ενασχόληση σε διαδικτυακές διαπροσωπικές σχέσεις στις σελίδες κοινωνικής δικτύωσης και τα δωμάτια συνομιλίας –γνωστά ως chat rooms- ή άλλων υπηρεσιών άμεσης ανταλλαγής μηνυμάτων, όπως το MSN.
- Ο τρίτος τύπος αφορά την ενασχόληση με τον τζόγο και τις διαδικτυακές αγορές.
- Στον τέταρτο τύπο περιλαμβάνεται η υπερβολική περιήγηση, δηλαδή συνεχόμενο και διαρκές «σερφάρισμα» στο διαδίκτυο και αναζητήσεις σε βάσεις δεδομένων.
- Τέλος, ο πέμπτος τύπος αφορά στην υπερβολική ενασχόληση με τους ηλεκτρονικούς υπολογιστές, εμμονή δηλαδή, με τα ηλεκτρονικά παιχνίδια, που όπως αναφέρεται στη χώρα μας, μαζί με τις σελίδες κοινωνικής δικτύωσης αποτελούν τους πρωταρχικούς παράγοντες που οδηγούν σε διαδικτυακές συμπεριφορές εξάρτησης.[16]

1.10.2 Εθισμός Των Παιδιών Στο Διαδίκτυο

Ο εθισμός στο διαδίκτυο και την τεχνολογία δεν αποτελεί ακόμη "επίσημη κατηγορία" στα εγχειρίδια ταξινόμησης ψυχικών διαταραχών. Ωστόσο έχει τα κριτήρια εκείνα που περιγράφουν τον εθισμό και τον καταναγκασμό αναφορικά με ουσίες και τον τζόγο. Πολλοί ερευνητές αντικαθιστούν την έννοια της «ουσίας» με αυτή του διαδικτύου και περιγράφουν το φαινόμενο. Πολλές είναι οι μελέτες που παρουσιάζουν τον εθισμό στο διαδίκτυο και με όρους ψυχαναγκασμού (obsessive and compulsive behavior).[17]
Ένα άτομο ή παιδί το οποίο είναι εθισμένο στο διαδίκτυο τις περισσότερες φορές εμφανίζει τα ακόλουθα συμπτώματα:
• *Εξιδανίκευση του μέσου*. Ο χρήστης θεωρεί τον ηλεκτρονικό υπολογιστή ή το Διαδίκτυο το σημαντικότερο «κεφάλαιο» της καθημερινότητάς του.

---

[15] Evans, J., (2015), Internet Addiction: Powerful Strategies For Internet Addiction, Depression And Anxiety And Stress Management (Social Media Addiction, Facebook, Addiction ... And Anxiety, Compulsive Behavior) USA: Yale University Press, pp. 59-62
[16] Evans, J., (2015), Internet Addiction: Powerful Strategies For Internet Addiction, Depression And Anxiety And Stress Management (Social Media Addiction, Facebook, Addiction ... And Anxiety, Compulsive Behavior) USA: Yale University Press, pp. 59-62
[17] Θεοφίλου, Μ., (http://www.paidiatros.com/efivos/psyxologia/internet-addiction-prevention, 2017, Διαδίκτυο: Εθισμός, πρόληψη και τρόποι αντιμετώπισης

•*Τροποποίηση της διάθεσης*. Σε όσους εθίζονται στα ηλεκτρονικά παιχνίδια παρουσιάζεται αύξηση της παραγωγής του νευροδιαβιβαστή του εγκεφάλου ντοπαμίνη, η οποία συνδέεται με την ευχαρίστηση.
• *Ανοχή*. Το άτομο χρειάζεται σταδιακά όλο και περισσότερες ώρες χρήσης του υπολογιστή ώστε να νιώθει ευχαρίστηση.
• *Σύγκρουση*. Ενώ το παιδί αισθάνεται ότι έχει πρόβλημα, δεν μπορεί να κάνει κάτι για να περιορίσει τη χρήση του υπολογιστή.
Αρκετοί δεν γνωρίζουν πώς να αντιδράσουν όταν διαπιστώνουν ότι, αντί να χρησιμοποιούν τα παιδιά τους το διαδίκτυο για τις εργασίες του σχολείου ή για έρευνες, αυτά στέλνουν μηνύματα στους φίλους τους, παίζουν παιχνίδια ή μιλούν σε αγνώστους στα δωμάτια συζητήσεων. Αυτό συμβαίνει γιατί είναι εύκολο να κρύψεις τι κάνεις στο διαδίκτυο και επειδή η εξάρτηση από το διαδίκτυο ακόμη δεν έχει ευρέως αναγνωριστεί. Τα παιδιά και οι νέοι εύκολα μπορεί να εγκλωβιστούν σε δικτυακές δραστηριότητες όπως τα παιχνίδια με πολλούς παίκτες, τα δωμάτια συζητήσεων κτλ.
Επιπτώσεις που μπορεί να έχει το διαδίκτυο στο παιδί
Όλα αυτά έχουν, όπως είναι επόμενο, σοβαρές επιπτώσεις σε διάφορους τομείς της λειτουργικότητας του ατόμου. Μειώνεται ο χρόνος που περνάει ο έφηβος με την οικογένειά του, περιορίζονται τα χόμπι και οι κοινωνικές συναναστροφές του, αυξάνεται ο κίνδυνος εμφάνισης παχυσαρκίας, μυοσκελετικών προβλημάτων και οφθαλμικών παθήσεων λόγω των πολλών ωρών- ακινησίας- μπροστά στην οθόνη. Παράλληλα, οι εθισμένοι στο Διαδίκτυο νεαροί παραμελούν τη σωματική τους υγιεινή, ενώ κάνουν πολλές απουσίες στο σχολείο με αποτέλεσμα ακόμη και να χάνουν την σχολική χρονιά.[18]

1.11 ΤΑ ΑΙΤΙΑ ΑΝΑΠΤΥΞΗΣ ΤΩΝ ΚΟΙΝΩΝΙΚΩΝ ΜΕΣΩΝ ΔΙΚΤΥΩΣΗΣ

1.11.1 Η Παγκοσμιοποίηση

Ο γενικός όρος που χρησιμοποιείται για την αύξουσα αμοιβαία εξάρτηση των κοινωνιών του κόσμου είναι «Παγκοσμιοποίηση». Σχεδόν καμία κοινωνία δεν ζει πια σε απόλυτη απομόνωση από τις άλλες. Ακόμα και στις πλουσιότερες κοινωνίες όλοι εξαρτώνται από τα αγαθά που μεταφέρονται από το εξωτερικό και τα προβλήματα που αντιμετωπίζει ο κόσμος ανάγονται σε παγκόσμια κλίμακα. Οι οργανώσεις που υπήρχαν σε διάφορες χώρες του κόσμου, τώρα πλέον υπάρχουν κατά κύριο λόγο υπό τη μορφή δικτύου και δραστηριοποιούνται σε αναδιατεταγμένο χώρο και χρόνο. Η τεχνολογία της πληροφορίας και οι ηλεκτρονικές επικοινωνίες έκαναν δυνατή την υπέρβαση των αποστάσεων και τον έλεγχο του χρόνου με τρόπους που θα ήταν αδιανόητοι παλαιότερα[19].

Οι διαδικασίες της παγκοσμιοποίησης που από τη μια μεριά δημιουργούνται από τις τεχνολογίες της επικοινωνίας και από την άλλη συνιστούν τη δύναμη που τις προωθεί, μεταβάλλουν τη μορφή των οργανώσεων, των κοινωνιών και γενικότερα της νέας γενιάς. Οι περισσότεροι νέοι σε αντίθεση με τις παλαιότερες γενιές, μεγαλώνουν σε μια χώρα και πολύ συχνά μεταβαίνουν σε μια άλλη για σπουδές.

---

[18] Θεοφίλου, Μ., (http://www.paidiatros.com/efivos/psyxologia/internet-addiction-prevention, 2017, Διαδίκτυο: Εθισμός, πρόληψη και τρόποι αντιμετώπισης
[19] Κιτρίδης, Δ., (2014), *Social Media Facebook Marketing*, Αθήνα: Ευρασία, σελ. 67-70

Ένας αρκετά μεγάλος αριθμός εργάζεται σε εταιρίες που δραστηριοποιούνται σε πολλές χώρες του κόσμου, ταξιδεύει και διαμένει σε αρκετά μέρη και ενδεχομένως να μην επιστρέψει ποτέ μόνιμα στον τόπο καταγωγής του. Εν γένει, οι άνθρωποι των νεότερων γενεών γίνονται παγκόσμιοι πολίτες, οι οποίοι μέχρι το τεσσαρακοστό έτος της ζωής τους έχουν, συνήθως, αλλάξει αρκετούς τόπους διαμονής και έχουν βρεθεί σε πολλές διαφορετικές θέσεις εργασίας .

Όλη αυτή η κατάσταση μετακίνησης και διαμονής ανά τον κόσμο, καθιστά τα κοινωνικά δίκτυα ενός ανθρώπου πολύ διαφορετικά από παλαιότερα. Ενώ το κοινωνικό δίκτυο ενός ανθρώπου στις προηγούμενες δεκαετίες περιοριζόταν στο οικογενειακό περιβάλλον, στο χώρο εργασίας, στο τοπικό κοινωνικό δίκτυο και ενδεχομένως σε κάποιες διασυνδέσεις από τη σχολική ηλικία και για τους άνδρες από τη στρατιωτική θητεία, σήμερα βρίσκεται διασκορπισμένο σε πολλά μέρη του κόσμου[20].

Κατά συνέπεια οι ιστότοποι κοινωνικής δικτύωσης αντανακλούν σε μεγάλο βαθμό το σημερινό τρόπο ζωής, όπου ο κυβερνοχώρος αποτελεί πλέον τον κοινό «χώρο συνεύρεσης». Θα μπορούσε να ισχυριστεί κανείς πως η δημιουργία αυτού του κοινού χώρου συνεύρεσης ακολουθεί δυο διαφορετικές πορείες.

1.12 Ο ΤΡΟΠΟΣ ΖΩΗΣ ΚΑΙ ΟΙ ΟΙΚΟΝΟΜΙΚΟΙ ΠΑΡΑΓΟΝΤΕΣ

Στην ανάπτυξη των ιστότοπων κοινωνικής δικτύωσης συμβάλει αποφασιστικά και ο σύγχρονος τρόπος ζωής. Η μετακίνηση μιας ολοένα μεγαλύτερης μάζας ανθρώπων στον τομέα της παροχής υπηρεσιών και στις δουλειές γραφείου, τα βεβαρημένα ωράρια, ο ελάχιστος ελεύθερος χρόνος σε μια κοινωνία που τρέχει με πρωτοφανείς ρυθμούς και η απομόνωση είναι από τα βασικότερα αίτια που ευνοούν την ανάπτυξη των ιστότοπων κοινωνικής δικτύωσης[21].

Όταν πολλοί άνθρωποι περνούν 12 με 16 ώρες καθηλωμένοι μπροστά σε μια οθόνη υπολογιστή, το μοναδικό τους διάλειμμα και η μοναδική τους κοινωνική αλληλεπίδραση είναι η επικοινωνία μέσω του ίδιου του υπολογιστή. Η αρχή έγινε με τη χρήση του email, έναν ασύγχρονο και απόμακρο τρόπο επικοινωνίας. Στη συνέχεια με τη διάδοση των εφαρμογών instant messaging (στιγμιαία μηνύματα) και τη δημιουργία chat rooms η επικοινωνία έγινε πιο προσωπική και πιο άμεση. Ακολούθησαν τα ιστολόγια και καθημερινή δημοσιοποίηση γεγονότων σε ένα κύκλο ανθρώπων και τέλος με τη σειρά τους οι ιστότοποι κοινωνικής δικτύωσης, όπου μεγάλο μέρος του κοινωνικού δικτύου ενός ανθρώπου εμφανίζεται στην οθόνη του υπολογιστή η οποία είναι και το εργαλείο της δουλειάς.

Πέρα από τον τρόπο ζωής του σύγχρονου ανθρώπου και τους κοινωνικούς παράγοντες που αναφέρθηκαν προηγούμενα, υπάρχουν και οικονομικά αίτια, τα οποία συντελούν στην ταχύτατη ανάπτυξη των ιστότοπων κοινωνικής δικτύωσης. Το σημαντικότερο, ίσως, από αυτά είναι τα κέρδη από τις διαφημίσεις που εμφανίζονται στην εκάστοτε σελίδα, κατά την πλοήγηση του χρήστη σε αυτούς τους ιστότοπους. Το γεγονός που καθιστά αυτόν τον τρόπο προώθησης προϊόντων τόσο επικερδή, είναι ότι πρόκειται για ένα είδος πολύ καλά στοχευμένης διαφήμισης. Με τον όρο «στοχευμένη διαφήμιση» εννοούμε πως οι διαφημίσεις

[20] Κιτρίδης, Δ., (2014), *Social Media Facebook Marketing*, Αθήνα: Ευρασία, σελ. 67-70
[21] Ό.π., σελ. 67-70

δεν προβάλλονται τυχαία σε όλους τους χρήστες, αλλά κάθε διαφήμιση προβάλλεται σε συγκεκριμένο απευθυνόμενο κοινό. Ουσιαστικά, τα δημογραφικά στοιχεία και τα ενδιαφέροντα που δηλώνουν οι χρήστες χρησιμοποιούνται, συνήθως από εταιρίες – μετόχους των εταιριών κοινωνικής δικτύωσης, οι οποίες «καταγράφουν» τις προτιμήσεις των χρηστών και τους προβάλλουν την αντίστοιχη διαφήμιση. Έτσι, οι διαφημιζόμενες εταιρίες προβάλλονται σε προκαθορισμένο αγοραστικό κοινό αποφέροντας, ταυτόχρονα, κέρδη στις εταιρίες στις οποίες ανήκουν οι ιστότοποι κοινωνικής δικτύωσης. Συγκεκριμένα, στον ιστότοπο του Facebook, υπάρχει ειδική σελίδα στην οποία μπορεί να δηλώσει κανείς την επιχείρηση του και το απευθυνόμενο κοινό του και στη συνέχεια να εμφανίζεται η διαφήμιση του σε προεπιλεγμένες ομάδες ανθρώπων[22].

Η στοχευόμενη διαφήμιση και κατ' επέκταση η απόκτηση ενός μεγάλου όγκου δημογραφικών στοιχείων αποτελούν, ενδεχομένως, τους βασικούς λόγους για τους οποίους μεγάλες εταιρίες επενδύουν σημαντικά ποσά στους ιστότοπους κοινωνικής δικτύωσης. Η εξαγορά μεριδίου του Facebook και του YouTube, έναντι υπέρογκων χρηματικών ποσών, από τις εταιρίες κολοσσούς, στηρίζουν αυτούς τους ιστότοπους καθιστώντας τους ραγδαία εξελισσόμενους κλάδους. Το τελευταίο ενισχύεται και από το γεγονός ότι η στοχευμένη διαφήμιση αποτελεί το επόμενο βήμα στον τομέα της προώθησης προϊόντων, καθώς αντί αυτά να προβάλλονται μέσω τηλεοπτικών σποτ σε μια μεγάλη μάζα ανθρώπων, προβάλλονται σε συγκεκριμένες πληθυσμιακές ομάδες. Οι ιστότοποι κοινωνικής δικτύωσης είναι η μεγαλύτερη βάση δημογραφικών δεδομένων και προτιμήσεων, η οποία κατά συνέπεια προσελκύει μεγάλο αριθμό επενδυτών που στηρίζουν την εξέλιξη τους[23].

1.13 ΤΑ ΚΥΡΙΟΤΕΡΑ SOCIAL MEDIA

1.13.1 Facebook

Το Facebook είναι χώρος κοινωνικής δικτύωσης που ξεκίνησε στις 4 Φεβρουαρίου του 2004. Οι χρήστες μπορούν να επικοινωνούν μέσω μηνυμάτων με τις επαφές τους και να τους ειδοποιούν όταν ανανεώνουν τις προσωπικές πληροφορίες τους.

Το Facebook σήμερα έχει πάνω από 800 εκατομμύρια ενεργούς χρήστες, κατατάσσοντάς το έτσι στη λίστα ταξινόμησης του Alexa ως ένα από τα δημοφιλέστερα web sites του πλανήτη (2ο μετά το google). Επίσης, το Facebook είναι ένα από τα δημοφιλέστερα sites για ανέβασμα φωτογραφιών με πάνω από 14 εκατομμύρια φωτογραφίες καθημερινά.[24]
Οι χρήστες του Facebook μπορούν να εγγραφούν σε αυτό καταχωρώντας προσωπικά στοιχεία όπως επίθετα, ηλεκτρονική διεύθυνση, ηλικία, κ.λπ. Σ' αυτόν τον χώρο μπορούν άτομα από οποιαδήποτε χώρα να επικοινωνήσουν, να μοιραστούν εικόνες, βίντεο, μουσική και ό, τι άλλο επιθυμούν χωρίς εμπόδια. Η εγγραφή είναι δωρεάν και δημιουργείται μέσα σε ελάχιστο χρόνο. Τα μέλη διατηρούν λίστα φίλων τους οποίους έχουν τη δυνατότητα να αναζητήσουν, να προσκαλέσουν ή να αποδεχτούν/αρνηθούν τη "φιλία" τους.

Το Facebook παρέχει στα μέλη του και μία σειρά ψυχαγωγικών εφαρμογών όπως τεστ προσωπικοτήτων, νοημοσύνης, ικανοτήτων καθώς και παιχνίδια ή υπηρεσίες προσομοίωσης

[22] Κιτρίδης, Δ., (2014), *Social Media Facebook Marketing*, Αθήνα: Ευρασία, σελ. 67-70
[23] Ό.π., σελ. 67-70
[24] http://www.snsagency.gr/about/facebook/ 2009. Τι είναι το Facebook

της πραγματικότητας, εικονικές φάρμες, κατοικίδια, εικονικές οικογένειες, τα οποία είναι πολύ δημοφιλή. Μέσω του facebook δίνεται η δυνατότητα συνομιλίας σε ζωντανό χρόνο με όλους τους facebook-φίλους, με την προϋπόθεση βέβαια να είναι κι οι δυο πλευρές ταυτόχρονα συνδεδεμένες. Οι υπηρεσίες που προσφέρει ποικίλουν και μπορεί κανείς να προσφέρει δώρα (ηλεκτρονικά), ν' αφιερώσει τραγούδια, να κεράσει ποτά κ.ο.κ στους φίλους του για τα γενέθλιά τους (υπάρχει ειδική ειδοποίηση) στη γιορτή τους ή έτσι απλά.[25]

Επίσης, μέσω του facebook μπορούμε να φτιάξουμε:

- Page
- Events
- Check in spots
- Facebook advertising

1.13.2 Twitter

Το twitter, αν και social network όπως το facebook, είναι κάτι εντελώς διαφορετικό. Το twitter, είναι ουσιαστικά μια υπηρεσία αποστολής σύντομων μηνυμάτων, που επιτρέπει να στέλνουμε σε πολλαπλούς παραλήπτες, ένα μήνυμα. Αντίστοιχα, λαμβάνουμε από άλλα άτομα που "παρακολουθούμε", τα σύντομα μηνύματά τους, που αποστέλλουν αυτοί στους πολλαπλούς αποδέκτες τους.

Το twitter λειτουργεί εξίσου απλά. Ο χρήστης δημιουργεί ένα λογαριασμό με το ψευδώνυμό του και τα πραγματικά στοιχεία του. Φίλοι του ή άτομα που ενδιαφέρονται για εκείνον, τον βρίσκουν, είτε μέσω αυτού, είτε μέσω ενημέρωσής τους, άμεσα ή έμμεσα. Έτσι, μπορούν να τον κάνουν follow: δηλαδή θα είναι οι παραλήπτες των σύντομων μηνυμάτων (μέχρι 140 χαρακτήρες). Αντίστοιχα, μπορεί κανείς να λαμβάνει τα μηνύματα των φίλων του, ή κοινώς των ατόμων που έχει κάνει follow. Με το που εγγραφεί κάποιος, δηλώνει ένα username, πχ coolwebgr.

Έτσι, αποκτά μία σελίδα με url: <http://www.twitter.com/coolwebgr>. Σε αυτή τη σελίδα, υπάρχει καταγεγραμμένη όλη η δραστηριότητα.

1.13.3 Youtube

Αν και όταν μιλάμε για κοινωνικά δίκτυα τα πρώτα που μας έρχονται στο μυαλό είναι το Facebook και το twitter, το YouTube είναι επίσης από τα μεγαλύτερα δίκτυα που ανεβάζει videoclips στο διαδίκτυο συγκεντρώνοντας εκατομμύρια από κόσμο παγκοσμίως. Όταν ξεκίνησε το YouTube το Φεβρουάριο του 2005 ο στόχος του ήταν να παρέχει online ψηφιακά video. Η Google αγόρασε το Youtube την επόμενη χρονιά. Η εταιρεία εκτιμά ότι κάθε λεπτό ανεβαίνουν στο διαδίκτυο 20 ώρες video.

[25] Σιδέρη, Μ., (2010), *Το βιβλίο του Facebook – Ένας οδηγός για «αθώους» χρήστες*, Αθήνα: Κλειδάριθμος, σελ. 25-28

Ανάλογα με την επιχείρηση και τους στόχους της, το YouTube μπορεί να βοηθήσει στην προβολή των χώρων, των event αλλά και σε πολλές άλλες παρουσιάσεις με στόχο να γνωρίσει καλύτερα ο υποψήφιος πελάτης την κάθε επιχείρηση και να δημιουργήσει fans.[26]
Το YouTube δίνει τη δυνατότητα στους χρήστες του, να εγγραφούν και να δημιουργήσουν λογαριασμό, για περαιτέρω χρήσεις. Αφού συμφωνήσουν με τους όρους χρήσης της υπηρεσίας, μπορούν όχι μόνο να παρακολουθούν τα βίντεο σαν θεατές, αλλά και να είναι αυτοί οι οποίοι τα ανεβάζουν. Επίσης μπορούν να αποθηκεύουν τα αγαπημένα τους βίντεο, χωρίς να χρειάζεται να κάνουν "Search", στην ιστοσελίδα.

Τα βίντεο που θεωρούνται ότι περιέχουν δυνητικά προσβλητικό περιεχόμενο είναι διαθέσιμα μόνο σε εγγεγραμμένους χρήστες και με ηλικία 18 ετών και άνω. Σημαντικό είναι να αναφερθεί, ότι το YouTube παρέχει στο κοινό μια εφαρμογή που λέγεται "YouTube Downloader", με την οποία οι χρήστες μπορούν να αποθηκεύουν τα βίντεο στον υπολογιστή τους, όπως επίσης και να μετατρέπουν τα βιντεοκλίπ σε MP3, ώστε να μπορούν να τα χρησιμοποιούν ως αρχεία μουσικής.[27]

1.13.4 Viber

Το Viber είναι μία δημοφιλής εφαρμογή messenger για υπολογιστές και κινητές συσκευές, η οποία επιτρέπει στους χρήστες να ανταλλάσσουν γραπτά μηνύματα, εικόνες, βίντεο και να πραγματοποιούν φωνητικές και βίντεο κλήσεις μέσω ιντερνέτ (WiFi ή 3G/4G).

Ιδιαίτερα στην Ελλάδα, η εφαρμογή είναι αρκετά δημοφιλής και μάλιστα υποστηρίζει την ελληνική γλώσσα. Συνολικά, η τελευταία μέτρηση μέσα στο καλοκαίρι έδειξε πως την εφαρμογή χρησιμοποιούν παγκοσμίως πάνω από 100 εκατ. ενεργοί μηνιαίοι χρήστες.[28]

Το Viber χρησιμοποιείται ως εναλλακτική επιλογή για πραγματοποίηση κλήσεων χωρίς χρεώσεις, αφού οι περισσότεροι το χρησιμοποιούν μέσω ασύρματων δικτύων WiFi. Δωρεάν κλήσεις, λοιπόν, ανάμεσα σε πολλών ειδών συσκευές, αφού η εφαρμογή υποστηρίζει πληθώρα λειτουργικών συστημάτων.

1.13.5 Instagram

Το Instagram είναι μία δημοφιλής mobile social εφαρμογή και συγχρόνως μία υπηρεσία κοινωνικής δικτύωσης, η οποία επιτρέπει τη λήψη και το διαμοιρασμό φωτογραφιών και βίντεο. Έγινε γνωστό χάρη στα φίλτρα φωτογραφιών του, ενώ σήμερα διαθέτει φίλτρα και για βίντεο, καθώς επίσης και πληθώρα άλλων εργαλείων φιλικών προς τους χρήστες.
Το Instagram ανήκει στο Facebook, με την εξαγορά να έχει πραγματοποιηθεί τον Απρίλιο του 2012 έναντι 1 δισ. δολαρίων.

---

[26] http://www.snsagency.gr/about/τι-είναι-το-youtube/ 2011, Τι είναι το YouTube

[27] Σιδέρη, Μ., (2010), *Το βιβλίο του Facebook – Ένας οδηγός για «αθώους» χρήστες*, Αθήνα: Κλειδάριθμος, σελ. 56-57

[28] Κόνσουλας, Θ., 2014, http://www.socialmedialife.gr/110183/ti-einai-to-viber-kai-pos-leitourgei/, τι είναι το viber και πως λειτουργεί;

Συνολικά υπάρχουν πάνω από 200 εκατ. εγγεγραμμένοι χρήστες, οι οποίοι έχουν ανεβάσει πάνω από 20 δισ. φωτογραφίες, ανεβάζουν καθημερινά πάνω από 60 εκατ. φωτογραφίες και πραγματοποιούν καθημερινά πάνω από 1,6 δισ. likes σε φωτογραφίες και βίντεο.

ΚΕΦΑΛΑΙΟ 2

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η ταχεία εξέλιξη και η συνεχώς αυξανόμενη διαθεσιμότητα της τεχνολογίας καθώς και η ραγδαία ανάπτυξη της επιστήμης της πληροφορικής, έχουν οδηγήσει σε σημαντικές αλλαγές σε όλους τους τομείς των καθημερινών δραστηριοτήτων, τόσο στην παραγωγική διαδικασία όσο και στις συναλλαγές, στην εκπαίδευση, στην ψυχαγωγία, ακόμα και στον τρόπο σκέψης του σύγχρονου ανθρώπου. Εκτός, όμως, από τις αλλαγές που επιφέρει η τεχνολογία και οι οποίες οδηγούν στην καλυτέρευση της ποιότητας της ζωής και στην ταχύτατη εξυπηρέτηση των αναγκών που δημιουργεί η σύγχρονη κοινωνία, διευκολύνθηκαν και δημιουργήθηκαν ιδανικές συνθήκες για την καλλιέργεια εκείνων των παραμέτρων που ευνοούν την ανάπτυξη νέων μορφών εγκληματικότητας που θεσμοθετούνται με τον όρο <Ηλεκτρονικό Έγκλημα>.

2.1 ΕΝΑ ΣΥΓΧΡΟΝΟ ΕΙΔΟΣ ΕΓΚΛΗΜΑΤΟΣ: ΤΟ ΠΛΗΡΟΦΟΡΙΚΟ ΕΓΚΛΗΜΑ.

Στις μέρες μας η πληροφορική τεχνολογία και για την ακρίβεια οι υπολογιστές έχουν ενταχθεί για τα καλά στην καθημερινή ζωή του σύγχρονου ανθρώπου. Από τις ΗΠΑ, χώρα πρωτοπόρο στην ανάπτυξη της πληροφορικής τεχνολογίας, μέχρι και τη χώρα μας, η οποία προσπαθεί να εναρμονισθεί με τις εξελίξεις της πληροφορικής τεχνολογίας, ο ηλεκτρονικός υπολογιστής υπάρχει σε κάθε σπίτι και σε κάθε επιχείρηση. Τα σύγχρονα προγράμματά του παρέχουν δυνατότητες όπως η επιτάχυνση των διαδικασιών, η οργάνωση μεγάλου όγκου πληροφοριών, ο άμεσος και ακριβής υπολογισμός και γενικότερα η δυνατότητα διαχείρισης σε πολύ μικρό χρονικό διάστημα τεράστιου όγκου δεδομένων, η άμεση πρόσβαση μέσω του διαδικτύου σε κάθε είδους πληροφορία, με αποτέλεσμα να απλοποιούν κατά πολύ την καθημερινότητα. Αυτές τις δυνατότητες φυσικά πρώτες έσπευσαν να εκμεταλλευθούν όλες οι μεγάλες επιχειρήσεις, ιδιωτικές και δημόσιες και σε μεγάλο βαθμό εξαρτούν την οργάνωσή τους από τα προγράμματα των ηλεκτρονικών υπολογιστών, ενώ πλέον υπάρχουν και επιχειρήσεις οι οποίες λειτουργούν αποκλειστικά στο διαδίκτυο.[29]

Αυτή όμως η εξάρτηση από τους ηλεκτρονικούς υπολογιστές καθιστά τον καθένα από εμάς αλλά και τις επιχειρήσεις ευάλωτες σε ένα πρωτοεμφανιζόμενο είδος εγκλήματος, το ηλεκτρονικό έγκλημα. Το ηλεκτρονικό έγκλημα σαν έννοια περιλαμβάνει ένα πολύ μεγάλο αριθμό εγκλημάτων, τα οποία για να εκτελεστούν απαιτούν υψηλή κατάρτιση επειδή γίνονται σε ηλεκτρονικό περιβάλλον. Επειδή δε η πληροφορική τεχνολογία εξελίσσεται διαρκώς,

[29] Δηλαδή, δεν έχουν κάποιο φυσικό χώρο στον οποίο θα μπορούσε κανείς να τις επισκεφτεί για να χρησιμοποιήσει τις υπηρεσίες που αυτές προσφέρουν.

εμφανίζονται συνέχεια νέες εγκληματικές μορφές του ηλεκτρονικού εγκλήματος και για αυτό το λόγο είναι δύσκολο να δοθεί κάποιος επίσημος ορισμός για αυτό.

Μέχρι τα μέσα της δεκαετίας του 1970, το ηλεκτρονικό έγκλημα ήταν σχεδόν άγνωστη έννοια. Τόσο στις ΗΠΑ όσο και στη Μ. Βρετανία οι ηλεκτρονικοί υπολογιστές εξυπηρετούσαν κυρίως τις ανάγκες του κράτους και τους στρατιωτικούς του σκοπούς, κυρίως δε τη διαχείριση απόρρητων πληροφοριών και την πληθυσμιακή απογραφή. Επίσης ελάχιστες ιδιωτικές επιχειρήσεις είχαν εγκαταστήσει και λειτουργούσαν εμπορικούς mainframe ηλεκτρονικούς υπολογιστές. Από τις αρχές της δεκαετίας του 1960 ο μετεξελιγμένος mainframe ηλεκτρονικός υπολογιστής άρχισε να προωθείται σε μεγάλες ιδιωτικές επιχειρήσεις και πανεπιστήμια. Τότε ήταν και η αφετηρία εμφάνισης του πρώιμου ηλεκτρονικού εγκλήματος. Δεν είχε όμως ακόμα επέλθει η μεγάλη ανάπτυξη της πληροφορικής τεχνολογίας, οι ηλεκτρονικοί υπολογιστές ήταν σε πολύ πρώιμο στάδιο, οπότε κάποιες αναφορές στη διεθνή βιβλιογραφία[30] της περιόδου αφορούσαν κυρίως παραβιάσεις συστημάτων πληροφορικής, οι οποίες γίνονταν είτε από υπαλλήλους επιχειρήσεων, οπότε αντιμετωπιζόταν ως υπαλληλικό έγκλημα, ή γίνονταν για την αλλοίωση οικονομικών στοιχείων, οπότε αντιμετωπιζόταν ως έγκλημα που εμπεριέχεται στα οικονομικά εγκλήματα.

Μέσα στη δεκαετία του 1980 όμως, που συνέβη η αλματώδης ανάπτυξη της πληροφορικής τεχνολογίας, και εμφανίστηκε ο ηλεκτρονικός υπολογιστής με τα χαρακτηριστικά και τον τρόπο λειτουργίας που ξέρουμε σήμερα, εμφανίστηκε πλέον το ηλεκτρονικό έγκλημα ως αυτόνομη μορφή εγκλήματος. Τότε αρχίζει και η προσπάθεια ορισμού και κατηγοριοποίησης του ηλεκτρονικού εγκλήματος. Όπως είναι φυσικό δεν υπήρχε νομικό πλαίσιο για την αντιμετώπισή του και στην αρχή επικράτησε χάος. Στα μέσα της δεκαετίας του 1980 όμως οι ΗΠΑ, άρχισαν σταδιακά να διαμορφώνουν ολοκληρωμένο νομικό σύστημα για την αντιμετώπισή του. Μεταξύ 1978 και 1988 έλαβε χώρα μια εκτεταμένη, τόσο σε εθνικό επίπεδο αλλά και σε διεθνές, ποινικοποίηση διαφόρων τύπων ενεργειών που σχετίζονταν με την πληροφορική τεχνολογία και τους ηλεκτρονικούς υπολογιστές. Μετά το 1984, στις ΗΠΑ προωθήθηκε το πρώτο νομοθέτημα για το ηλεκτρονικό έγκλημα σε ομοσπονδιακό επίπεδο. Κατόπιν όμως, τη δεκαετία του 1990 άρχισε και η εξάπλωση του διαδικτύου, με αποτέλεσμα να έχουμε την μετάβαση από το απλό ηλεκτρονικό/ πληροφορικό έγκλημα στο ηλεκτρονικό διαδικτυακό έγκλημα.

Ο ρυθμός ανάπτυξης της πληροφορικής τεχνολογίας και επέκτασής της είναι αλματώδης, ακόμα και στις μέρες μας. Η τάχιστη και πολύμορφη ανάπτυξη της τεχνολογίας δημιουργεί διαρκώς νέα δεδομένα και αλλαγές κατεύθυνσης στις προϋποθέσεις που ισχύουν, οι οποίες φυσικά μεταβάλλονται διαρκώς. Οι ηλεκτρονικοί εγκληματίες είναι άτομα άριστα καταρτισμένα σε ό,τι αφορά στη λειτουργία ενός ηλεκτρονικού υπολογιστή και πολλές φορές είναι ένα βήμα μπροστά από τη νομοθεσία στα εγκλήματα που διαπράττουν. Το ηλεκτρονικό έγκλημα είναι μια πολύ ρευστή μορφή εγκλήματος, με πολλές συνισταμένες και διαρκείς ανατροπές και για αυτό κανένα στοιχείο του δε μπορεί να θεωρηθεί ως δεδομένο.

[30] Η βιβλιογραφία αυτή προέρχεται κυρίως από τις ΗΠΑ. Στην Ελλάδα τότε ο ηλεκτρονικός υπολογιστής φάνταζε μακρινό όνειρο, συνεπώς δεν είχε εμφανιστεί το ηλεκτρονικό έγκλημα, ούτε καν στην πρώιμη μορφή του.

2.2 ΕΝΝΟΙΟΛΟΓΙΚΗ ΠΡΟΣΕΓΓΙΣΗ- ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ήδη από την δεκαετία του 1970 παρουσιάστηκε η εγκληματικότητα μέσω των ηλεκτρονικών υπολογιστών ως φαινόμενο που άπτεται του ποινικού ενδιαφέροντος, γεγονός που οδήγησε σταδιακά πολλές έννομες τάξεις στη λήψη ειδικών ποινικών νομοθετικών μέτρων. Τα τελευταία χρόνια ,όμως, έκαναν την εμφάνισή τους και περιπτώσεις κατάχρησης του κυβερνοχώρου, που δεν παρουσιάζουν πάντα τα χαρακτηριστικά της εγκληματικότητας μέσω των ηλεκτρονικών υπολογιστών.

Έτσι, είναι πλέον αναγκαίο να γίνεται διάκριση μεταξύ του λεγόμενου ηλεκτρονικού εγκλήματος και του διαδικτυακού (cyber crime)[31], το οποίο παρουσιάζει ποιοτικά σημαντικές διαφοροποιήσεις από το πρώτο λόγω των ιδιαίτερων χαρακτηριστικών του διαδικτύου, που συνοψίζονται στη δυνατότητα ανταλλαγής δεδομένων και προγραμμάτων μεταξύ όλων των συνδεδεμένων υπολογιστών.

Αξίζει, επίσης, να σημειωθεί η δυσκολία διατύπωσης ενός ενιαίου ορισμού που να περιλαμβάνει όλες τις πλευρές του διαδικτυακού εγκλήματος, κάτι που παρατηρείται και αναφορικά με τον εννοιολογικό προσδιορισμό εν γένει της ηλεκτρονικής εγκληματικότητας. Αυτό συμβαίνει, διότι οι παραβάσεις στο διαδίκτυο παρουσιάζουν ποικιλομορφία ως προς τις μορφές εκδήλωσής τους και αποβλέπουν στην προσβολή διάφορων κάθε φορά εννόμων αγαθών.

Πάντως, η άποψη ότι το διαδικτυακό έγκλημα αποτελεί τον ίδιο τύπο εγκλήματος με το κοινό και το μόνο στοιχείο που το διαφοροποιεί από το κοινό έγκλημα είναι ότι διαπράττεται σε διαφορετικό περιβάλλον, αυτό του διαδικτύου, μάλλον δεν ανταποκρίνεται στην πραγματικότητα. Και αυτό, διότι υπάρχουν μεν εγκλήματα που διαπράττονται τόσο σε κοινό όσο και σε ηλεκτρονικό και διαδικτυακό περιβάλλον, ωστόσο υπάρχουν και εγκλήματα που αποκλειστικά τελούνται στο περιβάλλον του κυβερνοχώρου.[32]

Κατά συνέπεια ένα πρώτο συμπέρασμα αναφορικά με τον εννοιολογικό προσδιορισμό του ηλεκτρονικού και διαδικτυακού εγκλήματος είναι η σαφής διαφοροποίηση των δύο εννοιών. Το διαδικτυακό έγκλημα είναι δηλαδή μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος.

Η δυσκολία της εννοιολογικής προσέγγισης του ηλεκτρονικού και διαδικτυακού εγκλήματος οδηγεί στο συμπέρασμα ότι ίσως ένας κοινά αποδεκτός ορισμός για το ηλεκτρονικό διαδικτυακό έγκλημα – με τον κίνδυνο βέβαια να θεωρηθεί αόριστος – θα ήταν ένας ευρύς, που περιλαμβάνει όλες εκείνες τις αξιόποινες πράξεις που τελούνται με τη χρήση του διαδικτύου.

Προς την κατεύθυνση αυτή ως ηλεκτρονικό έγκλημα θα μπορούσε να οριστεί εκείνο το έγκλημα που σχετίζεται με την οποιαδήποτε μορφή κατάχρησης των δυνατοτήτων των ηλεκτρονικών υπολογιστών, ενώ ως διαδικτυακό εκείνο που σχετίζεται με την οποιαδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο.[33] Στην έννοια της

---

[31] Ή έγκλημα του κυβερνοχώρου, όπως το αναφέρει ο Ι. Αγγελής στο <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 675

[32] Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 676

[33] Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, 678

κατάχρησης θα πρέπει να περιλαμβάνεται κάθε παράνομη, ανήθικη και χωρίς δικαίωμα συμπεριφορά.[34]

Το 1986, ο Christofer Chen επισήμανε τη σημασία κατάληξης σε ένα κοινά αποδεκτό ορισμό, διότι αν δεν ξέρουμε τι είναι το ηλεκτρονικό έγκλημα δε μπορούμε να πούμε πότε έλαβε χώρα, δε μπορούμε να αναπτύξουμε λύσεις για την αντιμετώπισή του ενώ αν συνέχιζε η διαφωνία και οι διαφορετικές απόψεις σε ότι αφορούσε στο ηλεκτρονικό έγκλημα, οι μελέτες πάνω σε αυτό θα συνέχιζαν να παράγουν μη συνεκτικά αποτελέσματα και συμπεράσματα.

Κατόπιν μια ομάδα επιστημόνων που είχαν ασχοληθεί με περιπτώσεις που εμπίπτουν στο ηλεκτρονικό έγκλημα, δεν προχώρησαν στην ανάπτυξη ορισμού, στηρίζοντας την άποψή τους στο επιχείρημα ότι το ηλεκτρονικό έγκλημα δεν είναι παρά το ήδη γνωστό έγκλημα τελούμενο με νέους τρόπους διάπραξης.[35] Άλλη ομάδα επιστημόνων έδωσαν ιδιαίτερη έμφαση στις ειδικές εκδοχές του ηλεκτρονικού εγκλήματος, προσεγγίζοντάς το ως είδος οικονομικού εγκλήματος, ή επαγγελματικού εγκλήματος, ή εγκλήματος λευκού περιλαιμίου.[36]

Παρ' όλες όμως τις διαφορετικές απόψεις, από τις αρχές της δεκαετίας του 1990 η πλειονότητα των νομικών, εγκληματολόγων και κοινωνιολόγων που ασχολήθηκαν με το ηλεκτρονικό έγκλημα, κατέληξαν σε μία ελάχιστη συμφωνία στις τρεις βασικές ποιοτικές διαφορές μεταξύ του ηλεκτρονικού και του μη ηλεκτρονικού εγκλήματος.

Η πρώτη ποιοτική διαφορά έχει να κάνει με τον τρόπο τέλεσης του ηλεκτρονικού εγκλήματος. Οι επιστήμονες συμφώνησαν ότι το πλαίσιο δράσης, ο χρόνος δράσης, η σε πραγματικούς χρόνους απόσταση μεταξύ δράσης και αποτελέσματος, ο προγραμματισμός της δράσης καθώς και το σύστημα συμπεριφορών μέσω των οποίων εκδηλώνεται το ηλεκτρονικό έγκλημα δεν είναι δυνατό να αναχθούν στο μικροηλεκτρονικό έγκλημα χωρίς να λάβουν χώρα απλουστεύσεις, οι οποίες επιτρέπουν τουλάχιστον στις σοβαρότερες μορφές ηλεκτρονικού εγκλήματος να βρεθούν εκτός των ορίων του νόμου.

Η δεύτερη ποιοτική διαφορά βρίσκεται στο μόνιμο και συχνά το αυτόματο των αποτελεσμάτων του ηλεκτρονικού εγκλήματος. Δηλαδή, από τη στιγμή που ο δράστης εντοπίζει ένα τρόπο παράκαμψης της βασική ρουτίνας ενός λογισμικού (software) και την αξιοποιεί για πρώτη φορά, έχει τη δυνατότητα να την αξιοποιεί συνεχώς, χωρίς καν να χρειάζεται να επαναλαμβάνει την αρχική του ενέργεια αφού το τροποποιημένο λογισμικό εκτελεί αυτόματα τις εντολές που του έχουν δοθεί ως μέρος των συνολικών εντολών που έχει πάρει. Ακόμα και αν κάποτε ο δράστης σταματήσει να κάνει την αρχική του ενέργεια, τα αποτελέσματά της θα επαναλαμβάνονται αυτόματα.

Η Τρίτη ποιοτική διαφορά αφορά στην ικανότητα της εξ' αποστάσεως διάπραξης ηλεκτρονικών εγκλημάτων μέσω τηλεφωνικών συνδέσεων και του διαδικτύου. Η φυσική παρουσία του δράστη στο χώρο που σκοπεύει να κάνει την παραβίαση είναι περιττή, έτσι

---

[34] Μυλωνόπουλος Χρ., <Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο>, σελ. 14

[35] Όπως ο Donald Ingraham, ο οποίος υποστήριζε ότι δεν υπάρχει το ηλεκτρονικό έγκλημα ως αυτόνομη κοινωνική πραγματικότητα, και ο Douglas Reimer, ο οποίος υποστήριζε ότι τα ηλεκτρονικά εγκλήματα δεν ήταν νέα εγκλήματα αλλά τα ίδια παλαιά εγκλήματα τα οποία διαπράττονται με νέους τρόπους χάρη στην πληροφορική τεχνολογία και τους ηλεκτρονικούς υπολογιστές για αναλυτική παράθεση των απόψεών τους ,βλέπε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 46

[36] Όπως οι Parker, Bequai και Bloomberg, για αναλυτική παράθεση των απόψεών τους, βλέπε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 37- 44.

αυτός παραμένει αόρατος και ο εντοπισμός του απαιτεί νέες τεχνολογίες, νέες αρχές και νέα πρότυπα δράσης από τις ιδιωτικές αρχές.

Ακολούθως μια σειρά επιστημόνων διατύπωσαν και άλλους ορισμούς για το ηλεκτρονικό έγκλημα και προσπάθησαν να το κατηγοριοποιήσουν περαιτέρω.[37]

Ο ορισμός ο οποίος είναι ο πιο αποδεκτός και ήρθε να δώσει τη λύση σε όλη την προηγούμενη πολυφωνία είναι ο ορισμός του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ), ο οποίος ήρθε για να δώσει λύση στο πρόβλημα το 1986. Σύμφωνα με τον ορισμό αυτό <Ηλεκτρονικό έγκλημα συνιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή και τη μετάδοση δεδομένων>. Ο ορισμός αυτός ολοκληρώνεται από μια οριοθέτηση βασικών κατηγοριών του ηλεκτρονικού εγκλήματος, που είναι οι εξής:

- Εισαγωγή ή μετατροπή δεδομένων χωρίς εξουσιοδότηση ή καταστροφή δεδομένων ή και προγραμμάτων ενός υπολογιστή (ακριβέστερα ενός συστήματος επεξεργασίας δεδομένων)
- Αλλοίωση ή μείωση της αξιοπιστίας δεδομένων ενός συστήματος επεξεργασίας δεδομένων
- Χωρίς άδεια παρείσδυση σε πληροφορικά συστήματα και αφαίρεση ή αντιγραφή στοιχείων
- Παρεμπόδιση της λειτουργίας πληροφορικών ή και τηλεπικοινωνιακών συστημάτων.

Ακόμα, μία Πέμπτη κατηγορία ηλεκτρονικού εγκλήματος είναι αυτή που αναφέρεται στην παραβίαση των αποκλειστικών δικαιωμάτων του δημιουργού ή του κατόχου οποιουδήποτε είδους (δεδομένα ή προγράμματα) πληροφορικού υλικού.

Η Interpol[38] ονομάζει το ηλεκτρονικό έγκλημα ψηφιακό (digital crime) και το χωρίζει σε τρεις κατηγορίες:

Στο ηλεκτρονικό έγκλημα, το οποίο περιλαμβάνει την πειρατεία, την κλοπή δεδομένων και την κλοπή χρόνου, το λεγόμενο computer break- ins,

Στο ηλεκτρονικό έγκλημα, το οποίο σχετίζεται με τραπεζικές απάτες,

Στο έγκλημα διαδικτύου, το οποίο περιλαμβάνει την παιδική πορνογραφία, την αγορά και την πώληση ναρκωτικών και το ξέπλυμα χρήματος.

Με έμφαση πρέπει να τονιστεί ότι τα ανωτέρω μόνο ως εννοιολογικές προσεγγίσεις και ως κατευθυντήριες γραμμές πρέπει να λαμβάνονται υπ' όψη, που σκοπό έχουν να μας εισάγουν στο φαινόμενο της ηλεκτρονικής εγκληματικότητας. Σε καμιά περίπτωση δεν αποτελούν ορισμούς εγκλημάτων, διότι δεν πληρούν τις προϋποθέσεις οριοθέτησης εγκληματικών συμπεριφορών με την έννοια που το ποινικό δόγμα απαιτεί, αφού δεν περιγράφονται σε αυτούς τους <ορισμούς> η αντικειμενική και υποκειμενική υπόσταση των εγκλημάτων, γεγονός που τους καθιστά αόριστους. Αφήνεται στη διάθεση, λοιπόν, η οριστικοποίηση και η πλήρης διασαφήνιση αυτών των όρων στους εθνικούς νομοθέτες και κυρίως η ερμηνεία τους στη νομολογία των δικαστηρίων.

---

[37] Όπως οι Martin Wasik, Karen Forcht, Daphyne Thomas, Karen Wigginton, Steve Shackelford, Scott Charney, Barry Hurewitz, Allen Lo, αναλυτικά οι απόψεις τους σε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 48- 51

[38] Clarke R., ''Technological Aspects of Internet Crime Prevention''

2.3 ΑΠΟ ΤΟ ΑΠΛΟ ΗΛΕΚΤΡΟΝΙΚΟ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΔΙΑΔΙΚΤΥΑΚΟ ΕΓΚΛΗΜΑ.

Μετά την εμφάνιση και εξάπλωση του διαδικτύου ένας νέος, συνδυαστικός τύπος εγκλήματος έκανε την εμφάνισή του, το ηλεκτρονικό διαδικτυακό έγκλημα, το οποίο αποτελεί νέα κατηγορία των ηλεκτρονικών εγκλημάτων. Η ραγδαία αύξηση του αριθμού των χρηστών του διαδικτύου και η σύνδεση μεταξύ τους όλο και περισσότερων ηλεκτρονικών υπολογιστών επέτρεψε τη μεταφορά πολλών ηλεκτρονικών εγκλημάτων στο χώρο του διαδικτύου. Παλαιότερα είχε υποστηριχθεί η θέση ότι η μόνη διαφορά που το διακρίνει από το κοινό έγκλημα είναι ότι αυτό διαπράττεται σε ηλεκτρονικό περιβάλλον, η οποία όμως δεν ανταποκρίνεται στην πραγματικότητα. Κατά μία άποψη το διαδικτυακό έγκλημα αποτελεί ένα πολύ νέο είδος εγκλήματος, το οποίο λαμβάνει χώρα στο διαδίκτυο, κατά άλλους είναι μία παραλλαγή των ήδη υπαρχόντων εγκλημάτων τα οποία διαπράττονται στο διαδίκτυο και κατά άλλη άποψη ταυτίζεται με κάθε εγκληματική πράξη που διαπράττεται στο διαδίκτυο.

Υπάρχουν εγκλήματα τα οποία διαπράττονται τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον, όπως η απάτη που μπορεί να γίνει στο κοινό περιβάλλον έχοντας το θύμα απέναντί σου αλλά και σε ηλεκτρονικό περιβάλλον, στέλνοντας παραδείγματος χάρη απατηλό e-mail. Υπάρχουν εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς αυτοί να είναι συνδεδεμένοι με το διαδίκτυο(το οποίο αποτελεί αμιγώς πληροφορικό έγκλημα), όπως η παράνομη αντιγραφή περιεχομένου CD σε ηλεκτρονικό υπολογιστή και άλλα εγκλήματα που διαπράττονται μόνο στο χώρο του διαδικτύου, τα γνήσια εγκλήματα κυβερνοχώρου (cyber crimes), όπως η διάδοση πορνογραφικού υλικού μέσω διαδικτύου.

Με την εξάπλωση του διαδικτύου και κατόπιν την εμφάνιση του διαδικτυακού εγκλήματος, ο τομέας του ποινικού δικαίου δεν αντέδρασε άμεσα στη νέα αυτή πρόκληση, σε αντίθεση με τον τομέα της πνευματικής ιδιοκτησίας, ο οποίος επέδειξε άμεσα αντανακλαστικά στις νέες τεχνολογίες και έχει διαμορφώσει των δικαιωμάτων τους.

Βέβαια, δεν πρέπει να αγνοήσουμε τις ιδιαιτερότητες του διαδικτύου, οι οποίες διαφοροποιούν κατά πολύ τα δεδομένα με τα οποία θα αντιμετωπιζόταν ένα κοινό έγκλημα. Βασική διαφοροποίηση, όπως αναφέρθηκε και στις ιδιαιτερότητες του διαδικτυακού εγκλήματος, είναι ότι τα χρονικά και τα τοπικά όριά του είναι πολύ δυσδιάκριτα. Η κάθε είδους ανταλλαγή δεδομένων και συναλλαγή μπορεί να γίνει σε δευτερόλεπτα, ενώ καταργούνται και τα τοπικά όρια με την παραδοσιακή τους μορφή, αφού ένας Έλληνας χρήστης, μέσω πρόσβασης σε αγγλικό server ηλεκτρονικού υπολογιστή μπορεί να επιφέρει βλάβη σε λογισμικό υπολογιστή που βρίσκεται στην Αυστραλία. Επομένως, γεννώνται εύλογα ερωτήματα, ως προς το ποια εθνική έννομη τάξη θα επιλαμβάνεται σε κάθε περίπτωση και κατά πόσο θα νομιμοποιείται, όταν υπάρχει υπερεθνική εμβέλεια.

Κατά την αρχή του το διαδίκτυο θεωρούνταν ως ένας χώρος ελεύθερος και ανοιχτός στον κάθε χρήστη, όπου ο καθένας περιπλανούνταν όπου ήθελε και οι διαμορφούμενες κοινωνίες μπορούσαν να διαμορφώσουν τους δικούς τους κανόνες δικαίου.[39] Αναπτύχθηκαν λοιπόν ισχυρές απόψεις που θέλουν την λειτουργία του απρόσκοπτη και απαλλαγμένη από κάθε είδους κρατικές παρεμβάσεις.

[39] Βλ. Κριθαράς Θ., <Ποινικό Δίκαιο και Διαδίκτυο>, σελ. 10

Η κυριότερη άποψη υποστήριξης αυτής της θέσης είναι η <Διακήρυξη για την Ανεξαρτησία του Κυβερνοχώρου> του John Perry Barlow, διάσημου ροκ τραγουδιστή τη δεκαετία του 1980 και αργότερα μαχητικού ακτιβιστή του διαδικτύου, ο οποίος ίδρυση μία μη κυβερνητική οργάνωση για την προστασία των θεμελιωδών δικαιωμάτων των χρηστών του διαδικτύου. Άποψη του John Perry Barlow είναι ότι στον κυβερνοχώρο δεν υπάρχουν όρια, ούτε σύνορα, όπως στον φυσικό κόσμο και για αυτό οι νομικές κατασκευές του κοινού δικαίου δεν έχουν καμία εφαρμογή εκεί. Στον Κυβερνοχώρο μπορεί να συμβεί ό,τι σκεφτεί το ανθρώπινο μυαλό και το κράτος δεν έχει καμία δικαιοδοσία, οι μόνοι που μπορούν να παρέμβουν για να λύσουν τυχόν προβλήματα είναι οι χρήστες του.[40] Η άποψη αυτή αναδεικνύει τις αυξημένες προσδοκίες που είχαν δημιουργηθεί κατά τη δημιουργία του διαδικτύου για την ελευθερία του πολίτη που θα συμμετείχε σε αυτό και για την αυτορρύθμιση όποιου προβλήματος και αν ανέκυπτε.

Υπάρχουν και άλλες απόψεις για την αυτορρύθμιση του διαδικτύου. Σύμφωνα με μία από αυτές, στο διαδίκτυο, μέσω της καθημερινής του χρήσης από εκατομμύρια χρηστών, εξελίσσεται και διαμορφώνεται ένα είδος εθιμικού δικαίου. Σύμφωνα με αυτή τη θεωρία, όλα τα προβλήματα που προκύπτουν στο διαδίκτυο μπορούν να επιλυθούν με τη χρήση των μέσων που η ίδια η τεχνολογία παρέχει. Με τον τρόπο αυτό δημιουργείται ένα εθιμικό πλαίσιο κανόνων συμπεριφοράς που ταιριάζει στο διαδίκτυο, το οποίο καλείται να συμβιβάσει τα διαφορετικά δικαιϊκά συστήματα και να αποτελέσει τη βάση για τη διαμόρφωση ενός ευέλικτου δικαιϊκού πλαισίου, κατάλληλου για το διαδίκτυο.

Ακόμα μία θεωρία για την αυτορρύθμιση του διαδικτύου είναι αυτή που ξεχωρίζει τον Κυβερνοχώρο από τον φυσικό χώρο και θεωρεί σημαντική την ανάπτυξη νέων μηχανισμών ρύθμισης και επιβολής του δικαίου. Κατά αυτή την άποψη, όσοι χρησιμοποιούν το διαδίκτυο γνωρίζουν ότι συναλλάσσονται και επικοινωνούν με ανθρώπους, των οποίων την πραγματική θέση δε γνωρίζουν. Το μόνο που γνωρίζουν είναι που να τους βρουν στον Κυβερνοχώρο, ο οποίος κάθε άλλο παρά ομοιογενής είναι, αφού κάθε λεπτό, σε διαφορετικά μέρη του εξελίσσονται άπειρες διαφορετικές δραστηριότητες. Τα όρια του διαδικτύου είναι πλήρως διακριτά από αυτά του φυσικού κόσμου, επομένως ως ξεχωριστός χώρος χρειάζεται να έχει τους δικούς του κανόνες, άλλους από αυτούς του φυσικού κόσμου.

Οι θεωρίες της αυτορρύθμισης, όσο ιδανικές και αν φαίνονται έχουν αρχίσει να εγκαταλείπονται πλήρως τα τελευταία χρόνια. Κατά την άποψή μου, αν η κοινωνία μας ήταν πιο <αθώα> και το έγκλημα δεν παραμόνευε παντού, θα ήταν πολύ ενδιαφέρον να τις δούμε στην πράξη. Επειδή όμως ζούμε σε μία κοινωνία όπου πρέπει να προστατεύουμε διαρκώς τις πληροφορίες που μας ανήκουν, τα προσωπικά μας στοιχεία και τα αποθηκευμένα δεδομένα μας από κακόβουλες επιθέσεις, πιο εφαρμόσιμη λύση θα ήταν η προσαρμογή των παραδοσιακών κανόνων στις απαιτήσεις των νέων τεχνολογιών και η δημιουργία κανόνων δικαίου προσαρμοσμένων στους κινδύνους του διαδικτύου.

Εκτός όμως από τις θεωρίες αυτορρύθμισης, αναπτύχθηκαν και θεωρίες περί εφαρμογής του ισχύοντος δικαίου. Μία από αυτές τια απόψεις υποστηρίζει ότι δεν υφίσταται κλάδος δικαίου που να ασχολείται με το Διαδίκτυο, δεν υπάρχει δηλαδή Δίκαιο του Διαδικτύου. Όπως, όταν με την εμφάνιση της ατμομηχανής κατά την Βιομηχανική Επανάσταση, δημιουργήθηκαν κοινωνικές αλλαγές, δεν δημιουργήθηκε όμως ειδικό δίκαιο της ατμομηχανής. Θεωρεί δηλαδή, ότι το δίκαιο διαθέτει την ευελιξία να προσαρμόζεται στα όποια προβλήματα δημιουργούνται από την εμφάνιση και ανάπτυξη του Διαδικτύου, όπως προσαρμόζεται σε

[40] John Perry Barlow, ‘’Declaration of Independence of the Internet’’

κάθε κοινωνική αλλαγή. Αντιμετωπίζει το διαδίκτυο ως ένα νέο τεχνολογικό μέσο, το οποίο δεν πρέπει να συγχέεται με κοινωνικές πρακτικές.

Ούτε αυτή η θεωρία είναι ικανοποιητική για το κοινό περί δικαίου αίσθημα, γιατί δεν υπολογίζει τις τεράστιες αλλαγές που έχει επιφέρει το διαδίκτυο στην κοινωνία, ούτε την ιδιαιτερότητα της εγκληματικής δράσης που αναπτύσσεται εντός του Κυβερνοχώρου.

Για την αντιμετώπιση του διαδικτυακού εγκλήματος, θα πρέπει να επέλθει προσαρμογή στην εθνική νομοθεσία των κρατών και εισαγωγή νέων διατάξεων προσαρμοσμένων στις ιδιαιτερότητές του. Αυτό όμως δεν είναι αρκετό, χρειάζεται και η θέσπιση διεθνών διατάξεων, υπερεθνικού επιπέδου, οι οποίες θα ακολουθούνται από περισσότερα κράτη, ώστε να υπάρχει συντονισμός μεταξύ τους σε περιπτώσεις που η εγκληματική συμπεριφορά υπερβαίνει τα όρια μίας εθνικής έννομης τάξης. Η ελληνική ποινική νομοθεσία προσπαθεί να προσαρμοστεί στα νέα αυτά δεδομένα, αλλά δεν έχει κάνει μεγάλη πρόοδο, παρόλο που προσπαθεί να εναρμονιστεί και με τους διεθνείς κανόνες.

2.4 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΗΣ ΗΛΕΚΤΡΟΝΙΚΗΣ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑΣ

Η εγκληματικότητα μέσω ηλεκτρονικών υπολογιστών, όπως έχει ήδη αναφερθεί, κάνει την εμφάνισή της ως ένα νέο ποινικό φαινόμενο στα μέσα της δεκαετίας του ’70. Γρήγορα συνειδητοποιείται από τους νομικούς κύκλους ότι οι υπάρχοντες νομικοί κανόνες δεν είναι δυνατό να καλύψουν εννοιολογικά τις νέες αυτές μορφές εγκληματικής συμπεριφοράς, διότι παρουσιάζουν τόσο ιδιαίτερα χαρακτηριστικά που δεν μπορούν να αντιμετωπιστούν με τους ήδη θεσπισμένους κανόνες δικαίου. Έτσι, εύλογα οι εθνικές, έννομες τάξεις προέβησαν σε τροποποίηση των ποινικών τους διατάξεων προκειμένου να προσαρμοστούν στα νέα δεδομένα.[41]

Με την εμφάνιση όμως του φαινομένου της συνεχούς δικτύωσης των ηλεκτρονικών υπολογιστών τα νομικά ζητήματα έγιναν ακόμη πιο πολύπλοκα και η ανάγκη νομικής αντιμετώπισης των συνεχώς νεοεμφανιζόμενων εγκληματικών συμπεριφορών πιο επιτακτική. Ο εντοπισμός, επομένως, των χαρακτηριστικών της <νέας γενιάς> εγκληματικότητας φωτίζει τη λογική της θέσπισης των νέων κανόνων ποινικού δικαίου αναδεικνύοντας ταυτόχρονα την επικινδυνότητα και τις προεκτάσεις του νέου αυτού ποινικού φαινομένου.

Πρωταρχικό χαρακτηριστικό της εγκληματικότητας στο διαδίκτυο που αναδεικνύει τη διαφορετικότητά της σε σχέση με άλλες μορφές εγκληματικότητας είναι η έλλειψη φυσικής επαφής του δράστη με το αντικείμενο του εγκλήματος και η έλλειψη βίας, χωρίς αυτό να σημαίνει ότι οι συνέπειές της δε σχετίζονται σε ορισμένες περιπτώσεις με βίαιες συμπεριφορές. Ο δράστης του διαδικτύου δεν εισβάλει στην κατοικία του θύματος, προκειμένου να αποσπάσει από τον ηλεκτρονικό υπολογιστή του τελευταίου αποθηκευμένα αρχεία, αλλά αποκτά πρόσβαση στο ηλεκτρονικό σύστημα του θύματος <σπάζοντας> τους κωδικούς πρόσβασης. Αντίστοιχα δεν προκαλεί ζημιά σε δεδομένα ή στη λειτουργία του

[41] Στην Γερμανία εισήχθησαν οι αντικειμενικές υποστάσεις της απάτης με τη χρήση ηλεκτρονικού υπολογιστή, της πλαστογραφίας σοβαρών αποδεικτικών δεδομένων της κατασκοπείας με ηλεκτρονικούς υπολογιστές και έπειτα στην Ελλάδα με το νόμο 1805/1988 εισήχθησαν οι αντικειμενικές υποστάσεις της απάτης με υπολογιστή, της παραβίασης απορρήτων με ηλεκτρονικό υπολογιστή, της χωρίς δικαίωμα αντιγραφής ή χρησιμοποίησης προγραμμάτων και της χωρίς δικαίωμα πρόσβασης σε δεδομένα, ενώ διερευνήθηκε η έννοια του εγγράφου.

υπολογιστή του θύματος με φυσικό τρόπο – παραδείγματος χάρη αφαιρώντας τον σκληρό δίσκο – απλά στέλνει έναν ιό που το ίδιο το θύμα ανυποψίαστο ενεργοποιεί.[42]

Ενώ η έλλειψη βίας παραπέμπει σε μορφές ήπιας εγκληματικής συμπεριφοράς, στην περίπτωση του διαδικτυακού εγκλήματος κάθε άλλο περί αυτού πρόκειται. Η ιδιαίτερη επικινδυνότητα αυτής της μορφής εγκληματικότητας έγκειται στο γεγονός ότι τα θύματα δεν μπορούν να αμυνθούν στην ολοφάνερη προσβολή των εννόμων αγαθών τους, αφού συχνά ούτε την αντιλαμβάνονται και όταν τα αποτελέσματα είναι αντιληπτά, ο εντοπισμός των δραστών συνήθως είναι εξαιρετικά δυσχερής. Επομένως, ο τρόπος τέλεσης των εγκλημάτων αυτών επιφέρει την ατιμωρησία των δραστών.

Το βασικότερο και μείζονος σημασίας χαρακτηριστικό της εγκληματικής συμπεριφοράς στο διαδίκτυο είναι η διεθνής φύση της, γεγονός που την καθιστά σπουδαίο κίνδυνο πέρα από τα όρια ενός κράτους για τη διεθνή κοινότητα. Η διευρυνόμενη διασύνδεση των ηλεκτρονικών υπολογιστών καταλύει τα εθνικά σύνορα και οι δράστες διαπράττουν τα εγκλήματά τους χωρίς αυτά να συνδέονται με ένα συγκεκριμένο τόπο. Το ότι το διαδικτυακό έγκλημα ανήκει στην κατηγορία των διεθνών εγκλημάτων αποδεικνύεται και από το γεγονός ότι τα αποτελέσματα μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους, ενώ λόγω της εκτεταμένης διαδικτύωσης καθίσταται εξαιρετικά δύσκολος ο προσδιορισμός του πραγματικού τόπου τέλεσής του, πόσο μάλλον του ιδίου του δράστη.

Από άποψη θυματολογικών χαρακτηριστικών και σε αντιδιαστολή με την εγκληματικότητα μέσω ηλεκτρονικών υπολογιστών ο δράστης του διαδικτυακού εγκλήματος συνήθως δε στοχεύει σε συγκεκριμένο θύμα[43], δεν έχει δηλαδή προεπιλέξει το θύμα του. Αποτέλεσμα αυτού είναι και ο μεγάλος <σκοτεινός αριθμός> της εγκληματικότητας στο χώρο του διαδικτύου, αφού ελάχιστες περιπτώσεις καταγγέλλονται.[44] Η διερεύνηση και η διαλεύκανση διαδικτυακών εγκλημάτων καθίστανται ακόμη πιο δύσκολες και από το γεγονός των πολλαπλών τόπων τέλεσής τους και από το γεγονός ότι η εξωτερίκευση της εγκληματικής συμπεριφοράς μπορεί να εντοπίζεται σε χώρα διαφορετική από εκείνη όπου βρίσκονται τα αποδεικτικά στοιχεία.

Ταυτόχρονα λόγω του μικρού αριθμού ποινικών αποφάσεων σε συνδυασμό με τον αυξημένο <σκοτεινό αριθμό> της διαδικτυακής εγκληματικότητας είναι δύσκολο να εξαχθούν ασφαλή συμπεράσματα για τον τύπο του δράστη που παρανομεί στο διαδίκτυο. Πάντως λόγω της ευρείας διάδοσης της χρήσης του διαδικτύου και της αντίστοιχης διάδοσης της τεχνογνωσίας η εγκληματικότητα που εκδηλώνεται στο διαδίκτυο πλέον δεν είναι εγκληματικότητα ειδικών, δηλαδή μιας μεμονωμένης κατηγορίας ατόμων με κάποιο ιδιαίτερο διανοητικό υπόβαθρο και με ειδικές τεχνικές γνώσεις. Δεδομένου της εύκολης και ελεύθερης πρόσβασης στο διαδίκτυο- αρκεί μία τηλεφωνική σύνδεση, ένας ηλεκτρονικός υπολογιστής μεσαίων δυνατοτήτων και σύνδεση στο διαδίκτυο- δράστης μπορεί να είναι οποιοσδήποτε.

Αυτό μπορεί να επιβεβαιωθεί ενδεικτικά στο αδίκημα της δυσφήμησης, η τέλεση του οποίου επιτυγχάνεται μάλλον πιο εύκολα σε διαδικτυακό περιβάλλον, διότι χωρίς την ύπαρξη ιδιαίτερων γνώσεων ηλεκτρονικής και χωρίς τη λήψη ιδιαίτερου ρίσκου δύναται κάποιος να

---

[42] Κιούπης Δ., <Αλλοίωση Ηλεκτρονικών Δεδομένων και Αθέμιτη Πρόσβαση σε Ηλεκτρονικά Δεδομένα- Κενά και Αδυναμίες της Ποινικής Νομοθεσίας>, σελ. 961

[43] Βασιλάκη Ε., <Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής καταστολής >, σελ. 28-29

[44] Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 677

δυσφημεί άλλον τη στιγμή που τα σχετικά συστήματα ασφαλείας αδυνατούν να εξαλείψουν ή έστω να περιορίσουν δραστικά τέτοιου είδους εκδηλώσεις.[45]

Σε γενικές γραμμές όσοι παραβατούν στο χώρο του διαδικτύου μπορούν να διακριθούν σε δύο κατηγορίες:[46]

- Σε όσους παρουσιάζουν παραβατική συμπεριφορά ορμώμενοι από την ανάγκη να ικανοποιήσουν την περιέργειά τους ή απλά να αποκομίσουν ευχαρίστηση χωρίς να επιδιώκουν κάποιο περιουσιακό όφελος και σε αυτή την κατηγορία ανήκουν κυρίως άτομα νεαρής ηλικίας και
- Σε όσους παραβατούν με σκοπό το περιουσιακό όφελος.

2.5 ΔΙΑΚΡΙΣΕΙΣ ΗΛΕΚΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Κάθε έγκλημα για το οποίο μέσο τέλεσης είναι ένας ηλεκτρονικός υπολογιστής δεν είναι και ηλεκτρονικό διαδικτυακό έγκλημα. Το ηλεκτρονικό διαδικτυακό έγκλημα έχει την ιδιαιτερότητα ότι η αξιόποινη πράξη πράττεται μέσω ενός ηλεκτρονικού υπολογιστή συνδεδεμένου στο διαδίκτυο. Χρειάζεται δηλαδή η σύνδεση στο διαδίκτυο ώστε ο δράστης μέσω του ηλεκτρονικού υπολογιστή να προσεγγίσει έναν άλλον ηλεκτρονικό υπολογιστή και να του επιφέρει το παράνομο αποτέλεσμα της εγκληματικής του πράξης. Έτσι, έγκλημα μεταξύ ηλεκτρονικών υπολογιστών οι οποίοι είναι μεταξύ τους συνδεδεμένοι σε δίκτυο, μέσω καλωδίων δικτύου, όπου για την σύνδεση δεν χρειάζεται η σύνδεση στο διαδίκτυο, δεν είναι διαδικτυακό έγκλημα, αλλά πληροφορικό ή ηλεκτρονικό. Λόγω, δε, της τάχιστης ανάπτυξης της τεχνολογίας, προκύπτουν συνεχώς νέες μορφές διαδικτυακών εγκλημάτων. Τα ηλεκτρονικά εγκλήματα ανάλογα με τον τρόπο και το περιβάλλον τέλεσής τους διακρίνονται σε διάφορες κατηγορίες μερικές από τις οποίες είναι:

2.5.1 Εγκλήματα τελούμενα τόσο σε κοινό όσο και σε ηλεκτρονικό περιβάλλον.

Είναι σαφές ότι το διαδίκτυο δεν προσφέρεται μόνο για την τέλεση εγκλημάτων που προϋποθέτουν αποκλειστικά την χρήση ηλεκτρονικού υπολογιστή, αλλά προσφέρεται και για την τέλεση των κλασικών εγκλημάτων. Μάλιστα θα μπορούσε κάποιος να πει ότι η εξέλιξη της ηλεκτρονικής τεχνολογίας και η εφαρμογή της στη σημερινή καθημερινότητα διευκόλυνε τη σύγχρονη εγκληματικότητα, διότι οι δράστες προσαρμόζονται στη νέα τεχνολογία και εξελίσσουν τους τρόπους τέλεσης των εγκλημάτων, προσλαμβάνοντας με αυτόν τον τρόπο η πραγματικότητα νέες διαστάσεις.

Έτσι, όταν ένα <κοινό> έγκλημα τελείται σε ηλεκτρονικό περιβάλλον, δεν έχουμε ένα πρόσθετο στοιχείο στην αντικειμενική υπόσταση του αδικήματος, αλλά έναν εναλλακτικό τρόπο τέλεσης του αδικήματος. Στη συγκεκριμένη περίπτωση η χρήση ηλεκτρονικού υπολογιστή και η σύνδεση με το διαδίκτυο είναι, δηλαδή, το μέσο τέλεσης της εγκληματικής

[45] Βλ. Αργυρόπουλος Α., <Ηλεκτρονική Εγκληματικότητα>, σελ., 24-25, ενώ αντίθετα υποστηρίζει ο Ι. Αγγελής, βλ. του ιδίου, <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 677

[46] Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο- Έγκλημα στον κυβερνοχώρο (Cybercrime- Internet Crime)>, σελ. 677-678

συμπεριφοράς. Οι δράστες διαπράττουν <κοινά> αδικήματα με τη διαφορά ότι ενεργούν στο ιδιόμορφο περιβάλλον του διαδικτύου.

Κλασικά παραδείγματα εγκληματικής συμπεριφοράς που εκδηλώνεται τόσο σε κοινό περιβάλλον όσο και σε ηλεκτρονικό είναι τα αδικήματα της απειλής, της εκβίασης, της εξύβρισης, της απλής ή συκοφαντικής δυσφήμισης με τη χρήση ηλεκτρονικού ταχυδρομείου, της πλαστογραφίας, της απάτης, της παραβίασης της πνευματικής ιδιοκτησίας με την αντιγραφή πνευματικού έργου (παραδείγματος χάρη ενός προγράμματος ηλεκτρονικού υπολογιστή).

Στις περιπτώσεις των εγκλημάτων αυτών η ήδη θεσπισμένη νομοθεσία κατ' αρχήν φαίνεται να είναι ικανοποιητική ως προς τη διατύπωση της ειδικής υπόστασης τους, αφού περιγράφονται σε αυτές επαρκώς τα αντικειμενικά και τα υποκειμενικά στοιχεία των ως άνω εγκλημάτων. Επιφυλάξεις όμως διατυπώνονται ως προς την πληρότητα της περιγραφής της ειδικής υπόστασης των μορφών αυτών εγκληματικής συμπεριφοράς και ως προς τον κολασμό των δραστών όπως αυτή προβλέπεται από την ήδη υφιστάμενη νομοθεσία.

Για αυτό και θα ήταν σκόπιμη η αναγωγή των κοινών εγκλημάτων που τελούνται στο διαδίκτυο σε ξεχωριστή μορφή εγκληματικότητας. Και αυτό λόγω των σημαντικών διαφορών που παρουσιάζει το ηλεκτρονικό περιβάλλον σε σχέση με το <κοινό>, οι οποίες συνίστανται τόσο στην ευρύτητά του (απευθύνεται σε απεριόριστο αριθμό ανθρώπων) όσο και στη διεθνή φύση του (πολλαπλοί τόποι τέλεσης), αλλά κυρίως στον τρόπο λειτουργίας των ηλεκτρονικών υπολογιστών και του διαδικτύου (αυτοματοποιημένες λειτουργίες, μεγάλη ταχύτητα διάδοσης δεδομένων, όχι συγκεκριμένοι και προκαθορισμένοι αποδέκτες).

Ειδικότερα, διαφορετικές είναι οι συνέπειες παραδείγματος χάρη που επέρχονται από τη δημοσίευση ενός συκοφαντικού άρθρου σε μια εφημερίδα που απευθύνεται σε περιορισμένο αριθμό αναγνωστών, οι οποίοι μάλιστα καλούνται να αγοράσουν την συγκεκριμένη έκδοση και διαφορετικές από τη δημοσίευση του ίδιου άρθρου σε ένα διαδικτυακό τόπο, τον οποίο δύνανται να επισκεφτεί απεριόριστος αριθμός χρηστών χωρίς κανένα κόστος.

Επομένως, σωστά ο νομοθέτης σε ορισμένες περιπτώσεις επιλέγει τη θέσπιση ειδικών κανόνων δικαίου που διασφαλίζουν τόσο την πρόληψη όσο και την καταστολή της παράνομης εκμετάλλευσης της τεχνολογίας της πληροφόρησης, αφού αυτή η μορφή παραβατικότητας παρουσιάζει τόσο ιδιαίτερα χαρακτηριστικά που καθιστούν μια ιδιαίτερη εγκληματική συμπεριφορά. Προς την κατεύθυνση αυτή κινήθηκε ο Έλληνας νομοθέτης με τη στοιχειοθέτηση του αδικήματος της απάτης με υπολογιστή(άρθρο 386^{A} ΠΚ).

2.5.2. Εγκλήματα τελούμενα μόνο σε ηλεκτρονικό περιβάλλον.

Στην κατηγορία αυτή εντάσσονται τα εγκλήματα τα οποία τελούνται αποκλειστικά σε ηλεκτρονικό περιβάλλον με την ευρεία έννοια. Απαιτείται δηλαδή η χρήση ηλεκτρονικού υπολογιστή προκειμένου να πληρωθεί η αντικειμενική υπόσταση του εγκλήματος. Η σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο δεν αποτελεί προαπαιτούμενο για την τέλεσή τους, σε αντιδιαστολή με την περίπτωση των διαδικτυακών εγκλημάτων, τέλεση των οποίων νοείται μόνο στο ηλεκτρονικό περιβάλλον του διαδικτύου.

Χαρακτηριστική διαφορά αυτής της κατηγορίας εγκλημάτων με την κατηγορία εκείνων που τελούνται τόσο σε <κοινό> όσο και σε ηλεκτρονικό περιβάλλον είναι ότι στα πρώτα

απαραίτητο στοιχείο της αντικειμενικής υπόστασής τους αποτελεί η χρήση ηλεκτρονικού υπολογιστή, χωρίς την οποία δεν υφίσταται τέλεσή τους, ενώ στα δεύτερα η χρήση ηλεκτρονικού υπολογιστή με ή χωρίς σύνδεση με το διαδίκτυο είναι ένα μέσο τέλεσης των εγκλημάτων αυτών.[47]

Ενδεικτικά σε αυτή την κατηγορία υπάγονται τα αδικήματα που προβλέπονται στα άρθρα 370Β ΠΚ και 370Γ του ελληνικού Ποινικού Δικαίου και σύμφωνα με τα οποία αξιόποινη είναι η αθέμιτη πρόσβαση σε δεδομένα ηλεκτρονικών υπολογιστών.[48] Επίσης, εγκλήματα που τελούνται σε ηλεκτρονικό περιβάλλον είναι το έγκλημα της αλλοίωσης ηλεκτρονικών δεδομένων (δηλαδή της διαγραφής, απόκρυψης, αχρήστευσης ή μεταβολής ηλεκτρονικών δεδομένων) του άρθρου 303a του Γερμανικού Ποινικού Κώδικα.[49]

Πέρα από τις εθνικές νομοθεσίες στη Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber- crime) προβλέπεται επίσης στο άρθρο 4 του δευτέρου κεφαλαίου η αθέμιτη τροποποίηση δεδομένων.

2.5.3. <Γνήσια> διαδικτυακά εγκλήματα (ή <εγκλήματα κυβερνοχώρου>).[50]

Αναφέραμε νωρίτερα πως τα διαδικτυακά εγκλήματα αποτελούν έννοια είδους σε σχέση με τα ηλεκτρονικά εγκλήματα, τα οποία είναι ευρύτερη έννοια και περιλαμβάνουν εννοιολογικά τα πρώτα. Όταν, λοιπόν, γίνεται λόγος για τα διαδικτυακά εγκλήματα νοούνται εκείνα που τελούνται σε διαδικτυακό περιβάλλον αποκλειστικά.

Απαιτείται, λοιπόν, για την πλήρωση της αντικειμενικής υπόστασής τους η σύνδεση του ηλεκτρονικού υπολογιστή με το διαδίκτυο. Δεν αρκεί για την διάπραξή τους μόνο η χρήση ηλεκτρονικού υπολογιστή. Σε περίπτωση δηλαδή που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και αν διαπραχθεί, θεωρείται έγκλημα τελούμενο σε ηλεκτρονικό περιβάλλον.

Τέτοιας κατηγορίας αδικήματα αποτελούν ενδεικτικά η μεταβίβαση αποκρυπτογραφημένων κειμένων χωρίς σχετική άδεια, η μη εξουσιοδοτημένη πρόσβαση σε συστήματα πληροφοριών και η μόλυνση συστήματος πληροφοριών με ιούς. Ως γνήσια διαδικτυακά εγκλήματα μπορούν να θεωρηθούν ακόμη και αυτά που θεσπίζονται από τη Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber- crime) στα άρθρα 2 έως 10.

---

[47] Κατά τη γνώμη του Ι. Αγγελή ως εγκλήματα που διαπράττονται σε περιβάλλον ηλεκτρονικών υπολογιστών νοούνται μόνο αυτά που τελούνται χωρίς τη χρήση του διαδικτύου. Βλ., Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο- Έγκλημα στον κυβερνοχώρο (Cybercrime- Internet Crime)>, σελ. 676- 677

[48] Η διάταξη του άρθρου 370Γ ΠΚ αποτελεί τη βασική διάταξη, αφού στο άρθρο 370Β ΠΚ απαιτούνται ιδιαίτερα χαρακτηριστικά των δεδομένων (κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, καθώς και όσα ο νομικός κάτοχός τους από δικαιολογημένο ενδιαφέρον διαχειρίζεται ως απόρρητα)

[49] Κιούπη Δ., <Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας>, σελ. 963- 964.

[50] Η πλειοψηφία των συγγραφέων χρησιμοποιούν τον όρο <εγκλήματα κυβερνοχώρου> σε πιστή μετάφραση του αντίστοιχου αγγλικού όρου <cyber crimes>. Ωστόσο, πιο δόκιμος φαίνεται ο όρος <διαδικτυακά εγκλήματα>, διότι στην έννοια αυτή περιλαμβάνονται όλες οι εγκληματικές δραστηριότητες που εκδηλώνονται σε σχέση με το διαδίκτυο και όλες τις υπηρεσίες που αυτό προσφέρει (ηλεκτρονικό ταχυδρομείο, περιήγηση στον κυβερνοχώρο, δίαυλοι συνομιλιών και τα λοιπά).

Καταληκτικά, αξίζει να αναφερθεί η νέα τάση στην ποινική επιστήμη που έχει ως στόχο να αποφεύγει την αυστηρή διάκριση μεταξύ των εγκλημάτων τελούμενων σε ηλεκτρονικό περιβάλλον και αυτών που τελούνται στο διαδίκτυο και να ενοποιεί αυτές τις κατηγορίες σε μία ενιαία των <εγκλημάτων πληροφορικής>.[51]

Εξάλλου η θέσπιση διατάξεων με όσο το δυνατόν ουδέτερους τεχνολογικούς όρους ενδείκνυται στα εγκλήματα αυτά προκειμένου το γλωσσικό κριτήριο να περιλαμβάνει στο εννοιολογικό περιεχόμενο των όρων αυτών κάθε νέα τεχνολογική εξέλιξη και να παραμένουν τα νομοθετικά μέτρα επίκαιρα.

ΚΕΦΑΛΑΙΟ 3

ΟΙ ΚΥΡΙΟΤΕΡΕΣ ΜΟΡΦΕΣ ΤΟΥ ΗΛΕΚΡΟΝΙΚΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

3.1 ΤΟ HACKING ΚΑΙ ΤΟ CRACKING.

Το hacking είναι η επιδίωξη πρόσβασης σε ξένο ηλεκτρονικό υπολογιστή ή σύστημα ηλεκτρονικών υπολογιστών, χωρίς καταρχήν να υπάρχει σκοπός περαιτέρω επιβλαβούς ενέργειας. Ακόμα και χωρίς όμως αυτό τον περαιτέρω σκοπό, η εισβολή στο ξένο δίκτυο από μόνη της έχει κακόβουλο χαρακτήρα, αφού όποιος εισέλθει σε ηλεκτρονικό υπολογιστή άλλου, μπορεί να διαβάσει τα αρχεία του, να παρέμβει σε μια σειρά προγραμματιστικών δραστηριοτήτων να τα τροποποιήσει ή να διαθέσει τις πληροφορίες σε τρίτους. Το έγκλημα του hacking υπάγεται στη γενικότερη κατηγορία των εγκλημάτων διαδικτυακού βανδαλισμού.[52]

Η εισβολή στον ξένο ηλεκτρονικό υπολογιστή από τον hacker αποσκοπεί στην απομακρυσμένη διαχείριση του ηλεκτρονικού υπολογιστή- στόχου. Έτσι, ο hacker έχει τη δυνατότητα, χωρίς τη φυσική του παρουσία στο μέρος που βρίσκεται ο ξένος ηλεκτρονικός υπολογιστής, να διαχειρίζεται αυτόν, να τελεί εργασίες, να ανεβάζει (upload) ιστοσελίδες, να ανοιγοκλείνει την οθόνη, να τυπώνει στον εκτυπωτή και γενικά να χειρίζεται τον ξένο ηλεκτρονικό υπολογιστή σαν να ήταν αυτός εκεί. Ο hacker μπορεί να επιλέξει την πλήρη

---

[51] Οι αναφορές στα σύγχρονα νομοθετικά κείμενα κάνουν πλέον λόγο για αξιόποινες πράξεις κατά πληροφορικών συστημάτων, τα οποία περιλαμβάνουν τόσο προγράμματα υπολογιστών όσο και δίκτυα επικοινωνιών μεταξύ συνδεδεμένων ηλεκτρονικών υπολογιστών. Βλ. τη Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber- crime) και βλ. την Πρόταση Απόφασης Πλαισίου του Συμβουλίου, για επιθέσεις κατά των συστημάτων πληροφοριών (27/8/2002), Επίκαιρα Νομοθετήματα, Ποινικό Δίκαιο 2/2003, σελ. 115 και εξής.

[52] Βλ. Ζάννη Α., <Το διαδικτυακό έγκλημα>, σελ. 85. Κατά άλλη άποψη συνιστά οικονομικό έγκλημα, βλ. Κιούπης Δ., <Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ε.Ε.>, σε Τιμητικό Τόμο Αργυρίου Καρρά, σελ. 1017, άποψη η οποία κατά τη γνώμη μου δεν μπορεί να γίνει εύκολα δεκτή, διότι στόχος του hacker είναι να αποδείξει ότι μπορεί να παρεισφρύσει και στην πιο ασφαλή ιστοσελίδα και να τη διαμορφώσει όπως αυτός θέλει και όχι να αποκομίσει κάποιο οικονομικό όφελος ή να ζημιώσει οικονομικά την ιστοσελίδα στην οποία παρεισφρύει.

διείσδυση στον ηλεκτρονικό υπολογιστή με δικαιώματα διαχειριστή συστήματος ή και τη διείσδυση με δικαιώματα απλού χρήστη συστήματος.

Στο ζήτημα του hacking έχουν διαμορφωθεί δύο βασικές απόψεις. Η πρώτη υποστηρίζει το απόλυτο και απεριόριστο της πρόσβασης στους ηλεκτρονικούς υπολογιστές και θεωρεί ότι όποιος δεν επιθυμεί ο ηλεκτρονικός υπολογιστής να μην είναι προσβάσιμος από άλλους οφείλει να παίρνει τα κατάλληλα μέτρα για αυτό. Η δεύτερη υποστηρίζει ότι η χωρίς συναίνεση πρόσβαση στους ηλεκτρονικούς υπολογιστές είναι ανήθικη και εγκληματική, ενώ υπάρχει και ακόμα μία άποψη, με λίγους όμως υποστηρικτές η οποία υποστηρίζει ότι η απλή χωρίς συναίνεση πρόσβαση σε ηλεκτρονικό υπολογιστή μπορεί και να μην είναι ανήθικη. Εγκληματική είναι μόνο εάν ο hacker παρέμβει στα αρχεία του ηλεκτρονικού υπολογιστή με σκοπό την κλοπή, καταστροφή, αλλαγή και τα λοιπά.

Για να ολοκληρωθεί μία επίθεση από hackers διέρχεται από τέσσερα στάδια[53]: Αρχικά συγκεντρώνονται όλες οι απαραίτητες πληροφορίες για τον ηλεκτρονικό υπολογιστή – στόχο[54], μετά αποκτάται πρόσβαση στο σύστημα[55], κατόπιν ξεκινά η εκμετάλλευση του συστήματος[56] και τέλος εξαφανίζονται τα ίχνη της πρόσβασης στο σύστημα, αφού σκοπός του hacker δεν είναι η ολοκληρωτική καταστροφή του συστήματος.

Στην Ελλάδα το θέμα του hacking αντιμετωπίζεται πλέον μέσω της διάταξης του άρθρου 370Γ παράγραφος 2 του Ποινικού Κώδικα για την χωρίς δικαίωμα πρόσβαση σε στοιχεία που έχουν εισαχθεί σε ηλεκτρονικό υπολογιστή, αφού στην παράγραφο αυτή τιμωρείται η χωρίς δικαίωμα πρόσβαση σε συστήματα επεξεργασίας δεδομένων, ακόμα και όταν αυτή γίνεται χωρίς πρόθεση βλάβης, αλλά με μόνη πρόθεση την άσκοπη γνώση των αποθηκευμένων σε αυτά πληροφοριών, που όπως είδαμε πολλές φορές είναι ο βασικός σκοπός του hacker.

Στην περίπτωση που το hacking αφορά σε αρχεία τα οποία αποτελούν κρατικό, επιστημονικό, επαγγελματικό απόρρητο, ή απόρρητο δημόσιας ή ιδιωτικής επιχείρησης εφαρμογή έχει το άρθρο 370Β παράγραφος 1 του Ποινικού Κώδικα.

---

[53] Βλ. Φαραντούρης Ν., <Σύγχρονες εγκληματολογικές δράσεις στο Διαδίκτυο- Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του hacking και του φαινομένου της μόλυνσης με ιούς.>, σελ. 191- 196.

[54] Αυτό το πετυχαίνουν μέσω της τεχνικής της σάρωσης θυρών (port scanning), που είναι μια διαδικασία αποστολής ερωτημάτων σε διακομιστές με σκοπό να συλλέξουν πληροφορίες για τις υπηρεσίες που προσφέρουν αλλά και για το χρησιμοποιούμενο επίπεδο ασφάλειας. Επίσης η ανίχνευση αποσκοπεί στην εύρεση λογαριασμών χρηστών χωρίς κανένα επίπεδο ασφαλείας, το οποίο προσφέρει εύκολη πρόσβαση στο σύστημα. Για περισσότερα βλ. Βλαχόπουλος Κ. <Ηλεκτρονικό έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση>, σελ. 41.

[55] Ο πιο συνηθισμένος τρόπος για να αποκτήσει ένας hacker πρόσβαση σε ξένο ηλεκτρονικό υπολογιστή είναι το IP spoofing (πλαστές διευθύνσεις IP δηλαδή) όπου δεν του είναι απαραίτητο password για να <μπει> στον ξένο ηλεκτρονικό υπολογιστή. Αυτό επιτυγχάνεται με τη χρήση του IP(Internet Protocol). Με τη διεύθυνση IP προσδιορίζονται όλοι οι ηλεκτρονικοί υπολογιστές οι οποίοι εισέρχονται στο διαδίκτυο και αυτή είναι αντίστοιχη με τη χώρα, την πόλη, την οδό και τον αριθμό που έχουν οι διευθύνσεις των σπιτιών. Αυτό που ουσιαστικά γίνεται με το IP spoofing είναι ότι ο hacker επιτυγχάνει να χρησιμοποιεί μια διεύθυνση IP την οποία ο χρήστης γνωρίζει και εμπιστεύεται και έτσι αποκτά πρόσβαση σε υπηρεσίες που προορίζονται για έμπιστους χρήστες του διαδικτύου. Άλλοι τρόποι απόκτησης πρόσβασης είναι η εκμετάλλευση των cookies, τα οποία είναι πολύ μικρά αρχεία κειμένου τα οποία τοποθετούνται στον ηλεκτρονικό υπολογιστή από τις ιστοσελίδες τις οποίες επισκέπτεται ο χρήστης. Καθώς τα αρχεία αυτά περιέχουν πληροφορίες για τα στοιχεία του χρήστη και τους κωδικούς για τις δραστηριότητές του, όταν τα αποκτά ο hacker αποκτά πρόσβαση σε αυτές τις δραστηριότητες. Βλ. Ζάννη Α. <Το διαδικτυακό έγκλημα>, σελ. 89 και Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση>, σελ. 40.

[56] Η εκμετάλλευση του συστήματος έχει δύο μορφές. Ο δράστης μπορεί να αφαιρέσει ή να καταστρέψει δεδομένα από τον ξένο ηλεκτρονικό υπολογιστή ή να μην περιοριστεί μόνο σε αυτό αλλά να τον χρησιμοποιήσει για εκτενέστερη δράση στο διαδίκτυο.

Η πιο πρόσφατη επίθεση hacker που είδε το φως της δημοσιότητας στην Ελλάδα είναι αυτή των Τούρκων hacker, οι οποίοι σε πρόσφατη συνέντευξή τους απειλούν με νέα επίθεση στο Υπουργείο Εξωτερικών.[57] Μάλιστα σε μία επίδειξη ισχύος δημοσιοποίησαν ένα βίντεο που αποδεικνύει ότι όχι μόνο έχουν πρόσβαση στην ιστοσελίδα αλλά είναι σε θέση να διαρρεύσουν ευαίσθητα κρατικά δεδομένα. Πηγές από το Υπουργείο Εξωτερικών που παρακολουθούν το ζήτημα δήλωσαν μεταξύ άλλων: <Ανάλογα περιστατικά αντιμετωπίζονται άμεσα από τις αρμόδιες υπηρεσίες. Η σελίδα του Υπουργείου ουδέποτε έπαψε να λειτουργεί>. Από την πλευρά τους οι Έλληνες hacker δηλώνουν έτοιμοι να επέμβουν ανά πάσα στιγμή. <Εκτιμούμε ότι οι Τούρκοι θα επιχειρήσουν μεγαλύτερες επιθέσεις εν όψει των τουρκικών εκλογών. Είμαστε έτοιμοι να τις αντιμετωπίσουμε>. Μερικές από τις πιο πρόσφατες επιθέσεις των Τούρκων hacker εντοπίζονται:

- Στη σελίδα της ελληνικής ομοσπονδίας χάντμπολ
- Στην ιστοσελίδα της εταιρείας SUZUKI
- Στην εφημερίδα <Ρεθυμνιώτικα Νέα>.

Οι crackers, από την άλλη μεριά, είναι εκείνα τα άτομα τα οποία χαρακτηρίζονται ως κακόβουλοι hackers αφού η παράνομη εισβολή τους στα υπολογιστικά συστήματα γίνεται με στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, τη δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την άρση της προστασίας των προγραμμάτων καθιστώντας δυνατή την παράνομη αντιγραφή τους, τις ενέργειες εκείνες που θα τους αποκομίσουν οικονομικά οφέλη, παραδείγματος χάρη μεταφορά σε προσωπικό λογαριασμό τραπέζης μεγάλων χρηματικών ποσών από υποκλοπή αριθμού πιστωτικής κάρτας.

Η ουσία του προβλήματος του cracking δεν εντοπίζεται σε επιθέσεις που γίνονται στο δικτυακό τρόπο μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, κάτι ου είναι πολύ εύκολο να γίνει αντιληπτό, αλλά στις ύπουλες επιθέσεις οι οποίες αφορούν τροποποίηση σημαντικών δεδομένων (χωρίς να γίνεται αντιληπτή) που τηρούνται από δημόσιες υπηρεσίες, όπως για παράδειγμα η αλλαγή της σειράς επιτυχίας σε ένα διαγωνισμό, η πιστή αντιγραφή ολόκληρων δικτυακών τόπων μεγάλων εταιρειών που κάνουν πωλήσεις μέσω διαδικτύου ή και μεγάλων οργανισμών ή δημόσιων υπηρεσιών και η εξαπάτηση ανυποψίαστων χρηστών των δικτυακών τόπων.

3.1.1 Οι Κατηγορίες Των Hackers.[58]

Η κοινότητα των hackers χωρίζεται σε αρκετές ξεχωριστές ομάδες, όπου η καθεμία έχει τα δικά της χαρακτηριστικά. Μια κατηγορία είναι αυτοί που αντιμετωπίζουν την πειρατεία ως τρόπο σκέψης και όχι απλά ως μια παράνομη είσοδο σε έναν υπολογιστή. Μια άλλη θεωρία αντιμετωπίζει το hacking ως την απασχόληση επί ώρες ολόκληρες για να μπορέσει κάποιος να δημιουργήσει ένα πρόγραμμα που θα κάνει κάποια λειτουργία, χρήσιμη ή όχι.

Στην κατηγορία των *ηθικών* ***hackers (ethical hackers)*** ανήκουν όσοι ανακαλύπτουν μεν ορισμένες σημαντικές αδυναμίες κάποιων συστημάτων υπολογιστών και ενημερώνουν σχετικά τον διαχειριστή του εν λόγω συστήματος, χωρίς όμως να υπάρχει εκ μέρους τους κάποια πρόθεση εκμετάλλευσης αυτής της αδυναμίας. Είναι οι <Ρομπέν των Δασών> των υπολογιστών. Πολλοί από αυτούς που ανήκουν στην κατηγορία των ηθικών hackers

[57] www.secnews.gr/tourkia-epitheseis-ellinon-hacker
[58] http://dide.flo.sch.gr/Plinet/ Tutorials/Tutorials-Hackers-Crackers.html

δημιούργησαν δικές τους εταιρείες συμβουλών ασφαλείας για να προσφέρουν τις γνώσεις, τις εμπειρίες και τις υπηρεσίες τους σε κάθε ενδιαφερόμενο. Υπάρχουν και οι hackers που δρουν με κοινωνικά κριτήρια και θέλουν να αλλάξουν τον κόσμο προς το καλύτερο, παρεμβαίνοντας με τις πράξεις τους συμβολικά ή και ουσιαστικά. Υπάρχουν και οι hackers που θέλουν να αποδείξουν τις τεχνικές δυνατότητες που διαθέτουν τα συστήματα ασφαλείας, βελτιώνοντάς τα και αποκαλύπτοντας πόσο ευαίσθητα είναι.

Μια άλλη κατηγορία hackers είναι οι ***hacktivists***, οι οποίοι έχουν ως στόχο να βοηθήσουν μια πολιτική άποψη ή ένα πολιτικό κόμμα ή και να εργαστούν με τον τρόπο τους εναντίον ενός πολιτικού συστήματος. Συνήθως αντιπροσωπεύουν κάποια πολιτική ή κοινωνική άποψη και ο στόχος τους είναι να περάσουν κάποιο μήνυμα προκαλώντας το ενδιαφέρον των μέσων μαζικής επικοινωνίας. Υπάρχουν και οι hackers που έχουν ως στόχο το οικονομικό κέρδος, κάνουν ηλεκτρονικές επιθέσεις σε οικονομικούς οργανισμούς και αντιγράφουν προγράμματα λογισμικού παράνομα. Υπάρχουν βέβαια και οι επίσημοι hackers που εργάζονται νόμιμα για λογαριασμό κυβερνήσεων, κυρίως για κατασκοπευτικούς λόγους.

Μια άλλη κατηγορία hackers είναι οι ***meta- hackers***, οι οποίοι παρακολουθούν τη δράση άλλων hackers χωρίς να γίνονται αντιληπτοί και προσπαθούν να εκμεταλλευτούν τις αδυναμίες των συστημάτων που οι άλλοι hackers ανακαλύπτουν.

Τέλος, η κατηγορία των hackers με την ονομασία ***darkdiders***, είναι αυτοί που εκμεταλλεύονται τις αδυναμίες των συστημάτων υπολογιστών ώστε να αποκομίσουν οικονομικό όφελος για τους ίδιους προσωπικά ή και να προκαλέσουν καταστροφές.

Μία άλλη κατηγοριοποίηση που μπορεί να γίνει είναι, στις διάφορες γενιές των hackers από τότε που εμφανίστηκαν μέχρι και σήμερα.[59]

Η *πρώτη γενιά* των hackers αποτελείται από μέλη πανεπιστημιακών ομάδων των μεγάλων τεχνολογικών πανεπιστημίων MIT και Stanford. Αυτοί οι επιστήμονες, σχεδόν αποκομμένοι από την υπόλοιπη κοινωνία ζούσαν εργαζόμενοι στα εργαστήριά τους και ανέπτυξαν τις πρώτες μεθόδους προγραμματισμού κατά το 1950 και 1960 στις υπηρεσίες κυρίως, βέβαια, της Αμερικανικής Κυβέρνησης.

Η *δεύτερη γενιά* αποτελείται από εμπορικά προσανατολισμένους επιστήμονες που ως σκοπό είχαν την ευρεία διάδοση της πληροφορικής τεχνολογίας στις μάζες. Ήταν αυτοί που δημιούργησαν τους πρώτους προσωπικούς ηλεκτρονικούς υπολογιστές. Επιπρόσθετος στόχος της νέας αυτής γενιάς ήταν η μελέτη και ο πειραματισμός για τη βελτίωση της αλληλεπίδρασης ανθρώπου με υπολογιστή, παραδειγματικό επίτευγμα της οποίας ήταν το γνωστό και απαραίτητο σήμερα <ποντίκι>.

Η *τρίτη γενιά* αποτελείται από τους προγραμματιστές, οι οποίοι δημιούργησαν τις βασικές δομές στις οποίες στηρίχτηκε μετέπειτα η δημιουργία των ηλεκτρονικών παιχνιδιών. Η γενιά αυτή δείχνει πλέον να αντιλαμβάνεται πλήρως την οικονομική δυναμική του συγκεκριμένου τομέα και εργάζεται δραστικά για να ανταποκριθεί στη ζήτηση που δημιουργεί η ευρεία εξάπλωση της χρήσης προσωπικού ηλεκτρονικού υπολογιστή αλλά και για να διαμορφώσει νέες προοπτικές αγοράς και νέες ανάγκες.

[59] http://www.theartofcrime.gr/artofcrime/assets/hackers.dot

Η *τέταρτη γενιά* όμως, είναι αυτή που συγκρότησε την κοινότητα των hackers όπως την ξέρουμε σήμερα. Ενώ με τις προηγούμενες γενιές υπήρχε μία τάση για εκλαΐκευση του νέου μέσου δίνοντας έμφαση στη χρήση αυτού προσανατολισμένη στις ανάγκες και τα δεδομένα της καθημερινότητας, η νέα αυτή γενιά εμφάνισε για πρώτη φορά μια ανεστραμμένη ψυχολογική συμπεριφορά, μία αναρχική τάση όχι σύνθεσης νέων δεδομένων και προγραμμάτων, αλλά αντίθετα μια αποδομητική και μία ενδοσκοπική τάση, που εξελίχθηκε στη μοντέρνα μορφή hacking, η οποία προσεγγίζει την εικόνα που έχουμε στο μυαλό μας για τον hacker, εικόνα που άπτεται και εγκληματικών συμπεριφορών.

3.2 ΤΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ.

Τα εγκλήματα του ηλεκτρονικού βανδαλισμού αποτελούν μία από τις πιο ενδιαφέρουσες μορφές ηλεκτρονικού διαδικτυακού εγκλήματος. Ο όρος βανδαλισμός, αναφέρεται στην αυθαίρετη έμμεση ή άμεση παρείσδυση σε ένα σύστημα ηλεκτρονικών υπολογιστών με βασικό σκοπό την παρεμπόδιση της λειτουργίας του ή την πρόκληση ζημιάς στο σύστημα ή στα περιεχόμενα του. Όπως είδαμε παραπάνω και το hacking υπάγεται στην κατηγορία των εγκλημάτων ηλεκτρονικού βανδαλισμού.

Το κακόβουλο λογισμικό αποτελείται από έναν κακόβουλο κώδικα ηλεκτρονικού υπολογιστή, ο οποίος δημιουργείται με σκοπό να προκαλέσει ζημιά σε άλλο ηλεκτρονικό υπολογιστή ή να εισχωρήσει σε αυτόν με σκοπό την υποκλοπή, αλλοίωση ή διαγραφή δεδομένων και προγραμμάτων. Ο κακόβουλος κώδικας διακρίνεται σε τρεις βασικές κατηγορίες τους ιούς (viruses), τα σκουλήκια (worms), τους δούρειους ίππους (trojan horses) και τις λογικές βόμβες (logic bombs), ή απλά βόμβες (bombs), με βάση τον τρόπο δράσης τους και τον τρόπο με τον οποίο κινούνται από σύστημα σε σύστημα, δηλαδή ανάλογα με τον τρόπο προγραμματισμού τους.

Οι ηλεκτρονικοί ιοί αποτελούν μία μορφή προγράμματος που εκμεταλλεύεται τις τεχνικές ατέλειες του ηλεκτρονικού συστήματος του ηλεκτρονικού υπολογιστή για να προκαλέσει ζημιά ή να εκτελέσει τη λειτουργία για την οποία δημιουργήθηκε.

Σύμφωνα με τον Cohen ιός υπολογιστή είναι <κάθε πρόγραμμα το οποίο μπορεί να 'μολύνει' άλλα προγράμματα ώστε να συμπεριλαμβάνουν ένα εξελιγμένο αντίγραφό του>. Ο πιο λεπτομερής όμως ορισμός του στηρίζει ότι <Ο ιός είναι ένα μικρό πρόγραμμα υπολογιστή το οποίο μπορεί να μείνει αδρανές για μήνες μέχρι να εκτελέσει την καταστροφική του αποστολή, που για παράδειγμα μπορεί να είναι η διαγραφή του σκληρού δίσκου. Η ομοιότητα στη δράση ενός ιού ηλεκτρονικού υπολογιστή με ένα βιολογικό ιό είναι μεγάλη. Ένας ιός ηλεκτρονικού υπολογιστή μπορεί να αυτοαντιγράφεται και να αυτοδιαδίδεται από σύστημα σε σύστημα. Μολύνει, ή κρύβεται μέσα σε άλλο πρόγραμμα, το οποίο μπορεί να είναι το λειτουργικό σύστημα του ηλεκτρονικού υπολογιστή ή κάποιο πρόγραμμα εφαρμογής.[60]>

Ο ηλεκτρονικός βανδαλισμός με τη χρήση ιών μπορεί να πάρει τρεις βασικές μορφές:

- Ο ιός είναι προορισμένος να σβήσει δεδομένα ή αρχεία ή να τα καταστρέφει ολοκληρωτικά.
- Ο ιός κωδικοποιεί αρχεία με τέτοιο τρόπο ώστε ο χρήστης να μη μπορεί να έχει πρόσβαση σε αυτά. Τα αρχεία δεν καταστρέφονται κατά ανάγκη αλλά δεν είναι προσβάσιμα.

[60] Βλ. Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 110

- Ο ιός οδηγεί σε υπερφόρτωση του συστήματος με αποτέλεσμα αυτό να λειτουργεί αργά ή να μη μπορεί να λειτουργήσει καθόλου. Και σε αυτή τη μορφή δεν υπάρχει καταστροφή δεδομένων, αλλά το σύστημα απλά καθηλώνεται.

  Ο <δούρειος ίππος> είναι ο πιο συνηθισμένος τύπος καταστροφικού ιού. Ο <δούρειος ίππος> είναι πρόγραμμα κρυμμένο μέσα σε άλλο χρήσιμο πρόγραμμα- τον ξενιστή- και υπό τις κατάλληλες συνθήκες εκτελεί μία εκ πρώτης όψεως αφανή λειτουργία με ζημιογόνα ή καταστροφικά αποτελέσματα. Η λειτουργία αυτή είναι κατά κανόνα απλή: δεν ξεπερνά τη μετάδοσή του- αντιγραφή του σε κάποιο άλλο πρόγραμμα μέσα στον ηλεκτρονικό υπολογιστή. Είναι όμως συχνό φαινόμενο μέσω δούρειου ίππου να επιδιώκονται πιο καταστροφικοί σκοποί, όπως είναι η διαγραφή των αρχείων και προγραμμάτων που είναι αποθηκευμένα στο σκληρό δίσκο ή η καταστροφή γραπτών κειμένων και στατιστικών προγραμμάτων. Ο δούρειος ίππος μπορεί να εισαχθεί στον ηλεκτρονικό υπολογιστή μέσω διαδικτύου[61] και να διαδοθεί σε όλο το σύστημα. Έτσι είναι δυνατό κάποιος που εργάζεται σε μολυσμένο ηλεκτρονικό υπολογιστή, να αποθηκεύσει δεδομένα σε cd rom και να τα μεταφέρει σε άλλο ηλεκτρονικό υπολογιστή, θέλοντας να συνεχίσει εκεί την εργασία του, και καταλήγει έτσι να μολύνει και τον άλλον ηλεκτρονικό υπολογιστή.

  Το <σκουλήκι> είναι και αυτό τύπος καταστροφικού ιού. Χρησιμοποιείται ο όρος σκουλήκι για να δηλώσει ότι το πρόγραμμα αυτοδιαδίδεται μέσω ενός δικτύου με συνεχείς ελιγμούς από ηλεκτρονικό υπολογιστή σε ηλεκτρονικό υπολογιστή με σκοπό να εξαπλωθεί σε όλα τα συνδεδεμένα συστήματα. Στην πιο απλή μορφή τους τα σκουλήκια δεν αποτελούν ιούς, αφού δεν χρησιμοποιούν τη λογική των ξενιστών τους. Επιπλέον τα σκουλήκια δεν πολλαπλασιάζονται με τη συνηθισμένη τεχνική των ιών, δηλαδή με την εισαγωγή της <λογικής> τους στους ξενιστές αλλά είναι αυτόνομα και χρησιμοποιούν τους μηχανισμούς επικοινωνίας μεταξύ ηλεκτρονικών υπολογιστών για να προκαλέσουν ζημιά.

  <Οι λογικές βόμβες> είναι αφανή μέρη σε ένα πρόγραμμα, που ενεργοποιούνται όταν λάβει χώρα ένα προκαθορισμένο γεγονός, όπως παραδείγματος χάρη η πάροδος συγκεκριμένου χρονικού διαστήματος μετά την εισαγωγή τους, ο αριθμός ενεργοποιήσεων του ξενιστή τους από το χρήστη, ή μια προκαθορισμένη ημερομηνία. Οι λογικές βόμβες είναι πιο καταστροφικές από τα σκουλήκια και τους δούρειους ίππους, γιατί είναι πιο απλές στην κατασκευή τους και μπορούν να επηρεάσουν διάφορα αποθηκευμένα αρχεία ή και ολόκληρο το λογισμικό. Η διαφορά τους από τα άλλα δύο είναι ότι δεν αυτοπολλαπλασιάζονται, εκτός αν οι ιδιότητές τους συνδυαστούν με τις ιδιότητες των άλλων τύπων.

  Βασική προϋπόθεση για τη μετάδοση των ιών ήταν η συμβατότητα που αναπτύχθηκε μεταξύ των προσωπικών ηλεκτρονικών υπολογιστών. Μέσω της εξασφάλισης της συμβατότητας έγινε δυνατό ένας ηλεκτρονικός υπολογιστής να μη χρειάζεται το δικό του λειτουργικό σύστημα, αλλά να μπορεί να χρησιμοποιεί ένα ήδη υπάρχον, κοινό για όλους τους ηλεκτρονικούς υπολογιστές. Η συμβατότητα αυτή όμως αυτομάτως σήμαινε συμβατότητα και σε όλους τους ιούς. Με την ανάπτυξη δε του Διαδικτύου, αυτό κατέστη ο σημαντικότερος <μεταφορέας> ιών. Οι κατασκευαστές τους δε, με την πάροδο των χρόνων, έχουν όλο και καλύτερη κατάρτιση καθώς και όλα τα μέσα στη διάθεσή τους, για τη δημιουργία όλο και πιο επικίνδυνων ιών, χαρακτηριστικό των οποίων είναι η δυνατότητά τους να μεταλλάσσονται.

  Ο πρώτος νόμος για την αντιμετώπιση των ιών δημιουργήθηκε το 1989 (Computer Virus Eradication Act of 1989) στις ΗΠΑ. Αυτός ο νόμος περιέγραφε τη δημιουργία των ιών, όριζε

[61] Αλλά και μέσω απλού δικτύου ηλεκτρονικού υπολογιστή, ή μέσω cd rom.

ποινές για τη δημιουργία και διάδοση των ιών και προέβλεπε αστική αποζημίωση των θυμάτων επίθεσης από ιούς. Ωστόσο αυτός ο νόμος δεν όριζε με επάρκεια βασικές έννοιες όπως πρόγραμμα, πληροφορία, εντολή, παρείσδυση και διείσδυση, με αποτέλεσμα να εμφανίζει πολλές αοριστίες.

Ακολούθησε ο νόμος της Μεγάλης Βρετανίας Computer Misuse Act, ο οποίος ποινικοποιεί κάθε είδους μη εξουσιοδοτημένη τροποποίηση στο υλικό σώμα ή το λογισμικό ενός ηλεκτρονικού υπολογιστή. Και πάλι όμως επρόκειτο για ένα νόμο ο οποίος επίσης εμφάνιζε πολλές αοριστίες, αφού μέχρι και τον ορισμό του ηλεκτρονικού εγκλήματος τον άφησε στο <κοινό νόημα>. Στην ελληνική έννομη τάξη δεν υπάρχει ακόμα συγκεκριμένο άρθρο για την αντιμετώπιση των ιών. Εάν αυτοί εισέλθουν στο σύστημα και προχωρήσουν σε παράνομη αντιγραφή δεδομένων, αντιμετωπίζονται με το άρθρο 370Γ του Ποινικού Κώδικα., αν όμως εισέλθουν στο σύστημα προκαλώντας μόνο αλλοιώσεις των στοιχείων του συστήματος δεν υπάρχει διάταξη ικανή για την ποινική αντιμετώπιση του ζητήματος.

3.3 Η ΑΝΕΠΙΘΥΜΗΤΗ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ.

Οι περισσότεροι από εμάς οι οποίοι διαθέτουν ενεργή διεύθυνση ηλεκτρονικού ταχυδρομείου, σχεδόν κάθε μέρα, χωρίς την προηγούμενη εκδήλωση ενδιαφέροντος από την πλευρά μας, λαμβάνουμε διαφημίσεις ή εμπορικές προτάσεις από εταιρείες, οι οποίες απέκτησαν με νόμιμο ή παράνομο τρόπο, τις διευθύνσεις της ηλεκτρονικής μας αλληλογραφίας. Τα παραπάνω ανεπιθύμητα μηνύματα ή spam, όπως μας είναι ευρύτερα γνωστά, αποστέλλονται μαζικά σε πολύ μεγάλο αριθμό ανθρώπων. Τα μηνύματα αυτά δεν είναι φορείς κινδύνων για τα δεδομένα, αλλά ενδέχεται να έχουν επιπτώσεις στην παραγωγικότητα της εργασίας.

Τις περισσότερες φορές αυτά τα μηνύματα δεν ενδιαφέρουν τον παραλήπτη, αλλά οι επιχειρήσεις καταφεύγουν στην αποστολή τους, λόγω του χαμηλού κόστους διαφήμισης και προώθησης των προϊόντων τους. Οι πηγές από τις οποίες οι spammers συλλέγουν τις διευθύνσεις ηλεκτρονικού ταχυδρομείου είναι είτε οι ομάδες ενδιαφερόντων (newsgroups), είτε οι ιστοσελίδες, είτε οι ταχυδρομικοί κατάλογοι.

Για να διακοπεί η αποστολή αυτή δεν αρκεί μία απλή απάντηση στη διεύθυνση του spam, καθότι αυτό δεν είναι εφικτό, λόγω του ότι η διεύθυνση είναι πλασματική. Οι spammers συνηθίζουν να καλύπτουν τα ίχνη τους με τη χρήση πολλαπλών mail servers σε διάφορους IP’s που επιλέγονται τυχαία. Η αποστολή αυτών των μηνυμάτων οδηγεί σε ανάλωση πολύτιμου χρόνου για την ανάγνωση και εκκαθάρισή τους από το φάκελο εισερχομένων του ηλεκτρονικού ταχυδρομείου.

Η ανεπιθύμητη ηλεκτρονική αλληλογραφία δεν περιλαμβάνει μόνο τα spam. Μία άλλη μορφή της είναι ο βομβαρδισμός του ηλεκτρονικού ταχυδρομείου, που ουσιαστικά και πάλι έγκειται στην αποστολή ανεπιθύμητων ηλεκτρονικών μηνυμάτων στην ηλεκτρονική διεύθυνση του παραλήπτη, με τη διαφορά ότι τα μηνύματα αυτά στέλνονται με σκοπό να μπλοκάρουν το ηλεκτρονικό ταχυδρομείο κάποιου, κάτι που συνήθως γίνεται με τη σύμπραξη πολλών δραστών.

Άλλη περίπτωση ανεπιθύμητης ηλεκτρονικής αλληλογραφίας είναι η αποστολή απειλητικών ή αισχρών μηνυμάτων. Σε αυτή την περίπτωση ένας συγκεκριμένος αποστολέας προσβάλει ή απειλεί ένα συγκεκριμένο παραλήπτη, ή αισχρολογεί σε βάρος του. Σχετίζεται άμεσα με τις

περιπτώσεις της διαδικτυακής τρομοκρατίας, της προπαγάνδας μίσους, του hacking και της μετάδοσης των ιών.

Η αδυναμία του διαδικτύου είναι η ιδιωτικότητά του. Έως ότου το μήνυμα να φτάσει στον τελικό του αποδέκτη, έχουν μεσολαβήσει πολλοί ηλεκτρονικοί υπολογιστές. Σε αυτούς τους σταθμούς όμως είναι δυνατός ο έλεγχος του μηνύματος και η υποκλοπή του. Ταυτόχρονα το ίδιο το διαδίκτυο επειδή έχει σχεδιαστεί ως αμφίδρομη επικοινωνία, αφήνει πολλές τεχνικές διόδους στους επίδοξους δράστες. Στην πλειοψηφία του σήμερα αυτό το έγκλημα αφορά κυρίως στις εταιρικές σχέσεις.

Στην Ελλάδα, δεν υπάρχει ακόμα ειδική νομοθεσία για την προστασία της ηλεκτρονικής αλληλογραφίας. Σε περίπτωση όμως που κάποιος είναι θύμα ενός από τα παραπάνω εγκλήματα, προστατεύεται από το Σύνταγμα[62] και από το νόμο για την προστασία των προσωπικών δεδομένων ν. 2472/1997. Τέλος, η υποκλοπή μηνυμάτων ηλεκτρονικής αλληλογραφίας υπάγεται στην αντικειμενική υπόσταση του εγκλήματος του άρθρου 370Γ παράγραφος 2 του Ποινικού Κώδικα, (όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών), αφού οι δράστες της υποκλοπής αποκτούν πρόσβαση σε ηλεκτρονικά μηνύματα αλληλογραφίας τα οποία έχουν εισαχθεί σε ηλεκτρονικό υπολογιστή.

3.4 Ο ΒΑΝΔΑΛΙΣΜΟΣ ΔΙΑΔΙΚΤΥΑΚΩΝ ΤΟΠΩΝ.

Ο βανδαλισμός διαδικτυακών τόπων αποτελεί μία από τις πιο ενδιαφέρουσες μορφές διαδικτυακού εγκλήματος. Πρόκειται για ένα είδος επίθεσης το οποίο παρουσίασε ιδιαίτερη αύξηση τα τελευταία χρόνια. Οι επιθέσεις πραγματοποιούνται από τους βανδάλους (vandals) και κυρίως στρέφονται κατά κυβερνητικών οργανισμών και υπηρεσιών.

Σκοπός του δράστη είναι μέσω της επίθεσής του να διαγράψει ορισμένες σελίδες ή γραφικά, και να ανεβάσει τις δικές του σελίδες, το περιεχόμενο των οποίων μπορεί να είναι προπαγανδιστικό αλλά και χιουμοριστικό. Όταν ο ιδιοκτήτης της ιστοσελίδας αντιληφθεί την επίθεση, μπορεί να διορθώσει την προβληματική σελίδα από τα εφεδρικά της αρχεία. Συχνά όμως απαιτείται πολύς χρόνος για να γίνει αυτή η επιδιόρθωση και αν η ζημιά είναι μεγάλη απαιτείται η ιστοσελίδα να παραμείνει εκτός δικτύου για μεγάλο χρονικό διάστημα.

Το τελευταίο διάστημα, δηλαδή από τον Σεπτέμβρη του 2010 και μετά παρατηρείται μία προσπάθεια από hackers να αλλοιώσουν διάφορες ελληνικές ιστοσελίδες, όπως η επίθεση στη σελίδα του Ιωάννη Μπουτάρη, Δημάρχου της Θεσσαλονίκης, η οποία ήταν επίθεση deface, δηλαδή οι hackers παρενέβησαν στην ιστοσελίδα και έσβησαν τη βασική της οθόνη, αντικαθιστώντας την με μία δική τους εικόνα. Όμοια επίθεση δέχτηκε και η ιστοσελίδα του γνωστού συγκροτήματος Onirama. Επίθεση δέχτηκε και η ιστοσελίδα του ΟΑΣΑ, στην οποία οι hackers τοποθέτησαν στην βασική σελίδα μια δικιά τους εικόνα- μήνυμα.

[62] Άρθρο 9, το οποίο προστατεύει την κατοικία ως άσυλο και την ιδιωτική και οικογενειακή ζωή του ατόμου, και το άρθρο 19, το οποίο καθιερώνει το απόρρητο των επιστολών και της κάθε μορφής επικοινωνίας.

3.5 ΤΟ PHOSING ΚΑΙ PHARMING.

Ως phising χαρακτηρίζεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου που έχουν σκοπό να αποκλέψουν εμπιστευτικές πληροφορίες που ανήκουν στον παραλήπτη του μηνύματος. Συχνά αυτά τα ηλεκτρονικά μηνύματα δίνουν την εντύπωση ότι προέρχονται από κάποια τράπεζα και με διάφορες δικαιολογίες ζητούν από τον παραλήπτη να αποκαλύψει ευαίσθητα προσωπικά του δεδομένα. Αν ο παραλήπτης απαντήσει στο e- mail αυτό, αποκαλύπτοντας τα στοιχεία αυτά, τότε οι phishers διεισδύουν σε αυτό το λογαριασμό άμεσα και μεταβιβάζουν χρηματικά ποσά σε δικούς τους λογαριασμούς.

Το pharming είναι και αυτό μέθοδος εξαπάτησης μέσω του διαδικτύου, αλλά πιο επικίνδυνο από το phising. Οι δράστες συντηρούν ένα μεγάλο αριθμό ηλεκτρονικών υπολογιστών συνδεδεμένων στο διαδίκτυο, οι οποίοι μπορούν να συγκριθούν με μία φάρμα (farm) ζώων. Ένα ειδικό πρόγραμμα, συνήθως ιός ή δούρειος ίππος, εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον ηλεκτρονικό υπολογιστή του θύματος και τον επηρεάζει κατά τέτοιο τρόπο, ώστε ο συγκεκριμένος ηλεκτρονικός υπολογιστής να μπορεί να επισκέπτεται μόνο πλαστές ιστοσελίδες, ακόμα και στην περίπτωση που ο χρήστης πληκτρολογεί τη σωστή διεύθυνση της ιστοσελίδας. Έτσι το θύμα γράφει τη σωστή διεύθυνση του διαδικτυακού χώρου και βλέπει στην οθόνη του μια ιστοσελίδα, η οποία εξωτερικά είναι απομίμηση της αυθεντικής και έτσι νομίζει ότι είναι αυθεντική και θεωρεί ότι είναι σε χώρο που μπορεί να έχει εμπιστοσύνη. Αποτέλεσμα είναι να εισάγει όλους τους κωδικούς του καθώς και άλλες προσωπικές πληροφορίες, οι οποίες περνούν αμέσως στη γνώση των δραστών, χωρίς το θύμα να έχει καταλάβει το οτιδήποτε. Επιπλέον, αν παραδείγματος χάρη νομίζει ότι βρίσκεται στην ιστοσελίδα της τράπεζας του και επιχειρήσει μεταφορά χρημάτων, τα χρήματα αυτά μεταφέρονται αυτόματα στους δράστες.[63]

3.6 Η ΠΕΙΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ.

Ο όρος πειρατεία λογισμικού αναφέρεται στην αναπαραγωγή ή και διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευματικών δικαιωμάτων, χωρίς τη γραπτή συναίνεση του δημιουργού τους.

Λόγω της ψηφιακής μορφής των εφαρμογών λογισμικού είναι πολύ εύκολη η αναπαραγωγή τους σε πολλαπλά αντίγραφα. Με την εξάπλωση του διαδικτύου και ιδιαίτερα των ευρυζωνικών συνδέσεων το λογισμικό μπορεί να διακινηθεί εύκολα και γρήγορα μέσω του ηλεκτρονικού ταχυδρομείου ή των εφαρμογών ανταλλαγής αρχείων (pear to pear).

Η πνευματική ιδιοκτησία των προϊόντων μέσων της πληροφορικής τεχνολογίας αποτελεί μείζον ζήτημα για τις επιχειρήσεις του χώρου. Οι νόμοι που προστατεύουν τα δικαιώματά τους, παραδείγματος χάρη οι νόμοι για το εμπορικό σήμα, την αντιγραφή και τα λοιπά, δεν αντιμετωπίζουν αποτελεσματικά την αντιγραφή ενός προγράμματος λογισμικού σε ένα cd rom,επειδή αυτή είναι πολύ εύκολο να λάβει χώρα. Ήδη στην αγορά κυκλοφορούν πολλά cd records και dvd records, τα οποία παρέχουν στο χρήστη τη δυνατότητα επανεγγραφής δεδομένων και προγραμμάτων. Η αντιγραφή λοιπόν του λογισμικού αφορά πρώτον όσους

[63] Σε επίθεση pharming στο Βερολίνο το 2005, προκλήθηκε οικονομική βλάβη σε βάρος των πελατών τράπεζας, ύψους άνω του ενός εκατομμυρίου ευρώ. Βλ. Βασιλάκη Ειρήνη, <Τα φαινόμενα phirsing και pharming και η ποινική τους αξιολόγηση, βλ. και Κιούπης Δ., <Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ε.Ε.>, σε Τιμητικό Τόμο Αργυρίου Καρρά, σελ. 1028.

διεκδικούν την πνευματική ιδιοκτησία των μαζικά αντιγραφόμενων προϊόντων, δηλαδή οι εταιρείες παραγωγής του λογισμικού. Βέβαια ο βασικότερος λόγος που οι εταιρείες παραγωγής λογισμικού δίνουν τόση μεγάλη σημασία στο ζήτημα είναι τα κέρδη τα οποία χάνουν, λόγω της αντιγραφής του λογισμικού τους από άλλο, ήδη υπάρχον, αντί της αγοράς αυτού.

Αυτή η ολοφάνερη καταπάτηση των νόμων πνευματικής ιδιοκτησίας, η αναπαραγωγή δηλαδή και διανομή προστατευμένων από τους νόμους έργων, είναι αυτό που από την προοπτική της πνευματικής ιδιοκτησίας, καλείται πειρατεία.

Ως αντικείμενα πειρατείας μπορούν να ορισθούν τύποι έργων που προστατεύονται από το νόμο του δικαιώματος της αντιγραφής. Ως έκθετα στη πειρατική δημιουργία και χρήση ηλεκτρονικά δεδομένα, πιο συχνά απαντώνται τα παρακάτω: έργα γραπτού λόγου, όπως οι οδηγίες χρήσης, τα συνοδευτικά κείμενα αντιμετώπισης προβλημάτων και οι πηγαίοι κώδικες προγραμμάτων όταν αποτυπώνονται σε γραπτή μορφή, μουσικά έργα, καλλιτεχνικά έργα, όπως φωτογραφίες και αρχιτεκτονικά σχέδια, κινηματογραφικές ταινίες, ηχητικές εγγραφές, ραδιοφωνικές μεταδόσεις, σήματα μεταφερόμενων προγραμμάτων, δημοσιευμένες εκδόσεις και προγράμματα ηλεκτρονικού υπολογιστή.

3.7 Η απάτη στο διαδίκτυο.

Ο κύριος όγκος των ηλεκτρονικών διαδικτυακών εγκλημάτων εντάσσεται στα ηλεκτρονικά οικονομικά εγκλήματα. Η σύγχρονη κοινωνία και οικονομία δε μπορεί να λειτουργήσει χωρίς τη στήριξη της πληροφορικής τεχνολογίας αν θέλει να βρίσκεται σε συνθήκες ανταγωνισμού.

Στα πλαίσια του διαδικτύου το ηλεκτρονικό επιχειρείν (e business) αναπτύσσεται διαρκώς και κερδίζει έδαφος στο χώρο των οικονομικών συναλλαγών. Η οικονομική δραστηριοποίηση στον κυβερνοχώρο, έχει ως αποτέλεσμα πολλά οικονομικά πλεονεκτήματα για τις επιχειρήσεις, τα σημαντικότερα από τα οποία είναι η άμεση πρόσβαση του ατόμου στην παγκόσμια αγορά χωρίς υψηλό κόστος, η πρόσβαση και η δυνατότητα λήψης παραγγελιών από τους καταναλωτές σε 24ωρη βάση, μέσω του mailbox, η μείωση της τελικής τιμής του προϊόντος εξαιτίας της εξάλειψης των μεσαζόντων και του περιορισμού των δαπανών για διαφημιστικές δαπάνες καθώς μείωση του χρόνου παράδοσης των προϊόντων και τέλος η προώθηση της άρτιας οργάνωσης των επιχειρήσεων, της ανάπτυξης σύγχρονων μεθόδων επικοινωνιών και εμπορικής δραστηριότητας που ωφελούν τον καταναλωτή. Ένας από τους κυριότερους τύπους ηλεκτρονικού διαδικτυακού οικονομικού εγκλήματος είναι η ηλεκτρονική διαδικτυακή απάτη.

Οι σύγχρονοι εγκληματίες πλέον έχουν ως όπλα τους το πληκτρολόγιο, το ποντίκι και το διαδίκτυο και χρησιμοποιώντας τα εισέρχονται σε απόρρητα συστήματα τραπεζών. Μέσω του διαδικτύου μπορούν να αποκτήσουν κωδικούς λογαριασμών, αριθμούς πιστωτικών καρτών, αριθμούς τηλεφώνων αλλά και πληροφορίες για το πώς θα επιτύχουν τον παράνομο σκοπό τους. Μερικές από τις σύγχρονες απάτες είναι οι διαδικτυακές δημοπρασίες, οι τραπεζικές συναλλαγές, η παραποιημένη εφαρμογή ηλεκτρονικών πληρωμών, η παραχάραξη στοιχείων και η προσβολή ηλεκτρονικών δικτύων.

Το πιο διαδεδομένο ηλεκτρονικό διαδικτυακό οικονομικό έγκλημα στην Ελλάδα είναι οι απάτες με πιστωτικές κάρτες. Οι δράστες μέσω διάφορων εγκληματικών δράσεων

υποκλέπτουν αριθμούς και κωδικούς πιστωτικών καρτών και κατόπιν προβαίνουν σε αγορές με την ξένη πιστωτική κάρτα.
Έτσι ο καταναλωτής βρίσκεται υπερχρεωμένος στο λογαριασμό της πιστωτικής του κάρτας και ο δράστης είναι δύσκολο να βρεθεί.

Η απάτη σε βάρος μιας επιχείρησης ή ενός ιδιώτη μέσω της εστίασης και παραποίησης, σε πληροφορίες και δεδομένα, τα οποία τους αφορούν άμεσα και έμμεσα, έχει να κάνει με τους άυλους πόρους, όπως χρηματικές καταθέσεις, οικονομικούς τίτλους και λογιστικά μεγέθη. Συχνά παρατηρούμε φαινόμενα βελτίωσης της πίστης μέσω της παραποίησης δεδομένων που αναφέρονται σε ένα άτομο ή σε μια επιχείρηση (έτσι ώστε να μπορεί να πάρει ένα δάνειο ή ένα δάνειο με καλύτερους όρους, το οποίο, αν φαίνονταν τα πραγματικά του στοιχεία, δε θα έπαιρνε), αλλά και της χειροτέρευσης της φερεγγυότητας των στοιχείων ενός ατόμου ή επιχείρησης για τους αντίθετους λόγους.

Μία ακόμη περίπτωση διαδικτυακής απάτης μέσω ηλεκτρονικού υπολογιστή είναι η παρέμβαση σο σύστημα επεξεργασίας δεδομένων ενός οργανισμού ή μιας επιχείρησης, η οποία απαντάται συχνά σε ζητήματα μισθών, συντάξεων αλλά και τραπεζικών καταθέσεων. Σε ένα σύστημα χωρίς καμία ασφάλεια ο μηδενισμός ενός λογαριασμού είναι θέμα δευτερολέπτων για έναν ειδικό στην πληροφορική τεχνολογία. Αν το σύστημα διαθέτει ένα μηχανισμό ασφάλειας προηγούμενης γενιάς, ο ειδικός χρειάζεται απλά λίγο περισσότερο χρόνο για να πετύχει το στόχο του.

3.8 Η διαδικτυακή τρομοκρατία.

Η τρομοκρατία είναι ένα φαινόμενο σε έξαρση τα τελευταία χρόνια. Όλο και συχνότερα μαθαίνουμε για νέες τρομοκρατικές επιθέσεις με μεγάλο αριθμό θυμάτων. Τα ο διαδίκτυο πλέον αποτελεί σημαντικό όπλο στα χέρια των τρομοκρατών της νέας γενιάς. Τα ο FBI ορίζει τη διαδικτυακή τρομοκρατία (cyber terrorism) ως <την προσχεδιασμένη πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων, προγραμμάτων ηλεκτρονικού υπολογιστή και δεδομένων που καταλήγουν στην άσκηση βίας έναντι άμαχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες.>[64]

Η χρήση του διαδικτύου προσφέρει μια σειρά από πλεονεκτήματα τα οποία φυσικά εκμεταλλεύονται οι τρομοκράτες, όπως το ότι είναι φθηνότερο από τις παραδοσιακές τρομοκρατικές μεθόδους, οι τρομοκρατικές ενέργειες είναι δύσκολο να εντοπιστούν, η τοποθεσία στην οποία βρίσκονται μπορεί να συγκαλυφθεί, μπορούν να κάνουν την επίθεσή τους από οποιοδήποτε σημείο του κόσμου ανώνυμα και μπορούν να επιτεθούν ταυτόχρονα σε περισσότερους στόχους. Επίσης μέσω του διαδικτύου οι τρομοκρατικές ομάδες ανά τον κόσμο μπορεί να συνεργάζονται ή και να ανταλλάσσουν μεταξύ τους πληροφορίες, ώστε να εξελίσσουν την τρομοκρατική τους δράση. Τέλος μέσω των ιστοσελίδων τους οι τρομοκρατικές οργανώσεις έχουν την δυνατότητα να προσεγγίζουν νέα μέλη από κάθε μέρος της γης.

Μέσω του διαδικτύου οι τρομοκράτες θα έχουν τη δυνατότητα να παραβιάσουν τα συστήματα ελέγχου κρίσιμων υποδομών μιας χώρας, όπως οι ενεργειακές εγκαταστάσεις, το δίκτυο διανομής νερού και τα τηλεπικοινωνιακά συστήματα και έτσι οι επιθέσεις τους θα καθίστανται όλο και πιο επικίνδυνες.

---

[64] Βλ. Βλαχόπουλος Κ., <Ηλεκτρονικό Έγκλημα>, σελ. 71.

3.9 ΤΟ ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ.

Ο όρος ξέπλυμα χρήματος, ή αλλιώς νομιμοποίηση εσόδων από παράνομες δραστηριότητες, χρησιμοποιείται για να περιγράψει εκείνες τις διαδικασίες μέσω των οποίων τα κέρδη των εγκλημάτων υπόκεινται σε μια σειρά διαδικασιών οι οποίες καλύπτουν την παράνομη προέλευσή τους και τα κάνουν να εμφανίζονται σα να προέρχονται από νόμιμες πηγές.

Η ανάπτυξη στην πληροφορική τεχνολογία και κυρίως η έλευση του διαδικτύου επέδρασε καθοριστικά στην απόκρυψη και τη διακίνηση των οικονομικών προϊόντων παρανόμων ενεργειών. Η τεχνολογία έχει δημιουργήσει την τεχνική υποδομή για τη χρήση του εντελώς μη- ανιχνεύσιμου ως προς την αφετηρία του ψηφιακού χρήματος. Οι υπάρχοντες νόμοι για το ξέπλυμα χρήματος, εφαρμόζονται για να αντιμετωπίσουν τη διαδικτυακή του μορφή αλλά αποδεικνύονται ανεπαρκείς, κυρίως λόγω της δυσκολίας στην ανακάλυψη και τη δίωξη ορισμένων περιπτώσεων νομιμοποίησης παράνομων εσόδων από εγκληματική δραστηριότητα.

Το διαδίκτυο και στην περίπτωση του ξεπλύματος βρώμικου χρήματος προσφέρει ταχύτητα, πλήρη ανωνυμία, ασφάλεια και ιδιωτικότητα. Αυτός που επιθυμεί να νομιμοποιήσει παράνομα έσοδα, προσλαμβάνει ανθρώπους ή καταθέτει ο ίδιος μέσω του διαδικτύου, το παράνομο ποσό σε τράπεζες που αποδέχονται ηλεκτρονικό χρήμα. Για να εξασφαλιστεί μια κάποια ασφάλεια οι καταθέσεις γίνονται σε μικρά ποσά. Η μετατροπή του χρήματος σε ηλεκτρονικό χρήμα προσφέρει στον παραβάτη την ανωνυμία του (μέσω ψηφιακών κωδικοποιημένων υπογραφών και κοινού κλειδάριθμου) και την πρόσβαση σε νόμιμο ηλεκτρονικό χρήμα. Για να συλληφθεί κάποιος για διαδικτυακό ξέπλυμα χρήματος θα πρέπει η τράπεζα να καλύπτεται από νομοθετικές διατάξεις που θα επιτρέπουν τον έλεγχο των λογαριασμών, κάτι το οποίο δεν επιδιώκεται γιατί μειώνεται η πελατεία τους, ή ο δράστης να πιαστεί επ' αυτοφόρω, κάτι σχεδόν αδύνατο.

3.10 Η ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ.

Η διαδικτυακή παιδική πορνογραφία εξελίσσεται στη πιο δημοφιλή και επικερδή εγκληματική μάστιγα καθώς διαθέτει υπερεθνικό χαρακτήρα, αποκτά ολοένα και μεγαλύτερες διαστάσεις και είναι ένα έγκλημα στο οποίο ο δράστης μπορεί να ανακαλυφθεί και αν αυτό γίνει τότε συγκεντρώνει πάνω του τα φώτα της δημοσιότητας.

Παιδική πορνογραφία είναι κάθε οπτικοακουστικό υλικό, ανεξαρτήτως του είδους του, όπως φωτογραφίες, video, δεδομένα ηλεκτρονικού υπολογιστή, που έχει κατασκευαστεί με τη χρήση ηλεκτρονικού, μηχανικού ή κάθε άλλου είδους μέσου και απεικονίζει παιδί ή δημιουργεί την εντύπωση ότι το πρόσωπο που απεικονίζεται είναι παιδί, να συμμετέχει ή να παρίσταται σε καταφανώς σεξουαλική πράξη ή έχει ως κύριο χαρακτηριστικό του την επίδειξη γεννητικών οργάνων ή της ηβικής χώρας του παιδιού για σεξουαλικό σκοπό. Επίσης κάθε οπτικοακουστικό υλικό που σκοπό έχει την παρότρυνση, υποβολή και υποκίνηση σε

πράξεις παιδεραστίας ή την προβολή ή παροχή πληροφοριών σχετικά με παιδί που μπορεί να χρησιμοποιηθεί για σκοπό σεξουαλικής εκμετάλλευσης.[65]

Ως <σκληρό> χαρακτηρίζεται το πορνογραφικό υλικό στο οποίο ο ανήλικος απεικονίζεται να συμμετέχει σε πραγματικές ή προσποιητές ή εικονικές σεξουαλικές δραστηριότητες αλλά και όταν απεικονίζονται κατά χυδαίο τρόπο μέρη του σώματός του. Ως πιο <ελαφριάς μορφής> χαρακτηρίζεται το πορνογραφικό υλικό το οποίο αφορά σε ερωτικής φύσεως εικόνες του ανήλικου, γυμνού ή όχι.

Εγκλήματα σχετικά με την παιδική πορνογραφία διαπράττει όποιος με πρόθεση:

- Παράγει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή.
- Προσφέρει ή διαθέτει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή.
- Διανέμει ή μεταδίδει παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή.
- Προμηθεύει ή προμηθεύεται παιδική πορνογραφία μέσω συστήματος ηλεκτρονικού υπολογιστή για τον εαυτό του ή για άλλον.
- Κατέχει παιδική πορνογραφία σε σύστημα ηλεκτρονικού υπολογιστή ή σε άλλο μέσο αποθήκευσης δεδομένων ηλεκτρονικού υπολογιστή.

Η παιδική πορνογραφία περιλαμβάνει πορνογραφικό υλικό, το οποίο δείχνει: α) ανήλικο που εμπλέκεται σε σαφή σεξουαλική συμπεριφορά, β) άτομο που παριστάνει τον ανήλικο και εμπλέκεται σε σαφή σεξουαλική συμπεριφορά ή γ) ρεαλιστικές εικόνες που παριστάνουν ανήλικο να εμπλέκεται σε σαφή σεξουαλική συμπεριφορά.

Το διαδίκτυο έδωσε τεράστια ώθηση στο χώρο της πορνογραφίας ανηλίκων και διευκόλυνε τη διαδικασία παραγωγής της, οδηγώντας τη σε ραγδαία αύξηση και επιτρέποντας τη διαμόρφωση ισχυρότατων κυκλωμάτων. Αυτό συνέβη γιατί το διαδίκτυο επιτρέπει τη πρόσβαση σε πορνογραφικό υλικό από όλο τον κόσμο, ανά πάσα στιγμή, από οπουδήποτε και με σχετικά χαμηλό κόστος και εξασφαλίζει φυσικά ανωνυμία και μυστικότητα, αφού ο χρήστης μπορεί πολύ εύκολα να αποκρύψει την ταυτότητά του. Επιπλέον διευκολύνει την άμεση επικοινωνία και την ανταλλαγή πορνογραφικού υλικού ανηλίκων όλων των ειδών και επιτρέπει την παρακολούθηση σεξουαλικής κακοποίησης- κακομεταχείρισης ανηλίκων σε πραγματικό χρόνο.

Στην Ελλάδα η παιδική πορνογραφία μέσω διαδικτύου αντιμετωπίζεται από το άρθρο 348^{A} του Ποινικού Κώδικα, το οποίο έχει δημιουργήσει ένα επαρκές νομικό πλαίσιο για τους δράστες οι οποίοι συλλαμβάνονται.

3.10.1 Ο ΟΡΟΣ GROOMING.[66]

Το grooming είναι η διαδικασία κατά την οποία παιδόφιλοι προσποιούνται ότι είναι έφηβοι και χρησιμοποιούν τα chat rooms για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν. Τα chat rooms φιλοξενούνται στο Διαδίκτυο και σε αυτά μπορεί να έχει πρόσβαση οποιοσδήποτε από οποιοδήποτε σημείο στον κόσμο. Συχνά θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο Διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους.

---

[65] βλ. Ζάννη Α., <Το διαδικτυακό έγκλημα>, σελ. 78

[66] www.saferinternet.gr

Οι παιδόφιλοι ξεκινούν συζητήσεις με τα πιθανά θύματα με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες.

Μέσα από την σχέση αυτή προκαλούν σιγά σιγά συζητήσεις σεξουαλικής φύσεως και πολλές φορές οι παιδόφιλοι στέλνουν στα υποψήφια θύματα φωτογραφίες παιδικής πορνογραφίας αλλά και πορνογραφίας ενηλίκων για να δώσουν την αίσθηση ότι αυτό είναι κάτι το αποδεκτό και φυσιολογικό. Η τακτική αυτή χρησιμοποιείται για να υπονομεύσει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή. Χρησιμοποιείται επίσης για να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.

3.10.2 Τρόποι Αντιμετώπισης.

Είναι γενικά αποδεκτό ότι η πλήρης εξάλειψη του φαινομένου της παιδικής πορνογραφίας και εκμετάλλευσης ανηλίκων από το διαδίκτυο είναι με τις σημερινές τεχνολογικές δυνατότητες και γνώσεις σχεδόν αδύνατη, εξαιτίας των χαρακτηριστικών του κυβερνοεγκλήματος. Δυνατή είναι ωστόσο, η μείωση του όγκου του επιδεικνυόμενου και διακινούμενου on line υλικού, καθώς και η αύξηση της δυσκολίας, της επικινδυνότητας και των πιθανοτήτων αναγνώρισης, εντοπισμού, σύλληψης και τιμωρίας όσων έχουν πρόσβαση, παράγουν, εκθέτουν και διακινούν τέτοιο υλικό στο διαδίκτυο. Για την επίτευξη των καλύτερων δυνατών αποτελεσμάτων στην προσπάθεια αντιμετώπισης του φαινομένου έχουν προταθεί και εφαρμόζονται μέτρα, τόσο δικαιικής όσο και μη δικαιικής φύσεως.

3.10.3 Οδηγίες προς τους γονείς.

Το διαδίκτυο προσφέρει εύκολα και γρήγορα ανεξάντλητες πηγές πληροφοριών και αποτελεί πλέον βασικό εργαλείο για την εκπαίδευση των παιδιών. Η πρόσβαση και η περιήγηση στο διαδίκτυο ωστόσο, σπάνια ακολουθείται από κάποια ενημέρωση για τους κινδύνους που αυτή ενέχει για τους ανήλικους, με δεδομένο μάλιστα ότι αυτοί συχνά χειρίζονται τους ηλεκτρονικούς υπολογιστές και τις παρεχόμενες από το διαδίκτυο υπηρεσίες με μεγαλύτερη άνεση από τους γονείς τους, οι οποίοι ωστόσο, φέρουν την πρωταρχική ευθύνη για την προστασία των παιδιών τους από την επαφή και την έκθεση σε βλαβερό και προσβλητικό για την προσωπικότητά τους υλικό στον κυβερνοχώρο και κάθε απόπειρα προσέγγισής τους από παραγωγούς παιδικής πορνογραφίας, παιδόφιλους και κάθε είδους εκμεταλλευτές ανηλίκων.

Οι γονείς οφείλουν επομένως να λαμβάνουν τα απαραίτητα μέτρα πρόληψης και προστασίας των παιδιών τους από κακόβουλες διαδικτυακές ενέργειες. Ειδικότερα, πρέπει να τοποθετούν τον ηλεκτρονικό υπολογιστή σε κεντρικά σημεία του σπιτιού, όπως στο σαλόνι ή στην κουζίνα, όπου το παιδί δε θα είναι απομονωμένο και με την οθόνη του στραμμένη προς το κέντρο του δωματίου, οπότε και θα έχουν οι γονείς τη δυνατότητα να επιβλέπουν τις δραστηριότητες και τις επαφές των ανηλίκων, να περιορίζουν το χρονικό διάστημα που παραμένουν συνδεδεμένοι στο διαδίκτυο και να είναι ιδιαίτερα προσεχτικοί όταν τα παιδιά χρησιμοποιούν τα δωμάτια συνομιλίας (chat rooms).Αντίθετα δε συνιστάται η πλήρης απαγόρευση πλοήγησης στο διαδίκτυο από τον οικιακό υπολογιστή, καθώς τα παιδιά μπορούν εύκολα να έχουν πρόσβαση σε υπολογιστή εκτός σπιτιού, χωρίς μάλιστα την επίβλεψη και τον έλεγχο των γονέων τους. Παράλληλα, οφείλουν οι γονείς να κάνουν την

πλοήγηση στο internet μια οικογενειακή δραστηριότητα, επισκεπτόμενοι από κοινού ιστοσελίδες με εκπαιδευτικό και κατάλληλο περιεχόμενο και διδάσκοντας τα παιδιά να χρησιμοποιούν μηχανές αναζήτησης και φυλλομετρητές προορισμένους για χρήση αποκλειστικά από παιδιά, ενώ επιβάλλεται να συζητούν με ευαισθησία για θέματα ασφαλείας και για τις ενδεχόμενες μελλοντικές απειλές μέσω του διαδικτύου, έτσι ώστε να κατανοήσουν τα ίδια τα παιδιά τους κινδύνους αυτούς.

Ταυτόχρονα πρέπει οι γονείς να διδάσκουν τα παιδιά τους να μη δίνουν προσωπικές πληροφορίες σε αγνώστους και κυρίως να μη συναντούν ζωντανά άτομα που γνώρισαν στο διαδίκτυο, χωρίς την παρουσία τους, ενώ απαιτείται να γνωρίζουν τους διαδικτυακούς φίλους των παιδιών τους, όπως ακριβώς κάνουν με τους φίλους της καθημερινής ζωής και να τα συμβουλεύουν να τους ενημερώνουν για κάθε είδους διαδικτυακή συναναστροφή και γνωριμία που δημιούργησαν, καθώς και για κάθε ενοχλητική, προσβλητική ή περίεργη εμπειρία που είχαν κατά την πλοήγηση στο διαδίκτυο.

Σε κάθε περίπτωση κρίνεται απαραίτητη η χρησιμοποίηση φίλτρων, ειδικών προϊόντων λογισμικού με στόχο την παρεμπόδιση της πρόσβασης σε τόπους του Κυβερνοχώρου με παράνομο ή επιβλαβές περιεχόμενο, ο έλεγχος του περιεχομένου του οπτικοακουστικού υλικού (cd, dvd, δισκέτες και άλλα) που αγοράζουν τα παιδιά ή που ανταλλάσσουν με τους φίλους τους αλλά και η διαρκής ενημέρωση των γονιών για τις εξελίξεις στο διαδίκτυο και τις αρμόδιες υπηρεσίες και ιστοσελίδες καταγγελίας, που μπορούν να συνδράμουν στο έργο τους.

3.10.4 Οδηγίες Προς Τα Παιδιά.

Τα παιδιά χειρίζονται πλέον με μεγαλύτερη ευκολία από τους γονείς τους ηλεκτρονικούς υπολογιστές, λόγω της καθημερινής και πολύωρης τριβής με αυτούς στο σχολείο και στο σπίτι. Κατά την πλοήγησή τους στον παγκόσμιο ιστό είναι πιθανό να συναντήσουν ενημερωτικές σελίδες και υλικό, ενώ παράλληλα είναι ενδεχόμενο να γνωρίσουν και να συνομιλήσουν με άγνωστα άτομα, κυρίως μέσα από τα <ανοιχτά δωμάτια επικοινωνίας>. Προς αποφυγή των κινδύνων, οι οποίοι ελλοχεύουν στο διαδίκτυο, τα ίδια τα παιδιά οφείλουν να ακολουθούν κάποιους κανόνες κατά την πλοήγησή τους στον κυβερνοχώρο.

Επιβάλλεται να μάθουν να μην απαντούν ποτέ σε πρόστυχα ή δελεαστικά online μηνύματα και να μιλούν πάντα στους γονείς τους ή σε κάποιον ενήλικο για εικόνες ή κείμενα που βρήκαν στο Διαδίκτυο και τους προκάλεσαν αισθήματα ανασφάλειας ή φόβου, ενώ παράλληλα θα πρέπει να τους γίνει συνείδηση ότι δε φέρουν καμία ευθύνη κι επομένως δεν πρέπει να αισθάνονται ντροπή και ενοχές όταν λαμβάνουν προσβλητικά μηνύματα ή μηνύματα που δεν κατανοούν ή ακόμη και απρεπείς εικόνες, οι οποίες τους είναι δυσάρεστες ή τους προκαλούν ταραχή και να ενημερώνουν για αυτές τους γονείς τους ή τον παροχέα υπηρεσιών δικτύου. Οφείλουν να προσέχουν όταν μιλούν μέσω chat room ή e- mail και να διακόψουν τη συνομιλία όταν κάποιοι τα κάνουν να νιώσουν άβολα και σε κάθε περίπτωση να διαφυλάσσουν τις προσωπικές τους πληροφορίες και ποτέ να μη δίνουν το όνομα και τη διεύθυνσή τους ή το όνομα και τη διεύθυνση του σχολείου τους, το τηλέφωνό τους και φωτογραφίες τους σε αγνώστους που συναντούν στο διαδίκτυο ακόμη και αν τους ζητηθεί. Κυρίως δε, δεν πρέπει να συναντούν κάποιον που γνώρισαν για πρώτη φορά στο διαδίκτυο, χωρίς να το αναφέρουν πρώτα στους γονείς τους προκειμένου να λάβουν την προηγούμενη έγκρισή τους και χωρίς να συνοδεύονται από κάποιον από αυτούς.

3.11 ΟΙ ΕΠΙΘΕΣΕΙΣ ΠΑΡΕΝΟΧΛΗΣΗΣ.

Με τον όρο παρενόχληση (cyberstalking ή harassment) περιγράφεται η εγκληματική συμπεριφορά όπου ο δράστης μέσω του διαδικτύου εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του για λόγους όπως εκδίκηση, επίλυση προσωπικών προβλημάτων και άλλα. Η συμπεριφορά αυτή, η οποία υπάρχει και εκτός διαδικτύου, με την εξάπλωση αυτού έχει λάβει τεράστιες διαστάσεις λόγω της δυνατότητας άμεσης επικοινωνίας από όποιο μέρος του κόσμου και αν βρίσκεται κανείς μέσω των καναλιών συζήτησης (chat), ή και του ηλεκτρονικού ταχυδρομείου. Την διαδικτυακή παρενόχληση τη διακρίνουμε σε άμεση, όταν ο δράστης στέλνει απευθείας τα μηνύματά του με το προσβλητικό ή απειλητικό περιεχόμενο στο θύμα του, ανεξάρτητα με το γεγονός αν οι απειλές του θα πραγματοποιηθούν και σε έμμεση, όταν το μήνυμα δε στέλνεται αμέσως στο θύμα αλλά σε τυχαίους χρήστες του διαδικτύου και περιλαμβάνει περιεχόμενο προσβλητικό ή απειλητικό για το θύμα.

3.12 Η ΠΡΟΠΑΓΑΝΔΑ ΜΙΣΟΥΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

Η προπαγάνδα μίσους στο διαδίκτυο συνίσταται στο εξευτελιστικό και υποτιμητικό περιεχόμενο που αναρτάται στο διαδίκτυο και στρέφεται εναντίον συγκεκριμένων εθνικών, ταξικών και φυλετικών ομάδων. Ο πιο διαδεδομένος τύπος είναι η ρατσιστική προπαγάνδα, κυρίως η φασιστική, η αντισημιτική και αυτή κατά των μαύρων. Βέβαια, υπάρχουν και διάφορες ιστοσελίδες με φανατικό θρησκευτικό περιεχόμενο, το οποίο προσβάλει πιστούς άλλων θρησκειών, ιστοσελίδες με ομοφοβικό περιεχόμενο, αλλά και ιστοσελίδες με ακραίο πολιτικό περιεχόμενο.

Το εύρος του διαδικτύου και η δυνατότητα επικοινωνίας μέσω αυτού με μέρη ανά τον κόσμο, δίνει τη δυνατότητα σε αυτές τις ομάδες να διαδίδουν τις ιδέες τους παγκοσμίως χωρίς ουσιαστικούς περιορισμούς και να προσελκύουν νέα μέλη με τρόπο ανέξοδο και αποτελεσματικό. Μέσω της νέας τεχνολογίας, οι χρήστες διαδικτύου μπορούν να έχουν πρόσβαση στις ομιλίες, στις συγκεντρώσεις και να διαβάσουν την αλληλογραφία που προηγουμένως θα παρεδίδετο προσωπικά ή ταχυδρομικά.

Οι ομάδες μίσους μπορούν να στέλνουν μεταξύ τους μηνύματα μέσω του ηλεκτρονικού ταχυδρομείου, ενώ μέσω των ανώνυμων mailers ενημερώνονται χιλιάδες άτομα.

Το πιο εντυπωσιακό στοιχείο αυτών των ομάδων είναι ότι εκφράζουν με ωμή ειλικρίνεια την έχθρα τους και δίνουν συμβουλές στα μέλη τους γα να αντιμετωπίζουν τους αντιπάλους, οι οποίες μπορεί να κυμαίνονται από σχετικές με σαμποτάζ, δολοφονίες και τρομοκρατικές επιθέσεις, μέχρι και πιο ήπιες μορφές όπως συκοφάντηση μέσω διαδικτύου.

3.13 ΤΡΟΠΟΙ ΕΞΙΧΝΙΑΣΗΣ.

Το ηλεκτρονικό έγκλημα και ιδιαίτερα το κυβερνοέγκλημα, κομμάτι του οποίου είναι η διαδικτυακή πορνογραφία και εκμετάλλευση ανηλίκων, παρουσιάζει σημαντικές δυσκολίες

κατά τη διερεύνηση και αντιμετώπισή του, εξαιτίας των ιδιαίτερων χαρακτηριστικών του γνωρισμάτων.[67]

Το έγκλημα στον Κυβερνοχώρο είναι εύκολο στην τέλεσή του, γρήγορο και διασυνοριακό, αφού τα αποτελέσματά του μπορεί να επέλθουν ταυτόχρονα σε πολλούς τόπους. Διαπράττεται σε χρόνο δευτερολέπτων, χωρίς πολλές φορές να γίνεται αντιληπτό ούτε από το ίδιο το θύμα, ενώ ο δράστης ενεργεί από το γραφείο ή το σπίτι του μέσω του υπολογιστή του, χωρίς να χρειαστεί να μετακινηθεί, αφήνοντας πίσω του μονάχα ψηφιακά ίχνη, των οποίων η ανίχνευση απαιτεί εξειδικευμένη τεχνογνωσία και χρήση εξελιγμένης τεχνολογίας. Οι δράστες των διαδικτυακών εγκλημάτων, ιδιαίτερα των σεξουαλικών εγκλημάτων, αποκρύπτουν την πραγματική τους ταυτότητα και αποστέλλουν ηλεκτρονικά μηνύματα, συμμετέχουν σε δημόσιες on-line συζητήσεις και προσεγγίζουν τα θύματά τους εμφανιζόμενοι με ψευδή στοιχεία. Επιπλέον, ο τεράστιος όγκος μεταφερόμενων πληροφοριών και η μεγάλη επισκεψιμότητα ιστοσελίδων με παράνομο περιεχόμενο, καθιστά δύσκολη τη διερεύνηση, τον εντοπισμό και τον έλεγχο τόσο του περιεχομένου όλων των ιστοσελίδων, όσο και των επισκεπτών τους.

Η διερεύνηση των ηλεκτρονικών και διαδικτυακών εγκλημάτων άλλωστε, είναι αρκετά δύσκολη και ιδιαίτερα χρονοβόρος, καθώς για τον εντοπισμό των <ηλεκτρονικών ιχνών> η έρευνα μπορεί να διαρκέσει από ένα μήνα έως και δύο χρόνια. Αυτό συμβαίνει διότι οι διερευνώμενοι χρήστες του internet λαμβάνουν μέτρα προστασίας, τα οποία καθιστούν τον εντοπισμό τους ιδιαίτερα δύσκολο. Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του <ηλεκτρονικού ίχνους> του δράστη, το οποίο για κάθε χρήστη του internet είναι μοναδικό και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο. Κυριότερες πηγές ψηφιακών αποδείξεων αποτελούν:
α. Ο *υπολογιστής του παραβάτη*, στον σκληρό δίσκο του οποίου συνήθως ανευρίσκονται αποθηκευμένες πορνογραφικές αναπαραστάσεις ή αποκαλύπτονται με τη βοήθεια εξειδικευμένων τεχνικών αρχεία και στοιχεία κρυφά ή αόρατα με γυμνό μάτι, όπως η ημερομηνία, η ώρα και η διάρκεια περιήγησης στο διαδίκτυο, οι ιστοσελίδες που ο παραβάτης επισκέφτηκε, με ποιους συνομίλησε και άλλα.
β. *Βοηθητικές συσκευές*, οι οποίες χρησιμοποιούνται παράλληλα με τον Η/Υ για την παραγωγή και διακίνηση υλικού παιδικής πορνογραφίας, όπως ψηφιακές κάμερες, φωτογραφικές μηχανές και κινητά τηλέφωνα, συσκευές στις κάρτες μνήμης των οποίων καταγράφονται οι παράνομες δραστηριότητες κι από τις οποίες συνήθως γίνεται uploading στο διαδίκτυο.
γ. *Παροχείς υπηρεσιών διαδικτύου*, οι οποίοι δίνουν πληροφορίες και με τη βοήθεια των οποίων καθίσταται δυνατός ο εντοπισμός χρηστών παιδικής πορνογραφίας, μέσω ενός μοναδικού για κάθε χρήστη ψηφιακού αριθμού ταυτότητας, του IP, ο οποίος εκτός από τα προσωπικά στοιχεία του ιδιοκτήτη του, όνομα, διεύθυνση και τα λοιπά, δίνει πληροφορίες για τις ιστοσελίδες και τα αρχεία τα οποία επισκέφτηκε.
δ. ***Online*** *δραστηριότητα.* Οι μηχανές διαδικτυακής αναζήτησης επιτρέπουν στις διωκτικές αρχές την καταγραφή της διαδικτυακής δραστηριότητας και της συμμετοχής παιδόφιλων στα δωμάτια ανοιχτής επικοινωνίας, όπως αυτή αποκαλύπτεται μέσω του προσωπικού IP αριθμού τους.

Τέλος, η καταγραφή της εγκληματικότητας στον κυβερνοχώρο ελάχιστα ανταποκρίνεται στην πραγματικότητα, διότι ελάχιστες περιπτώσεις εγκλημάτων του Κυβερνοχώρου,

[67] Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, <Έγκλημα στον Κυβερνοχώρο>, Ν/2000, σελ. 667- 668 και Δ. Αγγελόπουλος –Ι. Πάσχος, <Κατάσχεση- Ανάλυση ψηφιακών πειστηρίων>, Ποινική Δικαιοσύνη Τεύχος 4/2003, σελ. 439.

καταγγέλλονται διεθνώς. Ειδικότερα, όσον αφορά στις περιπτώσεις παιδικής πορνογραφίας και online σεξουαλικής κακοποίησης και εκμετάλλευσης ανηλίκων μέσω του διαδικτύου, υπάρχει τεράστιος σκοτεινός αριθμός, ο οποίος οφείλεται κυρίως στο φόβο επαναθυματοποίησης του ήδη θυματοποιημένου ανηλίκου, στις πιέσεις της οικογένειας προς αποφυγή της δημοσιότητας και στην πίστη των θυμάτων ότι κινδυνεύει η υπόληψή τους, στο φόβο τους για ενδεχόμενο <κοινωνικό> στιγματισμό, αλλά και στην έλλειψη εμπιστοσύνης στην αποτελεσματικότητα της ποινικής δικαιοσύνης. Γίνεται λοιπόν κατανοητό ότι η γνωστοποίηση του εγκλήματος, εξαιτίας τόσο του περιβάλλοντος στο οποίο λαμβάνει χώρα και της ανωνυμίας που αυτό προσφέρει, όσο και των ιδιαίτερων χαρακτηριστικών του ως σεξουαλικό έγκλημα, είναι πολύ πιο μικρή σε σχέση με αυτή του <κοινού> εγκλήματος. Κατά συνέπεια, το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου είναι <ακόμα πιο σκοτεινό>, από ότι στον κοινό εγκληματικό χώρο.

ΚΕΦΑΛΑΙΟ 4

ΝΟΜΟΘΕΣΙΑ ΗΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

4.1 ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.

Το διαδίκτυο έχει εισβάλλει στην ζωή των ανθρώπων σε ολόκληρο τον κόσμο και μας έχε γίνει πια απαραίτητο. Μας παρέχει πρόσβαση σε μια τεράστια δεξαμενή πληροφοριών, βοηθάει σημαντικά στην εργασία μας, μας ψυχαγωγεί. Δυστυχώς, όμως, παράλληλα διευκολύνει και τους εγκληματίες, οι οποίοι εκμεταλλεύτηκαν τις νέες δυνατότητες της τεχνολογίας για να επεκτείνουν την παράνομη δράση τους. Έτσι ένας νέος όρος μπήκε στη ζωή μας τα τελευταία χρόνια: το λεγόμενο «Ηλεκτρονικό Έγκλημα». Το διαδίκτυο μπορεί να αποτελέσει πρόσφορο πεδίο εκδήλωσης ποικίλων εγκληματικών συμπεριφορών. Αυτό οφείλεται κυρίως στις απεριόριστες δυνατότητες που προσφέρει και ιδίως, στην ανωνυμία που παρέχει. Οφείλεται, επίσης, και στα νομοθετικά κενά καθώς η νομοθεσία παραδοσιακά παρακολουθεί από απόσταση τις τεχνολογικές εξελίξεις. Στο διαδίκτυο βρίσκει πεδίο εφαρμογής η βασική αρχή που θέλει την ανθρώπινη δραστηριότητα και την κοινωνική πραγματικότητα να προπορεύονται της νομοθετικής τους ρύθμισης.

Εικόνα 1[68]

Ηλεκτρονικό έγκλημα θεωρείται η αξιόποινη πράξη, που τελείται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνικη νομοθεσία. Χωρίζεται σε α) έγκλημα τελούμενο με τη χρήση ηλεκτρονικών υπολογιστών και μόνο, χωρίς τη χρήση διαδικτύου (computer crime) και β) σε κυβερνοέγκλημα (cyber crime).

Τα κυριότερα χαρακτηριστικά του κυβερνοεγκλήματος είναι:

- η διαπραξη της αξιόποινης πράξης λαμβάνει χώρα χωρίς τη μετακίνηση του δράστη και μέσα σε σύντομο χρόο
- το έγκλημα πλέον δεν έχει σύνορα και ισχύει διαφορετική νομοθεσία σε κάθε κράτος
- τα ίχνη που αφήνονται είναι μόνο ψηφιακά, ο δράστης έχει πολλές ταυτότητες και καλύπτεται πίσω από την ανωνυμία
- ο δράστης κατέχει εξειδικευμένες γνώσεις πάνω στη χρήση των υπολογιστών
- το cracking και hacking (δλδ. η πρόσβαση χωρίς δικαίωμα σε ένα δίκτυο υπολογιστών)

[68] https://www.google.gr/

Εικόνα 2[69]

Οι κυριότερες μορφές που λαμβάνει το ηλεκτρονικό έγκλημα είναι:[70]

- η πορνογραφία ανηλίκων
- τα εγκλήματα περί τα ήθη
- οι απάτες μέσω διαδικτύου (π.χ. με πιστωτικές κάρτες)
- η παράνομη διείσδυση σε υπολογιστικά συστήματα
- η διακίνηση πειρατείας λογισμικού (δλδ. η παράνομη και χωρίς εξουσιοδότηση αναπαραγωγη ή και διάθεση προγραμμάτων ηλεκτρονικού υπολογιστή, τα οποία προστατεύονται από τους νόμους περί πνευμτικών δικαιωμάτων)
- η διακίνηση ναρκωτικών ουσιών και όπλων
- η σωματεμπορία
- η υφαρπαγή προσωπικών δεδομένων
- τα εγκλήματα στα chat rooms – facebook κ.λ.π. (όπως π.χ. η απωπλάνηση ανηλίκου) καθώς και η ηθική αυτουργία σε ανθρωποκτονία
- το cyberbullying (δλδ. η εγκληματική συμπεριφορά, όπου ο δράστης, μέσω του Διαδικτύου,εκφοβίζει, απειλεί, εκβιάζει και γενικότερα παρενοχλεί τα θύματά του).

[69] https://www.google.gr/
[70] Βλ. Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα», σελ 71

Εικόνα 3

4.2 ΠΟΙΝΙΚΗ ΝΟΜΟΘΕΣΙΑ ΣΧΕΤΙΚΑ ΜΕ ΤΗ ΧΡΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ.

Ανάλογα με τη μορφή τους, τα εγλήματα αυτά έχουν πολλές και σοβαρές επιπτώσεις αφού μπορούν να βλάψουν την περιουσία μας, να προσβάλλουν τη γενετήσια αξιοπρέπειά μας, να απειλήσουν την ιδιωτικότητα, την ασφάλεια, την υγεία ακόμα και την ίδια τη ζωή μας.
Στην ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα Διαδικτύου και ρυθμίζει τη συμπεριφορά των χρηστών του Διαδικτύου από άποψη Ποινικού Δικαίου. Ενδεικτικά, αξίζει να αναφέρουμε **την ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (ν.2472/1997 όπως τροποποιήθηκε με τον ν.3674/2008).** Στον Ποινικό Κώδικα**,** υπάρχει το ειδικό άρθρο **386^{A}(απάτη με υπολογιστή),** σύμφωνα με το οποίο, όποιος με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία,επηρεάζοντας τα αρχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές φυλάκισης που προβλέπονται για την απάτη. Ανάλογα με τη βαρύτητα του αδικήματος, οι ποινές αυτές μπορούν να ανέρχονται από φυλάκιση τριών μηνών έως φυλάκιση τουλάχιστον τριών ετών αν η ζημιά που προκλήθηκε είναι ιδιαίτερα μεγάλη. Επίσης, το άρθρο 348^{A} τιμωρεί με φυλάκιση και χρηματικές ποινές και την και την πορνογραφία ανηλίκων, που διακινείται μέσω του Διαδικτύου. Να σημειώσουμε ότι μπορούν να έχουν εφαρμογή και μια σειρά από άλλα άρθρα του Ποινικού Κώδικα, αφού στις μέρες μας τα παραδοσιακά εγκλήματα μπορούν να πάρουν μια άλλη μορφή και να τελεσθούν και μέσου του Διαδικτύου (π.χ. το άρθρο 148 περί κατασκοπείας, το άρθρο 164 που αφορά τη νόθευση εκλογής, το άρθρο 362 για τη δυσφήμιση και πολλά άλλα).

Ο Ποινικός Κώδικας περιλαμβάνει μια σειρά από άρθρα που αφορούν την καταστολή του ηλεκτρονικού εγκλήματος. Αυτά είναι:

4.2.1 Άρθρο 13 εδ. Γ ΠΚ – Έννοια εγγράφου.[71]

Ως έγγραφο θεωρείται κάθε μέσο που χρησιμοποιείται από ηλεκτρονικό υπολογιστή για εγγραφή, αποθήκευση, παραγωγή, αναπαραγωγή πληροφοριών και στοιχείων. Τέτοια μέσα θεωρούνται οι δισκέτες, οι σκληρή δίσκοι καθώς και γενικότερα τα συστήματα αποθήκευσης ηλεκτρονικών πληροφοριών. Από την νομολογία ο του Αρείου Πάγου έχει γίνει δεκτό ότι ως έγγραφα θεωροούνται ακόμα και οι φωτογραφίες, κινηματογραφικές παραστάσεις, φωνοληψίες, και κάθε είδους μηχανική απεικόνιση. Κάθε αυθαίρετη παρέμβαση σε αυτά τα έγγραφα, είτε με τη μορφή κατάρτισης, είτε με τη μορφή νόθευσης και με μέσω του διαδικτύου, υπάγεται στις διατάξεις του ΠΚ για πλαστογραφία.

4.2.2 Άρθρο 348 ΠΚ – Πορνογραφία ανηλίκων.

Το έγκλημα αυτό τελούν όσοι: α) κατέχουν παιδικό πορνογραφικό υλικό, το οποίο έχουν λάβει από το διαδίκτυο, β) δημιουργούν τέλειο υλικό και το διακινούν στο διαδίκτυο και γ) όσοι έχουν στο διαδίκτυο τέτοιο υλικό και επιτρέπουν την πρόσβαση σε αυτό έναντι αμοιβής. Το έγλημα αυτό, ενώ ανήκε στα λεγόμενα «παραδοσιακά», έχει εξαπλωθεί δραματικά και έχει μεταλλαχθεί ποιοτικά με τη χρήση του διαδικτύου.

4.2.3 Άρθρο 348 Β ΠΚ – Προσέλκυση παιδιών για γενετήσιους λόγους.

Το έγκλημα αυτό το τελεί και αυτός που μέσω διαδικτύου προτείνει σε ενήλικο να συναντήσει ανήλικο που δεν συμπλήρωσε τα 15 του χρόνια προκειμένου να τελέσει μαζί του τα εγκλήματα, είτε της αποπλάνησης, είτε της πορνογραφίας ανηλίκων. Με τη διάταξη αυτή επιδιώκεται η πάταξη της άγρας ανηλίκων για σεξουαλικούς σκοπούς, που τελείται μέσω του διαδικτύου.

4.2.4 Άρθρο 363 ΠΚ – Συκοφαντική δυσφήμηση.

Το έγκλημα αυτό μπορεί να τελεστεί και μέσω του διαδικτύου, με αναρτήσεις, ανακοινώσεις, φωτογραφικό υλικό κλπ. Έχει κριθεί ότι το έγκλημα αυτό τελεί: α) αυτός που δημοσιεύει για άλλον συκογαντικά γεγονότα σε ηλεκρονικό έντυπο π.χ. σε ηλεκτρονική εφημερίδα, β) αυτος που συντάσσει συκοφαντική ηλεκτρονική επιστολή για άλλον και την απευθύνει μέσω διαδικτύου σε άλλα πρόσωπα, αυτός που αναρτά στο διαδίκτυο αποκαλυπτικές – άσεμνες φωτογραφίες ενός προσώπου ή άλλα προσωπικά δεδομένα του (π.χ. τηλέφωνα, email, διεύθυνση κλπ.) και διαδίδει ψευδή γεγονότα ως αληθινά. Στις περιπτώσεις αυτές παραβιάζονται και οι διατάξεις της νομοθεσίας για την προστασία των προσωπικών δεδομένων (ν. 2472/1997).

[71] https://www.e-nomothesia.gr

4.2.5 Άρθρο 386 ΠΚ – Απάτη.

Οι ψευδείς παραστάσεις – που απαιτεί ο νόμος να συντρέχουν για να στοιχειοθετηθεί το έγκλημα της απάτης – που οδήγησαν στην παραπλάνηση του παθόντα ή την πρόκληση της ζημιάς σε αυτόν, μπορούν να γίνουν και μέσω διαδικτύου. Τόπος τέλεσης της πράξης είναι τόσο ο τόπος των ψευδών παραστάσεων όσο και ο τόπος όπου επήλθε η ζημία (ΑΠ 1080/1995).

4.2.6 Άρθρο 386 Α ΠΚ – Απάτη με υπολογιστές.

Το έγκλημα αυτό τελείται συνήθως με την διαδικτυακή παρέμβαση σε λογαριασμούς τραπεζών με συνέπεια να γίνει μεταφορά χρημάτων από το λογαριασμό του παθόντα στο λογαριασμό του δράστη. Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας το αποτέλεσμα της διαδικασίας επεξεργασίας ψηφιακών δεδομένων είτε με τη μη ορθή διαμόρφωση προγράμματος υπολογιστή είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με τη χωρίς δικαίωμα χρήση δεδομένων είτε με τη χωρίς δικαίωμα παρέμβαση σε πληροφοριακό σύστημα, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα άτομα.

4.3 ΤΟ ΗΛΕΚΤΡΟΝΙΚΌ ΔΙΑΔΙΚΤΥΑΚΌ ΕΓΚΛΗΜΑ ΣΤΗΝ ΕΛΛΆΔΑ: ΜΟΡΦΈΣ ΚΑΙ ΝΟΜΟΘΕΤΙΚΉ ΑΝΤΙΜΕΤΏΠΙΣΉ ΤΟΥ

4.3.1 - Το Ελληνικό Νομοθετικό Πλαίσιο Για Το Ηλεκτρονικό Διαδικτυακό Έγκλημα.

Οι ηλεκτρονικοί υπολογιστές έκαναν την εμφάνιση τους στην Ελλάδα πολύ αργότερα από ότι εμφανίστηκαν στις ΗΠΑ ενώ το διαδίκτυο άρχισε να χρησιμοποιείται στη χώρα μας μόλις το 1990, από πανεπιστημιακά ιδρύματα και πολύ αργότερα άρχισε να χρησιμοποιείται από τα άτομα μεμονωμένα. Επίσης το ηλεκτρονικό διαδικτυακό έγκλημα τότε δεν ήταν πολύ διαδεδομένο, ούτε καν στις ΗΠΑ, πόσο μάλλον στην χώρα μας, για αυτό είναι λογικό και αναμενόμενο ότι η ελληνική ποινική έννομη τάξη δεν διέθετε ποινικές διατάξεις για την αντιμετώπιση αυτού του νέου ποινικού φαινομένου, το οποίο εξελισσόταν διαρκώς και εκδηλωνόταν μέσα από νέες μορφές.

Πριν από το νόμο 1805/1988, ο οποίος ήταν ο πρώτος νόμος ο οποίος επιχείρησε να εισάγει ποινικές διατάξεις για την προστασία από την κακή χρήση των ηλεκτρονικών υπολογιστών, οι περισσότερες διατάξεις του Ποινικού Κώδικα και των Ειδικών Ποινικών Νόμων, ήταν διαμορφωμένες για να προστατεύουν περιπτώσεις απτής βλάβης ή διακινδύνευσης σε έννομα αγαθά και απτές προσβολές ενσώματων αντικειμένων, ούσες φυσικά προσαρμοσμένες στην κοινωνική κατάσταση που επικρατούσε μέχρι τότε. Έτσι, οι πράξεις πληροφορικού (τότε) εγκλήματος, οι οποίες βέβαια ήταν σπάνιες, όποτε συνέβαιναν δεν πληρούσαν την αντικειμενική υπόσταση κανενός από τα εγκλήματα που τυποποιούνταν στον Π.Κ. και έτσι δεν υπήρχε ουσιαστική ποινική αποτροπή για την τέλεση τους.

Υπό το προϊσχύον νομοθετικό πλαίσιο[72] (πριν το νόμο 1805/1998) η ηλεκτρονική, και ουσιαστικά πληροφορική, εγκληματικότητα στην Ελλάδα σχετιζόταν με τα παρακάτω εγκλήματα:

Με το έγκλημα της κλοπής: Με την πρώιμη εμφάνιση των ηλεκτρονικών υπολογιστών στην Ελλάδα υπήρξαν εγκλήματα κλοπής πληροφοριών από αυτούς, με τη μορφή δεδομένων ή προγραμμάτων. Ο ελληνικός Π.Κ. για την πλήρωση της αντικειμενικής υπόστασης της κλοπής απαιτούσε αντικείμενο της να είναι πράγματα, δηλαδή ενσώματα αντικείμενα, επομένως η κλοπή ηλεκτρονικών προγραμμάτων ή δεδομένων δε μπορούσε να ενταχθεί στις διατάξεις των άρθρων 372 επ. και 375 επ. Π.Κ., αφού δεν μπορούσαν να αποτελέσουν υλικά αντικείμενα κλοπής ή υπεξαίρεσης ενώ περίπτωση που αυτά εκλαμβάνονταν ως ενσώματα αντικείμενα, αυτό θα συνιστούσε απαγορευμένη αναλογία. Πράγματα αποτελούν μόνο τα υλικά μέρη στα οποία αποτυπώνονταν αυτές οι πληροφορίες (όπως οι δισκέτες, οι σκληροί δίσκοι) τα οποία ως ενσώματα αντικείμενα ήταν δυνατόν να αποτελέσουν το αντικείμενο της κλοπής.

Με το έγκλημα της «κλοπής χρόνου»: Το έγκλημα αυτό είναι ουσιαστικά η εκμετάλλευση ενός ξένου ηλεκτρονικού υπολογιστή, όσον αφορά στα εξωτερικά-μηχανικά του μέρη, αλλά και στο λογισμικό του. Αυτό το έγκλημα δεν μπορούσε να αντιμετωπιστεί ούτε με τη διάταξη για την κλοπή χρήσης (αφού προφανώς ο ηλεκτρονικός υπολογιστής δεν είναι μηχανοκίνητο μεταφορικό μέσο) αλλά ούτε και ως κλοπή ηλεκτρικής ενέργειας (α. 372§2 Π.Κ.) αφού ο δράστης δεν έχει σκοπό την ιδιοποίηση του ηλεκτρικού ρεύματος και ούτε οι πληροφορίες που είναι αποθηκευμένες σε έναν ηλεκτρονικό υπολογιστή μπορούν να εξομοιωθούν με ενέργεια.

Με το έγκλημα της πλαστογραφίας: Τη θεωρία και τη νομολογία απασχόλησε το ζήτημα αν η χωρίς δικαίωμα αντιγραφή ή αλλοίωση προγραμμάτων ή δεδομένων μπορούσε να αντιμετωπιστεί με τη διάταξη περί πλαστογραφίας (α. 216 Π.Κ.). Η κρατούσα άποψη απαντούσε θετικά με την αποδοχή ότι οι δισκέτες και οι λοιποί υλικοί φορείς δεδομένων αποτελούσαν έγγραφα ήδη από το προηγούμενο νομοθετικό καθεστώς. Από το 1983 η νομολογία του Αρείου Πάγου χαρακτήρισε τις μαγνητοταινίες ως έγγραφα έτσι ώστε να είναι δυνατό να χαρακτηρισθεί η παράνομη αναπαραγωγή και εκμετάλλευση τους ως πλαστογραφία σε βαθμό κακουργήματος, καθότι το μέχρι τότε νομικό πλαίσιο δεν ήταν ικανό να αποτρέψει αυτές τις προσβολές. Η νομολογία αλλά και η θεωρία κατέληξε σε αυτό το πόρισμα εκλαμβάνοντας ότι ουσιώδης προϋπόθεση για την ύπαρξη εγγράφου είναι το νοηματικό του περιεχόμενο να είναι προσιτό στις αισθήσεις, οπότε πλέον αποδεικνύει μέσω του νοήματος του και όχι μέσω της απλής υλικής του ύπαρξης. Ακόμα όμως και με αυτή τη διεύρυνση της έννοιας του εγγράφου, με το προ του ν. 1805/1988 νομοθετικό πλαίσιο, στην έννοια του εγγράφου δε μπορούσαν να υπαχθούν τα πληροφορικά προγράμματα και δεδομένα αφού στην κανονική τους μορφή απευθύνονται στο hardware του ηλεκτρονικού υπολογιστή, το οποίο αναλαμβάνει να τα αποκωδικοποιήσει και κατόπιν εμφανίζονται στην οθόνη του υπολογιστή «μεταφρασμένα» ώστε να είναι κατανοητά από τους χρήστες. Επομένως αφού στην αρχική τους μορφή είναι ακατανόητα από τον άνθρωπο και πάλι υπό το προϊσχύον νομοθετικό καθεστώς θα συνιστούσε απαγορευμένη αναλογία να χαρακτηρισθούν ως έγγραφα.

[72] Σχετικά Μυλωνόπουλος Χ. «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 22.

Παρατηρούμε λοιπόν ότι μέχρι το 1988, η ελληνική ποινική έννομη τάξη δε διέθετε νομοθετικό πλαίσιο ικανό να αντιμετωπίσει τα ηλεκτρονικά/πληροφορικά εγκλήματα. Και αυτό συνέβαινε διότι όταν ο νομοθέτης διαμόρφωσε τα άρθρα του Ποινικού Κώδικα, ούτε καν μπορούσε να έχει εικόνα για τις αλλαγές που θα επέφερε η εξέλιξη τη τεχνολογίας των ηλεκτρονικών υπολογιστών στον τομέα των συναλλαγών και εν γένει της κοινωνικής ζωής. Οι κοινωνικές και τεχνολογικές συνθήκες των αρχών του 20ου αιώνα δεν έδιναν τη δυνατότητα στον έλληνα ποινικό νομοθέτη να εισάγει διατάξεις στον Κώδικα που θα προϋπέθεταν ως μέσα τέλεσης του εγκλήματος αυτοματοποιημένες μηχανές, ώστε μέσω της διασταλτικής ερμηνείας του νόμου να καλύπτεται η σχετική παράνομη συμπεριφορά. Όταν πλέον επήλθε η αλματώδης ανάπτυξη της τεχνολογίας και η παγκόσμια εξάπλωση των ηλεκτρονικών υπολογιστών και του διαδικτύου, ήταν επόμενο ο ποινικός νομοθέτης να οδηγηθεί σε εισαγωγή νέων ποινικών διατάξεων, ώστε να συγχρονισθεί η έννομη τάξη με τις τεχνολογικές και κοινωνικές εξελίξεις και να μη μένουν ατιμώρητες νέες μορφές αθέμιτης συμπεριφοράς οι οποίες δεν καλύπτονταν από τις υπάρχουσες διατάξεις του Π.Κ. Απόρροια της προσπάθειας αυτής είναι και η εισαγωγή του Ν. 1805/1988[73] με τον οποίο προστέθηκαν στον ΠΚ τα άρθρα 13 εδάφιο β, περίπτωση γ, 370Β, 370Γ και 386Α.

Όπως αναφέρεται στην Εισηγητική Έκθεση του Ν. 1805/1988, σκοπός αυτού είναι «η θέσπιση ειδικών ποινικών διατάξεων για τη διασφάλιση της γνησιότητας των στοιχείων που εγγράφονται και αποθηκεύονται στους ηλεκτρονικούς υπολογιστές ή παράγονται και αναπαράγονται από αυτούς (ύστερα από εισαγωγή της πληροφορίας στη χώρα μας)» ενώ κρίθηκε αναγκαία η πρόβλεψη ειδικής ποινικής προστασίας για αυτό το ζήτημα «γιατί η αξιόποινη δραστηριότητα, η οποία μπορεί να αναπτυχθεί στον τομέα της πληροφορικής, δεν καλύπτεται πλήρως από την υπάρχουσα ποινική νομοθεσία ενώ η νέα αυτή μορφή τεχνολογίας μπορεί να ανοίξει δρόμους σε νέες, άγνωστες και με εφαρμογές αντίστοιχης τεχνολογίας μεθόδους εγκληματικής δράσης, οι οποίες δεν προβλέπονται από τον Π.Κ. και τους ισχύοντες ειδικούς ποινικούς νόμους»

Με το νόμο 1805/1988, ο οποίος είναι επηρεασμένος από το γερμανικό Δεύτερο Νόμο για την Οικονομική Εγκληματικότητα (2.WiKG) του 1986, επιχειρείται η προσαρμογή στις νέες τεχνολογικές εξελίξεις, η κάλυψη των νομικών κενών και των περιπτώσεων αθέμιτης συμπεριφοράς που δεν υπάγονταν στα υπάρχοντα άρθρα του Π.Κ. και γίνεται προσπάθεια επίλυσης των ζητημάτων του ηλεκτρονικού διαδικτυακού εγκλήματος και γενικά των εγκλημάτων που τελούνται μέσω ηλεκτρονικού υπολογιστή.

Αξιοσημείωτο είναι ότι μετά την εισαγωγή αυτών των διατάξεων, οι οποίες αναλύονται παρακάτω, αλλά και στα μεταγενέστερα χρόνια και μέχρι σήμερα, στο ελληνικό ποινικό δίκαιο δεν υπάρχουν επίσημοι ορισμοί του διαδικτύου και του κυβερνοχώρου, επομένως ο ορισμός τους είναι δανεικός από την τεχνολογία. Διαδίκτυο λοιπόν είναι ένα πλέγμα ψηφιακών γραμμών, το οποίο συνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα ανά τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών και εργαλείων. Ουσιαστικά είναι ένα παγκόσμιο δίκτυο ηλεκτρονικών υπολογιστών συνδεδεμένων μεταξύ τους μέσω αυτού, το οποίο αποτελείται από πολλά μικρότερα δίκτυα. Πιο απλοποιημένα δηλαδή είναι η παγκόσμια συλλογή δικτύων και πυλών που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ τους. Κυβερνοχώρος είναι το σύνολο των ηλεκτρονικών κόσμων, όπως το διαδίκτυο, στο οποίο οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων ηλεκτρονικών υπολογιστών και η επικοινωνία είναι ανεξάρτητα από την υλική υπόσταση[74]

[73] ΦΕΚ Α 199/31.08.1988.
[74] Ζάννη Α., «Το διαδικτυακό έγκλημα», σελ. 192

4.3.2 ΟΙ ΔΙΑΤΑΞΕΙΣ ΤΟΥ Π.Κ. ΓΙΑ ΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.

Το άρθρο 13γ ΠΚ

«Στον Κώδικα οι ακόλουθοι όροι χρησιμοποιούνται με την εξής σημασία: …..γ) έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο στο οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία".»
Σύμφωνα με την εισηγητική έκθεση του ν. 1805/1988, με το νέο περιεχόμενο του αρ. 13γ Π.Κ., διευρύνεται η έννοια του εγγράφου έτσι ώστε ως έγγραφα να θεωρούνται τα μέσα που χρησιμοποιούνται από ηλεκτρονικό υπολογιστή με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, τα οποία δεν μπορούν να διαβαστούν άμεσα. Επίσης με το νέο αυτό νόμο έγγραφο είναι και κάθε μαγνητικό ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο, ή ήχος αυτοτελώς το καθένα ή και συνδυασμένα μεταξύ τους. Έτσι, πλέον ως έγγραφα αντιμετωπίζονται ο σκληρός δίσκος, το cd, το dvd, το χαρτί του εκτυπωτή κλπ. Το ίδιο ισχύει και για βάσεις δεδομένων εφόσον έχουν αποθηκευτεί κατά τρόπο ηλεκτρομαγνητικό ή οπτικό[75] . Με τη διατύπωση αυτή επιδιώκεται η προσαρμογή της νομοθεσίας στις τεχνολογικές εξελίξεις αλλά και η εναρμόνιση της με την ως τότε πάγια νομολογία του Α.Π. και την έννοια του εγγράφου του α. 444ΚΠολΔ, η οποία πριν το ν. 1805/ 1988 κάλυπτε μόνο ως έγγραφο κάθε μαγνητικό ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο, ή ήχος αυτοτελώς το καθένα ή και συνδυασμένα μεταξύ τους.
Η ηλεκτρονική επιστολή αποτελεί έγγραφο διότι είναι κείμενο αποθηκευμένο στον ηλεκτρονικό υπολογιστή του παραλήπτη αλλά και του αποστολέα και σταθερά ενσωματωμένη στο σκληρό δίσκο, το οποίο συνοδεύεται και από τα στοιχεία ταυτότητας του αποστολέα της (όνομα αποστολέα σε συνδυασμό με τη ψηφιακή του διεύθυνση), επομένως αναγράφει το όνομα του εκδότη του.

Επίσης και οι ιστοσελίδες αποτελούν έγγραφο, αφού τα δεδομένα της ιστοσελίδας είναι αποθηκευμένα σε μέσο που χρησιμοποιείται από ηλεκτρονικό υπολογιστή , και πιο συγκεκριμένα, εκτός από τον ηλεκτρονικό υπολογιστή του δημιουργού τους, είναι αποθηκευμένα και στον ηλεκτρονικό υπολογιστή του παρόχου. Επιπλέον, η αποτύπωση αυτή των δεδομένων στον υλικό φορέα έχει τον χαρακτήρα της σταθερής ενσωμάτωσης. Τέλος η τοποθέτηση των δεδομένων αυτών σε τοποθεσία με ορισμένη ηλεκτρονική διεύθυνση τους προσδίδει ταυτότητα προέλευσης και εφόσον τα δεδομένα συνδέονται με το όνομα που αναγράφεται στην ηλεκτρονική διεύθυνση, έχουν και εκδότη.

[75] Δεν αποτελούν όμως έγγραφα όλα τα αρχεία που είναι αποθηκευμένα σε ηλεκτρονικό υπολογιστή γιατί δε συνδέονται άμεσα με συγκεκριμένο εκδότη (σε έναν ηλεκτρονικό υπολογιστή μπορούν να έχουν πρόσβαση περισσότεροι , επομένως η φυσική κυριότητα ενός ηλεκτρονικό υπολογιστή δε συνεπάγεται ότι ο κύριος έχει συντάξει και όλα τα αρχεία τα οποία είναι αποθηκευμένα στον ηλεκτρονικό υπολογιστή) και συχνά δεν έχουν αποδεικτική σημασία.

Έγγραφα δεν αποτελούν τα μηνύματα τα οποία αποστέλλονται κατά τη διάρκεια μιας ηλεκτρονικής συζήτησης στο διαδίκτυο, διότι υπάρχει παροδική εγγραφή δεδομένων στον ηλεκτρονικό υπολογιστή του διακομιστή και μία παροδική εμφάνιση των μηνυμάτων αυτών στις οθόνες των συμμετεχόντων. Επιπροσθέτως σύνταξη των μηνυμάτων αυτών συνήθως γίνεται με ψευδώνυμο, έτσι ώστε κανείς δε γνωρίζει ποιος είναι ο παραγωγός του μηνύματος και επομένως δε μπορεί να συνδεθεί το μήνυμα με τον εκδότη του.

Η νέα διάταξη, που υπάγει στην παραδοσιακή έννοια του εγγράφου τις δύο νέες παραπάνω κατηγορίες, ήταν αναγκαία διότι αποσαφηνίζει πλέον την έννοια του εγγράφου, ώστε να μην καλύπτεται καμία αμφιβολία ότι οι φορείς δεδομένων και πληροφοριών εμπίπτουν στην έννοια του εγγράφου με την έννοια του νόμου. Επιπλέον καθιστά σαφές ότι αυτοί οι φορείς είναι έγγραφα ακόμη και όταν τα δεδομένα και οι πληροφορίες που περιέχουν είναι προϊόν μιας μηχανής με την προϋπόθεση βέβαια ότι έχει προγραμματιστεί από άνθρωπο. Με τη διεύρυνση της έννοιας του εγγράφου δεν πρέπει βέβαια να θεωρήσουμε ότι το έγγραφο αποτελεί η μνήμη RAM, ο σκληρός δίσκος ή η οθόνη του ηλεκτρονικού υπολογιστή. Θα πρέπει δηλαδή να γίνει συσταλτική ερμηνεία της έννοιας του εγγράφου και να καταλήξουμε στο συμπέρασμα ότι δεδομένα θα πρέπει να έχουν εγγραφεί σε μία μη πτητική μνήμη και να είναι σταθερά ενσωματωμένα στους υλικούς φορείς τους.

Η εισαγωγή αυτής της διευκρινιστικής διάταξης, ενέταξε τα δεδομένα και τις πληροφορίες, που βρίσκονται αποθηκευμένες σε έναν ηλεκτρονικό υπολογιστή και συνδέονται με συγκεκριμένο εκδότη, στην έννοια του εγγράφου, και που όπως θα δούμε παρακάτω συνετέλεσε σε μεγάλο βαθμό την πιο αποτελεσματική αντιμετώπιση του ηλεκτρονικού εγκλήματος.

Το άρθρο 348Α Π.Κ[76]

«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 δέκα χιλιάδων έως εκατό χιλιάδων ευρώ.
2. 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 δια συστήματος ηλεκτρονικού υπολογιστή ή με τη χρήση διαδικτύου, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή πενήντα χιλιάδων έως τριακοσίων χιλιάδων ευρώ.
3. Υλικό παιδικής πορνογραφίας, κατά την έννοια των προηγούμενων παραγράφων, συνιστά η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο.
4. Οι πράξεις της πρώτης και δεύτερης παραγράφου τιμωρούνται με κάθειρξη μέχρι δέκα ετών και χρηματική ποινή πενήντα χιλιάδων έως εκατό χιλιάδων ευρώ: «α. αν τελέσθηκαν κατ' επάγγελμα ή κατά συνήθεια». «β. αν η παραγωγή του υλικού της παιδικής πορνογραφίας

[76] Βλ. Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 904-911, Ίδρυμα Μαραγκοπούλου για τα Δικαιώματα του Ανθρώπου, Σειρά Ομάδας Νέων (ΙΜΔΑ), «Η Παιδική Πορνογραφία στο Διαδίκτυο», Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 950 επ., Ζάννη Α., «Το διαδικτυακό έγκλημα», σελ. 76επ., Ιγγλεζάκη Ι., «Δίκαιο της Πληροφορικής», σελ.283 επ.

συνδέεται με την εκμετάλλευση της ανάγκης, της ψυχικής ή της διανοητικής ασθένειας ή 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». Αν η πράξη της περίπτωσης β' είχε ως αποτέλεσμα τη βαριά σωματική βλάβη του παθόντος, επιβάλλεται κάθειρξη τουλάχιστον δέκα ετών και χρηματική ποινή εκατό χιλιάδων έως πεντακοσίων χιλιάδων ευρώ αν δε αυτή είχε ως αποτέλεσμα το θάνατο, επιβάλλεται ισόβια κάθειρξη.»

Το άρθρο αυτό προστέθηκε στον Π.Κ. με το α. 6 ν 3064/2002 και αφορά στην πορνογραφία που αναφέρεται σε ανηλίκους. Η διακίνηση πορνογραφικού υλικού μπορεί να γίνεται και μέσω ηλεκτρονικού ταχυδρομείου[77]. Όσον αφορά στη δεύτερη παράγραφο, που καθίστανται αξιόποινες οι εικονική αποτύπωση σώματος ανηλίκου ή εικονικής ασελγούς πράξης, δεν προκαλείται αληθής βλάβη, η πράξη δεν αποτελεί εκμετάλλευση , οπότε η διάταξη φαίνεται ότι τιμωρεί τη διέγερση της πρόθεσης της προσβολής. Ωστόσο και η παιδική ηλικία (ανηλικότητα) η οποία κατοχυρώνεται συνταγματικά στο άρθρο 21 §§ 1,3 Σ, εμφανώς πλήττεται από τα παραπάνω εγκλήματα και χρήζει προστασίας. Κατά το νόμο υλικό παιδικής πορνογραφίας αποτελεί η «η αναπαράσταση ή η πραγματική ή εικονική αποτύπωση σε ηλεκτρονικό ή άλλο υλικό φορέα του σώματος ή μέρους του σώματος ανηλίκου, κατά τρόπο που προδήλως προκαλεί γενετήσια διέγερση, καθώς και πραγματικής ή εικονικής ασελγούς πράξης που διενεργείται από ή με ανήλικο». Το υλικό δεν αρκεί να είναι πορνογραφικό με τη γενική έννοια, αλλά θα πρέπει να αναφέρεται σε σώμα ανηλίκου, δηλαδή φυσικού προσώπου μικρότερου των 18 ετών[78].

Ο νομοθέτης διακρίνει δύο κατηγορίες πορνογραφικού υλικού: α) την περιγραφή με λόγο ή με σχήματα και την πραγματική (αληθινή) ή εικονική (μη αληθινή) αποτύπωση σε οποιονδήποτε υλικό φορέα του σώματος ανηλίκου, που αποσκοπεί στη γενετήσια διέγερση και β) την καταγραφή ή αποτύπωση σε οποιονδήποτε υλικό φορέα πραγματικής, προσποιητής ή ασελγούς πράξης που ενεργείται για τον ίδιο σκοπό από ή με ανήλικο. Υλικός φορέας στον οποίο μπορεί να αποτυπωθεί ή να περιγραφεί το υλικό της παιδικής πορνογραφίας μπορεί να είναι βιβλίο, περιοδικό, ζωγραφιά, φωτογραφία, cd rom, dvd, σκληρός δίσκος, ιστοσελίδα, λόγω της ευρείας και γενικής διατύπωσης του νόμου.

Το άρθρο 348^{A} Π.Κ. προβλέπει τους παρακάτω τρόπους τέλεσης της εγκληματικής δράσης: α) η παρασκευή υλικού πορνογραφίας είναι η πρωτογενής δημιουργία αυτού[79], όταν δηλαδή ο δράστης φτιάχνει μόνος του το σχετικό υλικό επεξεργαζόμενος κατάλληλα τα διάφορα στοιχεία που έχει συλλέξει, β) η κατοχή αυτού είναι η φυσική εξουσία του δράστη πάνω στο υλικό ακόμα και αν αυτό προορίζεται για την προσωπική του χρήση, γ) η προμήθεια πορνογραφικού υλικού είναι η εξασφάλιση του η με οποιονδήποτε νόμιμο ή παράνομο τρόπο απόκτηση ακόμη και για προσωπική χρήση του δ) η αγορά ή πώληση αυτού για τη στοιχειοθέτηση των οποίων τυγχάνουν εφαρμογής οι διατάξεις της πώλησης από το αστικό δίκαιο ε) η μεταφορά ή διακίνηση πορνογραφικού υλικού είναι η διαμετακόμιση του από τόπο σε διάφορες πηγές, με την προϋπόθεση ότι ο δράστης έχει την ευθύνη της μεταφοράς και εάν υπάρχουν βοηθητικά πρόσωπα η ευθύνη τους κρίνεται σύμφωνα με τις διατάξεις για τη συνέργεια, στ) η διάθεση του υλικού είναι ο αποχωρισμός του δράστη από το πορνογραφικό υλικό και η μεταβίβαση του σε άλλον, για οποιαδήποτε αιτία, ζ) η θέση του πορνογραφικού υλικού σε κυκλοφορία, με οποιονδήποτε τρόπο, δηλαδή κάθε περίπτωση που το σχετικό υλικό τίθεται ελεύθερα στη διάθεση των ενδιαφερομένων να το προμηθευτούν, η)

[77]Βλ. ΑΠ 628/2006 ΠοινΧρ ΝΖ/143
[78] Βλ. ΑΠ 810/2007, www.dsanet.gr
[79] Βλ. ΑΠ 810/2007, www.dsanet.gr.

η αποτύπωση του πορνογραφικού υλικού με κάποιον από τους ανωτέρω τρόπους, η οποία συνδέεται με την εκμετάλλευση της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας, ή της απειρίας ανηλίκου, με την άσκηση σωματικής βίας κατά αυτού, θ) η εγκληματική πράξη η οποία προκαλεί βαριά σωματική βλάβη στον ανήλικο.

Οι παραπάνω τρόποι α-ζ τρόποι τέλεσης στοιχειοθετούν τη βασική, πλημμεληματική μορφή του εγκλήματος, ενώ οι τρόποι η-θ αποτελούν διακεκριμένες παραλλαγές οι οποίες αποτελούν κακουργήματα. Από την διατύπωση της παραγράφου 3 του ως άνω άρθρου διαπιστώνουμε ότι προβλέπεται διακεκριμένη παραλλαγή του βασικού εγκλήματος : εάν κάποια από τις πράξεις της 1ης παραγράφου αφορά σε πορνογραφικό υλικό που συνδέεται με την εκμετάλλευσης της ανάγκης, της πνευματικής αδυναμίας, της κουφότητας ή της απειρίας ανηλίκου, ή την άσκηση σωματικής βίας κατά αυτού, ή και εάν η πράξη είχε ως αποτέλεσμα ο ανήλικος να υποστεί βαριά σωματική βλάβη, η προβλεπόμενη ποινή είναι κάθειρξη. Διαπιστώνουμε λοιπόν ότι προβλέπεται διακεκριμένη παραλλαγή του βασικού εγκλήματος.

Ως ανάγκη νοείται όχι μόνο η οικονομική αλλά και η προσωπική, όπως αντικειμενικά την αντιλαμβάνεται κανείς, ανεξάρτητα από το αν είναι παροδική ή μόνιμη, και η οποία πρέπει να είναι επιτακτική και ανεπίδεκτη αναβολής. Επίσης μπορεί να είναι υπαίτια ή ανυπαίτια. Ως ανάγκη πρέπει να νοηθεί και η κατάσταση που συνεπάγεται κίνδυνο της ζωής ή της υγείας και της οποίας η ικανοποίηση δεν επιδέχεται αναβολή[80].

Από τη διατύπωση του άρθρου 348Α Π.Κ. φαίνεται ότι ο νομοθέτης τυποποιεί ένα έγκλημα με υπερχειλή υποκειμενική υπόσταση[81], στο οποίο η κερδοσκοπία είναι υποκειμενικό στοιχείο του αδίκου. Δηλαδή με την πλήρωση της αντικειμενικής υπόστασης του εγκλήματος, η πράξη δεν καθίσταται αυτομάτως άδικη αλλά για την τελική κρίση για τον άδικο χαρακτήρα αυτής, απαιτείται η ύπαρξη του στοιχείου της κερδοσκοπίας.

Χαρακτηριστική νομολογική περίπτωση είναι η ΣυμβΠλημμΑΘ 2826/2014[82], όπου ο κατηγορούμενος για πορνογραφία ανηλίκων διέγραψε με μία εντολή του μέρους του αποδεικτικού των δοσοληψιών που ήταν αποθηκευμένο στον ηλεκτρονικό υπολογιστή του. Τα ηλεκτρονικά αποδεικτικά μέσα δεν έχουν υλική απόσταση, όπως είδαμε και παραπάνω, και μπορούν εύκολα να αλλάξουν περιεχόμενο ή να εξαφανιστούν, κάτι το οποίο μπορεί να οδηγήσει σε αθώωση πραγματικά ενόχου για το έγκλημα της παιδικής πορνογραφίας.

Με τη διατύπωση της συγκεκριμένης διάταξης επομένως ο νομοθέτης αφήνει ακάλυπτες τις περιπτώσεις πορνογραφίας ανηλίκων, οι οποίες πλέον τιμωρούνται με τις διατάξεις του ν 5060/1931 για τη διανομή άσεμνων δημοσιευμάτων ή αντικειμένων.

Το άρθρο 348^{Α} Π.Κ. δεν αφήνει συγκεκριμένη μορφή υπαιτιότητας που πρέπει να έχει ο δράστης κι επειδή το έγκλημα είναι πλημμέλημα (άρθρο 18 σε συνδυασμό με άρθρο 26 Π.Κ.) αρκεί και ενδεχόμενος δόλος, εκτός από την πράξη της προσβολής για την οποία ρητά απαιτείται δόλος α' βαθμού και εκτός από τα στοιχεία του εκ του αποτελέσματος χαρακτηριζόμενου εγκλήματος, που απαιτείται αμέλεια.

[80] 7 Περισσότερα για την έννοια του όρου ανάγκη βλ. ΑΠ 566/1989, ΕλΔικ 1991/96 και ΑΠ 785/1982, ΝοΒ 1983/670
[81] Βλ. Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 952 επ.σελ. 953.
[82] Βλ. ΠοινΔικ 2005/960.

Το άρθρο 370 Β Π.Κ.[83]

1. « Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί 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 μόνιμος 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. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο ή για απόρρητο που αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.
4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση.»

Με τη διάταξη αυτή παρατηρούμε ότι σκοπός του νομοθέτη είναι να προστατεύσει όχι μόνο εμπορικά και βιομηχανικά απόρρητα αλλά και κρατικά, επιστημονικά και επαγγελματικά απόρρητα. Επομένως το έννομο αγαθό που προστατεύεται από αυτό το άρθρο είναι όλα τα απόρρητα, ανεξάρτητα από την ιδιότητα τους ως επαγγελματικά, επιστημονικά, ιδιωτικά κ.λ.π. Στη διάταξη αυτή εμφανίζεται ο όρος «στοιχεία» όπως και στις επόμενες διατάξεις των άρθρων 370Γ και 386Α ΠΚ. Τα στοιχεία εμφανίζονται στις νομικές διατάξεις και προστατεύονται επειδή μέσω αυτών μεταφέρονται ή μπορούν να μεταφερθούν πληροφορίες.

Σύμφωνα με τη μικτή θεωρία, απόρρητα θεωρούνται τα στοιχεία ενός ηλεκτρονικού υπολογιστή όταν αυτά είναι γνωστά σε περιορισμένο κύκλο ατόμων, τα οποία υποχρεούνται να διαφυλάσσουν τη μυστικότητα τους και έτσι αυτά δεν είναι ευρέως γνωστά, όταν αυτά τα στοιχεία συνδέονται με τη λειτουργία μιας επιχείρησης και αυτό το γνωρίζουν τα πιο πάνω άτομα και τέλος όταν η πρόσβαση σε αυτά είναι δυσχερής και τηρούνται ως απόρρητα κατόπιν βούλησης του κατόχου τους, ο οποίος δείχνει δικαιολογημένο ενδιαφέρον να τα τηρεί απόρρητα (μικτή θεωρία). Αδιάφορο για την προστασία του απορρήτου είναι η δυνατότητα ενός τρίτου να δημιουργήσει ένα παρόμοιο πρόγραμμα.

Στο άρθρο 370Β Π.Κ. ο νομοθέτης συνδυάζει τα παραπάνω και εκλαμβάνει ένα στοιχείο ως απόρρητο όταν υπάρχει το δικαιολογημένο ενδιαφέρον ενός προσώπου για να κρατηθεί αυτό ως απόρρητο. Το δικαιολογημένο ενδιαφέρον αποδεικνύεται από την ύπαρξη συμφέροντος καθώς και από τη βούληση του φορέα του στοιχείου για τη διατήρηση του ως απορρήτου.

Την αντικειμενική υπόσταση του εγκλήματος τελεί 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. Η διάταξη ποινικοποιεί κάθε παραβίαση απορρήτων, χωρίς να διακρίνει τις συμπεριφορές σε άξιες και μη άξιες κολασμού, αλλά αναφέρει ενδεικτικά ορισμένους τρόπους τέλεσης: (αντιγραφή, αποτύπωση, αποκάλυψη, χρησιμοποίηση).

---

[83] Βλ. Μυλωνόπουλο Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 71 επ., Μαργαρίτη Μ. «Ποινικός Κώδικας Ερμηνεία- Εφαρμογή», σελ. 1032 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1026- 1030, Βασιλάκη Ε., «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ.159 επ.

Το Άρθρο 370Γ Π.Κ.[84]

1. « Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή ¨διακοσίων ενενήντα (290) ΕΥΡΩ έως και πέντε χιλιάδων εννιακοσίων (5.900) ΕΥΡΩ¨.
2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον ¨είκοσι εννέα (29) ΕΥΡΩ¨. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά άρθρο 148.
3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.
4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.»

Το άρθρο αυτό αποσκοπεί στην τιμώρηση της παράνομης αντιγραφής και χρήσης λογισμικού καθώς και τη χωρίς δικαίωμα πρόσβασης σε δεδομένα ηλεκτρονικού υπολογιστή. Ενώ λοιπόν το άρθρο 370Β Π.Κ. παρέχει προστασία απορρήτων με τη μορφή στοιχείου ή προγράμματος ηλεκτρονικού υπολογιστή, το άρθρο 370Γ Π.Κ. αφορά σε κάθε άλλο στοιχείο ή πρόγραμμα.

Η δημιουργία της πρώτης παραγράφου του άρθρου αυτού είναι η αντίδραση του νομοθέτη στην απαίτηση για προστασία των προγραμμάτων του ηλεκτρονικού υπολογιστή και μέσω αυτής γίνεται προσπάθεια να καλυφθούν οι περιπτώσεις «πειρατείας» προγραμμάτων .

Το άρθρο 370 Γ προστατεύει όχι τα προγράμματα καθ’ αυτά αλλά η οικονομική τους αξία που προέρχεται από την ικανότητά τους να παρέχουν πληροφορίες, δηλαδή προστατευόμενο έννομο αγαθό είναι πληροφορία, όπως περιέχεται στο πρόγραμμα που αποτελεί υλικό αντικείμενο του κανόνα δικαίου. Αντίθετη άποψη στη θεωρία υποστηρίζει ότι η διάταξη προστατεύει οποιοδήποτε είδος προγράμματος, έστω και αν δεν έχει το χαρακτήρα πνευματικής ιδιοκτησίας ή οικονομική αξία.

Η παράνομη συμπεριφορά που τιμωρεί η πρώτη παράγραφος του άρθρου 370Γ Π.Κ. είναι η χωρίς δικαίωμα αντιγραφή ενός προγράμματος. Αντιγραφή κατά την έννοια του παραπάνω άρθρου αποτελεί και η μεταφορά προγραμμάτων σε χαρτί, διάτρητες κάρτες, μαγνητικούς δίσκους ή ταινίες. Κατά την κρατούσα γνώμη δεν είναι απαραίτητη η δημιουργία υλικού υποστρώματος για την αντιγραφή και για την διάπραξη της παράνομης συμπεριφοράς αρκεί η απλή αποθήκευση του προγράμματος σε κάποια δευτερεύουσα μνήμη.

Στην εισηγητική έκθεση του νόμου 1805/1988 αναφέρεται ότι κατά το άρθρο 370Γ 2 Π.Κ. «τιμωρείται ως έγκλημα διακινδύνευσης η πρόσβαση σε στοιχεία που έχουν αποθηκευτεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών».

---

[84] Βλ. Μυλωνόπουλος Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 86. Βλ. Μαργαρίτη Μ. «Ποινικός Κώδικας Ερμηνεία- Εφαρμογή», σελ. 1034 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1030- 1033, Βασιλάκη Ε. «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ. 75 επ., Καϊάφα Γκμπάντι Μ. «Ποινικό δίκαιο και καταχρήσεις της πληροφορικής», Αρμενόπουλος 2007/1065 επ

Το άρθρο 386^{A} Π.Κ.[85]

«Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του προηγούμενου άρθρου. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την επέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.»

Όπως ειπώθηκε και παραπάνω όταν ο ποινικός νομοθέτης εισήγε στον Π.Κ. το άρθρο 386 για την απάτη, ούτε καν μπορούσε να συλλάβει ότι στο μέλλον και μέσω της εξέλιξης της τεχνολογίας, η αθέμιτη αυτή συμπεριφορά θα μπορούσε να πραγματοποιηθεί μέσα από αυτοματοποιημένες μηχανές με τρόπους οι οποίοι δε θα καλύπτονταν από το υπάρχον άρθρο. Η διάταξη του άρθρου αυτού, η οποία ακολουθεί τη διατύπωση της παρ. 263 A StGB του γερμανικού ποινικού κώδικα, ομοιάζει πολύ με τη ρύθμιση της κοινής απάτης αλλά διαφέρει ως προς το ότι εδώ δεν υπάρχει νοητική επικοινωνία μεταξύ δράστη και πλανώμενου προσώπου που προβαίνει σε πράξη, παράλειψη, ή ανοχή. Ο νομοθέτης εισάγοντας αυτή τη διάταξη είχε κυρίως υπ' όψιν του τη φυσική παρέμβαση στον ηλεκτρονικό υπολογιστή, πχ έναν προγραμματιστή που με παρέμβαση του στο πρόγραμμα της εταιρίας, μεταφέρει χρηματικά ποσά από λογαριασμό της εταιρίας σε δικό του λογαριασμό. Με την εξάπλωση του Διαδικτύου πολλαπλασιάστηκαν οι δυνατότητες επέμβασης σε ηλεκτρονικό υπολογιστή, αφού πλέον όλος ο χώρος του Διαδικτύου αποτελεί πιθανό στόχο του δράστη της απάτης με ηλεκτρονικό υπολογιστή. Η διάταξη μέσω της διατύπωσης της και τη συστηματική ένταξη της στα εγκλήματα κατά της περιουσίας, καταδεικνύει ότι προστατευόμενο έννομο αγαθό είναι η περιουσία.

Το έγκλημα του άρθρου 386^{A} Π.Κ. τελείται από όποιον βλάπτει ξένη περιουσία επηρεάζοντας τα στοιχεία ηλεκτρονικού υπολογιστή με τους αναφερόμενους στο νόμο τρόπους, με σκοπό να προσπορίσει στον εαυτό του παράνομο περιουσιακό όφελος. Τόσο στη θεωρία όσο και στη νομολογία, επικρατεί η άποψη ότι το άρθρο 386Α Π.Κ. θα πρέπει να ερμηνεύεται αναλογικά με την κοινή απάτη του άρθρου 386 Π.Κ. Σύμφωνα δε με το 386§1 Π.Κ. « Όποιος με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών».

[85] Βλ. Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 1192 επ., Μυλωνόπουλου Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 54 επ., Μυλωνόπουλου Χ., «Ποινικό ΔίκαιοΕιδικό Μέρος: Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, α. 372-406 Π.Κ.». σελ. 596 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1137-1142, Βασιλάκη Ε. «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ. 185 επ., Καϊάφα Γκμπάντι Μ. «Ποινικό δίκαιο και καταχρήσεις της πληροφορικής», Αρμενόπουλος 2007/1065 επ.

4.4 ΛΟΙΠΕΣ ΔΙΑΤΑΞΕΙΣ ΠΟΥ ΣΥΝΤΕΛΟΥΝ ΣΤΗΝ ΚΑΤΑΠΟΛΕΜΗΣΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΔΙΑΔΙΚΤΥΑΚΟΥ ΕΓΚΛΗΜΑΤΟΣ.

Εκτός από τις παραπάνω διατάξεις του Π.Κ. στην ελληνική νομοθεσία συναντάμε και κάποιες άλλες οι οποίες συντελούν στην προστασία από το ηλεκτρονικό διαδικτυακό έγκλημα οι οποίες είναι οι εξής:

1) Το Π.Δ. 131/2003, το οποίο θεσπίστηκε σε εφαρμογή Κοινοτικής Οδηγίας για το για το ηλεκτρονικό εμπόριο και αναφέρεται στην ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam mail) και στην ευθύνη των παρόχων υπηρεσιών διαδικτύου για τις πράξεις των συνδρομών – χρηστών τους.
2) Ο νόμος 2867/2000 για την «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών».
3) Οι νόμοι 2774/1999 και 2472/1997 «προσωπικών δεδομένων».
4) Ο νόμος 2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας».
5) Ο νόμος 2225/1994 για την «προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας » όπως τροποποιήθηκε με το ν. 3115/2003.
6) Ο νόμος 2819/2000 «Προσθήκη στο ν. 2121/1993 περί νομικής προστασίας βάσεων δεδομένων».
7) Ο νόμος 3431/2006 «Περί ηλεκτρονικών επικοινωνιών ».
   Καθένας από αυτούς τους νόμους προσεγγίζει συγκεκριμένες πτυχές του ηλεκτρονικού διαδικτυακού εγκλήματος .

4.5 ΝΟΜΟΘΕΣΙΑ ΑΛΛΟΔΑΠΩΝ ΕΝΝΟΜΩΝ ΤΑΞΕΩΝ.

Σε αυτή την υποενότητα θα γίνει μια μικρή ανασκόπηση στους μέχρι τώρα νόμους που έχουν θεσπισθεί στις ΗΠΑ για την αντιμετώπιση του ηλεκτρονικού εγκλήματος, επειδή εκεί έκανε την πρώτη του εμφάνιση αυτή η νέα μορφή εγκλήματος και κατόπιν εξαπλώθηκε ευρέως, αλλά και στους νόμους που έχουν θεσπισθεί στη Μεγάλη Βρετανία επειδή σε αυτή υπήρξαν σημαντικές πρωτοβουλίες για την αποτελεσματική αντιμετώπιση του φαινομένου του ηλεκτρονικού διαδικτυακού εγκλήματος. Επιπλέον θα εξεταστούν και οι διατάξεις κατά του ηλεκτρονικού διαδικτυακού εγκλήματος που έχουν θεσπισθεί στην Γερμανία, της οποίας η νομοθεσία εμφανίζει αρκετά κοινά σημεία με την ελληνική νομοθεσία κατά του ηλεκτρονικού διαδικτυακού εγκλήματος αλλά και οι ποινικές διατάξεις που ισχύουν στην Ελβετία.

4.5.1 Νομοθεσία Της Γερμανίας

Η ραγδαία ανάπτυξη της ηλεκτρονικής επεξεργασίας στοιχείων, προκάλεσε όπως ήταν αναμενόμενο, μεταβολές και νέες απαιτήσεις και στο δικαιικό χώρο της Γερμανίας, η οποία έπρεπε και αυτή να προσαρμοστεί με τα νέα δεδομένα της τεχνολογίας.

Έτσι στο άρθρο 11 της 3^{η} παρ. ορίζεται ότι «οπτικοακουστικά μέσα, συστήματα αποθήκευσης πληροφοριών, εικόνες και απεικονίσεις ισοδυναμούν με τα έγγραφα στις διατάξεις που αναφέρονται σε αυτό τμήμα». Είναι εμφανής η ομοιότητα του άρθρου του

γερμΠΚ με το άρθρο 13 γ' εδ. β Π.Κ. καθώς και στα δύο άρθρα γίνεται μνεία ότι στα έγγραφα εντάσσονται και τα ηλεκτρονικά μέσα που χρησιμοποιούνται από ηλεκτρονικούς υπολογιστές. Η ελληνική διάταξη βέβαια είναι πολύ πιο αναλυτική ως προς το ποια ηλεκτρονικά στοιχεία θεωρούνται πλέον έγγραφα, ενώ η γερμανική είναι εμφανώς πιο λακωνική.

Το άρθρο 202^{A} StGB τιμωρεί όποιον αποκτά παράνομα στοιχεία για τον εαυτό του ή για άλλον, τα οποία δεν προορίζονταν για αυτόν και ήταν ιδιαίτερα προστατευμένα από μη εξουσιοδοτημένη πρόσβαση.

Το άρθρο 263^{A} StGB ομοιάζει με το άρθρο 386^{A} Π.Κ. για την απάτη με υπολογιστή, το οποίο είναι σαφώς επηρεασμένο από τη διάταξη του γερμανικού Π.Κ. Συγκεκριμένα το άρθρο 263^{A} StGB έχει ως εξής: «Όποιος με πρόθεση να προσκομίσει στον εαυτό του ή σε τρίτο πρόσωπο παράνομο όφελος ζημιώνει την περιουσία του άλλου επηρεάζοντας το αποτέλεσμα μιας διαδικασίας επεξεργασίας δεδομένων μέσω εσφαλμένης διαμόρφωσης του προγράμματος ή μέσω χρήσης ανακριβών ή ελλιπών στοιχείων, χωρίς δικαίωμα χρήσης των δεδομένων ή άλλης χωρίς δικαίωμα επιρροής στην πορεία της επεξεργασίας, υπόκειται σε φυλάκιση που δεν υπερβαίνει τα πέντε έτη ή σε χρηματική ποινή.» Η ομοιότητα στην έκφραση και διατύπωση των δύο διατάξεων είναι μεγάλη με μόνη διαφορά στη διατύπωση ότι το άρθρο του γερμανικού Π.Κ. μιλά για επηρεασμό μιας διαδικασίας επεξεργασίας δεδομένων ενώ η ελληνική διάταξη μιλά για επηρεασμό στοιχείων υπολογιστή, αλλά όπως είδαμε στην αναλυτική ανάπτυξη του άρθρου 386^{A} Π.Κ. οι παραπάνω έννοιες ταυτίζονται. Και στις δύο όμως διατάξει τυποποιείται η χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων και προστατεύεται η περιουσία του ατόμου από επιθέσεις μέσω ηλεκτρονικού υπολογιστή.

4.5.2 Νομοθεσία Της Ελβετίας

Στην ελβετική έννομη τάξη, με το άρθρο 144bis Ελβετικού Π.Κ. τιμωρείται όποιος χωρίς άδεια διαγράφει, τροποποιεί, καθιστά άχρηστα δεδομένα που έχουν αποθηκευτεί με ηλεκτρονικό ή παράνομο τρόπο ή έχουν διαμετακομιστεί. Με τη δεύτερη παράγραφο του άρθρου τιμωρείται όποιος δημιουργεί, εισάγει, διανέμει, προωθεί, προσφέρει ή κυκλοφορεί με κάθε τρόπο προγράμματα, για τα οποία γνωρίζει ή οφείλει να γνωρίζει ότι χρησιμοποιούνται για τους σκοπούς της παραγράφου ένα ή δίνει οδηγίες για τη δημιουργία τέτοιων προγραμμάτων. Με αυτή την διάταξη ο ελβετικός νομοθέτης προσπαθεί να προστατέψει τα ηλεκτρονικά δεδομένα από την προσβολή των ιών. Στην ελληνική ποινική έννομη τάξη δεν υπάρχει αντίστοιχη διάταξη για την προστασία των δεδομένων από τους ιούς και ανάλογες περιπτώσει κρίνονται συνήθως με το άρθρο 381 Π.Κ. για τη φθορά ξένης ιδιοκτησίας στο βαθμό που η προσβολή των δεδομένων από τους ιούς προσβάλει και τους υλικούς φορείς που τα φέρουν. Με το άρθρο 147 του Ελβετικού Π.Κ. τιμωρείται όποιος, με πρόθεση να πλουτίσει παράνομα ο ίδιος ή τρίτος, επεμβαίνει σε μια ηλεκτρονική ή άλλη παρόμοια διαδικασία επεξεργασίας ή μετάδοσης δεδομένων με μη ορθή, ελλιπή ή χωρίς δικαίωμα χρησιμοποίηση δεδομένων και μέσω των ανακριβών αποτελεσμάτων που προέκυψαν προκαλεί μεταβίβαση περιουσιακών στοιχείων εις βάρος των άλλων ή καλύπτει έτσι έμμεσα μια περιουσιακή μετάθεση. Ο Ελβετός νομοθέτης φαίνεται να ενδιαφέρεται περισσότερο για τον τρόπο χρησιμοποίησης των δεδομένων, παρά για τα δεδομένα καθ' αυτά.

4.5.3 Νομοθεσία Της Μεγάλης Βρετανίας.[86]

Στο πλαίσιο της Ευρώπης, μια πολύ σημαντική προσπάθεια ποινικής αντιμετώπισης του πληροφορικού εγκλήματος, έλαβε χώρα στη Μεγάλη Βρετανία με το Computer Misuse Act 1990.

Με το νομοθέτημα αυτό δημιουργήθηκαν τρία νέα εγκλήματα. Τα δύο έχουν να κάνουν με το θέμα της χωρίς εξουσιοδότηση πρόσβασης. Το ένα, το οποίο αναφέρεται στο πρώτο άρθρο του νόμου, κατηγοριοποιεί ως εγκληματία το πρόσωπο που εν γνώσει του προκαλεί τη λειτουργία ενός ηλεκτρονικού υπολογιστή με σκοπό να καταφέρει τη μη εξουσιοδοτημένη πρόσβαση σε προγράμματα ή δεδομένα που βρίσκονται σε αυτόν. Με τον τρόπο αυτό ποινικοποιείται η χρήση ηλεκτρονικού υπολογιστή, εφόσον αποδειχθεί η πρόθεση του ατόμου για τη μη εξουσιοδοτημένη πρόσβαση. Για παράδειγμα ένας hacker, όταν χρησιμοποιεί τον ηλεκτρονικό υπολογιστή του για να αποκτήσει πρόσβαση χωρίς εξουσιοδότηση σε ηλεκτρονικό υπολογιστή άλλου <προκαλεί τη λειτουργία του ηλεκτρονικού υπολογιστή> από τη στιγμή που ο ηλεκτρονικός υπολογιστής- στόχος ενεργοποιεί το σύστημα ασφαλείας του ή ανοίγει το menu πρόσβασης (log on menu).

Το δεύτερο άρθρο του νόμου, διευρύνει το πρώτο αδίκημα, με τη δημιουργία ενός απώτερου σκοπού στη μη εξουσιοδοτημένη πρόσβαση, δηλαδή τιμωρεί ποινικά το πρόσωπο το οποίο μέσω της μη εξουσιοδοτημένης πρόσβασης αποσκοπεί στη διάπραξη ορισμένων αδικημάτων ή θέλει να προάγει τη τέλεση ορισμένων αδικημάτων.

Στο τρίτο άρθρο αυτού του νόμου ορίζεται ως αδίκημα οποιαδήποτε αλλαγή ή τροποποίηση περιεχομένου ενός ηλεκτρονικού υπολογιστή, υπό την προϋπόθεση ότι το άτομο που διέπραξε το ως άνω έγκλημα γνώριζε τη σημασία των ενεργειών του. Ο δράστης δηλαδή θα πρέπει να αποσκοπεί στην αλλαγή και η πράξη του θα πρέπει να εμποδίζει την ομαλή λειτουργία του ηλεκτρονικού υπολογιστή είτε μέσω της παρεμπόδισης ή παρακώληση πρόσβασης στα δεδομένα του ή στα προγράμματά του είτε μέσω της μείωσης της αξιοπιστίας των δεδομένων ή των προγραμμάτων που είναι προσβάσιμα διαμέσου του προσβαλλόμενου ηλεκτρονικού υπολογιστή. Το μόνο που χρειάζεται για την πλήρωση του συγκεκριμένου εγκλήματος είναι ότι το άτομο πρέπει να γνωρίζει ότι οι προσδοκώμενες αλλαγές είναι χωρίς εξουσιοδότηση και η επιτυχία των σκοπών του ατόμου είναι αδιάφορη για την πλήρωση των προϋποθέσεων του νόμου.

Η πιο σημαντική παράλειψη αυτού του νόμου ήταν ότι δεν υπήρχε ορισμός του ηλεκτρονικού υπολογιστή. Η επιτροπή είχε άποψη ότι ένας τέτοιος ορισμός ίσως αποδεικνυόταν παραπλανητικός, αφού οι μέχρι τότε ορισμοί ήταν τόσο πολύπλοκοι, ώστε ένας νέος ορισμός μόνο σύγχυση θα προκαλούσε. Επιπλέον, υποστήριξε ότι η εξέλιξη των ηλεκτρονικών υπολογιστών ήταν ραγδαία που σε σύντομο χρονικό διάστημα ο πιθανός νομικός ορισμός θα ήταν ξεπερασμένος. Για αυτούς τους λόγους πρότεινε ο όρος ηλεκτρονικός υπολογιστής να έχει το <κοινό νόημά του> (ordinary meaning) και με αφετηρία αυτό το γεγονός δεν ορίστηκαν ούτε τα <προγράμματα> και τα <δεδομένα>, τα οποία επίσης αποδίδονται με το <κοινό τους νόημα>.

Εκτός όμως από τις παραπάνω παραλείψεις στο νόμο υπήρξαν και σημαντικές καινοτομίες. Καταρχάς ορίζεται με σαφήνεια η ασφάλεια πρόσβασης σε οποιοδήποτε πρόγραμμα ή δεδομένο ηλεκτρονικού υπολογιστή ως η κατάσταση στην οποία το πρόγραμμα ή το

[86] Βλ. Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ. 70, Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα>, σελ. 131.

δεδομένο σβήνεται, αντιγράφεται, μετατίθεται, χρησιμοποιείται ή εξάγεται από τον ηλεκτρονικό υπολογιστή στον οποίο φυλάσσεται με οποιονδήποτε τρόπο. Επίσης ένα πρόγραμμα χρησιμοποιείται αν ένα άτομο προκαλεί την εκτέλεσή του ή προκαλεί μία λειτουργία στον ηλεκτρονικό υπολογιστή η οποία βασίζεται στο συγκεκριμένο πρόγραμμα. Τέλος, ένα πρόγραμμα εξάγεται, αν οι οδηγίες του εξαχθούν με οποιοδήποτε τρόπο, ανεξάρτητα από το γεγονός του αν και κατά πόσο η μορφή που έχει εξαχθεί είναι εκτελέσιμη ή επεξεργάσιμη από άλλο ηλεκτρονικό υπολογιστή.[87]

4.5.4 Νομοθεσία Των ΗΠΑ Σε Ομοσπονδιακό Επίπεδο.[88]

Ένας πρώτος νόμος των ΗΠΑ σε ομοσπονδιακό επίπεδο για την αντιμετώπιση του ηλεκτρονικού εγκλήματος εκδόθηκε το 1984, αλλά δεν ήταν ολοκληρωμένος και κατέστη αναποτελεσματικός, αφού προσπάθησε ανεπιτυχώς να θέσει βασικό νομικό πλαίσιο για τη νέα μορφή εγκλήματος. Δεν ήταν καν αυτόνομο νομοθέτημα αφού ήταν ενταγμένος σε άρθρο για σχετικά με τις απάτες, τις πιστωτικές κάρτες και την προσβολή πιστωτικών πληροφοριών. Δύο χρόνια αργότερα το Κογκρέσο δημιούργησε το νόμο για την Computer Fraud and Abuse Act (Απάτη και Προσβολή Υπολογιστών). Ο νόμος προέβλεπε το κακούργημα της εν γνώσει του δράστη μη εξουσιοδοτημένης ή καθ' υπέρβαση της εξουσιοδότησης, πρόσβασης σε ηλεκτρονικό υπολογιστή με σκοπό την βλάβη των ΗΠΑ και την ωφέλεια ξένης χώρας, το κακούργημα της πρόσβασης σε ηλεκτρονικό υπολογιστή ομοσπονδιακού συμφέροντος με σκοπό την εξαπάτηση των ΗΠΑ και την απόκτηση αξιών εκτός από τον ηλεκτρονικό υπολογιστή καθεαυτό και το κακούργημα της σκόπιμης μη εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικό υπολογιστή ομοσπονδιακού συμφέροντος με σκοπό την ανταλλαγή, αλλοίωση ή καταστροφή πληροφοριών ομοσπονδιακού ενδιαφέροντος ή τη παρεμπόδιση αξιοποίησης αυτών των πληροφοριών. Αντίστοιχα προβλέπονταν και τρία πλημμελήματα από τα οποία τα δύο αφορούσαν σε ομοσπονδιακά συμφέροντα, και συγκεκριμένα ένα πλημμέλημα για τη σκόπιμη μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικό υπολογιστή με σκοπό την απόκτηση πληροφοριών από δημόσια οικονομικά αρχεία ή από οικονομικούς οργανισμούς, ένα πλημμέλημα για την απαγόρευση της μη εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικό υπολογιστή ο οποίος χρησιμοποιούνταν από κρατική υπηρεσία των ΗΠΑ και το τελευταίο πλημμέλημα για την παράνομη διακίνηση κωδικών πρόσβασης ηλεκτρονικού υπολογιστή, εφόσον η διακίνηση επηρέαζε το εμπόριο των ΗΠΑ ή ο ηλεκτρονικός υπολογιστής χρησιμοποιούνταν από την κυβέρνηση των ΗΠΑ.

Ο πρώτος αυτός νόμος σε ομοσπονδιακό επίπεδο, δεν προέβλεπε κάποια διάταξη για τους ηλεκτρονικούς ιούς ή παρόμοια προγράμματα, δεν έδινε ορισμό των εννοιών της <πρόσβασης>, <χρήσης>, <χωρίς εξουσιοδότηση>, εφαρμοζόταν μόνο σε περιπτώσεις που εμπλέκονταν ηλεκτρονικός υπολογιστής της ομοσπονδιακής κυβέρνησης και για όλα τα παραπάνω δέχτηκε δριμεία κριτική.

Ο νόμος ενισχύθηκε σημαντικά με την τροπολογία του 1991 (The Computer Abuse Amendment of 1991), η οποία άλλαξε τις προϋποθέσεις που όριζαν την πρόθεση, επέκτεινε τις προϋποθέσεις που αφορούσαν τη ζημιά, εισήγε την αστική ευθύνη του δράστη και διεύρυνε τον ορισμό του ηλεκτρονικού υπολογιστή.

---

[87] Βλ. Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 70.
[88] Βλ. Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ.67, Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα>, σελ. 129.

Η πιο σημαντική τροποποίησή του όμως έγινε το 1994 και επέφερε αλλαγές σε τρία βασικά σημεία:
Α) Η ισχύς του νομοθετικού πλαισίου επεκτάθηκε και σε ηλεκτρονικούς υπολογιστές που χρησιμοποιούνταν στο διαπολιτειακό εμπόριο.
Β) Αφαιρέθηκε ο όρος <μη εξουσιοδοτημένη πρόσβαση> και έτσι πλέον μπορούσαν να διωχθούν και οι υπάλληλοι εταιρειών και οι εξουσιοδοτημένοι χρήστες.
Γ) Πλέον θεωρούνταν παράνομες συγκεκριμένες μορφές επικίνδυνων και σκόπιμων ενεργειών, όπως η διασπορά κακόβουλου λογισμικού και οι επιθέσεις άρνησης εξυπηρέτησης.

Τέλος, ο νόμος ολοκληρώθηκε το 1996, με τη National Information Infrastructure Protection Act (NIIPA), η οποία αναφέρεται στους προστατευμένους ηλεκτρονικούς υπολογιστές.[89]Η πιο σημαντική διάταξη αυτού του νομοθετήματος προβλέπει ότι κάθε μεμονωμένος χρήστης που εισέρχεται σε έναν προστατευμένο ηλεκτρονικό υπολογιστή είναι υπεύθυνος και για τις πράξεις του αλλά και για τις συνέπειές τους, ενώ αν η πρόσβασή του έγινε με εξουσιοδότηση είναι ποινικά υπεύθυνος μόνο αν είχε σκοπό να προξενήσει ζημία στο θύμα.

Σήμερα υπάρχει η διάταξη 18 USC 1030- US CODE ΤΜΗΜΑ 1030, σε ομοσπονδιακό επίπεδο, στην οποία έχουν ενσωματωθεί οι παραπάνω διατάξεις και η οποία αφορά στην απάτη και συναφείς δραστηριότητες σε σχέση με ηλεκτρονικό υπολογιστή, η οποία είναι μία πραγματικά λεπτομερής διάταξη, η οποία τυποποιεί ως εγκλήματα διάφορες μορφές παράνομης πρόσβασης σε ηλεκτρονικό υπολογιστή με σκοπό τη ζημία των ΗΠΑ όπως:
Α) Την παράνομη, χωρίς προηγούμενη εξουσιοδότηση ή κατά παράβαση υπάρχουσας εξουσιοδότησης, πρόσβαση σε ηλεκτρονικό υπολογιστή ο οποίος ανήκει στις υπηρεσίες των ΗΠΑ, και ως αποτέλεσμα αυτής της πρόσβασης να είναι η απόκτηση απόρρητων πληροφοριών, οι οποίες θα μπορούσαν να χρησιμοποιηθούν για να προκαλέσουν βλάβη στις ΗΠΑ και κατόπιν την παράδοση, μετάδοση ή επικοινωνία αυτών των πληροφοριών σε άτομο που δεν δικαιούται να τις παραλάβει.
Β) Την εν γνώσει του ατόμου μετάδοση ενός προγράμματος, πληροφορίας, κώδικα ή εντολής, και ως αποτέλεσμα αυτής της συμπεριφοράς, την εκ προθέσεως πρόκληση βλάβης, χωρίς άδεις, σε ένα προστατευόμενο υπολογιστή χωρίς άδεια, και ως αποτέλεσμα αυτής της συμπεριφοράς, την πρόκληση βλάβης από αμέλεια, ή την, με πρόθεση και χωρίς άδεια, απόκτηση πρόσβασης σε ένα προστατευόμενο υπολογιστή, και ως αποτέλεσμα αυτής της συμπεριφοράς, την πρόκληση βλάβης, και τις παραπάνω συμπεριφορές θα πρέπει ή 1) να προκαλείται απώλεια σε ένα ή περισσότερα πρόσωπα κατά τη διάρκεια ενός χρόνου (και, για τους σκοπούς της έρευνας, της δίωξης ή άλλης διαδικασίας που ασκούνται από τις Ηνωμένες Πολιτείες μόνο, η ζημία που προκύπτει από μια σχετική συμπεριφορά να επηρεάζει ένα ή περισσότερους προστατευόμενους υπολογιστές) η οποία να συνοψίζεται σε τουλάχιστον 5000 δολάρια σε αξία, ή 2) να προκληθεί τροποποίηση ή αδυναμία, ή εν δυνάμει τροποποίηση ή αδυναμία, της ιατρικής εξέτασης, διάγνωσης, θεραπείας ή φροντίδας ενός ή περισσοτέρων ατόμων, ή 3) να προκληθεί σωματική βλάβη σε οποιοδήποτε πρόσωπο, ή 4) να προκληθεί απειλή για τη δημόσια υγεία ή ασφάλεια, ή 5) να προκληθούν ζημίες που αφορούν σε ένα σύστημα ηλεκτρονικού υπολογιστή που χρησιμοποιείται από ή για ένα κρατικό φορέα για την προώθηση της απονομής της δικαιοσύνης, της εθνικής άμυνας ή της εθνικής ασφάλειας.
Γ) Την εν γνώσει και με σκοπό την εξαπάτηση διακίνηση κάθε κωδικού πρόσβασης ή παρόμοιων πληροφοριών μέσω των οποίων κάποιος μπορεί να αποκτήσει πρόσβαση σε ένα υπολογιστή χωρία άδεια, εφόσον αυτή η διακίνηση επηρεάζει το διαπολιτειακό ή διεθνές

[89] Ο όρος <protected computers> αναφέρεται σε ηλεκτρονικούς υπολογιστές που είτε προορίζονται για χρήση από ένα οικονομικό ίδρυμα ή την κυβέρνηση των ΗΠΑ είτε σε ηλεκτρονικούς υπολογιστές που χρησιμοποιούνται σε διαπολιτειακό ή εμπόριο με χώρες της αλλοδαπής και επικοινωνίες.

εμπόριο, ή ένας τέτοιος υπολογιστής χρησιμοποιείται από ή για την κυβέρνηση των Ηνωμένων Πολιτειών.
Δ) Την, με πρόθεση αποκόμισης από οποιοδήποτε πρόσωπο χρημάτων ή άλλων αντικειμένων αξίας, μετάδοση στο διαπολιτειακό ή το διεθνές εμπόριο οποιασδήποτε επικοινωνίας που περιέχει απειλή να προκαλέσει ζημιά σε ένα προστατευόμενο υπολογιστή.

Το άρθρο αυτό αποσαφηνίζει την έννοια του ηλεκτρονικού υπολογιστή, αλλά και την έννοια της υπέρβασης της εξουσιοδοτημένης πρόσβασης, ενώ για τα θύματα των παραπάνω εγκλημάτων προβλέπει τη δυνατότητα αστικής αποζημίωσης.

4.5.5 Νομοθεσία Των ΗΠΑ Σε Πολιτειακό Επίπεδο.[90]

Μέχρι τα τέλη της δεκαετίας του 1970 οι προσπάθειες αντιμετώπισης του πληροφορικού εγκλήματος στις ΗΠΑ αφορούσαν σε επεκτατική εφαρμογή του υπάρχοντος δικαίου, χωρίς όμως να αντιμετωπίζουν αποτελεσματικά τη νέα αυτή μορφή εγκλήματος. Το 1978 ψηφίστηκε στη Φλόριντα νομοθέτημα το οποίο κατηγοριοποίησε <εγκλήματα σχετιζόμενα με ηλεκτρονικό υπολογιστή> και όρισε ποινές για αυτά. Ακολούθησε νομοθέτημα της πολιτείας της Αριζόνας, στην ίδια κατεύθυνση και στις επόμενες δύο δεκαετίες ανάλογα νομοθετήματα δημιουργήθηκαν στην πλειοψηφία των πολιτειών.

Τα νομοθετήματα αυτά εισήγαγαν μια σειρά από καινοτόμες ρυθμίσεις και συνετέλεσαν στην καλύτερη προστασία από το ηλεκτρονικό έγκλημα. Κάποιες από αυτές τις καινοτομίες είναι οι παρακάτω:

Η επέκταση της παραδοσιακής έννοιας της ιδιοκτησίας ώστε να συμπεριλαμβάνεται η ηλεκτρονική τεχνολογία και η τεχνολογία των ηλεκτρονικών υπολογιστών.

Η ποινικοποίηση δράσεων όπως η αλλοίωση, η βλάβη, η διαγραφή και η οριστική καταστροφή προγραμμάτων ή αρχείων ηλεκτρονικού υπολογιστή.

Η απόδοση εκ νέου ενός περιοριστικού περιεχομένου στις έννοιες της πρόσβασης και της χρήσης των υπολογιστικών συστημάτων ώστε να απαιτείται η ρητή συναίνεση του ιδιοκτήτη προς τον χρήστη και ο δεύτερος να τιμωρείται και σε περιπτώσεις που δρα με τρόπο που περιορίζει την αποτελεσματικότητα του συστήματος.

Η διάκριση διαφορετικών επιπέδων δίωξης εγκλημάτων που αφορούν στη μη εξουσιοδοτημένη αντιγραφή προγραμμάτων και δεδομένων.

Η ποινικοποίηση της εισαγωγής ιών, σκουληκιών και λογικών βομβών σε συστήματα ηλεκτρονικού υπολογιστή, μέσω τηλεφωνικών γραμμών ή δισκετών και σε σύνδεση με αδικήματα που σχετίζονται με τη μη εξουσιοδοτημένη πρόσβαση.

Η ποινικοποίηση της μη εξουσιοδοτημένης πρόσβασης σε ηλεκτρονικό υπολογιστή με σκοπό την προστασία της ιδιωτικότητας του πολίτη.

---

[90] Βλ. Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ. 62.

Η απαγόρευση της ανάληψης του ελέγχου ενός συστήματος ηλεκτρονικού υπολογιστή ή/ και του περιεχομένου του χωρίς προηγούμενη εξουσιοδότηση.

Σήμερα οι νόμοι κατά του ηλεκτρονικού εγκλήματος σε πολλές πολιτείες απαγορεύουν σε ένα πρόσωπο την εκτέλεση ορισμένων πράξεων χωρίς άδεια, συμπεριλαμβανομένων 1) της πρόσβασης σε ηλεκτρονικό υπολογιστή, σε σύστημα ηλεκτρονικού υπολογιστή, ή δίκτυο ηλεκτρονικού υπολογιστή, 2) της τροποποίησης, καταστροφής, χρήσης, αντιγραφής ή κλοπής προγραμμάτων ή δεδομένων, 3) της εισαγωγής ιών ή άλλων τύπων <μόλυνσης> σε ένα σύστημα ηλεκτρονικού υπολογιστή, 4) της χρήσης ενός ηλεκτρονικού υπολογιστή με σκοπό την απάτη, 5) της παρέμβασης στην πρόσβαση ή χρήση ηλεκτρονικού υπολογιστή κάποιου άλλου ατόμου, 6) της χρήσης κρυπτογράφησης για τη διευκόλυνση ενός εγκλήματος, 7) της παραποίησης των πληροφοριών που προέρχονται e- mail, και 8) της κλοπής πληροφοριών από έναν πάροχο υπηρεσιών διαδικτύου.

Για παράδειγμα: Στην Πολιτεία της Καλιφόρνιας με το άρθρο 502 του Penal Code (Ποινικού Κώδικα)[91], τιμωρούνται ως πλημμελήματα η με πρόθεση πρόσβαση σε ηλεκτρονικό υπολογιστή, η εισαγωγή ιών σε ηλεκτρονικό υπολογιστή, η κλοπή υπηρεσιών με αξία κάτω των 400$, εφόσον δεν προκαλούν περαιτέρω βλάβη και ως κακουργήματα η παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή με σκοπό την εξαπάτηση, η μεταβολή, πρόκληση ζημίας, ή πλήρης καταστροφή σε hardware ή software με αξία άνω των 5000$, η κλοπή υπηρεσιών με αξία άνω των 400$, η παράνομη πρόσβαση και μεταβολή, καταστροφή, χρήση και αντιγραφή δεδομένων ή παρεμβολή σε υπηρεσίες ηλεκτρονικού υπολογιστή, εφόσον προκαλούν βλάβη ή περαιτέρω αδίκημα. Η απόπειρα των παραπάνω δε θεωρείται αδίκημα, ενώ προβλέπεται και αστική αποζημίωση των θυμάτων.

Στην πολιτεία της Νέας Υόρκης στα άρθρα 156 επ. Penal Code[92] τιμωρείται ως πλημμέλημα η με πρόθεση μη εξουσιοδοτημένη χρήση ηλεκτρονικού υπολογιστή και η με πρόθεση παραβίαση (tampering) Δ βαθμού σε ηλεκτρονικό υπολογιστή και ως κακούργημα η με πρόθεση παραβίαση Γ, Β και Α βαθμού σε ηλεκτρονικό υπολογιστή, η παράνομη αντιγραφή δεδομένων ηλεκτρονικού υπολογιστή και η εγκληματική κατοχή (criminal possession) υλικών που σχετίζονται με ηλεκτρονικό υπολογιστή. Εδώ η απόπειρα θεωρείται αδίκημα και δεν προβλέπεται αστική αποζημίωση των θυμάτων.

ΣΥΝΟΠΤΙΚΑ

Το νομοθετικό «οπλοστάσιο» που διαθέτει το εθνικό μας δίκαιο για την αντιμετώπιση του εγκλήματος μέσω διαδικτύου είναι ως ένα βαθμό ικανοποιητικό, αλλά χρειάζεται εμπλουτισμό και βελτίωση. Συνεχώς ανακύπτουν νέα ζητήματα και χρειάζονται νομοθετικές αποτελεσματικές παρεμβάσεις, χωρίς ωστόσο να θίγονται βασικά δικαιώματα και συνταγματικά κατοχυρωμένες ελευθερίες των πολιτών και χωρίς να οδηγούμαστε στην ποινικοποίηση της ελεύθερης ανθρώπινης έκφρασης. Το δίκαιο δεν μπορεί να παραμένει στάσιμο, αλλά οφείλει να ακολουθεί την συνεχιζόμενη εξέλιξη της κοινωνίας. Ιδιαίτερη προσοχή και μέριμνα οφείλουν να δείξουν, τόσο η πολιτεία, όσο και οι ίδιοι οι γονείς, αναφορικά με την εξάπλωση της χρήσης του διαδικτύου σε πολύ μικρές ηλικίες. Πολύ σημαντικό ρόλο παίζει η πρόληψη. Σημαντική, επίσης, είναι η ανάπτυξη επιμορφωτικών

[91] http://law.findlaw.com/state-laws/computer-crimes/california/.
[92] http://law.findlaw.com/state-laws/computer-crimes/new-york/.

προγραμμάτων από το σχολείο, την τοπική κοινωνία, τις διάφορες κοινωνικές οργανώσεις, που θα παρέχουν εκπαίδευση, ενημέρωση σχετικά με τους κινδύνους και τεχνική υποστήριξη.

ΚΕΦΑΛΑΙΟ 5

ΕΠΙΛΟΓΟΣ- ΣΥΜΠΕΡΑΣΜΑΤΑ

Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρέως φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως <Ηλεκτρονικό Έγκλημα>, λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Ανάλογα με τον τρόπο τέλεσης διαχωρίζονται σε εγκλήματα τελούμενα σε κοινό και ηλεκτρονικό περιβάλλον, τελούμενα μόνο με τη χρήση ηλεκτρονικών υπολογιστών (computer crime) και σε Κυβερνοεγκλήματα (cyber crime), εάν τελέσθηκε μέσω του διαδικτύου.

Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του διαδικτύου πολλαπλασιάζονται. Για την αντιμετώπιση του κινδύνου αυτού ήταν απαραίτητη η διακριτική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το ηλεκτρονικό έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη του οποίου όλα τα συμπεράσματα αποκρυσταλλώνονται στην Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του Συνεδρίου στις 23/11/2001. Στην ελληνική νομοθεσία όμως, δεν υπάρχει νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του διαδικτύου από άποψη Ποινικού Δικαίου. Μόνο ο Ν. 1805/88 και οι νόμοι περί των τηλεπικοινωνιών προσεγγίζουν ως ένα βαθμό τα ηλεκτρονικά εγκλήματα. Ως εκ τούτου, η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης, καθώς και άλλων διεθνών οργανισμών, για την αντιμετώπιση των σχετικών θεμάτων.

Οι πρώτες μορφές ηλεκτρονικού εγκλήματος εμφανίστηκαν την δεκαετία του ’70 στην Αμερική. Οι περισσότερες υποθέσεις περιλαμβάνουν την παράνομη εισβολή σε τηλεφωνικά συστήματα, την υπεξαίρεση μεγάλων χρηματικών ποσών από τράπεζες, την υποκλοπή αριθμών πιστωτικών καρτών και αρχείων μεγάλων εταιρειών και οργανισμών, όπως είναι το FBI, την παιδική πορνογραφία και αποπλάνηση ανηλίκων μέσω site και chat rooms και τέλος την παράνομη διακίνηση λογισμικού. Όμως οι πιο γνωστές και διασκεδαστικές ιστορίες είναι αυτές των hackers, οι οποίοι στην πλειοψηφία ενεργούν είτε για να ικανοποιήσουν την περιέργεια τους είτε για να διασκεδάσουν (βλ. Kevin Poulsen). Για τον λόγο αυτό είναι και οι μοναδικοί δράστες ηλεκτρονικού εγκλήματος οι οποίοι είναι αμφιλεγόμενοι και πολλές φορές χρήζουν της συμπάθειας του κόσμου.

Στην χώρα μας, οι κύριες μορφές ηλεκτρονικών εγκλημάτων και κυβερνοεγκλημάτων που παρουσιάστηκαν και εξιχνιάστηκαν είναι η παιδική πορνογραφία, το Cracking και hacking, η παράνομη διακίνηση λογισμικού και οι απάτες μέσω πιστωτικών καρτών. Για το λόγο αυτό η παρούσα επικεντρώνεται σε αυτές, περιγράφοντας και αναλύοντάς τες. Και στις τέσσερις μορφές βασικά σημεία αποτελούν η σωστή ενημέρωση του χρήστη, τα μέτρα πρόληψης και εξιχνίασης καθώς και οι τρόποι αντιμετώπισής τους.

Το ηλεκτρονικό έγκλημα είναι μία μορφή εγκλήματος το οποίο λόγω των συγκεκριμένων χαρακτηριστικών του είναι πολύ δύσκολο να εξιχνιαστεί. Πρώτον η έλλειψη φυσικής επαφής αδυνατεί να δώσει απτές αποδείξεις. Δεύτερον η έλλειψη βίας καθιστά την αντίληψη και την τιμωρία τους δύσκολη. Τρίτον η διεθνής φύση του καθιστά δύσκολο όχι μόνο τον προσδιορισμό του δράστη αλλά και του τόπου τέλεσης του εγκλήματος. Τέλος δεν υπάρχει συγκεκριμένο θύμα, κάτι το οποίο μεγαλώνει το εύρος της εγκληματικότητας. Υπάρχουν βέβαια κάποια στοιχεία που βοηθάνε στην εξιχνίασή του, όπως ο ηλεκτρονικός υπολογιστής του παραβάτη και τα ηλεκτρονικά του αποτυπώματα (διεύθυνση IP παραβάτη)

ΕΡΩΤΗΣΕΙΣ- ΑΠΑΝΤΗΣΕΙΣ

Ερώτηση 1

Θεωρείται πως το υπάρχον νομοθετικό πλαίσιο είναι δίκαιο για τους παραβάτες του ηλεκτρονικού εγκλήματος ή χρήζουν οι νόμοι αναθεώρησης;

Απάντηση:

Ως ηλεκτρονικό έγκλημα θεωρούνται οι αξιόποινες πράξεις, που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία. Τα ηλεκτρονικά εγκλήματα διακρίνονται σε αυτά που τελούνται με τη χρήση Ηλεκτρονικών Υπολογιστών και σε εκείνα, που τελούνται μέσω του Διαδικτύου, τα λεγόμενα Κυβερνοεγκλήματα. Στην Ελλάδα δεν υπάρχει νόμος, ο οποίος να αναφέρεται αποκλειστικά και μόνο σε θέματα Διαδικτύου και να ρυθμίζει τη συμπεριφορά των χρηστών του από άποψη ποινικού δικαίου. Ως εγκλήματα που τελούνται με τη χρήση Η/Υ η ελληνική ποινική νομοθεσία ορίζει την παράνομη αντιγραφή απορρήτων δεδομένων (370Β ΠΚ), την παράνομη χρήση ή πρόσβαση σε προγράμματα ή στοιχεία Η/Υ, όπου περιλαμβάνεται και το hacking (370Γ ΠΚ), και την απάτη με υπολογιστή (386Α ΠΚ). Αν τα εγκλήματα αυτά διαπράττονται και σε περιβάλλον Διαδικτύου (Κυβερνοεγκλήματα), τότε τα άρθρα αυτά εφαρμόζονται και σε τέτοιες περιπτώσεις. Ένας άλλος διαχωρισμός γίνεται με βάση το αν στοχεύουν απ' ευθείας σε ηλεκτρονικό υπολογιστή, π.χ. ιός Η/Υ, Denial of Services Attack, ή αν διευκολύνονται από τη χρήση δικτύων και συσκευών υπολογιστών, με διαφορετικό όμως στόχο, π.χ. απάτη, κλοπή ταυτότητας κλπ. Το Κυβερνοέγκλημα μπορεί να πάρει πάρα πολλές μορφές, πχ. α. απάτες μέσω Διαδικτύου, β. παιδική πορνογραφία, γ. cracking και hacking, δ. διακίνηση - πειρατεία λογισμικού, ε. εγκλήματα σχετικά με πιστωτικές κάρτες, στ. διακίνηση ναρκωτικών, ζ. και εγκλήματα στα chat rooms. Κάποια από τα Κυβερνοεγκλήματα μπορούν να τελεστούν και εκτός διαδικτύου, η ύπαρξη όμως ενός τόσο εκτενούς δικτύου υποβοηθάει σε μεγάλο βαθμό την τέλεσή τους. Για παράδειγμα η πορνογραφία ανηλίκων, η οποία υπάρχει και διώκεται ποινικά ακόμα και offline, έχει σημειώσει έξαρση λόγω της διάδοσης του διαδικτύου. Πολλά εγκλήματα που διαπράττονται μέσω διαδικτύου διώκονται με βάση υπάρχουσες διατάξεις του ποινικού κώδικα, όπως η εξύβριση, η εκβίαση και η δυσφήμηση (απλή και συκοφαντική). Το έγκλημα στον κυβερνοχώρο έχει ιδιαίτερα χαρακτηριστικά. Είναι γρήγορο, μπορεί να συμβεί σε οποιονδήποτε είναι συνδεδεμένος στο διαδίκτυο και είναι δυνατό να πραγματοποιηθεί από και προς οποιοδήποτε σημείο στον πλανήτη. Θεμιτός είναι και ένας διαχωρισμός εγκληματιών, πχ. αφ' ενός εραστής, που δεν έχει ιδιαίτερες ικανότητες σε σχέση με Η/Υ, ανεβάζει υβριστικά status στο facebook και αφ' ετέρου η δράση ενός cracker ή ενός διαδικτυακού απατεώνα. Τα ζητήματα δικαιοδοσίας, πχ. η επικοινωνία των ελληνικών αρχών με το Facebook, είναι ρυθμισμένα. Οι κυβερνοεγκληματίες όμως, που προκαλούν προβλήματα σε κράτη, οργανισμούς και ιδιώτες, είναι άτομα ευφυή, με γνώσεις και

εξοπλισμό που καθιστούν εξαιρετικά δύσκολο τον εντοπισμό τους. Στη Μ. Βρετανία οι hackers μπορεί να θεωρηθούν τρομοκράτες. Στις ΗΠΑ οποιαδήποτε πράξη μη εξουσιοδοτημένης πρόσβασης σε Η/Υ θεωρείται τρομοκρατική και τιμωρείται, ανάλογα με τη σημασία της εισβολής, μέχρι και με ισόβια κάθειρξη χωρίς δυνατότητα μείωσης της ποινής. Ακόμα όμως κι αν εντοπιστούν τα άτομα αυτά, η σύλληψή τους συχνά επαφίεται στη συνεργασία μεταξύ των χωρών, όπου εντοπίστηκε η δραστηριότητά τους και τη χώρα όπου βρίσκονται. Στην ουσία αυτό αποτελεί ένα από τα πιο μεγάλα εμπόδια για τις Αρχές που μπορεί να αντιμετωπιστεί μόνο με συνεργασίες και χάραξη κοινών πλαισίων δράσης. Στο διαδίκτυο υπάρχει ανωνυμία. Για να διαπιστωθεί ο τόπος και η ταυτότητα κάποιου εγκληματία, απαιτείται ακριβός εξοπλισμός και γνώσεις και σε αρκετές περιπτώσεις (ειδικά όσες αφορούν την εμπλοκή αρχών του εξωτερικού) αίτημα δικαστικής συνδρομής. Ένα από τα σοβαρά ζητήματα του ηλεκτρονικού εγκλήματος είναι ο καθορισμός του τόπου τέλεσής του. Ένα απλό παράδειγμα: Ο server, όπου φιλοξενείται μια ιστοσελίδα με απάτες online dating βρίσκεται στη Ρωσία, ο διαχειριστής της στη Ρουμανία και οι δραστηριότητες της επεκτείνονται σε πολλές χώρες, ανάμεσά τους και η Ελλάδα. Ως τόπο τέλεσης εν προκειμένω μπορεί κανείς να θεωρήσει την Ελλάδα, αφού εδώ λαμβάνει χώρα η εξαπάτηση. Αυτό όμως θα ήταν αναποτελεσματικό, αφού όσο ο κάτοχος του server δεν παραβιάζει νόμους της χώρας, όπου είναι εγκατεστημένος, οι πιθανότητες να πάψει να είναι online είναι ελάχιστες. Η Ελληνική Αστυνομία συνεργάζεται με διάφορες οργανώσεις αλλά και συναρμόδιους φορείς, όπως η Europol, η Interpol, και μέσω αυτής με τις αρχές διαφόρων κρατών, όπως οι ΗΠΑ, η Ολλανδία, το Ισραήλ, η Ρουμανία και άλλες. Αρκετές αλλαγές που θα συμβάλλουν στον πιο εύστοχο καθορισμό των κυβερνοεγκλημάτων, την άρση αδικιών αλλά και στη διεθνή συνεργασία αναμένεται να φέρει η Συνθήκη της Βουδαπέστης για το Κυβερνοέγκλημα. Παρά το ότι η εν λόγω συνθήκη έχει υπογραφεί από 50 χώρες, μεταξύ αυτών και η Ελλάδα, και είναι σε ισχύ από το 2004, δεν έχει κυρωθεί ακόμη από την Ελλάδα. Η συνθήκη αυτή περιέχει εκτενείς αναφορές σε όλες τις μορφές του κυβερνοεγκλήματος, ενώ αποτελεί μια καλή βάση για να αναπτυχθεί και στον τομέα αυτό η διακρατική συνεργασία.

Ερώτηση 2

Είναι κατά τη γνώμη σας το Διαδίκτυο ο ηθικός αυτουργός του ηλεκτρονικού εγκλήματος;

Απάντηση:

Το διαδίκτυο δεν είναι ο ηθικός αυτουργός του ηλεκτρονικού εγκλήματος. Είναι μέσο τέλεσης των κυβερνοεγκλημάτων, τα οποία αποτελούν μέρος των ηλεκτρονικών εγκλημάτων. Στην απάντηση στην 1η ερώτηση περιγράφονται αναλυτικά τα εγκλήματα, που διαπράττονται στο Διαδίκτυο.

Ερώτηση 3

Το ανθρώπινο δυναμικό της Δίωξης Ηλεκτρονικού Εγκλήματος στη χώρα μας είναι αρκετό ή θα έπρεπε να διερευνηθεί;

Απάντηση:

Η Υπηρεσία Οικονομικής Αστυνομίας και Διώξης Ηλεκτρονικού Εγκλήματος στελεχώνεται με έμπειρα στελέχη της Ελληνικής Αστυνομίας, που προέρχονται κυρίως από Υπηρεσίες της Ασφάλειας, καθώς και Αξιωματικούς Ειδικών Καθηκόντων, πτυχιούχους ανώτατων εκπαιδευτικών ιδρυμάτων, με μεταπτυχιακούς τίτλους στα γνωστικά αντικείμενα:

- Χρηματοοικονομικής 19
- Τραπεζικών εφαρμογών ·

- Φοροτεχνικών εφαρμογών
- Λογιστικής · Πληροφορικής
- Διερεύνησης ψηφιακών πειστηρίων
- Τηλεπικοινωνιών και δικτύων
- Μηχανικών ηλεκτρονικών υπολογιστών

  Τα στελέχη αυτά έχουν εκπαιδευτεί ειδικά με σκοπό να εξασφαλιστεί το μέγιστο της αποτελεσματικής συνεργασίας των Υπηρεσιών στις περιπτώσεις κοινής ή επικουρικής επιχειρησιακής δράσης. Η επιλογή του προσωπικού γίνεται με αυστηρά κριτήρια. Σε αυτά συνεκτιμάται η επαγγελματική επάρκεια, οι επιστημονικές γνώσεις, η αποδοτικότητα και το ήθος. Με αυτά τα δεδομένα είναι προφανές ότι το ανθρώπινο δυναμικό της εν λόγω Υπηρεσίας δεν μπορεί αλλά και δεν υπάρχει λόγος να αυξηθεί υπέρμετρα. Σημασία έχει να τηρούνται πάντα τα κριτήρια εισόδου σε αυτή των στελεχών της ΕΛΑΣ.

Ερώτηση 4

Πιστεύεται για να περιοριστεί το bullying αρκούν ημερίδες και ενημερώσεις γονέων – παιδιών ή απαιτούνται πιο δραστικά μέτρα;

Απάντηση:

Για να περιοριστεί το bullying, δηλαδή ο ενδοσχολικός εκφοβισμός, πρέπει να πάψει να θεωρείται ότι το προκαλεί γενικώς και αορίστως το κοινωνικό σύστημα και όχι αυτό, που όλοι μας βλέπουμε, οι συγκεκριμένες συμπεριφορές δηλαδή και οι στάσεις των ατόμων και της οικογένειας. Συγκεκριμένα πρέπει: 1. Τα παιδιά, που υφίστανται bullying, να μιλάνε στο όνομα της αλληλεγγύης και της προστασίας τους από τη βία χωρίς να φοβούνται ότι δήθεν συμμετέχουν σε μια βρώμικη προσπάθεια να νομιμοποιηθεί στις συνειδήσεις το “κάρφωμα”, ο χαφιεδισμός και η «καταστολή». 2. Οι γονείς να συνεργάζονται με το σχολείο και να μη θεωρείται «ρουφιανιά» η καταγγελία των φαινομένων bullying στον καθηγητή ή τον διευθυντή του σχολείου.

Ερώτηση 5

Ποια κοινωνικά στρώματα είναι ιδιαίτερα ευάλωτα σε εγκλήματα του Διαδικτύου;

Απάντηση:

Τα εγκλήματα του Διαδικτύου διαπράττονται εις βάρος ατόμων ή ομάδων ατόμων με ποινικό κίνητρο να βλάψουν σκόπιμα τη φήμη του θύματος ή να προκαλέσουν σωματική ή ψυχική βλάβη στο θύμα, άμεσα ή έμμεσα, με τη χρήση του Διαδικτύου. Πρόκειται για παράνομες πράξεις προσβολής περιουσιακών ή άλλων δικαιωμάτων φυσικών και νομικών προσώπων, που γίνονται μέσω της χρήσης μιας οποιασδήποτε συσκευής ηλεκτρονικής επεξεργασίας δεδομένων. Μέσο τέλεσης της πράξης μπορεί να είναι ένας ηλεκτρονικός υπολογιστής συνδεδεμένος σε ένα δίκτυο επικοινωνιών, όπως το Διαδίκτυο ή άλλη τερματική συσκευή, όπως ένα σταθερό ή κινητό τηλέφωνο. Τα εγκλήματα αυτά μπορεί να απειλήσουν μέχρι και την ασφάλεια ενός έθνους και βεβαίως την ασφάλεια των συναλλαγών. Συχνός στόχος τους η παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας, η παιδική πορνογραφία και τα προσωπικά δεδομένα. Προβλήματα προστασίας της ιδιωτικής ζωής προκύπτουν επίσης, όταν εμπιστευτικές πληροφορίες έχουν χαθεί ή υποκλαπεί. Σε διεθνές επίπεδο, τόσο κυβερνητικοί όσο και μη κρατικοί παράγοντες ασχολούνται με εγκλήματα στον κυβερνοχώρο, όπως η κατασκοπεία, η κλοπή και τα διασυνοριακά εγκλήματα. Είναι προφανές ότι εκείνα τα κοινωνικά στρώματα, που έχουν σχέση με τις δραστηριότητες αυτές είναι ιδιαίτερα ευάλωτα σε εγκλήματα του Διαδικτύου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική Βιβλιογραφία

Ζάννη Αναστασία, <Το διαδικτυακό έγκλημα>, σελ. 23

Ελαφρός Γιάννης, <Το διαδίκτυο αλλάζει άρδην την ζωή μας>, σελ.31

Sputnik. Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα. Σελ.59

Η λέξη Arpanet προκύπτει από τα αρχικά της υπηρεσίας του αμερικανικού στρατού

Δίκτυο είναι ένα σύνολο υπολογιστών συνδεδεμένων μεταξύ τους ασύρματα ή ασύρματα που δίνει την δυνατότητα να διαμοιράζονται πληροφορίες ταυτόχρονα σε ένα μεγάλο σύνολο ανθρώπων.

Κούρτη Ευαγγελία, 2003. Η επικοινωνία στο διαδίκτυο. Σύγχρονες Μορφές Επικοινωνίας. Αθήνα: Ελληνικά Γράμματα σελ. 63

Παναγιωτοπούλου, Ρ. (2003. Η ΨΗΦΙΑΚΗ ΠΡΟΚΛΗΣΗ: ΜΜΕ ΚΑΙ ΔΗΜΟΚΡΑΤΙΑ. ΤΥΠΟΘΗΤΩ

Θεοφίλου, Μ., (http://www.paidiatros.com/efivos/psyxologia/internet-addiction-prevention, 2017, Διαδίκτυο: Εθισμός, πρόληψη και τρόποι αντιμετώπισης

Κιτρίδης, Δ., (2014), *Social Media Facebook Marketing*, Αθήνα: Ευρασία, σελ. 67-70

Σιδέρη, Μ., (2010), *Το βιβλίο του Facebook – Ένας οδηγός για «αθώους» χρήστες*, Αθήνα: Κλειδάριθμος, σελ. 25-28

Κιτρίδης, Δ., (2014), *Social Media Facebook Marketing*, Αθήνα: Ευρασία, σελ. 67-70
Σιδέρη, Μ., (2010), *Το βιβλίο του Facebook – Ένας οδηγός για «αθώους» χρήστες*, Αθήνα: Κλειδάριθμος, σελ. 56-57

Κόνσουλας, Θ., 2014, http://www.socialmedialife.gr/110183/ti-einai-to-viber-kai-pos-leitourgei/, τι είναι το viber και πως λειτουργεί

Ή έγκλημα του κυβερνοχώρου, όπως το αναφέρει ο Ι. Αγγελής στο <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 675

Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 676

Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, 678

Μυλωνόπουλος Χρ., <Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο>, σελ. 14

Όπως ο Donald Ingraham, ο οποίος υποστήριζε ότι δεν υπάρχει το ηλεκτρονικό έγκλημα ως αυτόνομη κοινωνική πραγματικότητα, και ο Douglas Reimer, ο οποίος υποστήριζε ότι τα ηλεκτρονικά εγκλήματα δεν ήταν νέα εγκλήματα αλλά τα ίδια παλαιά εγκλήματα τα οποία διαπράττονται με νέους τρόπους χάρη στην πληροφορική τεχνολογία και τους ηλεκτρονικούς υπολογιστές για αναλυτική παράθεση των απόψεών τους ,βλέπε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 46

Όπως οι Parker, Bequai και Bloomberg, για αναλυτική παράθεση των απόψεών τους, βλέπε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 37- 44.

Όπως οι Martin Wasik, Karen Forcht, Daphyne Thomas, Karen Wigginton, Steve Shackelford, Scott Charney, Barry Hurewitz, Allen Lo, αναλυτικά οι απόψεις τους σε Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 48- 51

Βλ. Κριθαράς Θ., <Ποινικό Δίκαιο και Διαδίκτυο>, σελ. 10

Κιούπης Δ., <Αλλοίωση Ηλεκτρονικών Δεδομένων και Αθέμιτη Πρόσβαση σε Ηλεκτρονικά Δεδομένα- Κενά και Αδυναμίες της Ποινικής Νομοθεσίας>, σελ. 961

Βασιλάκη Ε., <Καταχρήσεις των νέων μέσων τηλεπικοινωνίας και θέματα ποινικής καταστολής >, σελ. 28-29

Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 677

Βλ. Αργυρόπουλος Α., <Ηλεκτρονική Εγκληματικότητα>, σελ., 24-25, ενώ αντίθετα υποστηρίζει ο Ι. Αγγελής, βλ. του ιδίου, <Διαδίκτυο και Ποινικό Δίκαιο>, σελ. 677

Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο- Έγκλημα στον κυβερνοχώρο (Cybercrime- Internet Crime)>, σελ. 677-678

Βλ., Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο- Έγκλημα στον κυβερνοχώρο (Cybercrime- Internet Crime)> Κατά τη γνώμη του Ι. Αγγελή ως εγκλήματα που διαπράττονται σε περιβάλλον ηλεκτρονικών υπολογιστών νοούνται μόνο αυτά που τελούνται χωρίς τη χρήση του διαδικτύου., σελ. 676- 677

Κιούπη Δ., <Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της ποινικής νομοθεσίας>, σελ. 963- 964.

Βλ. τη Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber- crime) και βλ. την Πρόταση Απόφασης Πλαισίου του Συμβουλίου, για επιθέσεις κατά των συστημάτων πληροφοριών (27/8/2002), Επίκαιρα Νομοθετήματα, Ποινικό Δίκαιο 2/2003, σελ. 115 και εξής.

Βλ. Ζάννη Α. <Το διαδικτυακό έγκλημα>, σελ. 89 και Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα, Μορφές, Πρόληψη, Αντιμετώπιση>, σελ. 40.

Βλ. Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 110
Βασιλάκη Ειρήνη, <Τα φαινόμενα phirsing και pharming και η ποινική τους αξιολόγηση, βλ. και Κιούπης Δ., <Καταπολέμηση της ηλεκτρονικής εγκληματικότητας στην Ε.Ε.>, σε Τιμητικό Τόμο Αργυρίου Καρρά, σελ. 1028

Βλαχόπουλος Κ., <Ηλεκτρονικό Έγκλημα>, σελ. 71.

Ζάννη Α., <Το διαδικτυακό έγκλημα>, σελ. 78

Αγγελής Ι., <Διαδίκτυο και Ποινικό Δίκαιο>, <Έγκλημα στον Κυβερνοχώρο>, Ν/2000, σελ. 667- 668 και Δ. Αγγελόπουλος –Ι. Πάσχος, <Κατάσχεση- Ανάλυση ψηφιακών πειστηρίων>, Ποινική Δικαιοσύνη Τεύχος 4/2003, σελ. 439

Βλαχόπουλος Κ., «Ηλεκτρονικό Έγκλημα», σελ 71

Μυλωνόπουλος Χ. «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 22

ΦΕΚ Α 199/31.08.1988.

Ζάννη Α., «Το διαδικτυακό έγκλημα», σελ. 192

Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 904-911, Ίδρυμα Μαραγκοπούλου για τα Δικαιώματα του Ανθρώπου, Σειρά Ομάδας Νέων (ΙΜΔΑ), «Η Παιδική Πορνογραφία στο Διαδίκτυο», Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 950 επ., Ζάννη Α., «Το διαδικτυακό έγκλημα», σελ. 76επ., Ιγγλεζάκη Ι., «Δίκαιο της Πληροφορικής», σελ.283 επ.

Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 952 επ.σελ. 953.

ΠοινΔικ 2005/960.

Μυλωνόπουλο Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 71 επ., Μαργαρίτη Μ. «Ποινικός Κώδικας Ερμηνεία- Εφαρμογή», σελ. 1032 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1026- 1030, Βασιλάκη Ε., «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ.159 επ.

Μυλωνόπουλος Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 86. Βλ. Μαργαρίτη Μ. «Ποινικός Κώδικας Ερμηνεία- Εφαρμογή», σελ. 1034 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1030- 1033, Βασιλάκη Ε. «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ. 75 επ., Καϊάφα Γκμπάντι Μ. «Ποινικό δίκαιο και καταχρήσεις της πληροφορικής», Αρμενόπουλος 2007/1065 επ

Μαργαρίτη Μ., «Ποινικός Κώδικας, Ερμηνεία- Εφαρμογή», σελ. 1192 επ., Μυλωνόπουλου Χ., «Ηλεκτρονικοί Υπολογιστές και Ποινικό Δίκαιο», σελ. 54 επ., Μυλωνόπουλου Χ., «Ποινικό ΔίκαιοΕιδικό Μέρος: Τα εγκλήματα κατά της ιδιοκτησίας και της περιουσίας, α. 372-406 Π.Κ.». σελ. 596 επ., Κωστάρα Α., «Ποινικό Δίκαιο, Επιτομή ειδικού μέρους», σελ. 1137-1142, Βασιλάκη Ε. «Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών», σελ. 185 επ., Καϊάφα Γκμπάντι Μ. «Ποινικό δίκαιο και καταχρήσεις της πληροφορικής», Αρμενόπουλος 2007/1065 επ.

Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ. 70, Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα>, σελ. 131.

Λάζος Γρ., <Πληροφορική και Έγκλημα>, σελ. 70.

Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ.67, Βλαχόπουλος Κ. <Ηλεκτρονικό Έγκλημα>, σελ. 129.

Λάζος Γρ. <Πληροφορική και Έγκλημα>, σελ. 62.

Ξένη Βιβλιογραφία

Evans, J., (2015), Internet Addiction: Powerful Strategies For Internet Addiction, Depression And Anxiety And Stress Management (Social Media Addiction, Facebook, Addiction ... And Anxiety, Compulsive Behavior) USA: Yale University Press, pp. 59-62

Evans, J., (2015), Internet Addiction: Powerful Strategies For Internet Addiction, Depression And Anxiety And Stress Management (Social Media Addiction, Facebook, Addiction ... And Anxiety, Compulsive Behavior) USA: Yale University Press, pp. 59-62

Tuten Tracy, (2016), *Social Media Marketing*, Εκδόσεις Δίαυλος, σελ. 23-27

Tuten Tracy, (2016), *Social Media Marketing*, Εκδόσεις Δίαυλος, σελ. 23-27

Clarke R., ‘’Technological Aspects of Internet Crime Prevention’’

John Perry Barlow, ‘’Declaration of Independence of the Internet’’

Kevin Poulsen

Murin Kotadial, <Education, not legislation will reduce e- crimes>

Ιστοσελίδες

https://el.wikipedia.org/wiki/Διαδίκτυο

ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΕΥΡΩΠΑΙΚΗ ΕΝΩΣΗ

http://www.snsagency.gr
Τι είναι το Facebook

http://www.snsagency.gr
Τι είναι το YouTube

www.secnews.gr/tourkia-epitheseis-ellinon-hacker

http://dide.flo.sch.gr

http://www.theartofcrime.gr/artofcrime/assets/hackers.dot

www.saferinternet.gr
https://www.google.gr (εικονα)

https://www.e-nomothesia.gr

www.dsanet.gr (ΑΠ 810/2007)

http://law.findlaw.com
state-laws/computer-crimes/california

http://law.findlaw.com
state-laws/computer-crimes/new-york