ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΟΙΝΩΝΙΚΩΝ
ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΤΜΗΜΑ ΔΙΚΑΙΟΥ
« ΔΙΚΑΙΟ ΚΑΙ ΕΥΡΩΠΑΪΚΗ ΕΝΟΠΟΙΗΣΗ»

ΚΑΤΕΥΘΥΝΣΗ: «ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΘΕΩΡΙΑ ΔΙΚΑΙΟΥ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΜΕ ΘΕΜΑ

«ΕΓΚΛΗΜΑ ΚΑΙ ΔΙΑΔΙΚΤΥΟ»

ΚΟΛΙΩΝΗ ΚΩΝΣΤΑΝΤΙΝΑ

ΑΘΗΝΑ, ΟΚΤΩΒΡΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή

Οι ηλεκτρονικοί υπολογιστές αποτελούν τμήμα της ζωής μας. Η αυξανόμενη χρήση των υπολογιστών δεν διαμόρφωσε απλώς νέες συνθήκες στην καθημερινή μας ζωή, την εργασία, τη διασκέδαση, την επικοινωνία, αλλά ταυτόχρονα δημιουργώντας ένα πεδίο δράσης διαπλάθει καθημερινά νέες μορφές κοινωνικής συμπεριφοράς. Άτομα, επιχειρήσεις, κράτη ολόκληρα στηρίζονται σε αυτούς. Η εκτεταμένη χρήση των ηλεκτρονικών υπολογιστών στη μηχανοργάνωση εταιρειών, κρατικών οργανισμών και υπηρεσιών, η χρήση τους για την εκτέλεση επαγγελματικών δραστηριοτήτων μετέβαλλαν τα δεδομένα των συναλλαγών. Η σημασία των Η.Υ. δεν αντανακλάται μόνο στην αύξηση του αριθμού τους, αλλά ακόμη περισσότερο στην αλματώδη τεχνολογική τους βελτίωση και στις διαρκώς περισσότερες χρήσεις του[1].

Ο ποινικός νομοθέτης δραστηριοποιήθηκε και θέλησε να καλύψει μορφές εγκληματικής δράσης που σχετίζονται με τους Η.Υ. Ενδεικτικά αναφέρεται η ψήφιση ειδικών διατάξεων για τους υπολογιστές (άρθρα 370Β, 370Γ, 386^{Α} Π.Κ.).

Ένα εντελώς καινούργιο σκηνικό δημιούργησε η εμφάνιση του Διαδικτύου καθώς εκατομμύρια χρήστες Η.Υ. συνδέθηκαν μεταξύ τους και αποτέλεσαν μια παγκόσμια κοινότητα που κατήργησε κάθε φράγμα (πέρα από το γλωσσικό βέβαια στο βαθμό που τα διαβιβαζόμενα δεδομένα αντιστοιχούν σε κείμενο[2]). Αυτό το παγκόσμιο πεδίο συνάντησης των χρηστών του διαδικτύου ονομάστηκε και κυβερνοχώρος. Η δημιουργία του διαδικτύου μετέβαλε ουσιαστικά τα δεδομένα του κόσμου των Η.Υ. και αναμόρφωσε δραστικά το αντικείμενο ρύθμισης του νομοθέτη[3].

---

[1] Κιούπης Δημήτριος: Ποινικό Δίκαιο και Internet, Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1999, σελ.17.

[2] Αν και με την ευρεία χρήση της Αγγλικής γλώσσας σήμερα έχει ξεπεραστεί και αυτού του είδους εμπόδιο.

[3] Κιούπης Δημήτριος: Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet, Ποιν. Δικ. ΜΗ/1998 σελ. 712.

Το Διαδίκτυο αποτελεί πιθανότατα την πλέον αμφιλεγόμενη έννοια των τελευταίων χρόνων. Αυτό κυρίως οφείλεται αφενός στην τεράστια επιτυχία του μέσου και στη διείσδυση που αυτό έχει επιτύχει στην καθημερινή μας ζωή και αφετέρου στη φοβία που εμφανώς ή αδιόρατα περιβάλλει τη χρήση του και η οποία πηγάζει από τον παγκόσμιο χαρακτήρα του Διαδικτύου σε συνδυασμό με τη φαινομενική έλλειψη ή έστω ανεπάρκεια μηχανισμών ελέγχου και ρύθμισης της χρήσης του.

Το Διαδίκτυο το οποίο αρχικά απευθυνόταν πρωτίστως στη σχετικά περιορισμένη ερευνητική/ακαδημαϊκή κοινότητα, εξελίχθηκε διαμέσου των τελευταίων χρόνων τόσο από άποψης προσβασιμότητας όσο και ως προς το διαθέσιμο περιεχόμενο και παρεχόμενες υπηρεσίες καταλαμβάνοντας τελικά δεσπόζουσα θέση στην προσωπική και επαγγελματική ζωή των περισσοτέρων ως μέσο επικοινωνίας, διασκέδασης και ενημέρωσης, αλλά και εργαλείο διεκπεραίωσης οικονομικών συνδιαλλαγών και προώθησης επιχειρηματικών στόχων και διαδικασιών. Ο ρόλος του Διαδικτύου στην επιτυχία επιχειρηματικών δράσεων αλλά και εν γένει ανάπτυξη και πρόοδο χωρών και κοινωνιών αντικατοπτρίζεται και στη σημασία η οποία αποδίδεται από τον ιδιωτικό και δημόσιο τομέα στην υλοποίηση και προώθηση των ηλεκτρονικών εφαρμογών (e-learning, e-government, e-culture, e-health, e-commerce, e-procurement, e-office κλπ). Παράλληλα εφαρμογές όπως το ηλεκτρονικό ταχυδρομείο και ο Παγκόσμιος Ιστός οι οποίες έδωσαν στο Διαδίκτυο την αρχική ώθηση εξακολουθούν να διατηρούν τη δυναμική τους, πλαισιωμένες πια από νέες τεχνολογίες οι οποίες κάνουν δυνατή τη χρήση του Διαδικτύου για μετάδοση φωνής και εικόνας, διεξαγωγή τηλε-διασκέψεων, παροχή περιεχομένου κλπ. Ταυτόχρονα, οι εξελίξεις στο χώρο της κινητής τηλεφωνίας (συσκευές/δίκτυα/υπηρεσίες) καθιστούν δυσδιάκριτες τις διαχωριστικές γραμμές τηλεπικοινωνιών και δικτύων υπολογιστών, προσεγγίζοντας το όραμα της καθολικής πρόσβασης και καταργώντας και τους εναπομείναντες χωρικούς και χρονικούς περιορισμούς. Τέλος και το επιχειρηματικό περιβάλλον όπως αυτό διαμορφώνεται από τους οικονομικούς παράγοντες, το ρυθμιστικό-

κανονιστικό πλαίσιο και την έλευση νέων τεχνολογιών διαδραματίζει το δικό του ιδιαίτερο ρόλο στην περαιτέρω διάδοση της χρήσης του Διαδικτύου.

Με την ανάπτυξη του διαδικτύου άρχισε να εμπεδώνεται η άποψη ότι υπάρχουν παράνομες πράξεις που διευκολύνονται με τη χρήση του υπολογιστή και προσβάλλουν έννομα αγαθά. Σήμερα γίνεται λόγος για πράξεις που στρέφονται εναντίον των συστημάτων πληροφοριών, τα οποία περιλαμβάνουν τον υπολογιστή, τα προγράμματα, και τα δίκτυα επικοινωνιών. Η διάκριση των εγκλημάτων, μεταξύ των εγκλημάτων που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών και εκείνων που τελούνται στον κυβερνοχώρο έχουν αντικατασταθεί από μια ενιαία κατηγορία «εγκλημάτων πληροφορικής»[4]. Η χρήση του διαδικτύου για τη διάπραξη εγκληματικών πράξεων προσδίδει από μόνη της κάποια ιδιαίτερα ποιοτικά χαρακτηριστικά, με αποτέλεσμα να συντίθεται μια ιδιαίτερη μορφή εγκληματικότητας η οποία δημιουργεί ένα νέο είδος modus operandi των δραστών. Δύο από τις πιο επικίνδυνες μορφές εγκληματικής συμπεριφοράς που παρουσιάζονται στο διαδίκτυο και απειλούν πρωταρχικά την ασφάλεια ροής των πληροφοριών, δημιουργώντας ταυτόχρονα σημαντικές βλάβες περιουσιακών αγαθών είναι η περιπτώσεις hacking και cracking.

Καθώς λοιπόν το Διαδίκτυο διεκδικεί και κατακτά διαρκώς μεγαλύτερο μερίδιο/ρόλο σε όλο το φάσμα των δραστηριοτήτων μας, θέματα που αφορούν στην ασφαλή χρήση του μέσου καθώς και οι επιπτώσεις που το Διαδίκτυο έχει στην καθημερινή μας ζωή αποκτούν ιδιαίτερη σημασία. Καλούμαστε να αντιμετωπίσουμε φαινόμενα όπως η διακίνηση παράνομου περιεχομένου, οργάνωση παράνομων δραστηριοτήτων, ηλεκτρονικό έγκλημα, προώθηση παράνομων ουσιών, υποκλοπή/εκμετάλλευση/δημοσιοποίηση προσωπικών και άλλων ευαίσθητων δεδομένων κλπ. Και όλα αυτά σε ένα παγκοσμιοποιημένο περιβάλλον, με εγγενώς κατεξοχήν δυναμικό χαρακτήρα, το οποίο μεταβάλλεται συνεχώς λόγω της ταχείας εξέλιξης και εισαγωγής νέων

[4] Νούσκαλης Γεώργιος. Απάτη με ηλεκτρονικό υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386^{A} Π.Κ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ε.Ε. Ποιν.Δικ.2/2003 σελ 178 επ.

τεχνολογιών, και στο οποίο φαίνεται να απουσιάζουν κεντρικοί μηχανισμοί ελέγχου τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Παράλληλα, δεν θα πρέπει να αγνοήσουμε και τις επιπτώσεις τις οποίες έχει το εικονικό αυτό περιβάλλον στην ανθρώπινη ψυχολογία και κοινωνική δραστηριότητα: στον τρόπο που επικοινωνούμε, συναναστρεφόμαστε, εργαζόμαστε, ψυχαγωγούμαστε κλπ.[5]

Αντικείμενο της παρούσης εργασίας είναι η μελέτη των εγκληματικών συμπεριφορών που σχετίζονται με το Διαδίκτυο καθώς επίσης και οι νομοθετικές ρυθμίσεις που πραγματοποιήθηκαν για την αντιμετώπισή τους σε ευρωπαϊκό και εθνικό επίπεδο .

[5]ΠΟΛΙΤΗΣ Διαδίκτυο: Όρια και Ασφάλεια (Κύπρος), www.politis-news.com

2. Τι είναι το internet-διαδίκτυο, η λειτουργία του και ο παγκόσμιος ιστός.

Το διαδίκτυο είναι ένα ανοιχτό μη ιεραρχικό σύστημα δικτύου[6]. Δεν υπάρχει δηλαδή ένας κεντρικός υπολογιστής ή ένα συντονιστικό κέντρο. Ο απλός χρήστης συνδέεται με τι διαδίκτυο μέσω των παροχέων πρόσβασης. Η σύνδεση με αυτούς γίνεται μέσω μιας τηλεφωνικής γραμμής, ενός ηλεκτρονικού υπολογιστή και μιας συσκευής, του modem. Ο χρήστης καλεί έναν αριθμό του παροχέα και μόλις επιτευχθεί η σύνδεση εισέρχεται στον κόσμο του διαδικτύου[7]. Το διαδίκτυο είναι το μεγαλύτερο σύστημα υπολογιστών στον κόσμο. Αποτελείται από χιλιάδες συνδεδεμένα μεταξύ τους δίκτυα[8] σε όλο τον κόσμο. Το πλεονέκτημα του διαδικτύου είναι ότι αν κάποιο δίκτυο καταστραφεί, οι πληροφορίες που είναι να μεταδοθούν ακολουθούν μια άλλη κατεύθυνση παρακάμπτοντας το κατεστραμμένο τμήμα.

Όταν αποστέλλουμε μια πληροφορία αυτή χωρίζεται σε μικρότερα κομμάτια που ονομάζονται πακέτα. Τα πακέτα αυτά, εκ των οποίων το καθένα έχει τη δική του ταυτότητα, μπορούν να ακολουθήσουν διαφορετικούς δρόμους για να φτάσουν στον κοινό προορισμό τους, όπου τελικά και

---

[6]Κιούπης Δημήτριος: Ποινικό Δίκαιο και Internet.σελ.21 επ. Εκδόσεις Αντ.Ν.Σάκκουλα. Αθήνα-Κομοτηνή 1999.

[7] Βλ. περιοδικό «Ο κόσμος του ίντερνετ». Τεύχος 36 σελ.110 επ.

[8] Υπάρχουν δύο είδη δικτύων, το ένα είναι το τοπικό δίκτυο (LAN) το οποίο συνδέει υπολογιστές, εκτυπωτές, και συσκευές μαζικής αποθήκευσης τα οποία βρίσκονται όλα σε φυσική εγγύτητα. Συνδέουν δηλαδή υπολογιστές μέσα σε ένα συγκεκριμένο χώρο, όπως ένα κτίριο για παράδειγμα. Επειδή το LAN είναι εγκατεστημένο σε ιδιωτικό χώρο ο ιδιοκτήτης του μπορεί να εγκαταστήσει οποιοδήποτε επικοινωνιακό σύστημα χωρίς να είναι υποχρεωμένος να αγοράσει υπηρεσίες από κάποιο παροχέα. Είναι στην ουσία ένα ιδιωτικό δίκτυο. Το άλλο είδος δικτύου ονομάζεται δίκτυο ευρείας περιοχής (WAN). Συνδέει συσκευές οι οποίες είναι η μία στο ένα άκρο της πόλης και η άλλη στο άλλο ή μία στη μια χώρα και η άλλη στην άλλη. Λόγω ότι τα WAN περνούν μέσα από δημόσια γη, οι χρήστες δε μπορούν να συνδέσουν τους υπολογιστές με καλώδιο αλλά πρέπει να αγοράσουν υπηρεσίες από τους παροχείς.

ξανασυναρμολογούνται[9]. Αυτό γίνεται λόγω της ψηφιακής τεχνολογίας και πιο συγκεκριμένα μέσω του TCP/IP (transmission control protocol / internet protocol).

Το διαδίκτυο λειτουργεί στο πλαίσιο ενός ευρύ παγκόσμιου ιστού όπως θα μπορούσε να μεταφραστεί στη γλώσσα μας ο όρος World Wide Web[10], κατά άλλους WWW. Δε θα πρέπει να γίνεται σύγχυση μεταξύ του World Wide Web και του διαδικτύου. Το πρώτο αναφέρεται σε ένα διασυνδεμένο χώρο γνώσεων και πληροφοριών, τις λεγόμενες ηλεκτρονικές σελίδες, ενώ το δεύτερο στο παγκόσμιο δίκτυο, στο σύνολο δηλαδή των υπολογιστών και των τρόπων που τους συνδέουν. Το WWW είναι δηλαδή ένα τμήμα του διαδικτύου. Η λειτουργία του WWW στηρίζεται κυρίως στη χρήση του «Υπερκειμένου»

---

[9] Καράκωστας Κ. Ιωάννης. « Δίκαιο και internet, Νομικά ζητήματα του διαδικτύου », σελ 3 επ. εκδόσεις Π.Ν. Σάκκουλας.

[10] Ο Tim Berners-Lee, ένας ερευνητής στο CERN, το Ευρωπαϊκό Εργαστήριο Φυσικής Υψηλής Ενέργειας, είχε πρώτος την ιδέα για έναν παγκόσμιο ιστό (World Wide Web), το 1989. Λόγω του ότι η έρευνα στη φυσική γίνεται συνήθως από ομάδες ανθρώπων από διαφορετικά πανεπιστήμια, ήθελε να βρει έναν τρόπο που θα επέτρεπε στους επιστήμονες σε ολόκληρη την Ευρώπη και τη Βόρειο Αμερική να ανταλλάσουν γρήγορα και εύκολα πληροφορίες, όπως ερευνητικά άρθρα, περιοδικά και πειραματικά στοιχεία. Αν και αυτοί μπορούσαν να χρησιμοποιήσουν το Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο ο Berners-Lee ήθελε να κάνει την ανταλλαγή πληροφοριών πιο εύκολη και εύληπτη για τους ανθρώπους που δεν ήταν εξοικειωμένοι ή που δεν αισθανόταν άνετα με τα δίκτυα των ηλεκτρονικών υπολογιστών. Για να το καταφέρει αυτό, σχεδίασε και δημιούργησε ένα σύστημα που παρουσίαζε τις πληροφορίες κάνοντας χρήση μιας έννοιας που ονομάζεται υπερ-κείμενο (hypertext), και ενός συνόλου από έγγραφα ή αρχεία συνδεδεμένα με δείκτες που ονομάζονται σύνδεσμοι ή συνδέσεις (links). Το σύστημα του Berners-Lee ονομάστηκε τελικά **World Wide Web** (σε ελληνική απόδοση, Παγκόσμιος Ιστός) .
Για περισσότερες πληροφορίες σχετικά με το World Wide Web βλ. Σφακιανάκης Μιχάλης, Εισαγωγή στην ηλεκτρονική σκέψη , εκδόσεις Κλειδάριθμος , σελ. 231 επ .

(hypertext) το οποίο αποτελεί ένα σύστημα που παρουσιάζει έγγραφα[11] ή αρχεία συνδεδεμένα με δείκτες που ονομάζονται σύνδεσμοι (links). Με βάση το υπερκείμενο αυτό που τις περισσότερες φορές είναι απλό κείμενο να το διορθώσει, να το αποθηκεύσει ή να μεταβεί σε κάποιο άλλο κείμενο ή σελίδα(site). Οι σύνδεσμοι που περιέχονται στα υπερκείμενα ονομάζονται υπερσύνδεσμοι, το δε σύνολο όλων των εγγράφων μαζί με τους υπερσυνδέσμους συμπληρώνουν την εικόνα του παγκόσμιου ιστού, η οποία μοιάζει με ένα τεράστιο ιστό αράχνης[12]. Τα έγγραφα του υπερκειμένου είναι αρχεία αποθηκευμένα σε εκατομμύρια μηχανές σε όλο τον κόσμο και μια σύνδεση γίνεται συμπληρώνοντας τη διεύθυνση της ιστοσελίδας στη μηχανή αναζήτησης.

Το internet ξεκίνησε το 1969 με την αρχική ονομασία Arpanet, και οργανώθηκε από το Υπουργείο Εθνικής Άμυνας των ΗΠΑ, με στόχο τη δημιουργία ενός δικτύου τηλεπικοινωνίας για στρατιωτικούς σκοπούς. Το 1972 γίνεται ευρύτερα γνωστό και συνδέονται με αυτό περί τα 50 πανεπιστήμια για την ανάπτυξη κάποιας δραστηριότητας που είχε σχέση με τις στρατιωτικές τεχνολογίες. Η καινοτομία του συστήματος ήταν ότι η σύνδεση με τους υπολογιστές ήταν πολλαπλές, ώστε αν κάποια στιγμή κοβόταν η επικοινωνία μεταξύ δύο υπολογιστών, να μπορέσουν οι πληροφορίες που μεταδίδονται να ακολουθήσουν κάποια άλλη οδό προκειμένου να φτάσουν στον παραλήπτη. Ο όρος internet αρχίζει να καθιερώνεται από το 1990[13].

---

[11] Όταν τα έγγραφα αυτά δεν είναι απλό κείμενο, αλλά εικόνες, video, ήχοι, τότε αυτά ονομάζονται υπερμέσα.

[12]Μαρίνος Ν. Αναστάσιος. «Το ίντερνετ και οι συνέπειες του κυρίως στο χώρο του δικαίου». Ελλ.Δικ.1998 σελ.5

[13] Καράκωστας Κ.Ιωάννης. Το Δίκαιο του Internet. ΝοΒ τόμος 46 σελ.1172.

3. Το Διαδίκτυο σήμερα.

Από το 1991 που επικράτησε η χρήση του για εμπορικούς σκοπούς, επήλθε μια επανάσταση στην πολιτική, τη διοίκηση και γενικά την ανθρώπινη επικοινωνία με αποτέλεσμα να διανύει μια ανοδική πορεία παγκοσμίως[14], σε σημείο ώστε να θεωρείται ότι μπορεί να αποτελέσει το νέο μέσο κοινωνικού αποκλεισμού, δημιουργώντας και οξύνοντας τις ήδη υπάρχουσες χωρικές, εισοδηματικές, φυλετικές, οικονομικές, εκπαιδευτικές[15], γλωσσικές, ηλικιακές[16] και πολιτικές ανισότητες[17].

Παρά τις προσπάθειες που καταβάλλονται σε εθνικό αλλά και σε υπερεθνικό επίπεδο, λχ μέσω της Ευρωπαϊκής Ένωσης ή του Οργανισμού Ηνωμένων Εθνών, τα προγράμματα που έχουν καταρτιστεί με στόχο την άμβλυνση του «ψηφιακού χάσματος», όπως είναι η «Πρωτοβουλία για την παγκόσμια ψηφιακή ευκαιρία»(Global Digital Opportunity Initiative, δεν έχουν επιφέρει καρπούς. Οπότε, μολονότι θεωρητικά οι νέες τεχνολογίες καθιστούν την πληροφορία πιο εύκολα προσβάσιμη, με μικρότερο κόστος και μπορούν να

---

[14] Οι χρήστες αυξάνονται με ρυθμό γεωμετρικής προόδου. Υπολογίζεται ότι κάθε δύο λεπτά ένας χρήστης προστίθεται. Βλ. το άρθρο «Έγκλημα στο Παγκόσμιο χωριό...» http://Knet.Compulink.Gr/Articles/ecrime.htm.. Συγκεκριμένα, το 1996 8 εκατομμύρια άτομα –εκτός ΗΠΑ- συνδέθηκαν με το Διαδίκτυο Βλ. Evagora, ΒήμαΝετ, σελ. 39. Τον Ιούλιο του 1997 παγκοσμίως ήταν συνδεδεμένοι παγκοσμίως 20 εκατομμύρια Η/Υ και 100 εκατομμύρια χρήστες . Βλ. Βήμα , 19/4/1998, Δ/13. Το 2000 οι χρήστες ανέρχονται σε 407.100.000.

[15] Μελέτη που έγινε στο National Geographic σε 178 χώρες με συμμετοχή 80.000 ατόμων έδειξε ότι η πλειοψηφία των χρηστών είναι άτομα με διετείς ή τετραετείς και μεταπτυχιακές σπουδές . Βλ. National Geografic τομ. 3, Δεκ. 1999, σελ. 222-225.

[16] Είναι γενικώς αποδεκτό ότι οι νεαρότερες ηλικίες έχουν μεγαλύτερη πρόσβαση λόγω εξοικείωσης με την πληροφορική. Οι ψηφιακοί πολίτες βρίσκονται περίπου στην ηλικία των 40 ετών.

[17] Η Αμερική διαθέτει την πρωτοκαθεδρία στην κοινωνία του Διαδικτύου . Αυτό έχει ως αποτέλεσμα να υπάρχει φόβος σχετικά με την κυριαρχία τους στο διαδίκτυο. Βλ. Evagora A, ΒήμαΝετ, σελ. 39.

αποτελέσουν αναπτυξιακό εργαλείο, στην πράξη οι ανισότητες, τόσο στο εσωτερικό των αναπτυγμένων χωρών όσο μεταξύ αναπτυγμένων και αναπτυσσόμενων χωρών όχι μόνο εξακολουθούν να υφίστανται αλλά επιπλέον διευρύνονται.

Οι πιο άμεσες και χρήσιμες πλευρές του διαδικτύου που χρησιμοποιούνται ευρύτατα είναι: Το ηλεκτρονικό ταχυδρομείο, ο παγκόσμιος ιστός, μεταφορά αρχείων, σύνδεση με απομακρυσμένο υπολογιστή, συνομιλία, ομάδες συζήτησης, ταχυδρομικές λίστες.

3.1 Ηλεκτρονικό Ταχυδρομείο (E-mail)[18]

Η υπηρεσία αυτή είναι ανάλογη με την υπηρεσία των επιστολών του συμβατικού ταχυδρομείου. Δηλαδή, δίνει τη δυνατότητα σε κάποιον να στείλει επιστολές σε έναν ή περισσότερους αποδέκτες αλλά και να λάβει επιστολές. Οι επιστολές στέλνονται με ηλεκτρονικό τρόπο και έτσι δεν απαιτείται να πάει κανείς στο ταχυδρομείο ή να βάλει γραμματόσημα.

Το ηλεκτρονικό ταχυδρομείο επιτρέπει την ανταλλαγή μηνυμάτων μεταξύ χρηστών που χρησιμοποιούν πιθανώς απομακρυσμένους κόμβους του δικτύου. Το σημαντικότερο πλεονέκτημα της υπηρεσίας αυτής είναι η μεγάλη ταχύτητα στην αποστολή και λήψη μηνυμάτων μεταξύ των χρηστών. Επίσης είναι πολύ οικονομικό σε ενέργεια: μια τηλεφωνική γραμμή μπορεί να μεταβιβάσει έναν πραγματικό πακτωλό από γράμματα και μηνύματα με ελάχιστο κόστος. Τα μηνύματα μεταδίδονται από τον υπολογιστή του αποστολέα στον υπολογιστή

---

[18] Δημιουργήθηκε το 1971 από τον Ray Tomlison (Βήμα 17/9/2002). Το πρότυπό του καθιερώθηκε το 1976, μετά τη βασιλική «επικύρωση». Το πρωτόκολλο λειτουργίας του ηλεκτρονικού ταχυδρομείου δημιουργήθηκε ύστερα από το e-mail που έστειλε στις 26 Μαρτίου η βασίλισσα της Βρετανίας Ελισσάβετ, επιδοκιμάζοντας έτσι επίσημα το νέο γνωστό μέσο επικοινωνίας. Το 1972 καθιερώθηκε το σύμβολο @ (γνωστό στα ελληνικά ως «παπάκυ») ως αναπαράσταση του «στο» (at) στις διευθύνσεις του ηλεκτρονικού ταχυδρομείου.

του παραλήπτη μέσω πολλών άλλων υπολογιστών του δικτύου χωρίς να χρειάζεται ο χρήστης να γνωρίζει τη διαδρομή του μηνύματος μέσα στο δίκτυο. Η δρομολόγηση ενός μηνύματος επιτυγχάνεται μέσω του πρωτοκόλλου επικοινωνίας SMTP (Simple Mail Transport Protocol), με τη χρήση ειδικών δρομολογητών (rooters) του δικτύου. Ο παραλήπτης δεν χρειάζεται να είναι συνδεδεμένος on line για να παραλάβει τα μηνύματα του. Το μήνυμα αποθηκεύεται προσωρινά στον υπολογιστή του παροχέα υπηρεσιών Internet (ISP-Internet Service Provider) και ο παραλήπτης μπορεί να το λάβει όταν τελικά συνδεθεί με το δίκτυο.

3.2 Ο παγκόσμιος Ιστός (World Wide Web).

Ο παγκόσμιος ιστός του Internet είναι η πιο πρόσφατη και πιο γρήγορη αναπτυσσόμενη υπηρεσία του διαδικτύου. Προσφέρει απεριόριστες δυνατότητες όσον αφορά τη συλλογή, τη μετάδοση, αλλά και την έρευνα πληροφοριών. Αυτή η υπηρεσία , που χρησιμοποιεί γραφικά και ο σχεδιασμός της βασίζεται στα πρότυπα hypermedia ήρθε πολύ γρήγορα στις προτιμήσεις των χρηστών και των εταιρειών για να συλλέγουν και να εκδίδουν πληροφορίες, αλλά και να υλοποιήσουν μια ηλεκτρονική παρουσία στον παγκόσμιο κυβερνοχώρο[19] .

Η σύλληψη αυτή αφορούσε τον τρόπο οργάνωσης των πληροφοριών μέσα στο Internet, έτσι ώστε οι ερευνητές να έχουν ευκολότερη πρόσβαση σε αυτές. Οι πληροφορίες στους εξυπηρετητές Web αποθηκεύονται ως μια συλλογή εγγράφων hypertext. Κάθε έγγραφο hypertext είναι κατασκευασμένο με τέτοιο τρόπο, ώστε να έχει τη δυνατότητα να συνδέεται με άλλα έγγραφα που μπορεί να είναι και αυτά hypertext ή απλά κείμενα. Οι συνδέσεις μεταξύ των εγγράφων hypertext προσφέρουν στο χρήστη τη δυνατότητα να βρίσκει τις πληροφορίες που τον ενδιαφέρουν και σε άλλα έγγραφα παρόμοιου περιεχομένου.

---

[19] Βλ. ΒήμαΝετ, 90 ερωτήσεις απαντήσεις για το διαδίκτυο, 1997, σελ.24

Ο χρήστης μπορεί απλά να παρακολουθεί τη συζήτηση στο κανάλι ή στα κανάλια της επιλογής του και να συμμετέχει σε αυτήν. Σε αυτήν την υπηρεσία η επικοινωνία είναι σύγχρονή και υπάρχουν αρκετοί κανόνες καλής συμπεριφοράς που πρέπει να τηρούνται. Αν κάποιος δεν συμπεριφέρεται κόσμια και σύμφωνα με αυτούς τους κανόνες στο κανάλι που βρίσκεται, υπάρχει περίπτωση να εκδιωχθεί ή και να απαγορευτεί η είσοδος του στο συγκεκριμένο κανάλι[22].

3.6 Ομάδες συζητήσεως (news groups) / Πίνακες ανακοινώσεων (BBS).

Η υπηρεσία αυτή προσφέρει τη δυνατότητα καταχώρησης και ανάγνωσης μηνυμάτων σε αναλογία με τις αγγελίες στις εφημερίδες. Τα μηνύματα αυτά ταξινομούνται κατά θεματικές ενότητες και τόσο η καταχώρηση όσο και η αναγνωσή τους γίνεται βάση αυτές τις ενότητες. Για την αποθήκευση και τη διαχείριση αυτών των μηνυμάτων χρησιμοποιούνται υπολογιστές. Τα προγράμματα αυτά που υλοποιούν αυτή την υπηρεσία είναι γνωστά με το όνομα BBS (Bulleting Board System) τα λεγόμενα newsgroups.

Τα Newsgroups είναι οργανωμένα κατά θέματα (πολιτιστικά, κοινωνικά, τεχνικά) και οι χρήστες μπορούν να γίνουν συνδρομητές στην κατηγορία θεμάτων που επιθυμούν, για να διαβάζουν και να αποστέλλουν μηνύματα μέσω ειδικών προγραμμάτων newsreaders και newsservers .

Τα άρθρα που γίνονται δεκτά καταχωρούνται στην αντίστοιχη ομάδα και μετά προωθούνται σε εκείνους τους υπολογιστές μέσα στο Internet που παρέχουν αυτήν την υπηρεσία και οποιοσδήποτε μπορεί να τα διαβάσει. Κάθε υπολογιστής ξέρει σε ποιους άλλους υπολογιστές να προωθήσει τα καινούργια άρθρα και αυτή η διαδικασία διαρκεί το πολύ 2 με 3 ημέρες[23].

---

[22] http://www.skypoint.com/gimonca/irc2.htm

[23] http://www.geocities.com/dim2pap

3.7 Ταχυδρομικές λίστες (mailing lists).

Η υπηρεσία αυτή είναι ανάλογη με εκείνη που επιτρέπει οι συνδρομητές στα συμβατικά έντυπα να λαμβάνουν εκδόσεις των αντίστοιχων εντύπων στη διεύθυνση που έχουν δηλώσει. Μια ταχυδρομική λίστα είναι αφιερωμένη σε ένα ορισμένο θέμα συζήτησης και έχει υπόσταση μέσα στο internet που ταυτοποιείται από μια ηλεκτρονική διεύθυνση. Οποιοσδήποτε μπορεί να στείλει ένα άρθρο σε αυτή τη διεύθυνση και όλοι όσοι είναι συνδρομητές λαμβάνουν ένα αντίγραφο του άρθρου αυτού χωρίς να απαιτούνται χρήματα. Για να γίνει κάποιος συνδρομητής σε μια ταχυδρομική λίστα πρέπει απλώς να στείλει ένα κατάλληλο μήνυμα με το ηλεκτρονικό ταχυδρομείο δηλώνοντας την πρόθεσή του να γίνει συνδρομητής. Με παρόμοιο τρόπο μπορεί κανείς να διαγραφεί από μια ταχυδρομική λίστα[24].

Υπάρχουν χιλιάδες ταχυδρομικές λίστες συζήτησης. Στις ομάδες συζήτησης επιλέγει κανείς τις ομάδες και τα άρθρα που θέλει να διαβάζει κάθε φορά. Αντίθετα, στις ταχυδρομικές λίστες προεπιλέγει κανείς τις λίστες που τον ενδιαφέρουν και γίνεται συνδρομητής τους. Έπειτα τα άρθρα έρχονται αυτόματα στο ταχυδρομικό του γραμματοκιβώτιο και τα διαβάζει. Πολλές λίστες έχουν αντίστοιχες ομάδες συζήτησης.

---

[24] Ζάννη Αναστασία: Το διαδικτυακό έγκλημα, εκδόσεις Α.Ν. Σάκκουλα, Αθήνα – Κομοτηνή 2005, σελ.45επ.

4. Διαδίκτυο και Δίκαιο.

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (internet). Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στον πεδίο του εγκλήματος στον κυβερνοχώρο (cyber crime), όπως άλλωστε συμβαίνει και στα εγκλήματα με ηλεκτρονικούς υπολογιστές (computer crimes) χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί "τον σταυρό του μαρτυρίου" για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

Ένα εξ ίσου σημαντικό πρόβλημα που αντιμετωπίζει αυτός που ασχολείται με την νομική πλευρά του θέματος από ποινική άποψη, είναι η έλλειψη επαρκούς βιβλιογραφίας και σχετικών άρθρων. Είναι ευνόητο ότι, η έλλειψη αυτή οφείλεται στο γεγονός ότι, το έγκλημα στον κυβερνοχώρο αποτελεί νέα μορφή εγκλήματος. Αποτελεί κοινή διαπίστωση ότι, η ανάπτυξη των σχετικών νομικών θεμάτων από αστική και εμπορική άποψη έχει διερευνηθεί σε μεγαλύτερη έκταση, από ότι η αντίστοιχη ποινική πλευρά. Αυτό οφείλεται στην μεγάλη επιρροή του κυβερνοχώρου, τόσο στο αστικό (σύναψη συμβάσεων εξ αποστάσεως δια του κυβερνοχώρου κλπ), όσο και στον οικονομικό τομέα (ηλεκτρονικό εμπόριο, νέα οικονομία κλπ).

Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του ημερήσιου Τύπου. Άλλωστε και το ίδιο το διαδίκτυο αποτελεί πηγή αντλήσεως

πληροφοριών (ίσως την σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες - θέσεις (Sites)[25].

4.1 Το γενικότερο πρόβλημα της νομικής ορολογίας.

Πρέπει ιδιαιτέρως να τονιστεί ότι, η διαφορετική κατανόηση - αντίληψη των ίδιων εννοιών από τον τεχνικό και νομικό αποτελεί ένα από τα σημαντικότερα προβλήματα του υπό εξέταση θέματος. Έτσι, π.χ. διαφορετικά αντιλαμβάνεται την έννοια του όρου "κυβερνοχώρος", "ασφάλεια", "χάκερ" κλπ ο τεχνικός και διαφορετικά ο νομικός. Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος. Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ανατρέχει ο νομικός στη νομολογία, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει "φθάσει" η υπόθεση ή άλλη παρόμοια στο δικαστήριο. Σε περίπτωση που, ούτε νομολογία υπάρχει, ο νομικός ανατρέχει στη νομική επιστήμη, προς αναζήτηση θεωρητικής τουλάχιστον λύσης του θέματος. Αυτό βέβαια δεν σημαίνει ότι, η νομική θεωρία, όπως αυτή έχει αναπτυχθεί ή αναπτύσσεται από τη (νομική) επιστήμη, γίνεται υποχρεωτικώς δεκτή στην νομική πρακτική, δηλαδή στην διερεύνηση ή την εκδίκαση των σχετικών εγκλημάτων[26].

4.2 Το πρόβλημα της Ελληνικής νομικής ορολογίας.

Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη - κατά κανόνα - στην Αγγλική γλώσσα. Η αντίστοιχη μεταφορά των όρων αυτών στα Ελληνικά, δεν είναι ούτε εύκολη, ούτε δόκιμη. Βέβαια κατά την καθημερινή πρακτική πολλοί όροι χρησιμοποιούνται στην

---

[25]http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

[26]http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

ξενόγλωσση διάστασή των, κατά τρόπο που τείνουν να ενσωματωθούν και στο Ελληνικό νομικό λεξιλόγιο. Έτσι π. χ. αντί του Ελληνικού όρου "διαδικτυακό 'έγκλημα" ή "έγκλημα στο διαδίκτυο" ή ``έγκλημα στον κυβερνοχώρο`` πολλές φορές χρησιμοποιείται αυτούσιος ο όρος Cyber crime ή Internet crime. Σχετικοί με το θέμα ξενόγλωσσοι όροι είναι: Cyber crime, Internet, crime, Crime in cyberspace, On line crime, On line computer crime, communication crime, digital crime, electronic crime, electronic evidence, Computer crimes (υπολογιστικά εγκλήματα), Computer related crime. Σχετικοί με τον δράστη όροι είναι: hacker, Cracker, Internet freak, Cyber crook, Cyber freak, Internet freak.

Το πρόβλημα αυτό της Ελληνικής νομικής ορολογίας παρουσιάζεται όχι μόνον στο πεδίο του ουσιαστικού ποινικού δικαίου, αλλά και στο αντίστοιχο του ποινικού δικονομικού .

Διευκρινίζεται ότι, στην παρούσα μελέτη γίνεται προσπάθεια χρησιμοποιήσεως των σχετικών όρων στην Ελληνική γλώσσα, για την πληρέστερη όμως κατανόηση των, χρησιμοποιείται σε παρένθεση και ο Αγγλικός όρος, όπου αυτό απαιτείται. Η ανάγκη παραθέσεως και των ξενόγλωσσων όρων προκύπτει από το γεγονός ότι, οι όροι αυτοί δεν έχουν ακόμα "δοκιμαστεί" στην Ελληνική νομική πρακτική. Έτσι για έννοιες με το ίδιο νομικό περιεχόμενο χρησιμοποιούνται στην Ελληνική γλώσσα διαφορετικοί όροι[27].

---

[27] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ.675.

5. Διαδίκτυο και έγκλημα.

Οι επιπτώσεις από την εμφάνιση και τη χρήση του Διαδικτύου είναι τεράστιες. Νέες μορφές συμπεριφορών έχουν εμφανιστεί σ' όλους τους τομείς της κοινωνικής ζωής, όπως στις συναλλαγές, στο εμπόριο, στην επικοινωνία, στην πολιτική, στη δικαιοσύνη , στην εκπαίδευση[28], στην οικονομία, στο δημόσιο τομέα και γενικώς σε όλους τους τομείς της ανθρώπινης δραστηριότητας. Πολλές φορές τα δικαστήρια καλούνται να επιλύσουν διαφορές που θεμελιώνονται και στηρίζονται όχι απλώς σε νέες τεχνολογίες αλλά ειδικότερα στη χρήση του διαδικτύου.

Οι παρανομίες που εντοπίζονται στο διαδίκτυο είναι πολλές και περίπλοκες. Να σημειωθεί ότι οι ίδιες Συνταγματικές Αρχές που ισχύουν στον «κοινό χώρο» ισχύουν και στον κυβερνοχώρο.

Η ελεύθερη διακίνηση των ιδεών , ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από τις βασικότερες Αρχές[29] του κυβερνοχώρου. Η εφαρμογή όμως αυτών των Αρχών , έχουν σχέση με τη λεγόμενη «Ασφάλεια του Κυβερνοχώρου» (internet security), ένα από τα πλέον δύσκολα και περίπλοκα θέματα του διαδικτύου, τόσο από τεχνικής όσο και από νομικής απόψεως.

Σε νομικό – ποινικό επίπεδο, η δυσκολία ενασχολήσεως με το θέμα εντοπίζεται στο γεγονός ότι βρισκόμαστε μπροστά σε καταστάσεις, γεγονότα κτλ. που δεν μπορούν να υπαχθούν στους ήδη υφιστάμενους (γενικούς) ποινικούς κανόνες, τόσο του ουσιαστικού όσο και του ποινικού δικονομικού πεδίου. Από την άλλη πλευρά η ραγδαία εξέλιξη της τεχνολογίας και της πληροφορικής καθιστά το όλο πρόβλημα ακόμα πιο δύσκολο και περίπλοκο

---

[28] Βλέπ. σχετικώς: Βασίλειος Αραβαντινός, εισαγωγή στη Νομοπληροφορική και τη δικαιοκυβερνητική, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1994, σελ. 173 επ.

[29] Σπ. Σταμούλης, Προβλήματα ευθύνης από την αθέμιτη χρήση των Ηλεκτρονικών Υπολογιστών, ΝοΒ 1987, σελ. 1021 επ.

για τον σύγχρονο νομικό. Επιπλέον οι έννομες τάξεις καλούνται να ρυθμίσουν με ψήφιση νέων νόμων τα παρουσιαζόμενα για πρώτη φορά θέματα, τα οποία είναι πάρα πολλά[30]. Ο χώρος του διαδικτύου δεν είναι νομικώς ανεξέλεγκτος[31]. Κατά συνέπεια η νομοθεσία και η δικαιοσύνη δεν μπορεί να μείνουν αδιάφοροι μπροστά στις νέες αυτές ανθρώπινες συμπεριφορές.

5.1 Προσδιορισμός της εννοίας του εγκλήματος στον κυβερνοχώρο.

Δεν υπάρχει ακόμα γενικά αποδεκτός ορισμός του εγκλήματος στον κυβερνοχώρο, ούτε στην διεθνή νομοθεσία, ούτε στην διεθνή νομολογία ή βιβλιογραφία . Ομοίως ούτε στην Ελληνική βιβλιογραφία υπάρχει ορισμός του εγκλήματος στον κυβερνοχώρο.

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το ``κοινό`` ή "συμβατικό έγκλημα" και η μόνη διαφορά που το διακρίνει απ΄ αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον, (δηλ. σε ηλεκτρονικό περιβάλλον και δη σε περιβάλλον διαδικτύου) δεν ανταποκρίνεται κατά την άποψή μου πλήρως στην πραγματικότητα. Υπάρχουν βέβαια εγκλήματα, που διαπράττονται τόσο σε κοινό, όσο και σε ηλεκτρονικό περιβάλλον. Άλλα εγκλήματα διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών, χωρίς δηλαδή να υπάρχει σύνδεση των υπολογιστών με το διαδίκτυο (ή ακόμα και εάν υπάρχει δεν χρησιμοποιείται). Μια άλλη κατηγορία ηλεκτρονικών εγκλημάτων διαπράττονται αποκλειστικώς σε περιβάλλον του κυβερνοχώρου. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν[32]:

α) Σε εγκλήματα που διαπράττονται τόσο σε " κοινό " περιβάλλον, όσο και στο διαδίκτυο (internet) π.χ. η συκοφαντική δυσφήμηση διαπράττεται και με

---

[30] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ.676.

[31] Ιωάννης Καράκωστας, Νομική αντιμετώπιση του Διαδικτύου, ΝοΒ 46, σελ. 1178.

[32] http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

την χρήση του ηλεκτρονικού ταχυδρομείου (αποστολή e-mail). Η αντιγραφή ενός πνευματικού έργου π.χ. μουσικού τραγουδιού (άρθρ. 66 Ν.2121/93) ή ενός προγράμματος ηλεκτρονικού υπολογιστή. Όταν το έγκλημα αυτό τελεστεί σε "περιβάλλον internet" (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (internet related crime).

β) Σε εγκλήματα που διαπράττονται μόνο σε περιβάλλον ηλεκτρονικών υπολογιστών (ενν. χωρίς την χρήση του διαδικτύου). Τέτοια είναι τα εγκλήματα που προβλέπονται από το άρθρο 370 Γ παράγρ. 1 του Π.Κ. π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από δισκέτα ή CD-ROM ή σε ηλεκτρονικό υπολογιστή.

γ) Σε "Γνήσια εγκλήματα κυβερνοχώρου" (Cyber crimes) με την έννοια της ποινικοποίησης συμπεριφοράς που αποκλειστικώς έχει σχέση με τον κυβερνοχώρο. Μια τέτοια αξιόποινη συμπεριφορά μπορεί να θεωρηθεί η παράνομη ή χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού δια του κυβερνοχώρου. Τέτοια εγκλήματα δεν υπάρχουν ακόμα στην Ελληνική έννομη τάξη, αφού δεν υπάρχει σχετική νομοθεσία. Δηλαδή τα γνήσια εγκλήματα του κυβερνοχώρου διαπράττονται αποκλειστικώς σε περιβάλλον διαδικτύου. Σε περίπτωση που ο υπολογιστής δεν είναι συνδεδεμένος με το διαδίκτυο, αλλά ενεργεί αυτοτελώς, οποιοδήποτε έγκλημα και εάν διαπραχθεί θεωρείται έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer crime).

5.2 Χαρακτηριστικά γνωρίσματα του εγκλήματος στον κυβερνοχώρο.[33]

Το έγκλημα στον κυβερνοχώρο είναι γρήγορο (quick), διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.

Είναι εύκολο (easy) στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα).

Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις, αυτή τη στιγμή είναι πιο προηγμένο (``ανεβασμένο``) και από το έγκλημα του λευκού περιλαιμίου .

Μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.

Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σ΄ όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδια ομάδες συζητήσεως (News groups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC- Internet Relay Chat).

Οι "εγκληματίες του κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές (e-mail) ανωνύμως ή και με ψευδή στοιχεία.

Είναι έγκλημα "χωρίς πατρίδα``, παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους.

Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεως του. Ακόμα όμως και αν προσδιοριστεί αυτός, είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης.

---

[33] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ.677 και

http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

Η εξωτερίκευσή του μπορεί να εντοπίζεται στην Α χώρα πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται στο άλλο άκρο της γης ή και να βρίσκονται ταυτόχρονα σε πολλούς τόπους.

Για την διερεύνησή του απαιτείται κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (δηλ. του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος, και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Περιπτώσεις που το έγκλημα στον κυβερνοχώρο (cyber-crime) περιορίζεται στα όρια ενός μόνον κράτους είναι (θεωρητικώς τουλάχιστον) ελάχιστες και σπάνιες.

Οι παραδοσιακές (κοινές) Συμβάσεις για αμοιβαία Δικαστική Συνδρομή δεν επαρκούν, λόγω της φύσεως του αποδεικτικού ολικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενεργείας των διωκτικών Αρχών.

Δεν υπάρχουν επαρκή στατιστικά στοιχεία, όχι μόνο στον Ελληνικό, αλλά και στον Διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια ο ``σκοτεινός αριθμός`` της εγκληματικότητας στον χώρο του διαδικτύου είναι ``ακόμα πιο σκοτεινός``, από ότι στον ``κοινό`` εγκληματικό χώρο.

Η Αστυνομική διερεύνησή γενικότερα, αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.

Εξειδικευμένες γνώσεις επίσης απαιτούνται και για όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (Εισαγγελείς, Δικαστές, Δικηγόρους).

5.3 Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή.[34]

Το έγκλημα στον κυβερνοχώρο (Cyber Crime) είναι μία ειδικότερη μορφή του ηλεκτρονικού εγκλήματος (Computer Crime), το οποίο με τη σειρά του είναι μία ειδικότερη μορφή του ``κοινού`` εγκλήματος, όπως αυτό προσδιορίζεται στο άρθρο 14 Π.Κ.

Ως ηλεκτρονικό έγκλημα μπορεί να οριστεί αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών.

Ως έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (computer related crime ή computer crime) μπορεί να χαρακτηριστεί κάθε παράνομη, ανήθικη ή χωρίς δικαίωμα συμπεριφορά, που σχετίζεται με την αυτόματη επεξεργασία ή μετάδοση δεδομένων .

Σημειώνεται ότι, ο ορισμός αυτός διατυπώθηκε για πρώτη φορά το 1983 από ειδική ομάδα εμπειρογνωμόνων του ΟΑΣΑ, που συνεστήθη ειδικώς για να εξετάσει το θέμα της ηλεκτρονικής εγκληματικότητας. Ο ορισμός αυτός βέβαια είναι πολύ ευρύς και είναι ευνόητο ότι, μόνον ως ``οδηγός`` μπορεί να χρησιμοποιηθεί. Η οριστικοποίησή του επαφίεται στον Εθνικό Νομοθέτη και στη νομολογία των Δικαστηρίων.

5.4 Σκιαγράφηση ("προφίλ ") εγκληματία του Κυβερνοχώρου.

Ο "εγκληματίας του κυβερνοχώρου" διαφέρει ουσιωδώς από τον "κοινό εγκληματία". Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. Ο δράστης πρέπει να διαθέτει ειδικές γνώσεις, τεχνική επιδεξιότητα, τεχνικά μέσα. Χαρακτηριστικώς αναφέρεται ότι, στο έγκλημα στον κυβερνοχώρο (cyber-crime) δεν υπάρχει "Γιάννης - Αγιάννης". Υπάρχουν

---

[34] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ.677 και http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

μόνο " άθλιοι ". Τι σημαίνει αυτό; Ο εγκληματίας του κυβερνοχώρου, (cyber-crook), δεν μπορεί να υποστηρίξει ότι ενήργησε "από ανάγκη" δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Τους "εγκληματίες του κυβερνοχώρου" μπορούμε να τους διακρίνουμε σε δύο κατηγορίες:

α) σ΄ αυτούς που "επιτίθενται" (εισβάλουν) στα computer απλώς από ευχαρίστηση ή περιέργεια, χωρίς όμως να επιδιώκουν (εμφανώς τουλάχιστον) κάποιο οικονομικό όφελος. Στην κατηγορία αυτή ανήκουν, οι δράστες που από το άλλο άκρο του πλανήτη "εισβάλουν " σε υπολογιστή δια της χρήσεως του διαδικτύου **(hackers)** για να μάθουν απλώς, κάποια προσωπικά στοιχεία.

β) σ΄ αυτούς που ενεργούν από οικονομικό όφελος **(cracker).** Στην δεύτερη ανήκουν αυτοί που δεν " εισβάλουν " απλώς για να μάθουν κάτι, αλλά μόλις μάθουν το στοιχείο που επιθυμούν (π.χ. τον αριθμό της πιστωτικής κάρτας) δίνουν και την κατάλληλη εντολή στην Τράπεζά για την μεταφορά ενός ποσού στον λογαριασμό τους.

Σε ειδική έρευνα που έγινε στη Βρετανία από την ``επιτροπή πρόβλεψης και πρόληψης εγκλήματος`` (Foresight Crime Prevention Panel) για το ``ποιόν`` (``who is who``) του μελλοντικού εγκληματία διαπιστώθηκε ότι: Το έτος 2020 οι κακοποιοί θα γνωρίζουν στην εντέλεια την λειτουργία των συστημάτων ασφαλείας των τραπεζικών κωδικών[35] και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, ακόμα δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του

[35] Για περισσότερες πληροφορίες βλ. ΝΟΥΣΚΑΛΗΣ Γεώργιος: Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ), Το παρελθόν και το μέλλο του άρθρου 386ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, Ποιν. Δικ. 2/2003, σελ. 178 επ.

οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον ``ξεγελούν`` με την ανάλογη κατασκευή φακών επαφής.

5.5 Σχέση ``εγκληματία του κυβερνοχώρου``(cyber - criminal) και του "εγκληματία του λευκού περιλαιμίου`` (white - collar criminal).[36]

Μπορεί να υποστηριχθεί ότι το έγκλημα στον κυβερνοχώρο (cyber-crime) είναι μια ειδικότερη μορφή του εγκλήματος του λευκού περιλαιμίου ". Και αυτό γιατί ο εγκληματίας του κυβερνοχώρου πρέπει να διαθέτει:

α) Εξειδικευμένη επιδεξιότητα: Ο εγκληματίας του κυβερνοχώρου πρέπει να είναι επιδέξιος , να έχει γνώσεις του όλου συστήματος πληροφορικής, είναι κοινωνικός και να μπορεί να αντιληφθεί, που θα ``πετύχει`` το θύμα του.

β) Γνώση : Ο εγκληματίας του κυβερνοχώρου δεν έχει απλώς γνώση του όλου συστήματος πληροφορικής και του διαδικτύου (internet). Γνωρίζει πολύ καλά το επιμέρους "περιβάλλον", καθώς και τα μυστικά του χώρου που θα παραβιάσει. Όπως ακριβώς ο " κοινός εγκληματίας " συλλέγει πληροφορίες, κατοπτεύει το χώρο κλπ. που πρόκειται να κλέψει ή να ληστέψει, κατ΄ ανάλογο τρόπο και ο εγκληματίας του κυβερνοχώρου (cyber-criminal) κατοπτεύει και παρακολουθεί το ηλεκτρονικό περιβάλλον (site), στο οποίο πρόκειται να ενεργήσει την παράνομη πράξη του.

γ) Απαραίτητα τεχνικά και οικονομικά μέσα: Ο εγκληματίας του κυβερνοχώρου πρέπει, εκτός από τη γνώση, να κατέχει και τα κατάλληλα τεχνικά μέσα. Χωρίς την οικονομική δυνατότητα για αγορά του εξοπλισμού (computer-software κλπ.) και χωρίς την κατοχή των τεχνικών μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

---

[36] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ.678 και
http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

Συμπερασματικά λοιπόν μπορεί να λεχθεί ότι, το έγκλη κυβερνοχώρου, είναι πιο προηγμένο (``ανεβασμένο``) και από το έγκ λευκού περιλαιμίου.

5.6 Συνήθη εγκλήματα του κυβερνοχώρου.[37]

Τα πλέον συνηθισμένα εγκλήματα που παρουσιάζονται αυτή την στιγμή στον κυβερνοχώρο είναι: Έκθεση υλικού παιδικής πορνογραφίας, έκθεση υβριστικού περιεχομένου για συγκεκριμένα άτομα ή κοινωνικές ομάδες, βίαια, ρατσιστική και τρομοκρατική θεματολογία, παράνομες on-line συναλλαγές (οικονομικό έγκλημα), παράνομος ηλεκτρονικός τζόγος, αποστολή μηνυμάτων με ακατάλληλο περιεχόμενο, χωρίς να είναι πάντα γνωστά τα στοιχεία του αποστολέα , αποστολή ιών (computer viruses) με σκοπό την πρόκληση ζημιάς στους υπολογιστές των αποδεκτών, τηλεσυνομιλίες (chatrooms) με άτομα που εκμεταλλεύονται τις τεχνολογικές τους δεξιότητες για να αντλήσουν προσωπικά δεδομένα και να προβούν σε παράνομες δράσεις, προώθηση ναρκωτικών και παράνομων ουσιών ή φαρμάκων για την χρήση των οποίων απαιτείται ειδική άδεια, διακίνηση αρχείων με προσωπικά ευαίσθητα δεδομένα και η παραβίαση του ιδιωτικού απορρήτου, προώθηση σατανιστικών και παραθρησκευτικών οργανώσεων, διάδοση μηνυμάτων με σκοπό τον προσηλυτισμό και γενικά η προώθηση προπαγανδιστικού υλικού, παρότρυνση σε αυτοκαταστροφικές ενέργειες, απάτες (με πιστωτικές κάρτες ή μη), εγκλήματα κατά της Εθνικής Ασφάλειας (οδηγίες για κατασκευή Βομβών, εισβολή σε συστήματα ασφαλείας, που έχουν σχέση με την εθνική υποδομή), οδηγίες για παρασκευή ναρκωτικών κ.α.

Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των

---

[37] http://www.safeweb.org.cy/tips.php?lang=el και http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_dikaio.asp

προσωπικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον περιουσιακών αγαθών.

6. Διαδίκτυο και νομοθεσία.[38]

Ένα πολύ σημαντικό ερώτημα που προκύπτει από τη σχέση δικτύου και νομοθεσίας είναι, αν ο παγκόσμιος ιστός (υπερδίκτυο του Internet) μπορεί να ελεγχθεί νομοθετικώς. Η απάντηση είναι: Πάρα πολύ δύσκολα και σε πολύ περιορισμένο τομέα. Και αυτό γιατί η τεχνολογία εξελίσσεται τόσο γρήγορα που η νομοθεσία, όσο και αν προσπαθεί «ασθμαίνουσα», αδυνατεί να την προφτάσει. Επιπλέον για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο απαιτούνται εξειδικευμένες γνώσεις, τις οποίες δεν κατέχουν στον Ελληνικό Δικαιικό χώρο οι αρμόδιες για την έρευνα, δίωξη και εκδίκαση των σχετικών εγκλημάτων Αρχές.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικώς τις καταστάσεις πιεζόμενες από τα πράγματα. Κλασικό παράδειγμα στον τομέα της τεχνολογίας αποτελεί η εμφάνιση των εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές (computers crimes)[39]. Πριν από δεκαπέντε χρόνια περίπου η «συμβατική νομοθεσία» δεν επαρκούσε για την αντιμετώπισή τους. Σήμερα, όλες οι προηγμένες (τουλάχιστον) χώρες έχουν καταρτίσει σχετική νομοθεσία για την αντιμετώπιση του ηλεκτρονικού εγκλήματος. Η νομοθεσία όμως αυτή, ενώ επαρκεί για την «κάλυψη» των εγκλημάτων που διαπράττονται με τη χρήση ηλεκτρονικών υπολογιστών, δεν επαρκεί για να «καλύψει» τα εγκλήματα που διαπράττονται στο διαδίκτυο.

Στο ίδιο σημείο με αυτό την προ δεκαπενταετίας νομοθετικής ελλείψεως, βρίσκονται σήμερα οι έννομες τάξεις όσον αφορά το θέμα του εγκλήματος στον κυβερνοχώρο ((cyber crime). Πολλά από τα εγκλήματα που έχουν παρουσιαστεί στο διαδίκτυο δεν μπορούν να αντιμετωπιστούν με τη συμβατική

---

[38] Αγγελής Εμμ. Ιωάννης, Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000 σελ. 678

[39] Γενικότερα για το νομοθετικό πλαίσιο αντιμετώπισης του ηλεκτρονικού εγκλήματος βλ. Μούρτος Ιωάννης : Ηλεκτρονικό έγκλημα και δικανική πληροφορική, εκδόσεις «ΛΥΧΝΙΑ», Αθήνα 2003, σελ. 49επ.

νομοθεσία, στο χώρο τουλάχιστο του ποινικού δικαίου. Σημειώνεται ότι ελάχιστα κράτη έχουν θεσπίσει μέχρι σήμερα νομοθεσία για την αντιμετώπιση του σχετικού προβλήματος.

Στη Γερμανία έχει ψηφιστεί από 13-06-1997 νόμος για τη ρύθμιση των γενικών συνθηκών σχετικά με τις υπηρεσίες πληροφόρησης και επικοινωνίας[40].

Στις ΗΠΑ ισχύει ο "Electronic Privacy Act" του 1986, ο οποίος αποβλέπει την προστασία από την παράνομη πρόσβαση σε αποθηκευμένα δεδομένα, ενώ ο Νόμος "NET ACT" (No electronic Act) του 1997 αποβλέπει στην προστασία των προϊόντων πνευματικής ιδιοκτησίας (copyright) που διακινούνται και διανέμονται παράνομα.

Στη Βρετανία ισχύει ο Νόμος "Computer Misuse Act" του 1990.

Έχει υποστηριχθεί η άποψη ότι δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομικό κενό[41] στο διαδίκτυο, διότι αναλογικά το «κοινό δίκαιο» μπορεί να εφαρμοστεί και στο χώρο του διαδικτύου. Η άποψη αυτή βέβαια είναι εμφανώς εσφαλμένη, καθότι στον ποινικό χώρο δεν ισχύει η αρχή της αναλογίας.

6.1 Ελληνική Νομοθεσία.

Στην Ελληνική νομοθεσία δεν υπάρχει νόμος που να αναφέρεται αποκλειστικώς σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει θέματα τη συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου. Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του

---

[40] Βλ.Δημήτριος Κιούπης, Ποινικό Δίκαιο και Internet, σειρά Ποινικά, No 57, σελ. 39 και 169.

[41] Βλ. άποψη της Εθνικής Επιτροπής Τηλεπικοινωνιών ΕΕΤ, στο περιοδικό «Ο κόσμος του Internet» Νοέμβριος 1997, σελ. 45.

Συμβουλίου της Ευρώπης , καθώς και άλλων Διεθνών Οργανισμών για την αντιμετώπιση των σχετικών θεμάτων.

Διευκρινίζεται ότι ο Νόμος 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes). Στο βαθμό που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386^{Α}) διαπράττονται και σε περιβάλλον διαδικτύου (Internet) , τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

Είναι γνωστό ότι για να «μπει» κάποιος στον κυβερνοχώρο απαραίτητη προϋπόθεση αποτελεί η χρήση του τομέα τηλεπικοινωνιών (σταθερού ή κινητού τηλεφώνου[42]). Κατά συνέπεια οι σχετικοί με τις τηλεπικοινωνίες νόμοι έχουν άμεση ή έμμεση σχέση με τη χρήση του διαδικτύου. Με άλλα λόγια το διαδίκτυο δεν είναι τίποτε άλλο από μια μορφή επικοινωνίας που γίνεται με τη βοήθεια ή διά μέσου των τηλεπικοινωνιών. Σύμφωνα με τα παραπάνω σχετικοί με το διαδίκτυο Νόμοι είναι:

α) Ο Ν.2867/2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις.

β) Ο Ν. 2774/22.12.1999 προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα , σε συνδυασμό με το Ν.2472/10.4.1997 «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

γ) Ο Ν. 2225/20.7.1994 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας.

6.1.1 Ο Ν.2867/2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις.

Ο νόμος αυτός αντικατέστησε το Ν.2246/1994[43] για την «Οργάνωση και Λειτουργία του Τομέα των Τηλεπικοινωνιών», πλην των διατάξεων που

---

[42] Η εξέλιξη της τεχνολογίας δεικνύει ότι στο μέλλον η σύνδεση με τον κυβερνοχώρο θα είναι πιο εύκολη και πιο εύχρηστη δια μέσου κινητού τηλεφώνου.

[43] Ο Νόμος αυτός ρύθμιζε και θέματα σχετικά με το διαδίκτυο. Σκοπός του ήταν η καθιέρωση ρυθμιστικού πλαισίου ολοκληρωμένης πολιτικής για τη λειτουργία του τομέα των τηλεπικοινωνιών της χώρας.

αφορούν στην παροχή ταχυδρομικών υπηρεσιών (άρθρο 13 πργ 12 Ν.2867/2000) και των διατάξεων εκείνων που αναφέρονται στη σύσταση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (άρθρο 31 Ν.2867/2000).

Ο εν λόγω νόμος ρυθμίζει κάθε είδους τηλεπικοινωνιακής δραστηριότητας που αναπτύσσεται εντός της Ελληνικής Επικράτειας. Είναι γνωστός και ως νόμος «για την απελευθέρωση των τηλεπικοινωνιών» καθότι επιτρέπει την ελεύθερη εγκατάσταση, λειτουργία, διαχείριση και εκμετάλλευση των

Χαρακτηριστικά γνωρίσματά του ήταν ότι :

Προσδιόριζε όχι μόνο τεχνικούς, αλλά και νομικούς όρους. Έτσι σύμφωνα με το άρθρο 2 περ. Δ, φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι τα φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού με βάση την άδεια ή τη δήλωση ή την έγκριση.

Σύμφωνα με το άρθρο 2 περ. Ε, φορείς εγκατάστασης – συντήρησης τηλεπικοινωνιακού τερματικού εξοπλισμού είναι τα φυσικά ή νομικά πρόσωπα, στα οποία έχουν χορηγηθεί άδεια σύνδεσης με το δημόσιο τηλεπικοινωνιακό δίκτυο και συντήρησης τηλεπικοινωνιακού τερματικού εξοπλισμού υπό καθεστώς ελεύθερου ανταγωνισμού.

Κατά το άρθρο 2 περ. ΚΑ, άδεια παροχής τηλεπικοινωνιακής υπηρεσίας είναι η ατομική διοικητική πράξη, βάση της οποίας επιτρέπεται σε ορισμένη τηλεπικοινωνιακή επιχείρηση να παρέχει ελευθέρως και σε εμπορική βάση, καθορισμένες τηλεπικοινωνιακές υπηρεσίες, καθώς και να αναλαμβάνει κάθε αναγκαία δραστηριότητα για την ίδρυση, την ανάπτυξη ή επέκταση, εγκατάσταση και λειτουργία των απαιτούμενων για την εν λόγω παροχή διευκολύνσεων.

Με το νόμο αυτό, (άρθρο 2 παρ 3 Ν.2246/94) συνιστάται Εθνική Επιτροπή Τηλεπικοινωνιών (ΕΕΤ), η οποία έχει όχι μόνο τεχνικές, αλλά και νομικές αρμοδιότητες. Ειδικότερα γνωμοδοτεί κατά την έκδοση κωδίκων δεοντολογίας. Επίσης επιβάλλει διοικητικά πρόστιμα, για όσες διοικητικές παραβάσεις προβλέπονται από το άρθρο 4 του νόμου αυτού. Έχει επίσης αρμοδιότητα ερευνητική (προανακριτική) για συλλογή στοιχείων σύμφωνα με όσα ορίζονται στα άρθρο 2 παρ. 4 περ.3γ του νόμου αυτού.

τηλεπικοινωνιακών δικτύων. Όπως και ο προηγούμενος Ν.2246/1994 έτσι και αυτός προσδιορίζει όχι μόνο τεχνικούς όρους αλλά και νομικούς όρους. Έτσι ως «παροχέας τηλεπικοινωνιακών υπηρεσιών» ορίζεται η τηλεπικοινωνιακή επιχείρηση που παρέχει τηλεπικοινωνιακές υπηρεσίες διαθέσιμες στο κοινό, ενώ ως «χρήστης» θεωρείται κάθε φυσικό ή νομικό πρόσωπο που χρησιμοποιεί ή ζητά να χρησιμοποιήσει δημόσιες τηλεπικοινωνιακές υπηρεσίες.

6.1.2 Ο Ν. 2774/22.12.1999 προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με το Ν.2472/10.4.1997 «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Ο Ν. 2774/22.12.1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, αποτελεί ειδικότερη μορφή του Ν.2471/97 και αποτελεί υλοποίηση της οδηγίας 97/66/Ε.Κ. Απαιτείται η χρήση τηλεπικοινωνιών στην προστασία δεδομένων προσωπικού χαρακτήρα. Δηλαδή οι προηγμένες ψηφιακές τεχνολογίες στα δημόσια τηλεπικοινωνιακά δίκτυα, δημιουργούν ειδικές απαιτήσεις στην προστασία δεδομένων προσωπικού χαρακτήρα.

Σκοπός του νόμου αυτού είναι η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.

Ο Ν.2472/97 προστατεύει το άτομο από την αυτοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Χαρακτηριστικό παράδειγμα εφαρμογής του Ν. 2472/97 στο διαδίκτυο αποτελεί η διασύνδεση αρχείων.

6.1.3 Ο Ν. 2225/20.7.1994 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας .

Ο νόμος αυτός έχει άμεση σχέση με τον κυβερνοχώρο αφού δεν είναι τίποτε άλλο παρά μια μορφή επικοινωνίας που γίνεται διά μέσω των τηλεπικοινωνιών.

Με το άρθρο 1 του νόμου αυτού ιδρύεται η Εθνική Επιτροπή Προστασίας Απορρήτου των Επικοινωνιών, της οποίας αποστολή είναι (μεταξύ των άλλων) και η προστασία του απορρήτου της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης. Έτσι με τις προϋποθέσεις του άρθρου 4 του νόμου αυτού μπορεί να γίνει η παρακολούθηση (ανταλλαγής) e-mail.π.χ. ο Α εκβιάζει (άρθρο 385) τον Β στέλνοντας e-mail. Ο Β καταγγέλλει στην Αστυνομία. Η αστυνομία ζητά από τον παροχέα να παρακολουθεί την ανταλλαγή e-mail. Ο παροχέας στην περίπτωση αυτή δεν μπορεί να επικαλεστεί το απόρρητο των επικοινωνιών.

6.1.4 Ειδικές ποινικές διατάξεις στο χώρο του διαδικτύου.

Τιμωρούνται ποινικώς , εάν διαπράττονται στο χώρο του διαδικτύου, οι παρακάτω συμπεριφορές[44]:

Α) Σύμφωνα με το άρθρο 11 του Ν. 2867/2000, η κατά παράβαση των άρθρων 5 (αναφέρεται στη χορήγηση γενικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) και 6 (αναφέρεται στη χορήγηση ειδικών αδειών τηλεπικοινωνιακών δραστηριοτήτων άσκηση τηλεπικοινωνιακών δραστηριοτήτων τιμωρείται με φυλάκιση τουλάχιστον δώδεκα (12) μηνών και με χρηματική ποινή ύψους από πέντε εκατομμύρια (5.000.000) έως πεντακόσια εκατομμύρια (500.000.000) δραχμές.

Επίσης όποιος παραβαίνει με οποιοδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρηση του απορρήτου των

---

[44] Βλ. ΑΓΓΕΛΗ Ιωάννη, Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το Ελληνικό Δίκαιο, Ποιν.Δικ.12/2001, σελ1297επ.

κάθε είδους δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο ετών και χρηματική ποινή πέντε έως είκοσι εκατομμυρίων δραχμών, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις. Σε περίπτωση που ο παραβάτης της παρούσας διάταξης ανήκει στο προσωπικού τηλεπικοινωνιακής επιχείρησης, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον τριών ετών και η χρηματική ποινή τουλάχιστον δέκα εκατομμύρια δραχμές.

Ο τεχνικός εξοπλισμός και τα μέσα που χρησιμοποιήθηκαν για την τέλεση των παραπάνω αξιοποίνων πράξεων δημοσιεύονται. Σε περιπτώσεις πολλαπλών ή καθ' υποτροπή παραβάσεων προβλεπόμενων στον παρόντα νόμο, όπως εκάστοτε ισχύει, ή στον Ποινικό Κώδικα, σε σχέση με τα παραπάνω αδικήματα , επιβάλλονται αθροιστικά οι βαρύτερες ποινές.

Β) Σύμφωνα επίσης με το άρθρο 13 Ν.2774/1999, για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα , όποιος κατά παράβαση του νόμου αυτού χρησιμοποιεί, επεξεργάζεται, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή ενός εκατομμυρίου έως δέκα εκατομμυρίων δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα με άλλες διατάξεις.

Υπεύθυνος επεξεργασίας που δεν συμμορφώνεται με τις πράξεις της Αρχής που επιβάλλει τις διοικητικές κυρώσεις των περιπτώσεων γ΄(προσωρινή ανάκληση αδείας), δ΄ (οριστική ανάκληση αδείας) και ε΄ (καταστροφή αρχείου ή διακοπή επεξεργασίας και καταστροφή των σχετικών δεδομένων) της πργ 1 του άρθρου 21 του Ν.2472/97, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών.

Οι διατάξεις των πργ 6 έως και 214 του άρθρου 22 του Ν.2472/97 εφαρμόζονται και επί πράξεων των προηγούμενων παραγράφων.

Γ) Σύμφωνα με το άρθρο 22 (πργ 1-7) του Ν.2472/97:

1. Όποιος παραλείπει να γνωστοποιήσει στη Αρχή, κατά το άρθρο 6 του παρόντος νόμου , τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της αδείας, που προβλέπεται από την παρ.3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών.

2. Όποιος, κατά παράβαση του άρθρου 7 του παρόντος νόμου , διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών.

3. Όποιος κατά παράβαση του άρθρου 8, προβαίνει σε διασύνδεση αρχείων χωρίς να το γνωστοποιήσει στην Αρχή τιμωρείται με φυλάκιση έως τριών ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών.

4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση αυτών ή τα αφαιρεί , αλλοιώνει , βλάπτει, καταστρέφει, επεξεργάζεται, μεταδίδει, ανακοινώνει, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο, τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως δέκα εκατομμύρια δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα με άλλες διατάξεις.

5. Υπεύθυνος επεξεργασίας που δε συμμορφώνεται με τις αποφάσεις της Αρχής, που εκδίδονται για την ικανοποίηση του δικαιώματος πρόσβασης , σύμφωνα με την πργ 4 του άρθρου 12, για την ικανοποίηση του δικαιώματος

της αντίρρησης, σύμφωνα με την πργ 2 του άρθρου 13, καθώς και με τις πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ΄, δ΄ και ε΄ της πργ 1 του άρθρου 21, τιμωρείται με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου έως πέντε εκατομμύρια δραχμών. Με τις ποινές αυτές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δε συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6. Αν ο υπαίτιος των πράξεων των πργ 1 έως 5 του παρόντος άρθρου είχε σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος ή να βλάψει τρίτον, επιβάλλεται κάθειρξη έως δέκα ετών και χρηματική ποινή τουλάχιστον δύο έως δέκα εκατομμυρίων δραχμών.

7. Αν από τις πράξεις των πργ 1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε έως δέκα εκατομμυρίων δραχμών.

7. Προσπάθεια νομικής αντιμετώπισης του θέματος στον Ευρωπαϊκό νομικό χώρο.

Η πρωτοπορία και στη νομική αντιμετώπιση το εγκλήματος στον κυβερνοχώρο ανήκει, όπως και η τεχνική, στις Η.Π.Α. 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 .

Στον Ευρωπαϊκό χώρο γίνεται συνεχώς προσπάθεια να ρυθμιστεί το θέμα. Σχετικές προσπάθειες πάντως έχουν γίνει τόσο στα πλαίσια του Συμβουλίου της Ευρώπης, όσο και στα πλαίσια της Ευρωπαϊκής Ένωσης.

7.1 Συμβούλιο Ευρώπης και έγκλημα στον κυβερνοχώρο.

Το Συμβούλιο της Ευρώπης έχει ασχοληθεί τόσο με το ηλεκτρονικό έγκλημα, όσο και με το έγκλημα στον κυβερνοχώρο. Έχουν εκδοθεί δύο σχετικές με το θέμα συστάσεις και ειδικότερα:

α) Η Σύσταση No R (89) 9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή (Recommendation No R (89) 9 on Computer - related crime).

(β) Η Σύσταση No R (95) 13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών (Recommendation No R (95) 13 Problems of criminal procedural Law connected with information technology).

Στο Συμβούλιο της Ευρώπης καταρτίζεται από το έτος 1997 Διεθνής Σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στο Κυβερνοχώρο. Στην κατάρτιση της Σύμβαση αυτής συμμετέχει και η Ελλάδα. Σκοπός της Συμβάσεως είναι η προστασία της Κοινωνίας από το έγκλημα στον κυβερνοχώρο, με την θέσπιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα Δικαστικής Συνεργασίας μεταξύ των κρατών, που θα υπογράψουν την Σύμβαση. Αρχικώς ως χρονοδιάγραμμα για την περαίωση

των εργασιών, είχε τεθεί το τέλος του έτους 1999. Επειδή όμως τα προβλήματα (νομικά και τεχνικά) που προέκυψαν κατά την συζήτηση ήταν τόσα πολλά και τόσο περίπλοκα, ζητήθηκε (και χορηγήθηκε) παράταση της προθεσμίας περαιώσεως μέχρι το τέλος του 2000. Ήδη η Σύμβαση έχει υπογραφεί το έτος 2001 στην Βουδαπέστη[45].

Η συγκεκριμένη σύμβαση καθιερώνει την υποχρέωση εναρμονίσεως των Εθνικών νομοθεσιών σε θέματα εγκλημάτων στον κυβερνοχώρο (internet crimes) τόσο σε θέματα ποινικού, όσο και Αστικού Δικαίου.

Κύριο χαρακτηριστικό της Διεθνούς αυτής Συμβάσεως είναι η υποχρέωση που αναλαμβάνουν τα κράτη-μέλη, να ποινικοποιήσουν ορισμένη συμπεριφορά στο διαδίκτυο. Ενδιαφέρουσες διατάξεις, που έχουν σχέση με την ασφάλεια στο διαδίκτυο, από ουσιαστική ποινική άποψη είναι οι παρακάτω:

7.1.1 Η Παράνομη πρόσβαση (illegal Access).

Σύμφωνα με το άρθρο 2 της Συμβάσεως κάθε μέλος θα θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως την πρόσβαση σε ολόκληρο ή σε μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα. Το μέρος μπορεί να απαιτεί ότι, το αδίκημα θα διαπράττεται ή με παραβίαση των μέτρων ασφαλείας ή με το σκοπό αποκτήσεως ηλεκτρονικών δεδομένων ή για άλλο παράνομο σκοπό ή σε σχέση με ένα σύστημα ηλεκτρονικών υπολογιστών, που συνδέεται με άλλο σύστημα ηλεκτρονικών υπολογιστών.

---

[45] Περισσότερες λεπτομέρειες για Σύμβαση της Βουδαπέστης του 2001 βλ. Αγγελής Ιωάννης: Νομοθετήματα προς επικύρωση, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), Ποιν. Δικ. 12/2001, σελ. 1218επ.

Το άρθρο αυτό έχει ως σκοπό να ποινικοποιήσει αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως ``hacking``. Ο όρος στα Ελληνικά μπορεί να αποδοθεί ως ``εισβολή``. Ως εισβολή μπορεί να οριστεί η ενέργεια το εισβολέα (``hacker``) να εισέλθει (διεισδύσει - αποκτήσει πρόσβαση), με διάφορους τεχνικούς τρόπους, σε ξένα συστήματα υπολογιστών. Προστατευόμενο έννομο αγαθό είναι η ασφάλεια του ηλεκτρονικού συστήματος, δηλαδή η πρόληψη της πρόσβασης από μη εξουσιοδοτημένα άτομα στο σύστημα. Αποτελεί δηλαδή το άρθρο αυτό, το ``ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο`` της διατάραξης οικιακής ειρήνης (άρθρο 334 Π.Κ.). Όπως δηλαδή ο δικαιούχος της κατοικίας έχει το δικαίωμα να ορίζει ποιος μπορεί να εισέρχεται και να παραμένει σ΄ αυτήν, έτσι και ο "δικαιούχος" του ηλεκτρονικού υπολογιστή δικαιούται να ορίζει ποιος θα τον χρησιμοποιεί και ποιος θα "εισέρχεται" σ΄ αυτόν.

Ο δικαιολογητικός λόγος της ποινικοποιήσεως της παράνομης πρόσβασης συνίσταται στο γεγονός ότι, ο κάθε κάτοχος ή χρήστης ηλεκτρονικού υπολογιστή πρέπει να έχει το δικαίωμα να ορίζει ο ίδιος, τα άτομα που μπορούν να έχουν πρόσβαση ή εξουσία χρήσεως του υπολογιστή ή του συστήματος υπολογιστή.

Ο όρος "πρόσβαση" περιλαμβάνει την "χωρίς εξουσιοδότηση είσοδο" σε ολόκληρο τον ηλεκτρονικό υπολογιστή ή μέρος αυτού (π.χ. σε επιμέρους φακέλους). Δεν περιλαμβάνει όμως την χωρίς δικαίωμα αποστολή ηλεκτρονικών μηνυμάτων ή φακέλων.

Για την θεμελίωση της υποκειμενικής υποστάσεως απαιτείται πρόθεση , όπως αυτή προσδιορίζεται σύμφωνα με το εσωτερικό δίκαιο κάθε μέλους κράτους. Οι περισσότερες νομοθεσίες των κρατών μελών του Συμβουλίου της Ευρώπης περιλαμβάνουν διατάξεις σχετικές με την παράνομη πρόσβαση σε ηλεκτρονικό υπολογιστή.

7.1.2 Η αθέμιτη παγίδευση - υποκλοπή (illegal interception).

Σύμφωνα με το άρθρο 3 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως

ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η παγίδευση - υποκλοπή, που γίνεται με τεχνικά μέσα, από μη δημόσια εκπομπή δεδομένων ηλεκτρονικών υπολογιστών, από, προς ή μέσα σ' ένα σύστημα υπολογιστών, συμπεριλαμβανομένων ηλεκτρομαγνητικών εκπομπών από ένα σύστημα υπολογιστών, που "μεταφέρει" τέτοια στοιχεία. Ένα μέλος μπορεί να απαιτήσει ότι το αδίκημα διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών, το οποίο συνδέεται με άλλο σύστημα.

Η διάταξη αυτή μπορεί να εφαρμοστεί σε κάθε μορφή υποκλοπής ηλεκτρονικών δεδομένων, είτε αυτά διακινούνται δια του κυβερνοχώρου με μεταφορά φακέλων (file transfer), είτε με e-mail, είτε με FAX.

Προστατευόμενο έννομο αγαθό είναι ``το δικαίωμα στην ιδιωτική ζωή και της ασφάλειας των τηλεπικοινωνιών στον κυβερνοχώρο`` Αποτελεί δηλαδή το άρθρο αυτό, το ``ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο`` της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας (υποκλοπή).

Στην Ελληνική έννομη τάξη η συμπεριφορά αυτή προβλέπεται στην στο άρθρο 370 Α §§1 και 2 Π.Κ. Σύμφωνα με αυτό όποιος αθέμιτα παγιδεύει ή με οποιαδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων τιμωρείται με φυλάκιση. Η χρησιμοποίηση από τον δράστη των πληροφοριών ή μαγνητοταινιών που αποκτήθηκαν με αυτόν τον τρόπο θεωρείται επιβαρυντική περίπτωση. Επίσης, όποιος αθέμιτα παρακολουθεί με ειδικά τεχνικά μέσα ή μαγνητοφωνεί προφορική συνομιλία μεταξύ τρίτων, που δεν διεξάγεται δημόσια ή μαγνητοσκοπεί μη δημόσιες πράξεις τρίτων τιμωρείται με φυλάκιση.

7.1.3 Επέμβαση σε δεδομένα (Data interference).

Σύμφωνα με το άρθρο 4 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εθνική του νομοθεσία, όταν διαπράττονται εκ προθέσεως η καταστροφή (damaging), η διαγραφή (deletion), η χειροτέρευση (deterioration), η μεταβολή (alteration), ή η απόκρυψη (suppression) δεδομένων χωρίς δικαίωμα. Σκοπός του άρθρου αυτού είναι να προστατεύσει τα δεδομένα (data) και τα προγράμματα των ηλεκτρονικών υπολογιστών ως "υλικές υποστάσεις" από οποιαδήποτε επέμβαση (παρεμβολή), που γίνεται με πρόθεση πρόκλησης ζημιάς σ΄ αυτά. Προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική λειτουργία ή χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

Ως εγγύτερο άρθρο στην Ελληνική έννομη τάξη μπορεί να θεωρηθεί αυτό της φοράς ξένης ιδιοκτησίας (άρθρο 381 Π.Κ.).

7.1.4 Επέμβαση σε σύστημα (System Interference).

Σύστημα ηλεκτρονικού υπολογιστή ("Computer system") σημαίνει κάθε συσκευή ή ομάδα συσκευών που είναι εσωτερικώς συνδεδεμένες μεταξύ των ή με άλλες σχετικές συσκευές, μια ή περισσότερες από τις οποίες επεξεργάζονται αυτομάτως δεδομένα (data), σύμφωνα με κάποιο πρόγραμμα.

Δεδομένα υπολογιστή (computer data) είναι κάθε αναπαράσταση (representation) γεγονότων (facts), πληροφοριών ή εννοιών (concepts) σε μορφή κατάλληλη για επεξεργασία σε σύστημα υπολογιστή, συμπεριλαμβανομένου προγράμματος κατάλληλο να προκαλέσει σ΄ ένα σύστημα υπολογιστή την εκτέλεση μιας λειτουργίας.

Σύμφωνα με το άρθρο 5 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα, για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την Εθνική του Νομοθεσία, όταν

διαπράττεται εκ προθέσεως η σοβαρή παρεμπόδιση, χωρίς δικαίωμα, της λειτουργίας ενός συστήματος υπολογιστή, που γίνεται με πρόσθεση (Inputting), μεταφορά (transmitting), καταστροφή (damaging), διαγραφή (deleting), χειροτέρευση (deterioration), μεταβολή (alteration), ή απόκρυψη (suppression) δεδομένων υπολογιστών.

Το προστατευόμενο έννομο αγαθό στο άρθρο αυτό είναι το δικαίωμα του χρήστη να έχει μια "κανονική" λειτουργία του υπολογιστή του. Η διάταξη αυτή ποινικοποιεί, αυτό που στην γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως ``computer sabotage`` (δολιοφθορά ηλεκτρονικού υπολογιστή).

7.1.5 Κακή χρήση συσκευών (misuse of devices).

Σύμφωνα με το άρθρο 6 της Συμβάσεως κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα, που είναι απαραίτητα προκειμένου να καθιερώσει ως ποινικά αδικήματα σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα η παραγωγή, πώληση, η προετοιμασία για χρήση εισαγωγή, διανομή ή με οποιοδήποτε άλλο τρόπο διάθεση μιας συσκευής συμπεριλαμβανομένου προγράμματος υπολογιστή που έχει σχεδιαστεί ή προσαρμοστεί πρωτίστως για τους σκοπούς διάπραξης οποιουδήποτε από τα αδικήματα που θεμελιώνονται στα άρθρα 2-5 της Συμβάσεως.

Στην Ελληνική έννομη τάξη το άρθρο αυτό αντιστοιχεί με το 370 Α §7 Π.Κ. Σύμφωνα με αυτό, όποιος διαθέτει στο εμπόριο ή με άλλον τρόπο προσφέρει για εγκατάσταση τεχνικά μέσα ειδικά μόνο για την τέλεση των πράξεων των §§ 1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεσή τους τιμωρείται με φυλάκιση και με χρηματική ποινή.

7.2 Η θέση της Ευρωπαϊκής Ένωσης απέναντι στο διαδίκτυο.

Η Ευρωπαϊκή Ένωση δεν έμεινε αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα[46] γενικότερα και στον κυβερνοχώρο ειδικότερα . Έτσι στις 17.2.1997 εκδίδεται το No 97/C 70/01ψήφισμα του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών, που συνήλθαν στα πλαίσια του Συμβουλίου της Ευρωπαϊκής Ένωσης.

Κύριο χαρακτηριστικό του ψηφίσματος αυτού είναι ότι η Ευρωπαϊκή Ένωση αναγνωρίζει τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητα στους πολίτες, μειώνοντας τα εμπόδια ως προς τη δημιουργία και τη διανομή περιεχομένου και προσφέροντας ευρεία πρόσβαση σε όλο και πλουσιότερες πηγές ψηφιακών πληροφοριών. Αναγνωρίζει επίσης το παραπάνω ψήφισης την ανάγκη καταπολέμησης της παράνομης χρήσης των τεχνικών δυνατοτήτων του κυβερνοχώρου, ιδιαίτερα για αξιόποινες πράξεις κατά των παιδιών. Πριν από την έκδοση του ψηφίσματος αυτού είχαν γίνει για το θέμα διάφορες επίσημες ή ανεπίσημες συναντήσεις[47] .

Χαρακτηριστικό επίσης του ψηφίσματος αυτού είναι ότι η Ευρωπαϊκή Ένωση διαχωρίζει το περιεχόμενο (content) του διαδικτύου, δηλαδή τα δεδομένα-στοιχεία (data), που διακινούνται, σε παράνομο και επιβλαβές .

7.2.1 παράνομο περιεχόμενο του Internet.

Το σχετικό ψήφισμα (97/C 70/01/17-2-1997) του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών μελών της Ε.Ε. για το παράνομο

---

[46] Βλ. σχετικά α) απόφαση του Συμβουλίου της 31-3-1992 στον Τομέα Ασφάλειας Πληροφοριών (92/242/ΕΟΚ) Επίσημη Εφημερίδα Ευρωπαϊκών Κοινοτήτων L123/19, β)Σύσταση του Συμβουλίου της 7-4-1995 για κοινά κριτήρια ασφαλείας της τεχνολογίας πληροφοριών (95/144/ΕΚ) Επίσημη Εφημερίδα Ευρωπαϊκών Κοινοτήτων L93/27.

[47] Βλ. σχετικά Επίσημη Εφημερίδα Ευρωπαϊκών Κοινοτήτων C- 70/1

και επιβλαβές περιεχόμενο του διαδικτύου[48], δεν καθορίζει τι είναι παράνομο και τι επιβλαβές περιεχόμενο.

Κατά συνέπεια λοιπόν οι έννοιες αυτές θα προσδιοριστούν από το νομοθέτη σε περίπτωση που ψηφιστεί σχετικός νόμος που θα ρυθμίζει τη συμπεριφορά όσων «κινούνται» στο χώρο του διαδικτύου. Και λέγοντας εδώ «νομοθέτη» εννοούμε τον εθνικό νομοθέτη κάθε χώρας. Στο σημείο όμως αυτό προκύπτει το ερώτημα, εάν «οι εσωτερικές νομοθεσίες» μπορούν αυτοτελώς, να αντιμετωπίσουν αποτελεσματικά τις παρανομίες του κυβερνοχώρου, λόγω της φύσης του εγκλήματος και του ιδιαίτερου τρόπου τελέσεώς του. Είναι προφανές ότι οι εσωτερικές νομοθεσίες από μόνες τους δεν επαρκούν και απαιτούνται πολυμερείς διεθνείς συμβάσεις[49].

Προς το παρόν ως παράνομο περιεχόμενο μπορεί να θεωρηθεί κάθε τι που είναι μεν παράνομο (και) εκτός δικτύου μπορεί δε (τεχνικώς) να κινηθεί και εντός κυβερνοχώρου (π.χ. συκοφαντική δυσφήμηση).

7.2.2 Επιβλαβές περιεχόμενο του Internet.

Το «επιβλαβές περιεχόμενο» αποτελεί ευρύτερη έννοια από αυτή του «παράνομου περιεχομένου». Εννοείται ότι οτιδήποτε είναι επιβλαβές, δεν είναι και οπωσδήποτε και παράνομο. Η έννοια του «επιβλαβούς περιεχομένου» ενέχει σε μεγάλο βαθμό και το υποκειμενικό στοιχείο.

Είναι ευνόητο ότι η έννοια του επιβλαβούς περιεχομένου έχει διαφορετική βαρύτητα, όταν πρόκειται για χρήση του διαδικτύου από ανηλίκους. Παράδειγμα: Στο Internet υπάρχουν εκατοντάδες θέσεις (sites) που αναφέρονται στο σατανισμό και στη λατρεία του σατανά. Για πολλούς το περιεχόμενο των sites αυτών αποτελεί κλασική μορφή «επιβλαβούς

---

[48] Βλ. σχετικά περιοδικό «Ο κόσμος του Internet», Νοέμβριος 1997, σελ. 45 επ.

[49] Βλ. Comelius Prittwitz, Ποινικό Δίκαιο και Παγκοσμιοποίηση, Υπεράσπιση 2000, σελ. 203 επ.

περιεχομένου». Για άλλους όμως αποτελεί μια μορφή ελεύθερης έκφρασης της προσωπικότητας ή ακόμη και μια μορφή ανεξιθρησκίας .

Γενικώς ως επιβλαβές περιεχόμενο μπορεί να θεωρηθεί, ότι αναφέρεται σε ρατσιστικές διακρίσεις ή σε παραπλανητική διαφήμιση. Ως χαρακτηριστικό παράδειγμα επιβλαβούς περιεχομένου υλικό του διαδικτύου μπορεί να θεωρηθεί και η περίπτωση (κατά τον Οκτώβριο του 1999) πλειοδοσίας κατά την πώληση ωαρίων εμφανίσιμων γυναικών («μανεκέν») σε ειδική τοποθεσία (site). Ομοίως η περίπτωση «της ερωτικής συνεύρεσης για πρώτη φορά» (Αύγουστος 1998) μεταξύ «δύο παρθένων νέων» που όμως τελικά δεν έγινε. Είναι ευνόητο ότι πριν από τη ματαίωση της «παράστασης» εκατομμύρια χρήστες από όλο τον κόσμο είχαν «επισκεφθεί» την αντίστοιχη τοποθεσία (site) με τεράστια οικονομικά κέρδη για τους «διοργανωτές». Η περίπτωση αυτή μπορεί να θεωρηθεί και ως απάτη που διαπράττεται στο διαδίκτυο. Είναι ευνόητο όμως ότι ουδείς βλαπτόμενος (ιδιώτης) ενδιαφέρθηκε για την υποβολή εγκλήσεως προς άσκηση ποινικής διώξεως, λαμβάνοντας υπόψη τη μικρή οικονομική ζημιά που υπέστη ως άτομο ή την «διαπόμπευση» του για τις «διαδικτυακές του προτιμήσεις», σε σχέση και με τα τεράστια δικαστικά έξοδα που απαιτούνται για την κίνηση ενός τέτοιου δικαστικού αγώνα.

Σημειώνεται ότι για την αντιμετώπιση του παράνομου και επιβλαβούς περιεχομένου του κυβερνοχώρου έχει προταθεί – μεταξύ των άλλων- κι δημιουργία «οργάνου αυτορύθμισης» στο πλαίσιο λειτουργίας των παροχέων υπηρεσιών καθώς και λειτουργία «θερμής γραμμής», όπου θα μπορούν να γίνονται σχετικές (επώνυμες ή και ανώνυμες) καταγγελίες[50] .

[50] Βλ. περιοδικό «Ο κόσμος του Internet», Νοέμβριος 1997, σελ. 47.

8. Η νομική αντιμετώπιση του "Χάκερ" κατά το γενικό ποινικό δίκαιο.[51]

Σύμφωνα με το άρθρο 370Γ§2 Π.Κ.[52], όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφ΄ όσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις του κράτους ή στην ασφάλεια του κράτους, τιμωρείται κατά το άρθρο 148. Η πράξη αυτή διώκεται μόνον ύστερα από έγκληση του παθόντα. Διευκρινίζεται δε ότι, το άρθρο 148 Π.Κ., το οποίο στην §2 αποτελεί κακούργημα, αναφέρεται στην κατασκοπεία, που διαπράττεται από πολίτη, παραπέμπει δε (το άρθρο 148 Π.Κ.) και στο άρθρο 146, το οποίο αναφέρεται στην παραβίαση των μυστικών της πολιτείας, όταν διαπράττεται βέβαια από πολίτη και όχι από στρατιωτικό. Το τελευταίο αυτό σημαίνει ότι, εάν ο χάκερ, ο οποίος εισήλθε παράνομα στα ηλεκτρονικά δεδομένα του Υπουργείου Εθνικής Αμύνης, έλαβε στην κατοχή του ή στη γνώση του αντικείμενα ή ειδήσεις, που τα συμφέρονται της πολιτείας ή των συμμάχων της επιβάλουν να τηρηθούν απόρρητα απέναντι σε ξένη κυβέρνηση τιμωρείται με φυλάκιση μέχρι ενός έτους. Αν όμως ο υπαίτιος ενήργησε με σκοπό να χρησιμοποιήσει τα ανωτέρω αντικείμενα ή ειδήσεις για να τα διαβιβάσει σε άλλον ή να τα ανακοινώσει έτσι ώστε να μπορούν να εκθέσουν σε κίνδυνο το συμφέρον του κράτους και ιδίως την ασφάλειά του ή κάποιου από τους συμμάχους του, τιμωρείται με ποινή κάθειρξης[53].

---

[51] http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_poiniki_nomothesia.as

[52] Βλ. σχετικά ΚΑΡΑΚΩΣΤΑ Ιωάννη, Το δίκαιο του Internet (Νομική αντιμετώπιση του διαδικτύου), Νομικό Βήμα, τόμος 46, σελ. 1172επ.

[53] Για περισσότερες λεπτομέρειες σχετικά με «μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή (hacking) βλ. ΛΑΖΟΣ Γρηγόρης: Πληροφορική και Έγκλημα, εκδόσεις Νομική Βιβλιοθήκη,Αθήνα 2001, σελ. 95επ.

Αξιοσημείωτο είναι επίσης ότι, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα.

Διευκρινίζεται ότι, το παραπάνω άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988. Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου. Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του "χάκερ" στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών "χάκερς", όπως είναι οι cracker, whacker κλπ .

Λέγοντας απόρρητο εννοούμε το δικαίωμα του κατόχου των δεδομένων να αποκλείει άλλους από την πρόσβαση σ΄αυτά, χωρίς να απαιτείται η ύπαρξη απορρήτου από ουσιαστική έννοια. Στο άρθρο 370 Β §1 ορίζεται ότι, ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Είναι ευνόητο βέβαια ότι, ή παραπάνω διάταξη του άρθρου 370 Γ §2 Π.Κ. θα εφαρμοστεί κατά την περίπτωση εκείνη που ο δράστης απλώς θα έχει εισέλθει χωρίς δικαίωμα σε σύστημα υπολογιστών, χωρίς να προκαλέσει οποιαδήποτε άλλη βλάβη. Σε περίπτωση δε, που από την χωρίς δικαίωμα διείσδυσή του έχει επέλθει και παραβίαση άλλων εννόμων αγαθών, η νομική αντιμετώπιση είναι κάθε φορά ανάλογη. Έτσι π.χ. στην πλέον γνωστή υπόθεση "χάκιγκ", που απασχόλησε την Ελληνική νομική πράξη τον Ιούλιο του 2000, εναντίον του Έλληνα "χάκερ" γνωστού ως cyberia ασκήθηκε ποινική δίωξη και για παράβαση του άρθρου 386 Α Π.Κ. σε βαθμό κακουργήματος. Το άρθρο αυτό, το οποίο περιλαμβάνεται στα εγκλήματα κατά των περιουσιακών δικαιωμάτων, προστατεύει την περιουσία.

8.1 Νομικός ορισμός του "χάκερ".

Σύμφωνα λοιπόν με όσα αναφέρθηκαν παραπάνω για το άρθρο 370 Γ Π.Κ., ως Χάκερ, μπορεί να οριστεί το άτομο εκείνο, το οποίο, χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών. Οι χάκερς εμφανίστηκαν για πρώτη φορά κατά την δεκαετία του 1970 στις ΗΠΑ, ως δράστες κατά των τηλεπικοινωνιακών συστημάτων. Σήμερα εμφανίζονται με δύο μορφές: α)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, χωρίς την πρόκληση βλάβης και β)με την μορφή εισόδου (διείσδυσης) σε σύστημα υπολογιστών, με πρόκληση βλάβης. Το είδος της βλάβης που θα προκαλέσει εξαρτάται από τις συγκεκριμένες περιπτώσεις. Στην δεύτερη αυτή περίπτωση έχει επικρατήσει ο όρος "κράκερ", ο οποίος όμως είναι και αυτός όρος τεχνικής φύσεως και όχι νομική έννοια.

Από άποψη νομικής επιστήμης, η εξέταση της προσωπικότητας του χάκερ αποτελεί αντικείμενο της επιστήμης της εγκληματολογίας[54] .

8.2 Νομικές προϋποθέσεις για την ύπαρξη "χάκιγκ" κατά το Ελληνικό Δίκαιο.

Για την ουσιαστική εφαρμογή του άρθρου 370 Γ §2 Π.Κ. πρέπει να συντρέχουν οι παρακάτω προϋποθέσεις:

α) πρόσβαση σε στοιχεία. Ως πρόσβαση θεωρείται κάθε διείσδυση του δράστη, που αποβλέπει να λάβει γνώση των στοιχείων. Αντικείμενο της πρόσβασης είναι στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

β) η πρόσβαση αυτή να γίνεται χωρίς δικαίωμα, δηλαδή χωρίς την συγκατάθεση του κατόχου των στοιχείων. Σε περίπτωση που υφίσταται η

[54] http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_poiniki_nomothesia.asp

συγκατάθεση αυτή, είναι ευνόητο ότι, δεν θεμελιώνεται η αντικειμενική υπόσταση του εγκλήματος του άρθρου 370 Γ §2 Π.Κ. Σε περίπτωση που ο δράστης είναι στην υπηρεσία του νομίμου κατόχου των στοιχείων, τότε τεκμαίρεται ότι, αυτός έχει το δικαίωμα νόμιμης πρόσβασης στα στοιχεία. Αυτό συνάγεται από την §3 του ίδιου άρθρου 370 Γ §2 Π.Κ., σύμφωνα με την οποία η πράξη της §2 τιμωρείται, μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμού ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

Η έλλειψη δικαιώματος πρόσβασης τεκμαίρεται ιδίως όταν, γίνεται (η πρόσβαση) με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που έχει λάβει νόμιμος κάτοχός τους. Ως τέτοια μέτρα ασφαλείας θεωρούνται οι κωδικοί λέξεων (passwords) οι κωδικοί αριθμοί χρηστών, μαγνητικές κάρτες κλπ. Η διατύπωση του άρθρου 370 Γ§2 Π.Κ. είναι "αρκούντως ευρεία", ώστε να περιλαμβάνει κάθε πρόσβαση σε δεδομένα και αρχεία. Στην ευρεία αυτή διατύπωση του, οφείλεται και το γεγονός ότι, μπορεί να υπαχθεί στο άρθρο αυτό η ενέργεια του "χάκερ", δηλαδή το "χάκιγκ". Άλλωστε, το έτος 1988 που θεσπίστηκε η συγκεκριμένη διάταξη, η χρήση του internet ήταν πολύ περιορισμένη και τα εγκλήματα στον κυβερνοχώρο σχεδόν άγνωστα. Το έγκλημα του άρθρου 370 Γ§2 Π.Κ. είναι έγκλημα διακινδύνευσης και όχι έγκλημα βλάβης[55].

[55]http://67.18.47.148/com/index/aboutinternet/data/astinomia/diadiktio_kai_poiniki_nomothesia.asp

παιδικής πορνογραφίας, με καταχωρήσεις ασέμνου υλικού σε Ελληνικές (διαδικτυακές) διευθύνσεις στον κυβερνοχώρο.

Για την καταπολέμηση της διάδοσης της παιδικής πορνογραφίας στο διαδίκτυο έχουν δημιουργηθεί διάφορες «ηλεκτρονικές οργανώσεις ατόμων» οι οποίες «ψάχνουν» στο διαδίκτυο και καταγγέλλουν στις Αρχές τη διακίνηση παιδικού πορνογραφικού υλικού .

Η διασφάλιση ενός αυστηρού πλαισίου λειτουργίας του Διαδικτύου για παιδιά και εφήβους απασχολεί την Ευρωπαϊκή Ένωση από το 1996, οπότε και ξεκίνησε η προσπάθεια ανάπτυξης ενός πανευρωπαϊκού δικτύου πληροφόρησης και εκπαίδευσης σχετικά με τους κινδύνους αλλά και τους τρόπους που μπορούν να συμβάλουν στην προστασία από τις αρνητικές πλευρές του Διαδικτύου. Το πρόγραμμα δράσης για την επίτευξη αυτού του στόχου έχει τρεις κύριες κατευθυντήριες[60]:

Τη δημιουργία ασφαλέστερου περιβάλλοντος. Για τον σκοπό αυτό δημιουργούνται οι ανοικτές γραμμές επικοινωνίας (hotlines). Πρόκειται για αποδέκτες καταγγελιών του κοινού σχετικά με σελίδες με παράνομο περιεχόμενο. Οι καταγγελίες, έπειτα από διεξοδική διερεύνηση, διαβιβάζονται στην αρμόδια υπηρεσία, για παράδειγμα στην αστυνομία, που αναλαμβάνει τον περαιτέρω χειρισμό του θέματος. Στο ευρωπαϊκό δίκτυο ανοικτών γραμμών συμμετέχουν έντεκα χώρες και σύντομα αναμένεται η λειτουργία ανοικτής γραμμής και στην Ελλάδα.

Τα τεχνικά μέσα άσκησης του γονικού ελέγχου. Πρόκειται για τα λεγόμενα «φίλτρα», προγράμματα δηλαδή, τα οποία εμποδίζουν την πρόσβαση σε συγκεκριμένες ιστοσελίδες. Ένα σημαντικό πρόβλημα που αντιμετωπίζουν οι χρήστες των ευρωπαϊκών χωρών σε σχέση με αυτή την τεχνολογία είναι ότι στη συντριπτική τους πλειονότητα τα προγράμματα προορίζονται για την αμερικανική αγορά και είναι αποτελεσματικά μόνον όσον αφορά το αγγλικό λεξιλόγιο.

---

[60] http://news.kathimerini.gr/4dcgi/_w_articles_ell_2763417_28/09/2002_39201

άρθρο: «Παγίδες» στο Διαδίκτυο για τα παιδιά.

Δράσεις συνειδητοποίησης και πληροφόρησης, που αφορούν γονείς και εκπαιδευτικούς, κυβερνητικούς φορείς και τη βιομηχανία που αναπτύσσεται σε σχέση με το Διαδίκτυο. Ειδικά όσον αφορά τους γονείς και εκπαιδευτικούς, από την Ευρωπαϊκή Επιτροπή ιδρύθηκε το Κέντρο Ανταλλαγής των Εμπειριών Συνειδητοποίησης για την Ασφαλέστερη Χρήση του Διαδικτύου (SIFKaL), το οποίο έχει στόχο την ορθή ενημέρωσή τους σχετικά με τις νέες τεχνολογίες, τα προτερήματα και τα μειονεκτήματά τους.

10. Προβλήματα απονομής δικαιοσύνης στο έγκλημα που σχετίζεται με το διαδίκτυο.

10.1 Γενικά.

Τα Ελληνικά Ποινικά Δικαστήρια καλούνται καθημερινά σχεδόν να αντιμετωπίσουν υποθέσεις ηλεκτρονικών εγκλημάτων και να επιλύσουν νομικά θέματα και προβλήματα που έχουν σχέση με τα ηλεκτρονικά αποδεικτικά στοιχεία. Επίσης οι Ελληνικές Ανακριτικές Αρχές καλούνται να αντιμετωπίσουν επί καθημερινής βάσης παρόμοια θέματα. Ενδεικτικά αναφέρονται οι περιπτώσεις εκείνες που σχετίζονται με την παιδική πορνογραφία στο διαδίκτυο.

Τα ερωτήματα που προκύπτουν είναι: α)Ποια επιμέρους προβλήματα αντιμετωπίζει ο Έλληνας δικαστής κα εισαγγελέας κατά τη διερεύνηση και εκδίκαση των υποθέσεων που σχετίζονται με εγκλήματα του διαδικτύου; β) Έχει ο μέσος δικαστής και εισαγγελέας τις απαιτούμενες γνώσεις για να διερευνήσει (ο εισαγγελέας) και να εκδικάσει (ο δικαστής) μια ποινική υπόθεση για την οποία απαιτούνται ειδικές γνώσεις τεχνολογίας; γ) τι πρέπει να γίνει για την αντιμετώπιση και επίλυση αυτών των θεμάτων;

10.2 Υποθέσεις από την πρακτική των Ελληνικών Δικαστηρίων.[61]

Η πλέον σημαντική περίπτωση που αντιμετώπισαν μέχρι σήμερα τα ελληνικά δικαστήρια είναι αυτή του Έλληνα φοιτητή hacker ο οποίος έγινε γνωστός με το όνομα «cyberia». Στην περίπτωση αυτή τα πραγματικά περιστατικά έχουν ως εξής: Την άνοιξη του έτους 2000 δύο τηλεφωνικές γραμμές του Εθνικού Ιδρύματος Ερευνών στην Αθήνα βρέθηκαν «υπερχρεωμένες». Το περίεργο είναι ότι, οι τηλεφωνικές αυτές συνδέσεις είχαν «¨φραγή εξωτερικών κλήσεων»και επομένως δεν ήταν δικαιολογημένη με λογικά και τεχνικά κριτήρια η χρέωση αυτών με τόσα πολλά εκατομμύρια

[61] Ιωάννη Αγγελή, Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, Ποινική Δικαιοσύνη 8-9/2005 σελ.1962.

δραχμές, που το Εθνικό Ίδρυμα Ερευνών εκκαλείτο να καταβάλει. Μετά από σχετική καταγγελία το αρμόδιο τμήμα της Ελληνικής Αστυνομίας και ειδικότερα το Τμήμα Δίωξης Οικονομικού Εγκλήματος διενήργησε ποινική έρευνα. Κατά την έρευνα αυτή διαπιστώθηκε ότι ο δράστης χρησιμοποιώντας το υπολογιστικό κέντρο του Πανεπιστημίου του Camerino της Ιταλίας διενεργούσε κλήσεις από τις συγκεκριμένες ψηφιακές – τηλεφωνικές γραμμές του Εθνικού Ιδρύματος Ερευνών. Συνδεόταν με «ροζ τηλεφωνικές γραμμές» και έμενε σε αυτές πολλές ώρες. Ακολουθώντας τα ηλεκτρονικά ίχνη του δράστη, διαπιστώθηκε ότι αυτός «ενεργούσε» από κάποια πόλη της Βορείου Ελλάδας. Συνελήφθη και ασκήθηκε εναντίον του ποινική δίωξη για απάτη με ηλεκτρονικό υπολογιστή σε βαθμό κακουργήματος (άρθρο 386^{A} σε συνδυασμό με το άρθρο 386 πργ 3 ΠΚ) και μετά την απολογία του κρίθηκε προσωρινά κρατούμενος. Διευκρινίζεται ότι, σύμφωνα με το κατηγορητήριο ο σκοπός του δράστη ήταν οικονομικός, διότι έπαιρνε ποσοστά, από τον παροχέα των «πορνοτηλεφώνων». Μετά το πέρας της κυρίας ανάκρισης το Δικαστικό Συμβούλιο δέχθηκε, ύστερα από σύμφωνη πρόταση του εισαγγελέα ότι, δεν πρέπει να γίνει κατηγορία εναντίον του λόγω ελλείψεως επαρκών ενδείξεων ενοχής (Συμβούλιο Πλημμελειοδικών Αθηνών 4328/2001). Το «νομικώς παράδοξο»σε αυτήν την περίπτωση είναι ότι, ενώ ο δράστης αρχικώς κρίθηκε προσωρινά κρατούμενος, στη συνέχεια ούτε καν παραπέμφθηκε στο ακροατήριο. Η «απόσταση» μεταξύ προσωρινής κράτησης και μη παραπομπής είναι πολύ μεγάλη . Σύμφωνα με τον Ι. Αγγελή αυτό σημαίνει ότι, είτε το Δικαστικό Συμβούλιο, είτε ο Ανακριτής με τον Εισαγγελέα γνωμοδοτήσεων εκτίμησαν εσφαλμένα τα αποδεικτικά στοιχεία με την προϋπόθεση βέβαια ότι από την απολογία του κατηγορουμένου μέχρι και το πέρας της κυρίας ανακρίσεως, δεν προέκυψαν νέα αποδεικτικά στοιχεία.

10.3 Ενδεικτικός προσδιορισμός προβλημάτων.

Στη συνέχεια γίνεται προσπάθεια να εξεταστούν ορισμένα από τα προβλήματα που αντιμετωπίζει ο Δικαστής και ο Εισαγγελέας κατά το χειρισμό των υποθέσεων, που έχουν ως αντικείμενο το ηλεκτρονικό έγκλημα και τη σύγχρονη τεχνολογία.

10.3.1 Προβλήματα γενικής φύσεως.

Το πρώτο σοβαρό πρόβλημα που αντιμετωπίζει ο Έλληνας νομικός (δικαστής, εισαγγελέας αλλά και δικηγόρος) είναι ότι η προσέγγιση των νομικών θεμάτων που αφορούν το έγκλημα του διαδικτύου (αλλά και τις σύγχρονες τεχνολογίες γενικότερα) ενέχει τη δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών(computers) και διαδικτύου (internet). Είναι σχεδόν αδύνατο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του ηλεκτρονικού εγκλήματος χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Αυτό σε πρακτικό επίπεδο σημαίνει ότι ο Δικαστής και ο Εισαγγελέας πρέπει να διαθέτει και τεχνικές γνώσεις, για να αντιληφθεί τις νομικές διατάξεις που αναφέρονται στο έγκλημα του κυβερνοχώρου και στις σύγχρονες τεχνολογίες γενικότερα.

Τόσο η τεχνική όσο και η νομική ορολογία στο συγκεκριμένο θέμα είναι διατυπωμένη –κατά κανόνα- στην Αγγλική γλώσσα. Η αντίστοιχη μεταφορά των όρων αυτών στα Ελληνικά δεν είναι ούτε εύκολη ούτε δόκιμη. Βέβαια κατά την καθημερινή πρακτική πολλοί όροι χρησιμοποιούνται στην ξενόγλωσση διάστασή τους κατά τρόπο που τείνουν να ενσωματωθούν και στο Ελληνικό νομικό λεξιλόγιο. Έτσι αντί του ελληνικού όρου «διαδικτυακό

έγκλημα» ή «έγκλημα στο διαδίκτυο» ή «έγκλημα στον κυβερνοχώρο», πολλές φορές χρησιμοποιείται αυτούσιος ο όρος cyber crime ή internet crime[62].

10.3.2 Προβλήματα κατά την προδικασία.

10.3.2.1 Δυσχέρειες κατά την άσκηση της ποινικής δίωξης.

Ο εισαγγελέας ο οποίος θα ασκήσει την ποινική δίωξη σε συγκεκριμένη υπόθεση εγκλήματος του διαδικτύου, πρέπει να έχει εξειδικευμένες νομικές γνώσεις. Δεν είναι σπάνιες οι περιπτώσεις εκείνες που για τα ίδια πραγματικά περιστατικά ασκείται διαφορετική ποινική δίωξη. Αυτό οφείλεται στο γεγονός ότι λόγω ελλείψεως των απαιτούμενων ειδικών γνώσεων, ο Εισαγγελέας ο οποίος ασκεί την ποινική δίωξη , δεν κάνει τίποτε άλλο από το αναγράφει τη δίωξη που αναφέρεται στη μήνυση ή στην έγκληση ή στο διαβιβαστικό της διωκτικής αρχής. Ευνόητο είναι βέβαια ότι η εσφαλμένη ποινική δίωξη θα οδηγήσει σε εσφαλμένη δικαστική απόφαση.

10.3.2.2 Δυσχέρειες κατά τη συλλογή και διατήρηση του αποδεικτικού υλικού.

Ο παραδοσιακός τρόπος διερευνήσεως του εγκλήματος, δηλαδή της περιγραφής του δράστη με την κατάθεση του θύματος, της συλλογής πληροφοριών από πληροφοριοδότες, της διεξαγωγής έρευνας, κατάσχεσης κτλ δεν ισχύει στο έγκλημα του διαδικτύου. Ο δράστης του κυβερνοχώρου δεν θα πάρει το όπλο, ούτε θα φορέσει τα γάντια και θα εισέλθει στην τράπεζα για να τη ληστέψει ή σε ένα σπίτι για να κλέψει. Αντίθετα, με τους κατάλληλους κωδικούς αριθμούς που παράνομα έχει αποκτήσει (πάλι διαπράττοντας ένα ηλεκτρονικό έγκλημα), θα δώσει εντολή για μεταφορά ενός χρηματικού ποσού

---

[62] Βλ. σχετικά: Δ. ΚΙΟΥΠΗ, «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα». Κενά και αδυναμίες της Ελληνικής Νομοθεσίας», Υπεράσπιση 2000, σελ. 959 επ.

από το λογαριασμό του «ηλεκτρονικού θύματος» σε έναν άλλο στο εξωτερικό. Και όταν το θύμα πάρει είδηση την εναντίον του ενέργεια ο δράστης ή θα έχει μεταφέρει τα χρήματα σε διάφορους άλλους λογαριασμούς για να χαθούν τα ηλεκτρονικά ίχνη του ή θα τα έχει «σηκώσει» και θα έχει εξαφανιστεί .

Ο «παραδοσιακός εισαγγελέας» και η «παραδοσιακή αστυνομία»[63] δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων. Στην «κοινή έρευνα» το αντικείμενο είναι ορατό «διά γυμνού οφθαλμού» και ο προανακριτικός υπάλληλος μπορεί εύκολα να το περιγράψει στην έκθεση κατασχέσεως. Αντίθετα στο έγκλημα του κυβερνοχώρου, το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές, οι οποίοι μάλιστα μπορεί να είναι εγκατεστημένοι σε πολλές χώρες. Το θέμα του τόπου τελέσεως σε συνδυασμό με την αστυνομική και δικαστική συνεργασία είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζονται στο στάδιο της προδικασίας[64]. Και αυτό γιατί η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή και χιλιάδες τόπους τελέσεως από πολλούς δράστες ταυτόχρονα.

Μετά τη συλλογή των αποδεικτικών στοιχείων τίθεται το πρόβλημα διατήρησής τους. Οι κατάλληλες συνθήκες φύλαξής τους αποτελούν σημαντικό παράγοντα. Έτσι η έκθεσή τους σε ήλιο, υγρασία, σκόνη κλπ, ενδεχομένως να οδηγήσει στην καταστροφή τους και κατά συνέπεια στην αδυναμία αξιολόγησής τους .

---

[63] Γνωστός είναι ο όρος « internet cop – computer cop» (αστυνομικός του διαδικτύου-ηλεκτρονικός αστυνομικός .

[64] Βλ. σχετικά Δ. ΚΙΟΥΠΗ, Ποινικό Δίκαιο και Internet, σελ. 75, σειρά Ποινικά, No 57.

10.3.2.3 Δυσχέρειες από την έλλειψη ειδικών γνώσεων των προανακριτικών υπαλλήλων.

Σημαντικοί παράγοντες για την απόκτηση των ηλεκτρονικών αποδεικτικών μέσων είναι οι παρακάτω:

- Η ταχύτητα ενεργείας του προανακριτικού υπαλλήλου. Τα ηλεκτρονικά αποδεικτικά μέσα κατά κανόνα «δεν περιμένουν». Με το πάτημα ενός απλού πλήκτρου (delete) μπορεί να χαθούν σε κλάσματα δευτερολέπτου αποδεικτικά στοιχεία που αντιστοιχούν σε χιλιάδες τόμους συμβατικών εγγράφων.
- Η παρατηρητικότητα του προανακριτικού υπαλλήλου. Ο συνδυασμός πχ αριθμών που μπορεί μεν να εμφανίζονται (εξωτερικώς) ως αριθμοί τηλεφώνων, ενδεχομένως όμως, να αποτελούν «κλειδιά» πρόσβασης στο σύστημα ή ακόμα και τους κωδικούς αποκρυπτογράφησης, σε περίπτωση που τα στοιχεία τηρούνται κρυπτογραφημένα. Επίσης, η εσφαλμένη αποσύνδεση των καλωδίων του ηλεκτρονικού υπολογιστή στον οποίον είναι αποθηκεμένα τα αποδεικτικά στοιχεία, μπορεί να οδηγήσει στην εξαφάνισή τους (χάσιμο).
- Η τήρηση τεχνικών μέσων. Για τη συλλογή των ηλεκτρονικών αποδεικτικών στοιχείων απαιτείται κατά κανόνα η χρήση άλλων ηλεκτρονικών συσκευών (ηλεκτρονικών υπολογιστών, βίντεο κλπ) ή άλλων τεχνικών εξαρτημάτων. Κατά την απόκτηση των ηλεκτρονικών αποδεικτικών στοιχείων σημαντικό παράγοντα αποτελούν οι τηλεπικοινωνίες. Μέχρι τώρα η έννοια της υποκλοπής συνειρμικά μας οδηγούσε στην παραβίαση των τηλεφωνημάτων και της προφορικής συνομιλίας. Σήμερα όμως , μέσα από τα τηλεφωνικά δίκτυα , δεν μεταφέρεται μόνο φωνή , αλλά και καθετί άλλο που μπορεί να λάβει ψηφιακή μορφή, όπως κείμενα, εικόνες, ήχοι, τραγούδια, κινηματογραφικά έργα κλπ.
- Η συμβολή του παροχέα υπηρεσιών. Ο ρόλος του παροχέα υπηρεσιών στην ασφάλεια και τη μυστικότητα του διαδικτύου είναι πολύ σημαντικός. Αποτελεί μάλιστα «κομβικό σημείο» για τον εντοπισμό των παρανομιών και τη συλλογή των αποδεικτικών στοιχείων, δεδομένου ότι, όλα τα δεδομένα

στοιχεία (data) «περνούν» από τις εγκαταστάσεις του. Ερώτημα γεννάται κατά πόσο ο παροχέας μπορεί να έχει ποινική ευθύνη για τις παρανομίες που «περνούν» από τις εγκαταστάσεις του, υποπίπτουν στην αντίληψη του και ουδέν πράττει για να σταματήσει τη διάπραξή τους. Ένα δεύτερο, εξίσου σημαντικό ερώτημα είναι κατά πόσο μπορεί (νομοθετικώς) να υποχρεωθεί ο παροχέας να φυλλάτει τα δεδομένα που διέρχονται από τις εγκαταστάσεις του, για ένα ορισμένο χρονικό διάστημα προκειμένου να τα παραδώσει στις Αρχές, σε περίπτωση που του ζητηθούν κατά την ποινική διερεύνηση των ηλεκτρονικών εγκλημάτων.

10.4 Το πρόβλημα της συμμετοχής του ιδιώτη κατά τη διενέργεια των προανακριτικών πράξεων.

Η συμβολή του ιδιώτη – παθόντα, ο οποίος έχει πέσει θύμα εγκλήματος διαδικτύου, παρουσιάζει διαφοροποιήσεις με τη συνήθη συμβολή του σε περιπτώσεις «κοινών εγκλημάτων» και αυτό, λόγω της απροθυμίας τους να καταγγείλουν τις εναντίον τους πράξεις.

- Δεν υπάρχει η κατάλληλη οργανωτική-διοικητική υποδομή για τον εντοπισμό του από την πλευρά της πολιτείας .
- Αμφισβητείται από τους παθόντες εάν οι αρμόδιες για την έρευνα, δίωξη και εκδίκαση Αρχές (Εισαγγελικές, Δικαστικές, Αστυνομικές κλπ) έχουν τις απαιτούμενες γνώσεις για το σχετικό θέμα και
- Συνήθως παθόντες από το έγκλημα του διαδικτύου είναι τράπεζες, εταιρείες, δημόσιοι οργανισμοί, των οποίων η φήμη και η επαγγελματική δραστηριότητα μειώνεται σε περίπτωση που δημοσιοποιείται ότι το σύστημά τους είναι ευπρόσβλητο σε τέτοιου είδους επιθέσεις.

Δεν είναι επίσης σπάνιες οι περιπτώσεις εκείνες που η (προ)ανακριτική διερεύνηση των σχετικών ποινικών παραβάσεων γίνεται στην πράξη (κατά κανόνα) με ιδιωτική πρωτοβουλία των ενδιαφερομένων , με ενέργειες που είναι τουλάχιστον αμφιβόλου νομιμότητας. Ως κλασικό παράδειγμα μπορεί να αναφερθεί η πρακτική ορισμένων οργανισμών συλλογικής διαχείρισης, για την

προστασία από την παράβαση των πνευματικών δικαιωμάτων τους . Δηλαδή, με «ειδικά προγράμματα ανιχνεύσεως» οι ενδιαφερόμενοι «σερφάρουν» στο διαδίκτυο, εντοπίζουν αυτούς που «κατεβάζουν» μουσικά έργα, ερευνούν τα στοιχεία τους και διατηρούν καταλόγους με ονόματα. Αυτό σημαίνει (πρακτικώς) ότι, συλλέγουν και διατηρούν δεδομένα προσωπικού χαρακτήρα, πολλά από τα οποία είναι ευαίσθητα προσωπικά δεδομένα για μεγάλο αριθμό ατόμων. Ουδείς μπορεί να αποκλείσει ότι, η επεξεργασία των στοιχείων αυτών ενδεχομένως να γίνεται κατά παράβαση του Ν.2472/97, περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Στη συνέχεια, σε περίπτωση που (οι ιδιωτικοί φορείς) κρίνουν σκόπιμο ότι, πρέπει να μηνυθεί ο δράστης μιας τέτοιας πράξεως, καταγγέλλουν αυτή στην αρμόδια διωκτική αρχή, χωρίς βέβαια να αποκαλύπτουν τον τρόπο με τον οποίο συνέλλεξαν τα σχετικά αποδεικτικά στοιχεία. Κατά κανόνα επίσης, στις έρευνες που γίνονται (κατά την έννοια του άρθρου 253επ ΚΠΔ), παρευρίσκοντας και οι ιδιώτες –υπάλληλοι των οργανισμών συλλογικής διαχείρισης, οι οποίοι όχι σπάνια, κατευθύνουν τις έρευνες όσον αφορά τη συλλογή των αποδεικτικών στοιχείων. Σύμφωνα με τον Ι. Αγγελή, αυτό γίνεται λόγω της «ανοχής» που επιδεικνύεται από τους (προ)ανακριτικούς υπαλλήλους, η οποία οφείλεται στην έλλειψη ειδικών γνώσεων.

11. Επίλογος

Αναμφισβήτητα η ευκολία και η ταχύτητα της επικοινωνίας μέσω του Διαδικτύου κρύβει πολλούς κινδύνους «κακής χρήσης» του μέσου και διάπραξης εγκληματικών πράξεων. Η εγκληματικότητα του Διαδικτύου αποτελεί πλέον μια απτή πραγματικότητα. Η διερεύνηση μάλιστα των διαφόρων μορφών εμφάνισης και των χαρακτηριστικών της αποδεικνύει ότι πρόκειται για ένα νέο φαινόμενο που δημιουργεί εγκληματολογικά προβλήματα και προβλήματα ουσιαστικού ποινικού δικαίου. Πρέπει στο σημείο αυτό να υπογραμμιστεί ότι τα τεχνικά δεδομένα της μεταφοράς ηλεκτρονικών δεδομένων μέσω του διαδικτύου συνδέονται με μια σειρά ζητημάτων και εννοιών του δόγματος του ποινικού δικαίου, όπως για παράδειγμα συμβαίνει σχετικά με την έννοια του εγγράφου[65].

Χαρακτηριστικό γνώρισμα της λειτουργίας του διαδικτύου αποτελεί ο παγκόσμιος χαρακτήρας του, όπου τα κρατικά σύνορα δεν αποτελούν όριο για τη διάδοση παράνομου περιεχομένου ή για την περιχάραξη του πλαισίου μιας εγκληματικής δραστηριότητας. Η σπουδαιότητα της ασφαλούς και απρόσκοπτης κυκλοφορίας της πληροφορίας στο διαδικτυακό περιβάλλον δημιουργεί την ανάγκη ανάδειξης της και προστασίας της ως ένα παγκόσμιο έννομο αγαθό. Εγκληματικές δραστηριότητες που απειλούν το αγαθό της παγκόσμιας επικοινωνίας μέσω του διαδικτύου, όπως η παράνομη διείσδυση, η επέμβαση, η αναχαίτιση και η παρεμβολή παρασίτων και ιών, δεν είναι δυνατόν να αντιμετωπίζονται με ποινικές διατάξεις που απηχούν αντιλήψεις και καλύπτουν ανάγκες του πρώτου μισού του προηγούμενου αιώνα. Είναι αναγκαίο να αναζητηθεί η συνεργασία και η συνεννόηση σε διεθνές επίπεδο[66] για τη σύγκληση των εθνικών ποινικών νομοθεσιών.

---

[65] Φαραντούρης Νικόλαος, Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο-Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, Ποιν. Δικ. 2/2003, σελ. 196.

[66] Η διεθνής συνεργασία αποδεικνύεται έμπρακτα από μια σειρά από οδηγίες της Ευρωπαϊκής Ένωσης και από τη Συνθήκη του Συμβουλίου της Ευρώπης, Βουδαπέστη 23.11.2001.

Σημαντικά θεωρούνται τα ζητήματα που αντιμετωπίζουν οι διωκτικές κρατικές αρχές στην προσπάθεια δίωξης, διερεύνησης και συλλογής αποδεικτικών μέσων σχετικά με εγκλήματα που τελούνται στο Διαδίκτυο.

Η προτεινόμενη απάντηση σε μια εγκληματικότητα που λόγω μέσου επεκτείνεται σε παγκόσμια κλίμακα είναι η συνένωση των δυνάμεων των εθνικών τάξεων για την από κοινού αντιμετώπισή της. Αυτό επιτυγχάνεται στο πλαίσιο μιας πολυεπίπεδης προσέγγισης και συνεργασίας.

Το ποινικό δίκαιο αντιμετωπίζει σήμερα την πρόκληση να συνθέσει ένα συνολικό σχέδιο που θα είναι κατάλληλο να αντιταχθεί στο έγκλημα στον κυβερνοχώρο και στις νέες μορφές εγκληματικότητας που μελλοντικά θα προκύψουν. Επειδή όμως οι διεθνείς συμβάσεις με αντικείμενο την από κοινού και ενιαία αντιμετώπιση της εγκληματικότητας στο διαδίκτυο περιγράφουν το πλαίσιο δράσης του εθνικού νομοθέτη, κατά καμία έννοια δεν παρουσιάζεται εξασφαλισμένη η απαρασάλευτη διατήρηση του δόγματος του ποινικού δικαίου, τη στιγμή μάλιστα που αναγνωρίζονται παντάπασι οι δυσκολίες εναρμόνισης των διαφόρων ποινικών διατάξεων των κρατών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΑ

Αραβαντινός Βασίλειος: Εισαγωγή στη Νομοπληροφορική και τη δικαιοκυβερνητική, εκδόσεις Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1994.

Βασιλάκη Ειρήνη: Η καταπολέμηση της εγκληματικότητας μέσω Ηλεκτρονικών Υπολογιστών, εκδόσεις Α.Ν. Σάκκουλας, Αθήνα – Κομοτηνή 1993.

Ζάννη Αναστασία: Το διαδικτυακό έγκλημα, εκδόσεις Α.Ν. Σάκκουλα, Αθήνα – Κομοτηνή 2005

Καράκωστας Κ. Ιωάννης: Δίκαιο και internet, Νομικά ζητήματα του διαδικτύου, εκδόσεις Π.Ν. Σάκκουλας.

Κιούπης Δημήτριος: Ποινικό Δίκαιο και Internet, Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή 1999.

Λάζος Γρηγόρης: Πληροφορική και Έγκλημα, εκδόσεις Νομική Βιβλιοθήκη, Αθήνα 2001.

Μούρτος Ιωάννης: Ηλεκτρονικό έγκλημα και δικανική πληροφορική, εκδόσεις «ΛΥΧΝΙΑ», Αθήνα 2003.

ΝΟΥΣΚΑΛΗΣ Γεώργιος: Απάτη με ηλεκτρονικό υπολογιστή (Η/Υ), Το παρελθόν και το μέλλο του άρθρου 386ΠΚ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ευρωπαϊκή Ένωση, Ποιν. Δικ. 2/2003.

Σφακιανάκης Μιχάλης: Εισαγωγή στην ηλεκτρονική σκέψη, εκδόσεις Κλειδάριθμος, Αθήνα 2003.

ΑΡΘΡΑ

Αγγελής Ιωάννης: Ηλεκτρονικό έγκλημα και απονομή της ποινικής δικαιοσύνης, Ποινική Δικαιοσύνη 8-9/2005.

Αγγελής Ιωάννης: Διαδίκτυο και ποινικό δίκαιο-Έγκλημα στον κυβερνοχώρο (Cybercime – Internet), Ποιν. Χρον. Ν/2000.

Αγγελής Ιωάννης: Το νομικό πλαίσιο για την ασφάλεια του κυβερνοχώρου κατά το Ελληνικό Δίκαιο, Ποιν.Δικ.12/2001.

Αγγελής Ιωάννης: Νομοθετήματα προς επικύρωση, Η Σύμβαση του Συμβουλίου της Ευρώπης για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο (Convention on Cyber-crime), Ποιν. Δικ. 12/2001

Καράκωστας Ιωάννης: Το δίκαιο του Internet (Νομική αντιμετώπιση του διαδικτύου), Νομικό Βήμα, τόμος 46.

Κιούπης Δημήτριος: Ποινική ευθύνη των εταιρειών παροχής πρόσβασης στο Internet, Ποιν. Δικ. ΜΗ/1998.

Κιούπης Δημήτριος: «Αλλοίωση ηλεκτρονικών δεδομένων και αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα. Κενά και αδυναμίες της Ελληνικής Νομοθεσίας», Υπεράσπιση 2000.

Κιούπης Δημήτριος: Ποινικό Δίκαιο και Internet, σειρά Ποινικά, Νο 57.

Μαρίνος Ν. Αναστάσιος: «Το ίντερνετ και οι συνέπειες του κυρίως στο χώρο του δικαίου». Ελλ.Δικ.1998.

Νούσκαλης Γεώργιος: Απάτη με ηλεκτρονικό υπολογιστή: Το παρελθόν και το μέλλον του άρθρου 386^{A} Π.Κ, ιδίως υπό το πρίσμα των εξελίξεων στο Συμβούλιο της Ευρώπης και στην Ε.Ε. Ποιν.Δικ.2/2003 σελ 178 επ.

Prittwitz Cornelius: Ποινικό Δίκαιο και Παγκοσμιοποίηση, Υπεράσπιση 2000.

Σταμούλης Σπ.: Προβλήματα ευθύνης από την αθέμιτη χρήση των Ηλεκτρονικών Υπολογιστών, ΝοΒ 1987.

Φαραντούρης Νικόλαος: Σύγχρονες εγκληματικές δράσεις στο Διαδίκτυο-Εννοιολογική προσέγγιση και ποινική αντιμετώπιση του Hacking και του φαινομένου της μόλυνσης με ιούς, Ποιν. Δικ. 2/2003.

ΠΕΡΙΟΔΙΚΑ

ΒήμαΝετ
Ο κόσμος του ίντερνετ
Computer για όλους
National Geografic

ΕΦΗΜΕΡΙΔΕΣ

Το Βήμα
Καθημερινή
Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης.