ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΚΑΤΑ ΤΟ ΕΛΛΗΝΙΚΟ ΔΙΚΑΙΟ (ΤΟ ΔΙΑΔΙΚΤΥΟ ΩΣ ΜΕΣΟ ΔΙΑΠΡΑΞΗΣ ΕΓΚΛΗΜΑΤΟΣ)

ΓΕΩΡΓΑΣ ΕΜΜΑΝΟΥΗΛ
ΑΜ: 6947

Μεσολόγγι , Νοέμβριος 2006

Μεσολόγγι , Νοέμβριος 2006

Η παρούσα εργασία είναι αποτέλεσμα προσωπικής εργασίας μου. Αναφορές σε βιβλιογραφικές
πηγές μέσα στο κείμενο διευκρινίζουν ποιες πληροφορίες, στοιχεία και γνώσεις αντλήθηκαν
από άλλες εργασίες, βιβλία, διαδίκτυο, κ.λπ.

(όνομα φοιτητή) .....ΓΕΩΡΓΑΣ ΘΑΝΑΣΟΥΛΑ.....

(Υπογραφή) .....

ΣΤΟΥΣ ΓΟΝΕΙΣ ΜΟΥ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΚ	Αστικός Κώδικας	**π.χ**	Παραδείγματος χάρη
ΑΠ	Άρειος Πάγος	**ΕΕ**	Ευρωπαϊκή Ένωση
Αριθμ.	Αριθμός	**ΕΚ**	Ευρωπαϊκές Κοινότητες
Άρθρ,	άρθρο	**ΕΕΤΤ**	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
βλ.	Βλέπε	**ΕΟΚ**	Ευρωπαϊκή Οικονομική Κοινότητα
σελ.	σελίδα	**ΔτΑ**	Δικαιώματα του Ανθρώπου (περιοδικό)
κ.λπ.	και τα λοιπά	**Π.Δ.**	Προεδρικό Διάταγμα
κ.ά	και άλλα	**ΑΔΑ**	Ανεξάρτητη Διοικητική Αρχή
ν.	νόμος	**ΥΑ**	Υπουργική Απόφαση
δηλ.	δηλαδή	**ΜΜΕ**	Μέσα Μαζικής Ενημέρωσης και Επικοινωνίας
Σ	Σύνταγμα	**Η/Υ**	Ηλεκτρονικός Υπολογιστής
Π.Κ.	Ποινικός Κώδικας	**ΚΠολΔ**	Κώδικας Πολιτικής Δικονομίας
κ.ο.κ.	και ούτω καθεξής	**ΔΕΕ**	Διεύθυνση Εγκληματολογικών Ερευνών
παρ.	παράγραφος	**ΔΕΚ**	Δικαστήριο Ευρωπαϊκών Κοινοτήτων
εδ.	εδάφιο	**ΦΕΚ**	Φύλλο Εφημερίδος της Κυβερνήσεως

ΕΙΣΑΓΩΓΗ

Είναι γνωστό ότι ο χώρος του Δικτύου είναι ένας χώρος που υπερβαίνει το εδαφικά σύνορα μεταξύ των διαφόρων κρατών. Το γεγονός ότι για να εισαχθείς σ' αυτόν τον χώρο πρέπει να χρησιμοποιήσεις ένα ηλεκτρονικό υπολογιστή και να εισαγάγεις ένα σύνθημα που είναι μοναδικό για τον καθένα που χρησιμοποιεί αυτόν τον χώρο σαν μέσο απόκτησης πληροφοριών πιστοποιεί την αυτοτέλεια του. Παρόλα αυτά, οι ανάγκες της επιβολής του νόμου και της τάξης στο Διαδίκτυο, καθώς και οι προκλήσεις που κρύβει το Internet πρέπει να αναγνωριστούν ως ύψιστης σημασίας.

Το Διαδίκτυο πρέπει να αντιμετωπιστεί νομικά ως μέσο διάπραξης εγκλήματος, μέχρις ότου διαμορφωθεί η κατάλληλη νομική βάση σε ελληνικό επίπεδο, με την αντίστοιχη λειτουργία νέων θεσμών και φορέων απονομής δικαιοσύνης, ώστε να μπορέσει να χαρακτηρισθεί και ως τόπος διάπραξης εγκλήματος.

Η σημερινή νομική κατάσταση, σε επίπεδο ποινικού δικαίου, κυρίως, δεν κάνει διάκριση μεταξύ των εγκλημάτων, που τελέστηκαν με χρήση του Διαδικτύου, ή χωρίς αυτή, με εξαίρεση τα άρθρα του Ποινικού Κώδικα, που αφορούν περιπτώσεις διείσδυσης σε υπολογιστικό σύστημα. Η αναλογική αυτή εφαρμογή των νόμων δεν βλάπτει, πλην όμως υπάρχουν περιπτώσεις, που κρίνεται ανεπαρκής. Το Διαδίκτυο δρα ως καταλυτής ικανός να μεταλλάσει κοινά εγκλήματα. Ως παράδειγμα , αναφέρεται το έγκλημα της εξύβρισης, που στο κοινό Ποινικό Δίκαιο λαμβάνει ως δεδομένη τη φυσική ύπαρξη του εξυβρίζοντα , ενώ στην εξύβριση μέσω Διαδικτύου τίθεται σε αμφισβήτηση ακόμη κι η ίδια η ταυτότητα του δράστη. Πέραν των νομικών κενών που σήμερα υφίστανται, το Διαδίκτυο προκαλεί σήμερα ,ακόμη περισσότερο, την ίδια την επιβολή του νόμου σε όλα τα επίπεδα.

Κεφάλαιο 1: ΕΓΚΛΗΜΑΤΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

1.1 Ηλεκτρονικά Εγκλήματα

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. Ως ηλεκτρονικό έγκλημα μπορεί να οριστεί αυτό που σχετίζεται άμεσα με την κατάχρηση των δυνατοτήτων των ηλεκτρονικών υπολογιστών αυτό προσδιορίζεται στο άρθρο 14 Π.Κ. 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 .

Η άποψη ότι το έγκλημα στον κυβερνοχώρο (cyber crime) αποτελεί τον ίδιο τύπο εγκλήματος με το "κοινό" ή "συμβατικό έγκλημα" με την μόνη διαφορά που το διακρίνει απ' αυτό είναι ότι, διαπράττεται σε διαφορετικό περιβάλλον, (δηλ. σε ηλεκτρονικό περιβάλλον) 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 αποκλειστικός σε περιβάλλον του κυβερνοχώρου[1]. Με το παραπάνω λοιπόν κριτήριο τα σχετικά (ηλεκτρονικά) εγκλήματα μπορούν να διακριθούν:

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

[1] Αγγελή, Ι., Έγκλημα στον Κυβερνοχώρο & Ελληνικό Δίκαιο ΠοινΔικ 12/2001(ΕΤΟΣ 4ο)

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 παράγ. 1 του Π.Κ. π.χ. η χωρίς δικαίωμα αντιγραφή προγράμματος από USB ή DVD-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 η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή (hacking) ή η διάδοση παιδικού πορνογραφικού υλικού διαμέσου 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).

1.2 Οι Εγκληματίες του Κυβερνοχώρου

1.2.1 Κατηγορίες – Κίνητρα Εγκληματιών

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 με τη χρήση του διαδικτύου (hackers) για να μάθουν απλώς, κάποια προσωπικά στοιχεία,

β) σ' αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη κατηγορία 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 και των τεχνικών αναγνώρισης, θα μπορούν να ξεπεράσουν οποιοδήποτε ηλεκτρονικό εμπόδιο, καθώς επίσης και τα εμπόδια που θα αντιμετωπίζουν θα μπορούν να αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον "ξεγελούν" με την ανάλογη κατασκευή φακών επαφής .

1.2.2 Μέσα Διάπραξης Εγκλημάτων

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, να 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 κ.λπ. 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 κ.λπ.) και χωρίς την κατοχή των τεχνικών μέσων, είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

Συμπερασματικώς λοιπόν μπορεί να λεχθεί ότι, το έγκλημα του κυβερνοχώρου, είναι πιο προηγμένο ("ανεβασμένο") και από το έγκλημα του λευκού περιλαίμιου. Στο μέλλον οι κλέφτες δεν θα κυκλοφορούν με την κουκούλα και το περίστροφο στο χέρι ούτε θα τους περιμένει ο συνεργός τους με την μηχανή αναμμένη για να διαφύγουν. Οι μελλοντικοί κλέφτες θα είναι σκυμμένοι πάνω σε ένα πληκτρολόγιο,

μέσω του οποίου θα δίνουν εντολές σε μικρούς αλλά πανίσχυρους ηλεκτρονικούς υπολογιστές και οι κλοπές τους θα απαιτούν από τους Αστυνομικούς όλο και πιο εξειδικευμένες γνώσεις.

1.2.3 Συνήθη Εγκλήματα του Κυβερνοχώρου

Τα πλέον συνηθισμένα εγκλήματα που παρουσιάζονται αυτή την στιγμή στον κυβερνοχώρο είναι : Οι απάτες (με πιστωτικές κάρτες ή μη), η διακίνηση παιδικής πορνογραφίας, εγκλήματα κατά της Εθνικής Ασφάλειας (οδηγίες για κατασκευή Βομβών, εισβολή σε συστήματα ασφαλείας, που έχουν σχέση με την εθνική υποδομή), οδηγίες για παρασκευή ναρκωτικών. Με κριτήριο το προσβαλλόμενο έννομο αγαθό, τα εγκλήματα που διαπράττονται στο διαδίκτυο μπορούν να διακριθούν: σε εγκλήματα κατά των προσωπικών δικαιωμάτων του πολίτη, σε εγκλήματα εναντίον του κοινωνικού συνόλου και σε εγκλήματα εναντίον περιουσιακών αγαθών .

1.3 Εγκλήματα Σχετικά με Υπολογιστές

1.3.1 Πλαστογραφία Σχετική με Ηλεκτρονικό Υπολογιστή

Πλαστογραφία σχετική με Η/Υ διαπράττει όποιος από πρόθεση και χωρίς δικαίωμα προβαίνει στην εισαγωγή, μεταβολή, διαγραφή ή απόκρυψη δεδομένων ηλεκτρονικών υπολογιστών με σκοπό τα δεδομένα αυτά να θεωρούνται ή να χρησιμοποιούνται για νόμιμους σκοπούς σαν να ήταν αυθεντικά.

Σκοπός του άρθρου αυτού είναι να εναρμονίσει τις επιμέρους νομοθεσίες των κρατών - μελών σε θέματα πλαστογραφίας, που διαπράττονται με τη χρήση ηλεκτρονικού υπολογιστή. Κατά το άρθρο 7 της Σύμβασης για τον κυβερνοχώρο την 23-11-2001 στην Βουδαπέστη κάθε κράτος - μέλος, που θα αποδεχθεί τη Σύμβαση θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττονται εκ προθέσεως και χωρίς δικαίωμα, την εισαγωγή, τη μεταβολή, τη διαγραφή ή την απόκρυψη στοιχείων, που έχουν ως αποτέλεσμα την παραγωγή μη αυθεντικών δεδομένων, με στόχο να θεωρηθούν ή να χρησιμοποιηθούν για νόμιμους σκοπούς, σαν να ήταν αυθεντικά, ανεξάρτητα από το εάν τα στοιχεία είναι ευθέως

αναγνωρίσιμα και κατανοητά. Για τη θεμελίωση της ποινικής ευθύνης, ένα μέλος μπορεί να απαιτήσει τον σκοπό εξαπάτησης ή άλλο παρόμοιο παράνομο σκοπό.

Το προστατευόμενο έννομο αγαθό του άρθρου αυτού είναι το ίδιο με αυτό του άρθρου 216 Π.Κ. (σε συνδυασμό με άρθρο 13 παρ. γ, όπως αυτό προστέθηκε με το άρθρο 2 ν.1805/88), δηλ. η ασφάλεια, η αξιοπιστία, η πίστη και η εγκυρότητα των ηλεκτρονικών δεδομένων, των οποίων η χρήση μπορεί να έχει έννομες συνέπειες.

Η ηλεκτρονική πλαστογραφία ρυθμίστηκε με τη διεύρυνση του άρθρου 13 παρ. γ Π.Κ., που έγινε με το άρθρο 2 ν. 1805/88. Σύμφωνα με αυτό ως έγγραφο θεωρείται και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφονται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα.[2]

1.3.2 Απάτη Σχετική με Ηλεκτρονικό Υπολογιστή

Σκοπός του άρθρου αυτού είναι να ποινικοποιήσει κάθε παράνομη παραποίηση που γίνεται κατά τη διαδικασία της επεξεργασίας των δεδομένων, με σκοπό να επιτευχθεί η παράνομη μεταφορά ιδιοκτησίας (χρημάτων).

Σύμφωνα με το άρθρο 8 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να καθιερώσει ως ποινικό αδίκημα, σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως και χωρίς δικαίωμα, την απώλεια περιουσίας με:

α) οποιαδήποτε εισαγωγή, τροποποίηση, διαγραφή ή απόκρυψη δεδομένων υπολογιστών,

β) οποιαδήποτε επέμβαση στη λειτουργία ενός υπολογιστή ή συστήματος υπολογιστών, με σκοπό να επιφέρει χωρίς δικαίωμα οικονομικό όφελος στον εαυτό του ή σε άλλον.

---

[2] Η καταπολέμηση της εγκληματικότητας μέσω ηλεκτρονικών υπολογιστών, σειρά ΠΟΙΝΙΚΑ, No 40, σελ. 133επ. να αποδείξουν γεγονότα που έχουν έννομη σημασία

Για τη θεμελίωση της ποινικής ευθύνης[3], ένα μέλος μπορεί να απαιτήσει σκοπό εξαπάτησης ή άλλο παρόμοιο παράνομο σκοπό. Αντιστοιχεί το άρθρο αυτό της Σύμβασης στο 386 Α Π.Κ., όπως αυτό προστέθηκε Ανάλυση του άρθρου 386 Α Π.Κ.

1.3.3 Εγκλήματα Σχετικά με το Περιεχόμενο

Στην κατηγορία των εγκλημάτων που έχουν σχέση με το περιεχόμενο η Ευρωπαϊκή Ένωση δεν έμεινε αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα γενικότερα και στον κυβερνοχώρο (Internet) ειδικότερα. Έτσι στις 17.2.1997 εκδίδεται το No 97/C 70/01 ψήφισμα 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 τις ωφέλειες που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητες 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 στο παραπάνω ψήφισμα 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. 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, που διακινείται στον κυβερνοχώρο περιλαμβάνεται η ποινικοποίηση συγκεκριμένης συμπεριφοράς, που σχετίζεται με την παιδική πορνογραφία. Σκοπός της διάταξης αυτής είναι να εναρμονίσει τις νομοθεσίες των κρατών - μελών, που θα αποδεχθούν τη Σύμβαση, κατά τέτοιο τρόπο, ώστε να προστατεύσουν τη σεξουαλική εκμετάλλευση των ανηλίκων.

Η σχέση των ανηλίκων με το διαδίκτυο (Internet) θα πρέπει να εξεταστεί από δύο οπτικές γωνίες. Από την πλευρά του ανήλικου ως χρήστη και από την πλευρά του ανήλικου ως θύματος του διαδικτύου. Το πότε, σε ποια δηλαδή ηλικία, θα αρχίσει ο ανήλικος να χρησιμοποιεί το διαδίκτυο δεν είναι θέμα νομικό, αλλά θέμα της

[3] Ποινικό Δίκαιο, Ειδικό Μέρος, σελ. 548επ με το άρθρο 5 ν.1805/88.

παιδαγωγικής επιστήμης. Σχετικές γνώσεις βέβαια για τους ηλεκτρονικούς υπολογιστές (Computer) λαμβάνουν οι μαθητές από τις πρώτες τάξεις του Γυμνασίου. Η προστασία όμως των ανηλίκων από τους κινδύνους που διατρέχουν λόγω κακής χρήσης του διαδικτύου είναι θέμα και της πολιτείας και του ποινικού δικαίου. Οι κίνδυνοι που μπορεί ν' αντιμετωπίσει ένα παιδί κατά τη χρήση του διαδικτύου εντοπίζονται: Στην επαφή με ακατάλληλο υλικό (βία, sex κ.λπ.), στη σεξουαλική παρενόχληση (επαφή με παιδεραστές κ.λπ.), στην απόσπαση διαφόρων στοιχείων που αφορούν τον ίδιο ή την οικογένεια του και τα οποία θα χρησιμοποιηθούν από το δράστη σε βάρος του παιδιού ή της οικογένειας η οποία, σημειωτέον, κατά τα τελευταία χρόνια έχει λάβει τεράστιες διαστάσεις, ιδιαίτερα στο χώρο του διαδικτύου.

Πορνογραφία είναι γενικά η αναπαράσταση της ερωτικής συμπεριφοράς. Αναπαράσταση σε βιβλία, πίνακες, κινηματογραφικές ταινίες κ.λπ. Γενικώς η εξέλιξη της τεχνολογίας συνέβαλε τα μέγιστα στον πολλαπλασιασμό και τη διάδοση του πορνογραφικού υλικού.

Οι εμπλεκόμενοι στο θέμα παράνομοι εκμεταλλεύονται τη διαφορά της νομοθεσίας από κράτος σε κράτος, καθότι αλλού η παιδική πορνογραφία θεωρείται αδίκημα με καθορισμένη αντικειμενική υπόσταση, ενώ αλλού εμπίπτει στο γενικό νόμο περί ασέμνων. Οι σχετικοί (διεθνείς) όροι που χρησιμοποιούνται στο διαδίκτυο για θέματα πορνογραφίας είναι cyber porn (κυβερνοπορνό) και cyber-sex (κυβερνοσεξ). Γενικώς η πώληση sex, και ειδικότερα η πορνογραφία, αποτελεί τη μεγαλύτερη βιομηχανία του κυβερνοχώρου. Δυστυχώς, η βιομηχανία αυτή έχει πέσει στα χέρια επιχειρηματιών, οι οποίοι έχουν δημιουργήσει χιλιάδες θέσεις (sites) που πουλάνε sex οποιασδήποτε μορφής. Η παιδική πορνογραφία είναι ειδικότερη μορφή της πορνογραφίας. Περιλαμβάνει υλικό με ανήλικους σε σεξουαλικές ερωτικές επαφές. Το υλικό αυτό διανέμεται δια μέσου του διαδικτύου, με διάφορους τρόπους. Πριν την ανάπτυξη και διάδοση του διαδικτύου, η ικανοποίηση των σχετικών με την παιδική πορνογραφία ιδιαιτεροτήτων γινόταν με διάφορα μέσα, π.χ. κλειστές ομάδες (club) ατόμων, σεξοτουρισμός σε διάφορες χώρες κ.λπ. Σύμφωνα με το άρθρο 9 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να καθιερώσει ως ποινικά αδικήματα, σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττονται χωρίς δικαίωμα και εκ προθέσεως τις παρακάτω συμπεριφορές:

α) παραγωγή παιδικής πορνογραφίας με σκοπό τη διανομή της, δια μέσου συστήματος ηλεκτρονικού υπολογιστή,

β) προσφορά ή διάθεση πορνογραφικού υλικού δια μέσου συστήματος ηλεκτρονικού υπολογιστή,

γ) διανομή ή εκπομπή πορνογραφικού υλικού δια μέσου συστήματος ηλεκτρονικού υπολογιστή,

δ) προετοιμασία παιδικής πορνογραφίας δια μέσου ενός συστήματος υπολογιστών για τον εαυτό του ή για κάποιον άλλο,

ε) κατοχή παιδικής πορνογραφίας σε σύστημα ηλεκτρονικού υπολογιστή ή σε δεδομένα ηλεκτρονικού υπολογιστή αποθηκευμένα σε κάποιο μέσο.

Για τους σκοπούς της περίπτωσης α, η παιδική πορνογραφία θα περιλαμβάνει πορνογραφικό υλικό που οπτικώς αναπαριστά:

I. ανήλικο εμπλεκόμενο σε σεξουαλική επαφή,

II. άτομο που παριστάνει έναν ανήλικο να εμπλέκεται σε σεξουαλική επαφή,

III. ρεαλιστικές εικόνες που παριστάνουν έναν ανήλικο να εμπλέκεται σε σεξουαλική επαφή.

Ο όρος ανήλικος θα περιλαμβάνει όλα τα πρόσωπα ηλικίας κάτω των δεκαοκτώ (18) ετών. Ένα μέλος μπορεί, όμως, να απαιτήσει κατώτερο όριο ηλικίας, το οποίο δεν πρέπει να είναι μικρότερο των δεκαέξι (16) ετών.

Στην ελληνική έννομη τάξη δεν υπάρχει ειδική νομοθεσία σχετική με την παιδική πορνογραφία. Διευκρινίζεται ότι ήδη καταρτίζεται σχετικό νομοθετικό πλαίσιο από την επιτροπή του Υπουργείου Δικαιοσύνης. Το θέμα καλύπτεται, όχι όμως κατά την άποψη μας επαρκώς, από το άρθρο 29 ν.5060/1931 περί τύπου, προσβολών της τιμής εν γένει και άλλων σχετικών διατάξεων. Ομοίως το θέμα της παιδικής πορνογραφίας δεν καλύπτεται από το άρθρο 349 Π.Κ. (μαστροπεία), για τη θεμελίωση της αντικειμενικής υπόστασης του οποίου, πρέπει να αποδειχθεί ότι ο δράστης προάγει σε πορνεία ή εξωθεί στη διαφθορά ανήλικα πρόσωπα.

1.3.4 Αδικήματα Σχετικά με Παραβιάσεις Πνευματικών και Συγγενικών Δικαιωμάτων

Τα εγκλήματα που σχετίζονται με τις παραβιάσεις των πνευματικών δικαιωμάτων είναι από τα συχνότερα και ίσως από τα πλέον διαδεδομένα στον κυβερνοχώρο.

Σύμφωνα με το άρθρο 10 της Σύμβασης κάθε μέλος θα πρέπει να θεσπίσει τέτοια νομοθετικά και άλλα μέτρα που είναι αναγκαία για να τα θεμελιώσει ως ποινικά αδικήματα, σύμφωνα με την εθνική του νομοθεσία, την παραβίαση των πνευματικών δικαιωμάτων, όπως αυτά προσδιορίζονται σύμφωνα με το νόμο αυτού του μέρους, σύμφωνα με υποχρεώσεις που έχουν αναληφθεί με την πράξη των Παρισίων της 24ης Ιουλίου 1971, τη Σύμβαση της Βέρνης για την προστασία των λογοτεχνικών και καλλιτεχνικών δημιουργημάτων , τη Συμφωνία του Εμπορίου, σχετική με τα δικαιώματα πνευματικής ιδιοκτησίας και τη συνθήκη WIPO για τα πνευματικά δικαιώματα[4] (the WIPO copyright Treaty) με την εξαίρεση κάθε ηθικού δικαιώματος, που προκύπτει από τέτοιες Συμβάσεις, όταν αυτές οι πράξεις διαπράττονται εκ προθέσεως για εμπορικούς σκοπούς μέσω ενός συστήματος υπολογιστών.

Ένα μέλος μπορεί να διατηρήσει το δικαίωμα του να μην επιβάλλει ποινική ευθύνη σε περιορισμένες περιπτώσεις, με την προϋπόθεση ότι άλλα αποτελεσματικά μέτρα είναι διαθέσιμα και ότι αυτή η επιφύλαξη δεν αποκλίνει από τις διεθνείς υποχρεώσεις του μέλους, όπως προωθούνται από τα διεθνή όργανα, που αναφέρονται στο άρθρο. Σκοπός της διάταξης του άρθρου 10 της Σύμβασης είναι να εναρμονίσει τις νομοθεσίες των κρατών - μελών, που θα αποδεχθούν τη Σύμβαση κατά τέτοιο τρόπο, έτσι ώστε να αντιμετωπίζουν ενιαία από ποινική άποψη τις σχετικές παραβιάσεις των πνευματικών δικαιωμάτων.

Για τις σχετικές με το θέμα παραβάσεις ισχύει στην ελληνική έννομη τάξη ο ν.2121/1993. Δεν είναι υπερβολικό να λεχθεί ότι ο νόμος αυτός μπορεί να καλύψει (θεωρητικά τουλάχιστον) κάθε περίπτωση παράβασης πνευματικής ιδιοκτησίας που διαπράττεται στον κυβερνοχώρο. Έχει λεχθεί ότι ο νόμος αυτός διαπνέεται από όλα τα σύγχρονα ρεύματα, που έχουν αποτυπωθεί στις εθνικές νομοθεσίες των ευρωπαϊκών κυρίως χωρών και είναι εναρμονισμένος με την οδηγία 91/250/ΕΟΚ για τη νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών.

[4] Λ. Κατσίρη, «Κοινωνια των πληροφοριών και πνευματική ιδιοκτησία»

Κεφάλαιο 2: ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΕΙΔΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

Η προσέγγιση των νομικών θεμάτων που αφορούν στον Κυβερνοχώρο έχει τη δυσκολία ότι προϋποθέτει όχι μόνο νομικές, αλλά μέχρι έναν βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου(internet).Είναι πολύ δύσκολο να αντιληφθεί κάποιος τι συμβαίνει στο 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 δε επαρκούν για τη 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 δυο βασικών αλλά και διαφορετικών τρόπων σκέψεως αποτελεί «το σταυρό του μαρτυρίου» για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

2.1 Βασικές Αρχές του όρου "Ασφάλεια" στο Διαδίκτυο

Στο διαδίκτυο "διακινούνται" πληροφορίες - δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα "αδιάκριτα βλέμματα". Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. 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 του δικαίου. Είναι ευνόητο ότι, οι θεμελιώδεις αυτές Αρχές πρέπει να εφαρμόζονται και στον κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω Αρχές. Δεν μπορούμε να μιλάμε για κρατικό έλεγχο, καθότι η έννοια του κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο διαδίκτυο.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του

διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται από ένα άλλο τρόπο "αντιασφάλειας". Από νομική άποψη διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογικές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειες των νόμων, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν "σταθεροποιηθεί" κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο , σε ουσιαστικό ή δικονομικό επίπεδο.

2.2 Έρευνες Σχετικές με το Έγκλημα στον Κυβερνοχώρο

Οι δικαστικές αστυνομικές έρευνες που γίνονται προς διακρίβωση εγκλημάτων του κυβερνοχώρου, καμία σχέση δεν έχουν με τις έρευνες, που μέχρι τώρα γνωρίζουμε. Στις μέχρι τώρα «παραδοσιακές» έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κ.λπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα πρέπει να ψάξει files, note pads, botes, data, κρυπτογραφημένα στοιχεία κ.λπ. Μπορεί το προς έρευνα αντικείμενο να βρίσκεται μπροστά στα μάτια του ερευνητή και να μην μπορεί να το εντοπίσει, εάν δεν έχει τις απαραίτητες τεχνικές γνώσεις. Ερωτάται λοιπόν. Πως θα διεξαχθεί σε μια τέτοια περίπτωση η αστυνομική έρευνα;

Ο «παραδοσιακός Εισαγγελέας» και η «παραδοσιακή αστυνομία» δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων.

Ένα άλλο πρόβλημα είναι στην κοινή έρευνα το αντικείμενο βρίσκεται σε ένα συγκεκριμένο σημείο. Αντίθετα, στο έγκλημα του κυβερνοχώρου το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές, οι οποίοι μάλιστα μπορεί να βρίσκονται σε διάφορες χώρες. Το πρόβλημα του τόπου τελέσεως είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζεται κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή και σε χιλιάδες τόπους τελέσεως. Γενικώς ο αριθμός των τόπων τελέσεως εξαρτάται από την συγκεκριμένη λειτουργία του διαδικτύου (αποστολή e-mails, new groups, internet relay chat, κ.λπ.). Ακόμα και σε δορυφόρους (Satellite - technology) είναι δυνατό να βρίσκονται τα αποδεικτικά στοιχεία, δεδομένου ότι οι επικοινωνίες (κινητά τηλέφωνα κ.λπ.) γίνονται πλέον δορυφορικά. Διότι, όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ τους

ολόκληρος ο πλανήτης αποτελεί «μία χώρα». Κατά συνέπεια, οι μέχρι τώρα Διεθνείς Συμβάσεις περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασία είναι «παραχωρημένες» στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη.

Στην Ελληνική αστυνομία δεν υπάρχει ακόμα ειδικό Τμήμα, που να ερευνά αποκλειστικός το έγκλημα εξετάζεται από το αντίστοιχο «συμβατικό» τμήμα της Αστυνομίας. Έτσι η παιδική πορνογραφία ερευνάται από το Τμήμα Ανηλίκων, ενώ μια ανθρωποκτονία θα ερευνηθεί από το Τμήμα Ανθρωποκτονιών.

Επειδή κατά κανόνα τα περισσότερα εγκλήματα του κυβερνοχώρου έχουν οικονομικό αντικείμενο, το Τμήμα Οικονομικού Εγκλήματος θεωρείται πιο εξειδικευμένο στο σχετικό αντικείμενο. Έχει μάλιστα συσταθεί ειδική ομάδα αντιμετωπίσεως του Ηλεκτρονικού Οικονομικού Εγκλήματος, το οποίο στελεχώνεται από εκπαιδευμένους στο ηλεκτρονικό έγκλημα αστυνομικούς.

Σε κάθε περίπτωση όμως τη σχετική έρευνα συνδράμει με τις ειδικές της γνώσεις η Διεύθυνση Εγκληματολογικών Ερευνών (ΔΕΕ) και ειδικότερα το εργαστήριο γραφολογίας, στο οποίο υπάγεται και λειτουργεί ο Τομέας Ανάλυσης Ψηφιακών Δεδομένων. Ο Τομέας αυτός δημιουργήθηκε το 1992, στελεχώνεται δε από ειδικά εκπαιδευμένους αστυνομικούς, με τεχνογνωδοσία στην εξέταση λογισμικού κατασχεθέντων ηλεκτρονικών υπολογιστών, στο «σπάσιμο» κωδίκων κ.λπ.

Επίσης στο Υπουργείο Δημοσίας Τάξεως λειτουργεί η Διεύθυνση Πληροφορικής, η οποία όμως δεν έχει σχέση με την έρευνα των εγκλημάτων του κυβερνοχώρου. Η Διεύθυνση αυτή υπάγεται στον κλάδο Διοικητικής Υποστήριξης του Υπουργείου Δημόσιας Τάξης και έχει ως αρμοδιότητα την ανάπτυξη και την τεχνική υποστήριξη στον τομέα της πληροφορικής για όλες τις υπηρεσίες της Αστυνομίας.

2.3 Ασφάλεια Προσωπικών Δεδομένων

Οι απειλές στο διαδίκτυο πληθαίνουν διαρκώς επειδή υπάρχει ένας μεγάλος όγκος πληροφοριών που μπορούν να συλλεχθούν από οποιονδήποτε χρήστη χωρίς πολλές φορές να είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιηθούν αυτές οι πληροφορίες. Δυο σημαντικές τεχνολογίες που σχετίζονται με το θέμα είναι τα *Cookies* και το *Web Tracking*.

Τα cookies που βρίσκονται στο σκληρό δίσκο περιλαμβάνουν το όνομα του χρήστη και το password, με αποτέλεσμα να μη χρειάζεται να δηλώνονται κάθε φορά, αφού τα στέλνει στον server και ο χρήστης εισέρχεται στο site ελεύθερα. Τα cookies μπορεί να περιλαμβάνουν σχεδόν κάθε είδος πληροφοριών, όπως την τελευταία φορά που ένας χρήστης επισκέφθηκε κάποιο site, τα αγαπημένα του sites και άλλες παρόμοιες πληροφορίες. Μπορούν επίσης, να χρησιμοποιηθούν για την παρακολούθηση των χρηστών όσοι βρίσκονται σε κάποιο site και τη συλλογή πληροφοριών σχετικών με τις σελίδες που προτιμούν να επισκέπτονται.

Οι χρήστες χρησιμοποιούν και άλλες μεθόδους παρακολούθησης προτείνοντας την λεπτομερή εξέταση του ημερολογίου λειτουργίας του Web server. Η εξέταση αυτή επιτρέπει τον προσδιορισμό των δημοφιλέστερων σελίδων του site, των sites που μόλις επισκέφτηκαν οι χρήστες, του αριθμού των σελίδων που διαβάζουν σε μια τυπική επίσκεψη και άλλων σχετικών πληροφοριών. Άλλες μέθοδοι στηρίζονται στη χρήση ορισμένων προγραμμάτων λογισμικού, ονόματι sniffers, τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site.

Τα internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites, καθώς επίσης και τον τρόπο τον οποίο αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν, επίσης, στους χρηστές να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησης τους και το πως θα τις χρησιμοποιήσει.

Τέλος, ειδική πρόβλεψη γίνεται από την Οδηγία και το ΠΔ για την τήρηση της νομοθεσίας περί προστασίας των δεδομένων και της ιδιωτικής ζωής[5] από τους Παρόχους Υπηρεσιών Πιστοποίησης. Η Οδηγία (άρθρο 8 παρ. 1) παραπέμπει ρητά στις σχετικές διατάξεις της οδηγίας 95/46/ΕΚ «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων αυτών», ενώ το άρθρο 7 του ΠΔ ορίζει ότι «οι πάροχοι υπηρεσιών πιστοποίησης, η ΕΕΤΤ και οι φορείς του άρθρ. 4 υπόκεινται στις διατάξεις του ν.2472/97 και του ν.2774/99 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

Περαιτέρω, ορίζεται ότι ένας παροχέας υπηρεσιών πιστοποίησης που εκδίδει πιστοποιητικά στο κοινό, είναι δυνατό να συλλέγει δεδομένα προσωπικού χαρακτήρα μόνο απευθείας από το πρόσωπο το οποίο αφορούν, ή κατόπιν ρητής συγκατάθεσης του και μόνο στο βαθμό που είναι απαραίτητο για τους σκοπούς

[5] Μήτρου, Λ., Η αρχή προστασίας προσωπικών δεδομένων(1999)

έκδοσης και διατήρησης του πιστοποιητικού. Η συλλογή ή επεξεργασία δεδομένων προσωπικού χαρακτήρα για οποιουσδήποτε άλλους σκοπούς χωρίς τη ρητή συναίνεση του εν λόγω προσώπου απαγορεύεται (παρ. 2 άρθρ. 8 Οδηγίας και παρ. 2 άρθρ. 7 ΠΔ).

2.4 Η Τεχνική Διάσταση του Όρου «Ασφάλεια» στο Διαδίκτυο

Από τεχνικής απόψεως , ασφάλεια είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημία. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα. Κλασικό παράδειγμα ασφάλειας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με τη χρήση πιστωτικής κάρτας. Σε αυτήν την περίπτωση πρέπει να εξασφαλιστεί ότι δε είναι δυνατόν να «συλλάβει» (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αναγράψει από τον διακομιστή, που είναι αποθηκευμένος. Επίσης πρέπει να επαληθευτεί ότι ο αριθμός της πιστωτικής κάρτας αποστέλλεται πράγματι από το πρόσωπο που ισχυρίζεται ότι τον στέλνει.

Το internet, όπως και ο υπόλοιπος κόσμος, δε είναι ασφαλές μέρος. Οι κίνδυνοι που εμπεριέχει είναι πολλοί, τόσο από επιθέσεις κακόβουλων όσο και από διάχυση πολύτιμων προσωπικών δεδομένων. Η σύνδεση ή η έξοδος στο Διαδίκτυο ισοδυναμεί με το να τοποθετεί κανείς την είσοδο της επιχείρησής του σε κάθε browser από οποιοδήποτε μέρος του κόσμου. Αυτό σημαίνει ότι είναι ευάλωτος σε επιθέσεις και εισβολείς.

Οι παραβιάσεις στο διαδίκτυο πραγματοποιούνται από hackers, οι οποίοι χρησιμοποιούν πολύπλοκες μεθόδους για την υποπλοκή ευαίσθητων πληροφοριών για προσωπικό ή πολιτικό όφελος. Αυτό που χαρακτηρίζει τους hackers είναι η προοπτική της πρόσβασης σε υπολογιστές απλών χρηστών που περιέχουν προσωπικά αρχεία, βάσεις δεδομένων με διευθύνσεις και τηλέφωνα, αριθμούς πιστωτικών καρτών ή οτιδήποτε άλλο.

Η ασφάλεια δηλαδή των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιούν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων.

- **Εμπιστευτικότητα (confidentiality)** των δεδομένων είναι η ιδιότητα τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος.[6]
- **Ακεραιότητα (integrity)** των δεδομένων είναι η ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή τους είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας.[7]
- **Διαθεσιμότητα (availability)** των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητα τους να άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος.[8]

2.5 Σχέση Ασφάλειας και Μυστικότητας στο Διαδίκτυο

Μυστικότητα είναι το δικαίωμα που έχει κάποιος να μην μοιράζεται τις πληροφορίες (π.χ. ηλικία, θρήσκευμα, αριθμούς πιστωτικής κάρτας κ.λπ.) που αφορούν το άτομο του με άλλους. Οι πληροφορίες αυτές είναι καταγεγραμμένες στο διαδίκτυο. Η ασφάλεια και η μυστικότητα στο χώρο του διαδικτύου είναι (ουσιαστικώς) θεωρητικές έννοιες. Στην πράξη, ό,τι κινείται στον χώρο του διαδικτύου μπορεί να γίνει γνωστό, ουσιαστικώς δηλαδή να υποκλαπεί.

Έχει χαρακτηριστικά λεχθεί ότι «κανένα κινούμενο ηλεκτρόνιο του πλανήτη δεν μπορεί να τρέφει σοβαρές ελπίδες ότι θα ξεφύγει από τον ιστό της παρακολούθησης »[9]. Κατά συνέπεια η ασφάλεια και η μυστικότητα του διαδικτύου δεν είναι μόνο νομικές, αλλά και τεχνικές έννοιες . Μπορεί όμως να λεχθεί ότι, η ασφάλεια είναι πρωτίστως τεχνική και δευτερευόντως νομική έννοια, ενώ αντίθετα η μυστικότητα είναι πρωτίστως νομική και δευτερευόντως τεχνική έννοια. Σε κάθε περίπτωση όμως, με την χρήση της τεχνολογίας και ιδιαίτερα του διαδικτύου, η προσωπική ζωή του ατόμου έχει γίνει "διαφανής" .

Είναι γνωστό ότι κάθε χρήστης του διαδικτύου (internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητα του. Με κατάλληλες όμως τεχνικές παρεμβάσεις μπορεί να έχει κάποιος πρόσβαση στο διαδίκτυο ως ανώνυμος ή ακόμα και με ψευδή στοιχεία που αναφέρονται σε άλλο άτομο. Η παρουσίαση βέβαια με ψευδή στοιχεία μπορεί να γίνει και στο «κοινό» εγκληματικό περιβάλλον. Εκεί όμως ο εντοπισμός του δράστη

---

[6] Βλ. Ασφάλεια Πληροφοριών, Εκδόσεις Νέων Πληροφοριών, Αθήνα 1995, σελ.389.
[7] Βλ. Ασφάλεια Πληροφοριών, όπ., σελ.18.
[8] Βλ. Ασφάλεια Πληροφοριών, ό.π., σελ.389.
[9] Βλ.Ζαν Γκισνέλ, «Πόλεμοι στον Κυβερνοχώρο, Μυστικές Υπηρεσίες και Internet», εκδόσεις Σταχύ, Αθήνα 1997, σελ.18

ταχυδρομείο (e-mail) έχει αυξηθεί αλματωδώς, η κρυπτογραφία αποτελεί σημαντικό παράγοντα του κυβερνοχώρου. Με την χρήση της κρυπτογραφίας δεν διακινούνται βέβαια μόνον νόμιμα, αλλά και παράνομα δεδομένα στον κυβερνοχώρο, όπως π.χ. ανταλλαγή πορνογραφικού υλικού, ανταλλαγή παράνομων μηνυμάτων από οργανωμένους ή μη εγκληματίες κ.λπ.

2.7 Ηλεκτρονική Υπογραφή

Ένας από τους πιο ανασταλτικούς παράγοντες στην ανάπτυξη του ηλεκτρονικού εμπορίου είναι η ανασφάλεια που χαρακτηρίζει τις ηλεκτρονικές συναλλαγές. Αποτελεί ασφαλώς κοινό τόπο ότι τα ανοικτά δίκτυα, όπως κατ' εξοχήν είναι το διαδίκτυο, είναι ιδιαίτερα επιρρεπή στην υποκλοπή, αλλοίωση ή τροποποίηση του περιεχομένου της πληροφορίας την οποία μεταφέρουν και πως η κοινή λογική λέει πως οι κίνδυνοι αυτοί αυξάνονται με γεωμετρική πρόοδο καθώς αυξάνονται οι χρήστες των ανοικτών δικτύων. Καθιστάται κατά συνέπεια επιτακτική η ανάγκη εξασφάλισης τόσο του απορρήτου των ηλεκτρονικών αρχείων όσο και της αντιμετώπισης των κινδύνων παραποίησης τους, επειδή υπάρχει η αβεβαιότητα με τη χειρόγραφη υπογραφή του εκδότη. Το έγγραφο για να είναι έγκυρο θα πρέπει να φέρει την ιδιόχειρη υπογραφή του εκδότη του, εάν δεν πρόκειται για σύμβαση, απαιτείται η ιδιόγραφη υπογραφή αμφοτέρων των συμβαλλομένων, η δε υπογραφή αυτών να τεθεί στο ίδιο έγγραφο(ΑΚ 160).

Χαρακτηριστική περίπτωση ηλεκτρονικής αποδείξεως αποτελεί η αξιολόγηση της ηλεκτρονικής ή ψηφιακής υπογραφής (digital signature). Στα πλαίσια αυτά, η ψηφιακή υπογραφή περιλαμβάνει δύο διαδικασίες, την δημιουργία της υπογραφής από τον αποστολέα των δεδομένων, με το ιδιωτικό του κλειδί και την επαλήθευση από τον παραλήπτη με το δημόσιο κλειδί. Η ψηφιακή υπογραφή πρέπει να διακρίνεται από την ηλεκτρονική υπογραφή που είναι μια έννοια πρωτίστως νομική.

Η ηλεκτρονική υπογραφή θα μπορούσε να μας παραπέμψει σε κάποιο είδος ηλεκτρονικής αποτύπωσης της ιδιόχειρης υπογραφής, π.χ. μέσω ενός «σαρωτή εγγράφου» (scanner), ούτε και στην μεταβίβαση μιας ιδιόχειρης υπογραφής με ηλεκτρονικά μέσα, αλλά με μια μέθοδο τεκμηρίωσης με αυτά τα ηλεκτρονικά μέσα που χρησιμοποιούνται σε συγκεκριμένες μηχανικές απεικονίσεις π.χ. εγγραφές δεδομένων σε μαγνητικά μέσα ηλεκτρονικού υπολογιστή, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής δεδομένων και της ηλεκτρονικής αλληλογραφίας.

Πρόκειται ουσιαστικά για μια ηλεκτρονική συναλλαγή που προκύπτει πρώτον από το ηλεκτρονικό έγγραφο το οποίο συνοδεύει και δεύτερον από απόρρητα δηλωτικά στοιχεία που υπογράφονται (π.χ. password).

Στα πλαίσια λοιπόν αυτά για την διαφύλαξη της ασφαλής μετάδοσης των ηλεκτρονικών μηνυμάτων και την προφύλαξη των συναλλαγών από ανεπιθύμητες παρεμβάσεις έχουν αναπτυχθεί προηγμένες κρυπτογραφικές μέθοδοι[10]. Ως κρυπτογράφηση εννοείται ειδικότερα, ο μετασχηματισμός των δεδομένων ενός ηλεκτρονικού υπολογιστή με την χρήση κατάλληλων αλγορίθμων, δηλαδή ενός συνόλου μαθηματικών συναρτήσεων, κατά τέτοιον τρόπο ώστε τα δεδομένα να μπορούν να αναγνωρισθούν μόνο μέσω ενός κλειδιού αποκρυπτογράφησης. Έτσι λοιπόν, ο αποστολέας ενός ηλεκτρονικού εγγράφου, χρησιμοποιώντας κάποια μαθηματική συνάρτηση, ένα «κλειδί» δηλαδή, μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή σε οποιονδήποτε τρίτο. Ο παραλήπτης με τη σειρά του, με το δικό του κλειδί, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό μέχρι να αποκρυπτογραφηθεί.

Η ψηφιακή υπογραφή πρέπει να διακρίνεται από την ηλεκτρονική υπογραφή που είναι μία έννοια πρωτίστως νομική. Η ψηφιακή υπογραφή αποτελεί έννοια «είδος» σε σχέση με την ηλεκτρονική υπογραφή που χρησιμοποιούνται συμμετρικά συστήματα κρυπτογράφησης. Η ψηφιακή υπογραφή ως μέθοδος κρυπτογράφησης των δεδομένων, αποτελεί μια από τις μορφές ηλεκτρονικής υπογραφής, δηλώνει ότι την προηγμένη ηλεκτρονική υπογραφή, που αναγνωρίζει η Οδηγία 99/93/ΕΚ και το ΠΔ 150/01 ως ισοδύναμη προς την ιδιόχειρη υπογραφή.

Η Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «σχετικά με ένα κοινό πλαίσιο για ηλεκτρονικές υπογραφές» ψηφίσθηκε το Δεκέμβριο του 1999 και αναμφισβήτητα παίζει καθοριστικό ρόλο στην ανάπτυξη του ηλεκτρονικού εμπορίου στην Ευρωπαϊκή Ένωση, καθώς διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και συμβάλλει στη νομική αναγνώριση τους. Ειδικότερα, η Οδηγία θεσπίζει ένα γενικό νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και για τις υπηρεσίες πιστοποίησης, ώστε να διασφαλίζεται η ομαλή λειτουργία της εσωτερικής αγοράς, ενώ, όπως ρητά ορίζεται στο άρθρο 1 παρ.2 αυτής, δεν καλύπτει πτυχές που αφορούν τη σύναψη και τη ισχύ συμβάσεων ή άλλων νομικών υποχρεώσεων που διέπονται από απαιτήσεις ως προς τον τύπο δυνάμει του εθνικού ή

[10] Βλ. Ι. Καράκωστα, , «Δίκαιο & Internet»

του κοινοτικού δικαίου και δε θίγει κανόνες και περιορισμούς σχετικά με τη χρήση των εγγράφων οι οποίοι περιέχονται στο εθνικό ή κοινοτικό δίκαιο.

Σκοπός επομένως της οδηγίας είναι η δημιουργία ενός ενιαίου νομικού πλαισίου για την αντιμετώπιση των νομικών ζητημάτων που γεννώνται από ηλεκτρονικές υπογραφές στον ευρωπαϊκό χώρο και η συμβολή στην αναγνώριση αυτής, όχι όμως και η εναρμόνιση των κανόνων ενοχικού δικαίου των κρατών - μελών. Κατά συνέπεια, γενικές διατάξεις που αφορούν την κατάρτιση ή εκτέλεση των συμβάσεων ή και άλλες διατυπώσεις μη συμβατικού χαρακτήρα με τις υπογραφές δεν θίγονται[11].

Στο Ποινικό Δίκαιο ο νομοθέτης προσδιορίζει την έννοια του ηλεκτρονικού εγγράφου στο άρθρο 13 παρ. γ΄ του ΠΚ, όπως αυτό τροποποιήθηκε με άρθρο 2 του Ν 1805/1988. Σύμφωνα λοιπόν με το άρθρο αυτό, το έγγραφο είναι γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλον τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.

Σχετική με την έννοια του ηλεκτρονικού εγγράφου είναι και η διάταξη του άρθρου 444 παρ. 3 ΚΠολΔ, σύμφωνα με την οποία ιδιωτικά έγγραφα θεωρούνται και φωτογραφικές ή κινηματογραφικές αναπαραστάσεις, φωνοληψίες και κάθε άλλη μηχανική απεικόνιση.

Σκοπός της ηλεκτρονικής υπογραφής είναι να εξασφαλίσει τη γνησιότητα του ηλεκτρονικού εγγράφου τόσο ως προς τον εκδότη του όσο και ως προς το περιεχόμενο του. Με άλλα λόγια με την ψηφιακή υπογραφή, το ηλεκτρονικό έγγραφο αποκτά ανάλογη αποδεικτική δύναμη με το «φυσικό» έγγραφο, που φέρει την ιδιόχειρη υπογραφή. Η ψηφιακή υπογραφή, όπως και όλο το περιεχόμενο ενός ηλεκτρονικού εγγράφου, μπορεί να πλαστογραφηθεί, και μάλιστα χωρίς να αφήσει καθόλου (ορατά) ίχνη.

---

[11] Ιγγλεζάκη, Ι., Οι νομικές ρυθμίσεις για τις ψηφιακές υπογραφές. Η Οδηγία 1999/93/ΕΚ και οι εθνικές νομοθεσίες, ΕπισκΕΔ Γ (2000),σ.619 επ.

2.8 Γενικό και Ειδικό Ποινικό Δίκαιο

2.8.1 Γενικές Ποινικές Διατάξεις στον Χώρο του Διαδικτύου

Είναι γνωστό ότι για να «μπει» κάποιος στον κυβερνοχώρο (internet) απαραίτητη προϋπόθεση αποτελεί η χρήση του τομέα τηλεπικοινωνιών (σταθερού ή κινητού τηλεφώνου). Η χρήση αυτή επιτυγχάνεται με τη σύνδεση του χρήστη με μία εταιρία παροχής υπηρεσιών διαδικτύου σε ιδιώτες. Απαραίτητο βέβαια είναι να διαθέτει ο χρήστης τον κατάλληλο τεχνολογικό εξοπλισμό.

Κατά συνέπεια, οι σχετικοί με τις τηλεπικοινωνίες νόμοι έχουν άμεση ή έμμεση σχέση με τη χρήση του διαδικτύου. Με άλλα λόγια, το διαδίκτυο (internet) δεν είναι τίποτα άλλο παρά μια μορφή επικοινωνίας που γίνεται με τη βοήθεια ή δια μέσου των τηλεπικοινωνιών. Σύμφωνα λοιπόν με τα παραπάνω, σχετικοί με το διαδίκτυο νόμοι είναι:

Α) Ο Ν 2867/19.12.2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις. Ο πρόσφατος αυτός νόμος αντικατέστησε τον Ν 2246/20.10.1994 για την «Οργάνωση και Λειτουργία του Τομέα Τηλεπικοινωνιών», πλην των διατάξεων του που αφορούν στην παροχή ταχυδρομικών υπηρεσιών (άρθρο 13 παρ. 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 επικοινωνιακής δραστηριότητας, που αναπτύσσεται εντός της Ελληνικής Επικρατείας. Είναι γνωστός και ως νόμος «για την απελευθέρωση των τηλεπικοινωνιών», καθότι επιτρέπει την ελεύθερη εγκατάσταση, λειτουργία, διαχείριση και εκμετάλλευση των Ν 2246/1994 έτσι ώστε αυτός να προσδιορίζει όχι μόνο τεχνικούς αλλά και νομικούς όρους. Έτσι ως «πάροχος 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.

Β) Ο Ν 2774/22.12.1999 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με τον Ν 2472/10.4.1997 «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Ο Ν 2774/1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, αποτελεί ειδικότερη μορφή του Ν 2472/1997 και αποτελεί υλοποίηση της Οδηγίας 97/66/ΕΚ. Δηλαδή, οι προηγούμενες 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 2472/1997 (ΦΕΚ Α΄50/10.4.1997) προστατεύει το άτομο από την αυτοποιημένη ή μη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νόμιμος κάτοχος των δεδομένων (ακόμα και των προσωπικών) προστατεύεται από το άρθρο 370 Β ΠΚ, όπως αυτό προστέθηκε με το άρθρο 3 Ν 1805/1988. Ο Ν 2472/1997 προστατεύει το ίδιο το άτομο από την επεξεργασία των στοιχείων αυτών.

Χαρακτηριστικό παράδειγμα εφαρμογής του Ν 2472/1997 στο διαδίκτυο αποτελεί η διασύνδεση αρχείων.

Γ) 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 όπως ήδη έχει λεχθεί το internet δεν είναι τίποτα άλλο παρά μία μορφή επικοινωνίας που γίνεται διαμέσου 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 ΠΚ) τον Β, στέλνοντας e-mail. Ο Β καταγγέλλει στην Αστυνομία. Η αστυνομία ζητά από τον παροχέα (ISP) να παρακολουθεί την ανταλλαγή e-mail. Ο παροχέας στην περίπτωση αυτή δεν μπορεί να επικαλεστεί το απόρρητο των επικοινωνιών.

2.8.2 Ειδικές Ποινικές Διατάξεις στον Χώρο του Διαδικτύου

Τιμωρούνται ποινικώς, εάν διαπράττονται στον χώρο του διαδικτύου, οι παρακάτω συμπεριφορές:

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 οποιονδήποτε τρόπο τις υποχρεώσεις εχεμύθειας, σεβασμού της ιδιωτικής ζωής και τήρησης του απορρήτου των κάθε είδους δεδομένων που μεταβιβάζονται ή μετάγονται μέσω των τηλεπικοινωνιακών συστημάτων που χρησιμοποιεί ή διαθέτει, τιμωρείται με ποινή φυλάκισης τουλάχιστον δύο(2) ετών και χρηματική ποινή πέντε εκατομμύρια (5.000.000) έως είκοσι εκατομμύρια (20.000.000) δραχμών, εφόσον δεν προβλέπονται βαρύτερες ποινές από άλλες ισχύουσες διατάξεις. Σε περίπτωση που ο παραβάτης της παρούσας διάταξης ανήκει στο προσωπικό τηλεπικοινωνιακής επιχείρησης, η επιβαλλόμενη ποινή φυλάκισης είναι τουλάχιστον τριών (3) ετών και η χρηματική ποινή τουλάχιστον δέκα εκατομμύρια (10.000.000) δραχμές.

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

Β) Σύμφωνα επίσης με το άρθρο 13 του Ν 2774/1999, για την προστασία δεδομένων προσωπικού χαρακτήρα στο 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 φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως δέκα εκατομμύρια (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από 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 παρ. 1 του άρθρου 21 του Ν 2472/1997, τιμωρείται με φυλάκιση τουλάχιστον δύο(2) ετών και με χρηματική

ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως πέντε εκατομμύρια (5.000.000) δραχμών.

Γ) Σύμφωνα με το άρθρο 22 (παρ. 1-7) του Ν 2472/1997.

1. Όποιος, παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 του παρόντος νόμου, τη σύσταση και λειτουργία αρχείου ή οποιαδήποτε μεταβολή στους όρους και τις προϋποθέσεις χορηγήσεως της άδειας, που προβλέπεται από την παρ.3 του άρθρου 7 του παρόντος νόμου, τιμωρείται με φυλάκιση έως τριών (3) χρόνων και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως πέντε εκατομμύρια (5.000.000) δραχμών,

2. Όποιος , κατά παράβαση του άρθρου 7 του παρόντος νόμου, διατηρεί αρχείο χωρίς άδεια ή κατά παράβαση των όρων και προϋποθέσεων της αδείας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως πέντε εκατομμύρια (5.000.000) δραχμών.

3. Όποιος, κατά παράβαση του άρθρου 8 του παρόντος νόμου, προβαίνει σε διασύνδεση αρχείων χωρίς να την γνωστοποιήσει στην Αρχή, τιμωρείται με φυλάκιση έως τριών (3) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως πέντε εκατομμύρια (5.000.000) δραχμών. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της αδείας που του έχει χορηγηθεί , τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμές έως πέντε εκατομμύρια (5.000.000) δραχμών.

4. Όποιος χωρίς δικαίωμα επεμβαίνει με οποιονδήποτε τρόπο σε αρχείο δεδομένων προσωπικού χαρακτήρα ή λαμβάνει γνώση των δεδομένων 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 και χρηματική ποινή και εάν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (10.000.000) δραχμών, αν η πράξη δεν τιμωρείται βαρύτερα από άλλες διατάξεις.

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

σύμφωνα με την παρ.2 του άρθρου 13, καθώς και με πράξεις επιβολής των διοικητικών κυρώσεων των περιπτώσεων γ΄, δ΄ και ε΄ της παρ. 1 του άρθρου 21, τιμωρείται με φυλάκιση τουλάχιστον δύο (2) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμύρια (5.000.000) δραχμών. Με τις ποινές του προηγούμενου εδαφίου τιμωρείται ο υπεύθυνος επεξεργασίας που διαβιβάζει δεδομένα προσωπικού χαρακτήρα κατά παράβαση του άρθρου 9, καθώς και εκείνος που δεν συμμορφώνεται προς τη δικαστική απόφαση του άρθρου 14 του παρόντος νόμου.

6. Αν ο υπαίτιος των πράξεων των παρ.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 10 ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμύρια (10.000.000) δραχμών.

2.9 Νομοθετικό Πλαίσιο στην Ελλάδα και την Ευρωπαϊκή Ένωση

Η νομοθετική αντιμετώπιση του ηλεκτρονικού εγκλήματος σε Ελλάδα και Ευρωπαϊκή Ένωση παρουσιάζεται ενιαία, με δεδομένη τη συμμετοχή της χώρας μας σε όλες τις Αποφάσεις, Συμβάσεις και Συστάσεις της Ευρωπαϊκής Ένωσης, που σχετίζονται με το ζήτημα. Στην Ελλάδα ισχύει ο Νόμος 2928/2001, ο οποίος περιλαμβάνει τροποποιήσεις διατάξεων και διατάξεις του Ποινικού Κώδικα και του Κώδικα Ποινικής Δικονομίας για την προστασία του πολίτη από αξιόποινες πράξεις εγκληματικών οργανώσεων.

Επίσης, γίνονται αναφορές σε διάφορες διατάξεις του Αστικού και του Ποινικού Κώδικα. Συγκεκριμένα στα άρθρα 57, 58, 577, 578, 914, 919 του Αστικού Κώδικα και στα άρθρα 361, 361Α, 362, 363, 364, 365, 366, 367, 368, 369, 381, 386, 386Α (Απάτη μέσω υπολογιστή), 370Β του Ποινικού Κώδικα. Κατά τα άρθρα 914 και 919 του Αστικού Κώδικα γεννάται και η αδικοπρακτική ευθύνη του δράστη. Ο υπαίτιος, όμως, έχει και ποινική ευθύνη σύμφωνα με το άρθρο 381 του Ποινικού Κώδικα.

Για την προστασία της πνευματικής ιδιοκτησίας ισχύει ο Νόμος 2121/1993 με τίτλο «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα». Με το νόμο αυτό ρυθμίζονται θέματα σχετικά με το δίκαιο της πνευματικής ιδιοκτησίας,

το σήμα, τη λειτουργία του, τον τρόπο κτήσης του δικαιώματος, την απολυτότητα του δικαιώματος, τον χρονικό περιορισμό του, τον φορέα του.

Η προστασία των βάσεων δεδομένων αναφέρεται στην Οδηγία 96/6/ΕΚ, η οποία αποτελεί νέο ρυθμιστικό πλαίσιο που αναμένεται να ενσωματωθεί σύντομα στην εθνική νομοθεσία. Η Συνθήκη του Παγκόσμιου Οργανισμού για τα Πνευματικά Δικαιώματα, για τα Συγγραφικά Δικαιώματα και η Συνθήκη για τις Εκτελέσεις και τις Εγγραφές Ήχου, εκσυγχρονίζει σε μεγάλο βαθμό τη διεθνή προστασία της πνευματικής ιδιοκτησίας.

Περιέχει διατάξεις που θα αποτελέσουν τη βάση για δίκαιες συνθήκες συναλλαγών, σχετικά με την πνευματική ιδιοκτησία στην ψηφιακή εποχή. Αυτές αποτελούν σημαντικό σημείο για την αναθεώρηση της κοινοτικής και εθνικής νομοθεσίας. Η πνευματική ιδιοκτησία (Copyright) προστατεύει τα πνευματικά δικαιώματα από αντιγραφή το λιγότερο για 70 χρόνια. Στην Ευρώπη ισχύει η Οδηγία 93/98/ΕΟΚ (29/10/1993) για την εναρμόνιση της διάρκειας προστασίας του δικαιώματος πνευματικής ιδιοκτησίας και άλλων δικαιωμάτων. Επίσης, ισχύει η Οδηγία 2001/29 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (22/5/2001) για την εναρμόνιση μερικών πτυχών του δικαιώματος του δημιουργού και συγγενικών δικαιωμάτων στην κοινωνία της πληροφορίας[12]. Γενικά για το ηλεκτρονικό έγκλημα στην Ευρωπαϊκή Ένωση ισχύουν τα εξής γενικά νομοθετήματα:

- Σύσταση του Συμβουλίου 9193/01
- Ψήφισμα συμβουλίου 2003/C48/01
- Σύσταση Συμβουλίου 95/144/ΕΚ
- Ψήφισμα Συμβουλίου 2002/C43/02
- Έγγραφο 2000/C124/01
- Σχέδιο Δράσης 97/C251/01

Οι διάφορες μορφές ηλεκτρονικού εγκλήματος ρυθμίζονται και τιμωρούνται ξεχωριστά και από άλλα ειδικότερα νομοθετήματα στην Ελλάδα και την Ευρωπαϊκή Ένωση. Αξίζει να αναφερθεί η πρόβλεψη του ελληνικού νομοθετήματος Ν. 1085/88 σχετικά με την, χωρίς εξουσιοδότηση, πρόσβαση σε Η/Υ.

Σχετικά με το cracking, στην Ελλάδα ισχύει το άρθρο 370Γ του Ποινικού Κώδικα, με το οποίο τιμωρείται η χωρίς δικαίωμα, διείσδυση - πρόσβαση σε συστήματα επεξεργασίας δεδομένων, έστω και εάν γίνεται χωρίς πρόθεση βλάβης.

[12] Σύμβαση για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης 23-11-2001

Στην Ευρωπαϊκή Ένωση δεν έχουν ψηφιστεί ειδικά νομοθετήματα για την αντιμετώπιση του, αλλά έχουν αρχίσει προπαρασκευαστικές εργασίες για τη δημιουργία τους. Στη συνέχεια αναφέρονται 3 Ανακοινώσεις - Προτάσεις από την Ευρωπαϊκή Ένωση σχετικά με το θέμα:

- Ανακοίνωση Επιτροπής COM/2001/0298
- Πρόταση κανονισμού 2003.0063
- Πρόταση Απόφασης Πλαισίου του Συμβουλίου COM/2002/0173CNS 2002/0086

Σχετικά με την προστασία δεδομένων προσωπικού χαρακτήρα, στην Ελλάδα και την Ευρωπαϊκή Ένωση ισχύουν οι εξής Οδηγίες:

- Οδηγία 2002/58
- Οδηγία 95/46

Για τα εγκλήματα κατά της ηθικής και της αξιοπρέπειας, την προστασία των ανηλίκων από τη διάδοση πορνογραφικού υλικού και γενικότερα τη δυσφήμιση μέσω Διαδικτύου στην Ελλάδα ισχύουν τα άρθρα 361, 362, 366 και 367 του Ποινικού Κώδικα. Για την πορνογραφία ανηλίκων, στην Ευρωπαϊκή Ένωση ισχύουν τα εξής:

- Απόφαση Συμβουλίου 2000/C8/06
- Σύσταση 98/560/ΕΚ
- Απόφαση Συμβουλίου 2000/375/ΔΕΚ
- Απόφαση Συμβουλίου 2001/C213/0301
- Απόφαση Συμβουλίου 1999/C362/06
- Απόφαση 276/1999/ΕΚ
- Ανακοίνωση Επιτροπής COM/2002/0152

Σχετικά με τους «ηλεκτρονικούς ιούς» στην Ελλάδα ισχύουν τα άρθρα 577 και 578 του Αστικού Κώδικα και τα άρθρα 914, 919 και 381 του Ποινικού Κώδικα. Στην Ευρωπαϊκή Ένωση ισχύει η Ανακοίνωση της Επιτροπής COM/2001/0298 για την ασφάλεια των δικτύων και των πληροφοριών, στην οποία υπάρχει εξήγηση της έννοιας του ιού, του τρόπου λειτουργίας του και των τρόπων αντιμετώπισης του, αλλά δεν έχει ακόμη ψηφιστεί.

Η απάτη μέσω Διαδικτύου, εφόσον ο Η/Υ αποτελεί μέσο τέλεσης κοινής απάτης, αναφέρεται στα άρθρα 386 και 386Α του ελληνικού Ποινικού Κώδικα. Στην Ευρωπαϊκή Ένωση ισχύει η Απόφαση του Συμβουλίου 2001/413/ΔΕΚ.

Σχετικά με το spamming (αποστολή διαφημιστικών e-mail) στην Ευρωπαϊκή Ένωση ισχύει η Οδηγία 2002.58. Στην Ελλάδα ισχύουν νομοθετήματα σχετικά με την προστασία των καταναλωτών.

Κεφάλαιο 3: Η ΝΟΜΙΚΗ ΕΝΝΟΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρονται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο "τον κίνδυνο να επέλθει κάποια βλάβη", θα πρέπει να ορίσει ταυτόχρονα και τους όρους "κίνδυνο" και "βλάβη".

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα έλεγα, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό .

3.1 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" κ.λπ. 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.

Στο υπό εξέταση λοιπόν θέμα, είναι απαραίτητο να προσδιοριστεί η νομική έννοια των όρων "ασφάλεια", "κυβερνοχώρος - διαδίκτυο", "χάκερ". Πριν απ' αυτό όμως κρίνεται απαραίτητο να οριοθετηθεί η έννοια του εγκλήματος στον κυβερνοχώρο, να προσδιοριστούν τα χαρακτηριστικά του (εγκλήματος στον κυβερνοχώρο), να καθοριστεί η σχέση μεταξύ εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή και να δοθεί το "προφίλ" του εγκληματία στον κυβερνοχώρο, όπως αναφερθήκαμε σε προηγούμενα κεφάλαια.

3.2 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 ξενόγλωσση διάσταση τους, κατά τρόπο που τείνουν να ενσωματωθούν και στο Ελληνικό νομικό λεξιλόγιο[13]. 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.

Ο νομοθέτης δημιουργεί νέες αντικειμενικές υποστάσεις εγκλημάτων (όπως στις περιπτώσεις των άρθρων 370 Α, Β και κυρίως Γ του Ποινικού Κώδικα για την παραβίαση απορρήτου τηλεφωνημάτων και προφορικής συνομιλίας, την αθέμιτη πρόσβαση σε ηλεκτρονικό υπολογιστή, την αποκάλυψη και παραβίαση κρατικών και επιστημονικών απορρήτων και χρήση προγραμμάτων Η/Υ). Τα εγκλήματα αυτά διώκονται κατ' έγκληση και τιμωρούνται με φυλάκιση που μπορεί κατά περίπτωση να

[13] Δωρή, Φ., Νομικές Μελέτες

φθάνει και μέχρι ένα έτος, εκτός αν προσβάλλονται στρατιωτικά ή διπλωματικά απόρρητα, οπότε οι πράξεις αυτές διώκονται κατά τα άρθρα 146 και 147 του Π.Κ. για την παραβίαση μυστικών της Πολιτείας, οπότε και μπορούν να επιβάλλονται βαρύτατες ποινές κάθειρξης δέκα και πλέον ετών, ανάλογα με τις περιστάσεις διάπραξης του εγκλήματος.

Βαριές ποινές προβλέπονται και στην περίπτωση του άρθρου 386 Α Π.Κ. για την απάτη μέσω υπολογιστή. Σύμφωνα με το νόμο, όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του άρθρου 386 περί απάτης. Οι προβλεπόμενες ποινές περιλαμβάνουν, κατά περίπτωση, από φυλάκιση έως κάθειρξη μέχρι δέκα ετών αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημία υπερβαίνουν το ποσό των πέντε εκατομμυρίων (5.000.000) δραχμών, ή αν το περιουσιακό όφελος ή η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσό των είκοσι πέντε εκατομμυρίων (25.000.000) δραχμών.

Ποινικές διατάξεις βρίσκονται ακόμα διάσπαρτες σε ειδικούς νόμους, όπως το άρθρο 22 παρ. 4 του νόμου 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, το άρθρο 11 του νόμου 2867/2000 για την Οργάνωση και λειτουργία των τηλεπικοινωνιών, ο νόμος 2225/1994 περι απορρήτου των επικοινωνιών, ή το άρθρο 29 του νόμου 5060/1931 περί ασέμνων δημοσιευμάτων (η διάταξη αυτή αφορά, λόγω του έτους ψήφισής του, όπως είναι φυσικό, τα έντυπα και όχι τα ηλεκτρονικά έγγραφα).

3.3 Η Πληροφορική Εγκληματικότητα στο Ελληνικό Δίκαιο

Το Ελληνικό ποινικό δίκαιο θεωρεί ότι αυτή καθαυτή η χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικό υπολογιστή μπορεί να αποτελέσει ποινικά κολάσιμο αδίκημα, έστω και αν ο δράστης δεν έχει προχωρήσει σε ενέργειες όπως η κλοπή, η φθορά ή η καταστροφή λογισμικού, εφόσον αυτός επέτυχε την πρόσβαση με τη χρήση αθέμιτων μέσων ή προσποίησης (π.χ. με το "σπάσιμο" του κώδικα ή με σκοπό τη διάπραξη άλλων αδικημάτων).

Στην προσπάθεια του να αντιμετωπίσει την πληροφορική εγκληματικότητα, ο ποινικός νομοθέτης, σε μερικές περιπτώσεις διευρύνει (ανεπίτρεπτα κατά μία άποψη της θεωρίας) τις ήδη χρησιμοποιούμενες νομικές έννοιες (όπως αυτή του εγγράφου του άρθρου 13 παρ. γ΄ Π.Κ ώστε να συμπεριλάβει σε αυτή και το "ηλεκτρονικό έγγραφο"). Ειδικότερα, το ανωτέρω άρθρο, το οποίο προσδιορίζει την παραδοσιακή έννοια του εγγράφου ως γραπτού ή σημείου με έννομη σημασία, προσθέτει, με τον νόμο 1805/1988, ότι "..."Εγγραφο είναι και κάθε μέσο στο οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ' όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι προσφορά να αποδείξουν γεγονότα που έχουν έννομη σημασία".

3.4 Η Νομική Έννοια του Διαδικτύου και του Κυβερνοχώρου

Η Ελληνική νομοθεσία δεν προσδιορίζει την έννοια του διαδικτύου ή του κυβερνοχώρου. Κατά συνέπεια οι έννοιες αυτές λαμβάνονται από την τεχνολογία. Έτσι λοιπόν, ως διαδίκτυο (internet) μπορεί να οριστεί η παγκόσμια συλλογή δικτύων και πυλών, που χρησιμοποιούν την ομάδα πρωτοκόλλων TCP/IP για να επικοινωνούν μεταξύ τους, ενώ ως κυβερνοχώρος μπορεί να οριστεί το σύνολο των ηλεκτρονικών κόσμων, όπως το internet, όπου οι άνθρωποι έρχονται σε αλληλεπίδραση μέσω συνδεδεμένων υπολογιστών, όπου δηλαδή η επικοινωνία είναι ανεξάρτητη από την υλική υπόσταση. Στο άρθρο 2 του Ν 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών προσδιορίζονται οι έννοιες "δίκτυο καλωδιακής τηλεόρασης", "ιδιωτικό δίκτυο", "παροχή ανοικτού δικτύου" και "τηλεπικοινωνιακό δίκτυο". Δεν προσδιορίζεται όμως η έννοια του διαδικτύου ή του κυβερνοχώρου.

Πρέπει να λεχθεί ότι, στη συνείδηση του μέσου νομικού, δεν γίνεται διάκριση μεταξύ διαδικτύου και κυβερνοχώρου και κατά κανόνα οι έννοιες αυτές θεωρούνται ως ταυτόσημες και χρησιμοποιούνται πάντα με το ίδιο περιεχόμενο.

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επομένως, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της

ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη που είναι σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέλος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

Συμπερασματικώς μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

Κεφάλαιο 4: ΜΟΡΦΕΣ ΗΛΕΚΤΡΟΝΙΚΩΝ ΕΓΚΛΗΜΑΤΩΝ

ΕΛΛΗΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

Στην Ελληνική έννομη τάξη δεν υπάρχει Νόμος που να αναφέρεται αποκλειστικά σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού Δικαίου. 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.

Διευκρινίζεται ότι ο Ν. 1805/88, αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes). Στο βαθμό λοιπόν που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου (internet), τότε τα άρθρα αυτά εφαρμόζονται και στις συγκεκριμένες περιπτώσεις.

Ανεξάρτητα όμως από το εάν ο παραπάνω Νόμος επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής, το βέβαιο είναι ότι, δεν επαρκεί να «καλύψει» τα εγκλήματα που έχουν παρουσιαστεί από τη χρήση του διαδικτύου.

Είναι γνωστό ότι για να «μπει» κάποιος στον κυβερνοχώρο (internet) απαραίτητη προϋπόθεση αποτελεί η χρήση του τομέα τηλεπικοινωνιών (σταθερού ή κινητού τηλεφώνου). 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 τίποτα άλλο παρά μια μορφή επικοινωνίας που γίνεται με τη βοήθεια ή δια μέσου των επικοινωνιών[14]. Σύμφωνα λοιπόν με τα παραπάνω οι σχετικοί με το διαδίκτυο Νόμοι είναι:

α) Ο Ν. 2246/94 για την «οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών».

β) Ο Ν. 2774/99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με τον Ν. 2472/97 για την «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».

γ) Ο Ν. 2225/94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας.

---

[14] Αυγουστιανάκη, Μ., Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων, ΔτΑ,(2001)

4.1 Συμβούλιο Ευρώπης και Εγκλήματα 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:

I. Η σύσταση No R(89)9 σχετική με το έγκλημα που διαπράττεται με ηλεκτρονικό υπολογιστή .

II.Η σύσταση No R(95)13 για τα ποινικά δικονομικά προβλήματα που συνδέονται με την τεχνολογία των πληροφοριών.

Στη Βουδαπέστη στις 23 Νοεμβρίου 2001 καταρτίσθηκε διεθνής σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Την σύμβαση αυτή προσυπόγραψε και η Χώρα μας. Σκοπός της σύμβασης είναι η προστασία της κοινωνίας από το έγκλημα στον κυβερνοχώρο, με την κατάρτιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα συνεργασίας μεταξύ των κρατών, που την υπέγραψαν.

Η συγκεκριμένη σύμβαση καθιερώνει την υποχρέωση εναρμονίσεως των Εθνικών νομοθεσιών σε θέματα εγκλημάτων στον κυβερνοχώρο (internet crimes).

Κύριο χαρακτηριστικό της διεθνούς αυτής συμβάσεως είναι η υποχρέωση που αναλαμβάνουν τα κράτη - μέλη να ποινοικοποιήσουν ορισμένη συμπεριφορά στο διαδίκτυο (internet), όπως είναι η διανομή πορνογραφικού υλικού στο internet, η «εμπλοκή ανηλίκου σε ερωτική επαφή» με τη χρήση του διαδικτύου, η αντιγραφή (χωρίς δικαίωμα) έργων πνευματικής ιδιοκτησίας. Η καθιέρωση ποινικής ευθύνης και νομικών προσώπων, που εμπλέκονται σε καθορισμένες συμπεριφορές.

4.2 Η θέση της Ευρωπαϊκής Ένωσης Απέναντι στο διαδίκτυο

Η Ευρωπαϊκή Ένωση δεν έμεινε αδιάφορη απέναντι στο ηλεκτρονικό έγκλημα γενικότερα και στον κυβερνοχώρο ειδικότερα. Έτσι το 1997 εκδίδεται το No 97/C70/01 ψήφισμα 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 αναγνωρίζονται τα θετικά οφέλη που προσφέρει ο κυβερνοχώρος, ιδιαίτερα στον τομέα της εκπαίδευσης, παρέχοντας δυνατότητες 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 ψήφισμα την ανάγκη καταπολέμησης της παράνομης χρήσης των τεχνικών δυνατοτήτων του κυβερνοχώρου, ιδιαίτερα για αξιόποινες πράξεις κατά των παιδιών.

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

4.3 Παράνομο Περιεχόμενο του Internet

Το σχετικό ψήφισμα (97/C70/01/17-2-1997) του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών - μελών της Ευρωπαϊκής Ένωσης για το παράνομο και επιβλαβές περιεχόμενο του διαδικτύου (internet), δεν καθορίζει τι είναι παράνομο και τι είναι επιβλαβές περιεχόμενο.

Κατά συνέπεια λοιπόν οι έννοιες αυτές θα προσδιοριστούν από το νομοθέτη σε περίπτωση που ψηφιστεί σχετικός Νόμος που θα ρυθμίζει την συμπεριφορά, όσων «κινούνται» στον χώρο του διαδικτύου. Και λέγοντας εδώ «νομοθέτη» εννοούμε τον Εθνικό νομοθέτη κάθε επιμέρους Χώρας.

Στο σημείο όμως αυτό προκύπτει το ερώτημα, εάν οι «εσωτερικές νομοθεσίες» μπορούν αυτοτελώς, να αντιμετωπίσουν αποτελεσματικά τις παρανομίες στον κυβερνοχώρο, λόγω της φύσεως του εγκλήματος και του ιδιαίτερου τρόπου τελέσεως τους. Οι εσωτερικές νομοθεσίες από μόνες τους δεν επαρκούν, απαιτούνται πολυμερείς Διεθνείς Συμβάσεις.

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

4.4 Επιβλαβές Περιεχόμενο του Internet

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

Είναι ευνόητο βέβαια ότι, η έννοια του επιβλαβούς περιεχομένου έχει

διαφορετική βαρύτητα, όταν πρόκειται για χρήση του διαδικτύου (internet) από ανηλίκους. Παράδειγμα: Στο Internet υπάρχουν εκατοντάδες θέσεις (sites) που αναφέρονται στον Σατανισμό και στη Λατρεία του Σατανά. Για πολλούς το περιεχόμενο των sites αυτών αποτελεί κλασική μορφή «επιβλαβούς περιεχομένου». Για άλλους όμως αποτελεί μια μορφή ελεύθερης έκφρασης της προσωπικότητας ή ακόμα και μια μορφή ανεξιθρησκίας. Γενικά ως επιβλαβές περιεχόμενο μπορεί να θεωρηθεί, ότι αναφέρεται σε ρατσιστικές διακρίσεις ή σε παραπλανητική διαφήμιση.

Για την αντιμετώπιση του παρανόμου και επιβλαβούς περιεχομένου του κυβερνοχώρου έχει προταθεί μεταξύ άλλων και η δημιουργία «οργάνου αυτορρύθμισης» στο πλαίσιο λειτουργίας των παροχέων υπηρεσιών, καθώς και λειτουργία «θερμής γραμμής», όπου θα μπορούν να γίνονται σχετικές (επώνυμες ή και ανώνυμες) καταγγελίες.

4.5 Η Νομική Φύση του Παροχέα Υπηρεσιών (ISP Internet Service Provider)

Ιδιαίτερη σημασία για την ασφάλεια και τη μυστικότητα του διαδικτύου έχει η συμμετοχή του παροχέα (τηλεπικοινωνιακών) υπηρεσιών. Αποτελεί μάλιστα «κομβικό σημείο» για τον εντοπισμό των παρανομιών και τη συλλογή των αποδεικτικών στοιχείων, δεδομένου ότι όλα τα στοιχεία (data) «περνούν» από τις εγκαταστάσεις του.

Σύμφωνα με το άρθρο 1 & 2 περίπτωση δ του Ν. 2246/91 φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι φυσικά ή νομικά πρόσωπα, τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες υπό καθεστώς ελεύθερου ανταγωνισμού με βάση την άδεια ή δήλωση ή έγκριση.

Σύμφωνα με την αριθμό Υ.Α 74.631/95 υπουργική απόφαση του Υπουργού Μεταφορών που εκδόθηκε προς υλοποίηση του Ν. 2249/94 για τη λήψη της σχετικής άδειας, ο ενδιαφερόμενος οφείλει να υπογράψει και σχετική δήλωση του Ν. 1599/86 με την οποία να βεβαιώνει ότι, έχει λάβει γνώση του κανονισμού, του κώδικα δεοντολογίας και των λοιπών διατάξεων, που διέπουν την άσκηση των τηλεπικοινωνιακών δραστηριοτήτων. Επίσης δεσμεύεται ότι θα τηρεί τις απαιτήσεις που υπαγορεύονται από την Εθνική Άμυνα και την Δημόσια Ασφάλεια, ότι θα τηρεί τις διατάξεις τις σχετικές με τη διασφάλιση του απορρήτου των τηλεπικοινωνιών και

ότι θα αποφεύγει κάθε ενέργεια αθέμιτου ανταγωνισμού.

Ευλόγως γεννάται το ερώτημα, για το κατά πόσο ο ίδιος ο παροχέας μπορεί να υπέχει ποινική ευθύνη από αμέλεια ή και από ενδεχόμενο δόλο για τις παρανομίες που «περνούν» από τις εγκαταστάσεις του, που υποπίπτουν στην αντίληψή του χωρίς να ενεργεί με κάποιο τρόπο για να σταματήσει την διάπραξη τους. Κατά πόσο μπορεί (νομοθετικά) να υποχρεωθεί ο παροχέας να διαφυλάξει τα δεδομένα που διέρχονται από τις εγκαταστάσεις του, για ένα ορισμένο χρονικό διάστημα προκειμένου να τα παραδώσει στις Αρχές, σε περίπτωση που του ζητηθούν. Κάτι τέτοιο βέβαια θα επιβαρύνει οικονομικά τον παροχέα δεδομένου ότι θα πρέπει να πολλαπλασιάσει τον τεχνικό του εξοπλισμό.

Οι κατωτέρω μορφές εγκλημάτων καθορίστηκαν και προσυπογράφηκαν από τα κράτη - μέλη που έλαβαν μέρος στην σύνταξη της Σύμβασης για τον κυβερνοχώρο την 23-11-2001 στην Βουδαπέστη. Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων των ηλεκτρονικών υπολογιστών.

4.5.1 Παράνομη Πρόσβαση

Σύμφωνα με το άρθρο 2 της Σύμβασης κάθε μέλος θα θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει τα ποινικά αδικήματα σύμφωνα με την εσωτερική του νομοθεσία, όταν διαπράττεται εκ προθέσεως η πρόσβαση σε ολόκληρο ή σε ένα μέρος συστήματος ηλεκτρονικών υπολογιστών, χωρίς δικαίωμα. Το μέρος μπορεί να απαιτεί ότι, το αδίκημα θα διαπράττεται ή με παραβίαση των μέτρων ασφάλειας 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.

Το άρθρο αυτό έχει ως σκοπό να ποινικοποίηση αυτό που στη γλώσσα των ηλεκτρονικών υπολογιστών είναι γνωστό ως «hacking». Ο όρος στα Ελληνικά μπορεί να αποδοθεί ως «εισβολή». Ως εισβολή μπορεί να οριστεί η ενέργειες του 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. 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 τη θεμελίωση της υποκειμενικής υποστάσεως απαιτείται πρόθεση, όπως αυτός 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.

4.5.2 Αθέμιτη Παγίδευση-Υποκλοπή

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 διαμέσου 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 (υποκλοπής).

Στην Ελληνική έννομη τάξη η συμπεριφορά αυτή προβλέπεται στο άρθρο 370 Α παρ.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 τιμωρείται με φυλάκιση.

4.5.3 Επέμβαση σε Δεδομένα

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 φθοράς ξένης ιδιοκτησία (άρθρο 381 Π.Κ.).

4.5.4 Επέμβαση σε Σύστημα

Επέμβαση σε σύστημα ηλεκτρονικού υπολογιστή (Computer system) σημαίνει κάθε συσκευή ή ομάδα συσκευών που είναι εσωτερικώς συνδεδεμένες μεταξύ τους ή με άλλες σχετικές συσκευές, οι 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 κάποιου 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 λειτουργία 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).

4.5.5 Κακή Χρήση Συσκευών

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 οποιαδήποτε 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 παρ. 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 παρ.1 και 2 αυτού του άρθρου ή δημόσια διαφημίζει ή προσφέρει τις υπηρεσίες του για την τέλεση τους τιμωρείται με φυλάκιση και με χρηματική ποινή.

4.6 Η Ποινικοποίηση των Παραβάσεων με Η/Υ στην Ελληνική Νομοθεσία

Με τα ά.25 του Ν.1805/1988 προστέθηκαν στον Ποινικό μας Κώδικα διατάξεις που αφορούν τις παραβάσεις με Η/Υ. Ειδικότερα:

α) Εξετάσθηκε η έννοια του εγγράφου στο ά. 13γ. Συγκεκριμένα ως έγγραφο πλέον θεωρείται και, κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβαστούν άμεσα, όπως επίσης και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφ΄ όσον τα μέσα και τα υλικά αυτά προορίζονται ή είναι πρόσφορα να αποδείξουν γεγονότα που έχουν έννομη σημασία.

β) Απαγορεύτηκε η παραβίαση απορρήτων που πραγματοποιείται με τη χρήση Η/Υ. Έτσι, στο ά. 370Β, ορίσθηκαν τα εξής:

1. Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτους ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι, να λάβουν γνώση τους.

2. Αν ο δράστης είναι στην υπηρεσία του κατόχου των στοιχείων, καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής σημασίας, επιβάλλεται φυλάκιση τουλάχιστον ενός έτους.

3. Αν πρόκειται για στρατιωτικό ή διπλωματικό απόρρητο αναφέρεται στην ασφάλεια του κράτους, η κατά την παράγραφο 1 πράξη τιμωρείται κατά τα άρθρα 146 και 147.

4. Οι πράξεις που προβλέπονται στις παραγράφους 1 και 2 διώκονται ύστερα από έγκληση.

γ) Απαγορεύτηκε η χωρίς δικαίωμα αντιγραφή ή χρησιμοποίηση προγραμμάτων Η/Υ και η χωρίς δικαίωμα, πρόσβαση σε δεδομένα. Το ά. 370Γ που αφορά τις περιπτώσεις αυτές ορίζει τα εξής:

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με φυλάκιση μέχρι έξι μήνες και με χρηματική ποινή εκατό χιλιάδων έως δύο εκατομμυρίων δραχμών.

2. Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρείς μήνες ή με χρηματική ποινή τουλάχιστον δέκα χιλιάδων δραχμών. Αν η πράξη αναφέρεται στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, τιμωρείται κατά το ά. 148.

3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνον αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμοδίου υπαλλήλου του.

4. Οι πράξεις των παραγράφων 1 έως 3 διώκονται ύστερα από έγκληση.

δ) Τέλος καθιερώθηκε ως ιδιαίτερο είδος απάτης, η απάτη με την χρήση του Η/Υ. Συγκεκριμένα το ά.386Α όρισε τα ακόλουθα:

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

Προστασία κατά των καταχρήσεων που γίνονται με τους Η/Υ, προσφέρουν και οι αναλογικά στις περιπτώσεις αυτές εφαρμοζόμενες διατάξεις του ά. 16, του Ν. 2387/1920 για τη βιομηχανική ιδιοκτησία και των ά. 16 (κατάχρηση εμπορικού απορρήτου), 17 (χρησιμοποίηση ή ανακοίνωση σε τρίτους, χωρίς δικαίωμα, σχεδίων ή τεχνικής φύσεως κανόνων) και 18 εδ. 2 (προσπάθεια εξώθησης άλλου σε πράξη αντικειμένη στις διατάξεις των ά. 16 παρ. 1 και 17 ν. 146/14) του Ν. 146/1914 για τον αθέμιτο ανταγωνισμό(11).

Ανακεφαλαίωση - Συμπεράσματα

1. Η Ηλεκτρονική Οικονομική Παραβατικότητα, που διαπραγματευόμαστε στο τμήμα αυτό, αφορά τις ποινικοποιημένες, κατά κύριο λόγο, παραβάσεις που έχουν οικονομική χροιά και τελούνται με τη χρήση (ή την κατάχρηση) των υπηρεσιών που προσφέρουν οι Ηλεκτρονικοί Υπολογιστές(Η/Υ).

2. Ο ευρύτατα σήμερα αποδεκτός ορισμός των παραβάσεων αυτών τις προσδιορίζει ως κάθε είδους παράνομες πράξεις για την τέλεση των οποίων είναι απαραίτητη η γνώση της τεχνολογίας των Η/Υ.

3. Οι πέντε γενικές κατηγορίες στις οποίες χωρίσαμε τις παραβάσεις αυτές είναι: Π. που σχετίζονται με την ίδια τη λειτουργία του Η/Υ, Π. που αφορούν τη χρήση των Η/Υ στις τηλεπικοινωνίες, Π. που γίνονται με τη βοήθεια των Η/Υ, Π. στις οποίες οι Η/Υ υποστηρίζουν την τέλεση άλλων βασικά ποινικοποιημένων παραβάσεων και Π. που έχουν σχέση με κλοπές software και hardware.

4. Τα χαρακτηριστικά των παραβατών δείχνουν, μεταξύ άλλων, ότι αυτοί ανήκουν στο προσωπικό, κυρίως, των επιχειρήσεων θυμάτων τους, κατέχοντας συνήθως και εμπιστευτική θέση. Στον κατάλογο δε των θυμάτων περιλαμβάνονται εκτός από τις κάθε είδους επιχειρήσεις, Τράπεζες και πιστωτικοί γενικά οργανισμοί, μηχανογραφημένες κρατικές υπηρεσίες και ιδιώτες καταναλωτές προϊόντων Η/Υ.

5. Τα προβλήματα στη δίωξη των παραβατών είναι, κατά βάση, δύο. Το πρώτο έχει να κάνει με την απροθυμία των θυμάτων να καταγγείλουν για διάφορους λόγους τη θυματοποίηση τους ενώ το δεύτερο αφορά την απουσία προληπτικών μέτρων για την αποτροπή των συγκεκριμένων αυτών παραβάσεων.

Κεφάλαιο 5: ΑΝΤΙΜΕΤΩΠΙΣΗ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ ΚΑΙ ΚΑΤΑΝΟΜΗ ΕΥΘΥΝΩΝ - ΠΡΟΤΑΣΕΙΣ

Με δεδομένη την αύξηση των μορφών του ηλεκτρονικού εγκλήματος, η αντιμετώπιση του θεωρείται επιβεβλημένη. Για το λόγο αυτό σχεδόν όλα τα κράτη του κόσμου έχουν θεσπίσει νομοθετικές διατάξεις, σχετικές με το πληροφορικό έγκλημα. Ωστόσο, το νομοθετικό πλαίσιο που ισχύει είναι εξαιρετικά ελλιπές και συνήθως καλύπτεται από γενικότερες διατάξεις.

Τα τελευταία χρόνια έχουν πραγματοποιηθεί Συνέδρια τόσο στην Ελλάδα, όσο και παγκοσμίως, με σκοπό τη συζήτηση και τη λήψη αποφάσεων, σχετικά με το ζήτημα. Συγκεκριμένα, πραγματοποιήθηκε Συνέδριο για το Ηλεκτρονικό Έγκλημα στη Βουδαπέστη και υπογράφτηκε συνθήκη, στις 23/11/2001, στην οποία εντάσσονται όλα τα συμπεράσματα για το ζήτημα. Τη Συνθήκη υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας. Αυτή περιλαμβάνει ορισμούς, εξηγήσεις και ρυθμίσεις για όλες τις μορφές του ηλεκτρονικού εγκλήματος όπως αναφερθήκαμε σε προηγούμενα κεφάλαια.

Στην Ελλάδα, πραγματοποιήθηκε το Α' Πανελλήνιο Συνέδριο για το Ηλεκτρονικό Έγκλημα - Διερεύνηση και Αντιμετώπιση, στις 27 και 28 Νοεμβρίου 2002.Επιπλέον, στις 25 και 26 Νοεμβρίου 2003 πραγματοποιήθηκε Συνέδριο με θέμα: «Ηλεκτρονικό Έγκλημα 2003» Δικτυοπειρατεία και Τηλεπικοινωνιακή απάτη[15].

5.1 Μη Νομοθετικές Παρεμβάσεις για την Καταπολέμηση Μερικών Μορφών του Ηλεκτρονικού Εγκλήματος

Για την αντιμετώπιση του hacking και την παρεμπόδιση από τις διεισδύσεις των hackers στα ξένα συστήματα, τέθηκε σε εφαρμογή, τον Απρίλιο του 1995 το πρόγραμμα SATAN (Security Administrator Tool for Analysis Networks), το οποίο διατίθεται στο Διαδίκτυο και ο καθένας μπορεί να έχει χωρίς έξοδα πρόσβαση σε αυτό. Με το πρόγραμμα αυτό, αρχικά εντοπίζονται και μετά διορθώνονται λάθη και κενά στα συστήματα. Στα γενικά προστατευτικά μέτρα υπάγεται η αλλαγή του password σε τακτά χρονικά διαστήματα και η χρησιμοποίηση πρόσθετων

[15] Συνέδριο «Ασφάλεια στον κυβερνοχώρο και δικτυοπειρατεία "Hacking"» 30 & 31-10-2001, συνδιοργάνωση από το Γενικό Επιτελείο Στρατού & Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών.

προγραμμάτων ελέγχου, με τα οποία αυξάνεται ο βαθμός προστασίας αρχείων και προγραμμάτων. Στο πλαίσιο της επιχείρησης γίνεται πλέον ευρεία χρήση των firewalls(«αντιπυρικές ζώνες»), που λειτουργούν ως φράγματα ανάμεσα στο δίκτυο της εταιρείας και το Διαδίκτυο, εποπτεύουν την κυκλοφορία των δεδομένων και εμποδίζουν επιθέσεις στα δίκτυα των επιχειρήσεων.

Για την αντιμετώπιση των ιών, θεωρείται απαραίτητη η χρήση αντιβιοτικών προγραμμάτων, τα οποία έχουν τη δυνατότητα να ανιχνεύουν, να αναγνωρίζουν και πολλά από αυτά να απομακρύνουν τα περισσότερα είδη ιών.

5.2 Κατανομή Ευθυνών

Η θεσμοθέτηση ενός Ειδικού Φορέα Διαδικτυακής Ασφαλείας από την Πολιτεία, που θα τροφοδοτεί τη κοινωνία με την ενημέρωση, που απαιτείται να υπάρχει, η παροχή κινήτρων στον ιδιωτικό τομέα, που με τη σειρά του καλείται να επενδύσει στην ανάπτυξη κοινής με την Πολιτεία στρατηγικής για την ασφάλεια στο Διαδίκτυο, η υποστήριξη των Μέσων Μαζικής Ενημέρωσης στις προσπάθειες της Πολιτείας και του ιδιωτικού τομέα για την ενημέρωση του κοινού κι η ανάπτυξη της σχετικής κυβερνο-ηθικής και των αποδεκτών κανόνων ασφαλείας, καθώς και των εθελοντικών σχημάτων αλληλοβοηθείας στο Διαδίκτυο, περιγράφουν τα πρώτα βήματα για τη δημιουργία μίας συγκροτημένης αντεγκληματικής πολιτικής και στρατηγικής σε όλα τα επίπεδα.

5.2.1 Ευθύνες Πολιτείας (Ειδικός Φορέας Διαδικτυακής Ασφάλειας)

Οι αμέτρητοι παροχείς σταθερής τηλεφωνίας ανά τον κόσμο, η είσοδος νέων εταιρειών στην ελληνική τηλεφωνία, για την χώρα μας, οι ασύρματες και δορυφορικές επικοινωνίες, προσφέρουν τεράστια πλεονεκτήματα για τον δράστη του διαδικτυακού εγκλήματος, που μπορεί να κάνει χρήση όλων ή μερικών από τα παραπάνω είδη επικοινωνίας, προκειμένου να πλήξει τον στόχο του όσο το δυνατό πιο ανώνυμα, ταχύτερα και πιο αποτελεσματικά. Όσο διαρκεί η έλλειψη ειδικευμένου προσωπικού στη χώρα μας και σε κάθε χώρα, για την διατήρηση της ασφάλειας στο διαδίκτυο και την αντιμετώπιση της αντίστοιχης εγκληματικής συμπεριφοράς, το πλεονέκτημα αυτό του δράστη θα αποτελεί ταυτόχρονα το μειονέκτημα των διωκτικών αρχών, που με τα παραδοσιακά μέσα, θα προσπαθούν να εντοπίσουν τον

αόρατο εχθρό. Για να καταστεί το πλεονέκτημα του δράστη, πλεονέκτημα και της Πολιτείας πρέπει να δημιουργηθεί ο προαναφερόμενος Ειδικός Φορέας Διαδικτυακής Ασφάλειας.

Στην Ελλάδα ολοκληρώθηκε μία αξιέπαινη προσπάθεια του Υπουργείου Ανάπτυξης, που οδήγησε στην κατάρτιση δύο δεκαλόγων για ασφαλέστερη χρήση του Διαδικτύου. Ο πρώτος δεκάλογος αφορά τους καταναλωτές και ο δεύτερος δεκάλογος αφορά τους εμπόρους, που θέλουν να κάνουν χρήση του ηλεκτρονικού εμπορίου. Το στοιχείο του επαίνου στη προσπάθεια αυτή, που πρέπει να γίνει παράδειγμα προς μίμηση για το μέλλον, ήταν η συμμετοχή στις ομάδες εργασίας πολλών επαγγελματιών του χώρου του Διαδικτύου κι εν τέλει η παρουσίαση αποτελεσμάτων. Θα πρέπει, όμως, η αντιμετώπιση της ασφάλειας του Διαδικτύου να αποτελέσει ξεχωριστό αντικείμενο έρευνας από ειδικό φορέα, που θα δημιουργηθεί για τον σκοπό αυτό, ώστε τα αποτελέσματα των ερευνών να αποτελέσουν το ΚΟΙΝΟ υλικό, που θα διοχετευθεί σε όλες τις άλλες δημόσιες υπηρεσίες, στον ιδιωτικό τομέα και στο κοινό.

Καθήκον της Πολιτείας είναι να δημιουργήσει άμεσα τον Ειδικό Φορέα Διαδικτυακής Ασφάλειας με τμήματα ισάριθμα με τα ζητήματα, που προκύπτουν από τη χρήση του Διαδικτύου και με μοναδικό αντικείμενο τη μελέτη των ζητημάτων αυτών, τη διαμόρφωση της σχετικής εθνικής πολιτικής και την αντίστοιχη υποστήριξη όλων των δημόσιων υπηρεσιών, του ιδιωτικού τομέα, των Μέσων Μαζικής Ενημέρωσης και του κοινού σε επίπεδο θεωρίας και πράξης. Η ανάγκη της δημιουργίας του ειδικού αυτού δημόσιου ερευνητικού φορέα για την καταπολέμηση των προβλημάτων που προκύπτουν από τη χρήση του Διαδικτύου, επιβάλλεται και από την ανάγκη ύπαρξης ενός ενδιάμεσου μεταξύ της Πολιτείας και του ιδιωτικού τομέα, ώστε ο τελευταίος να ενημερώνει μέσω ενός ειδικού καναλιού επικοινωνίας την Πολιτεία κι η Πολιτεία να προσφέρει τις οδηγίες που απαιτούνται σε κάθε περίσταση ξεχωριστά. Ο νέος αυτός φορέας θα αναλάβει τον εκσυγχρονισμό των υπάρχοντων νομικών κειμένων με πρόβλεψη της σύγχρονης τεχνολογίας στον χαρακτηρισμό των αντικειμενικών υποστάσεων των εγκλημάτων και θα προβεί επίσης σε ριζική αναθεώρηση όλων των νομικών κειμένων, ώστε να εισαχθούν σε αυτά οι απαραίτητοι τεχνολογικοί όροι, για να αντικατοπτρίζεται σε αυτά η υπάρχουσα κατάσταση στην ελληνική κοινωνία του 21ου αιώνα. Εάν μετά από εμπεριστατωμένη μελέτη, κριθεί ότι για μία συγκεκριμένη παράνομη δικτυακή συμπεριφορά δεν απαιτείται η θέσπιση νέων νόμων, ο φορέας αυτός θα αναλάβει τότε

να εκπαιδεύσει τις διωκτικές αρχές για την αντιμετώπιση της νέας μορφής τέλεσης των εγκλημάτων αυτών, ενώ ο ίδιος φορέας θα αναλάβει τη δημιουργία ενός δικτύου της Ελλάδας με άλλες χώρες, για την αμοιβαία βοήθεια στον τρόπο εντοπισμού και διερεύνησης των διαδικτυακών εγκλημάτων και τη συνεργασία μεταξύ των διωκτικών αρχών σε εθνικό -πανευρωπαϊκό και διεθνές επίπεδο.

Η ύπαρξη των ειδικών τμημάτων διατήρησης της διαδικτυακής ασφάλειας σε κάθε δημόσια υπηρεσία κι ειδικότερα σε αυτές, που σχετίζονται με την Άμυνα της χώρας, τη Δικαιοσύνη, τη Δημόσια Τάξη, την Εθνική Οικονομία κ.ο.κ. απαιτείται για την εξυπηρέτηση των δημοσίων αυτών υπηρεσιών, αλλά πρωτίστως για την δημιουργία ενός δικτύου τροφοδότησης του Ειδικού Φορέα Διαδικτυακής Ασφαλείας, από την ίδια την υπηρεσία, το προσωπικό της και το κοινό που εξυπηρετεί, με τα προβλήματα ασφαλείας, που συναντάμε σε καθημερινή βάση. Η λύση αυτή της ύπαρξης πολλών ξεχωριστών ειδικών τμημάτων μπορεί να λειτουργήσει μόνο αν τα ειδικά αυτά τμήματα, που θα πλαισιώσουν κάθε δημόσια υπηρεσία προέρχονται από τον παραπάνω ειδικό φορέα, τροφοδοτούνται σε κεντρική βάση από αυτόν και τον ενημερώνουν για ό,τι συναντούν στο έργο τους.

Η 24ωρη βάση λειτουργίας και διαθεσιμότητας των ειδημόνων, που θα συγκροτήσουν τα ειδικά αυτά τμήματα αντιμετώπισης διαδικτυακών εγκλημάτων, απαιτείται λόγω της ίδιας της φύσης του Διαδικτύου, που δεν κοιμάται ποτέ, αλλά κυρίως λόγω της απουσίας συνόρων κι ωραρίων στην ίδια την εγκληματική δραστηριότητα. Για παράδειγμα, εάν ένας Έλληνας χρήστης πέσει θύμα δικτυακής κλοπής δεδομένων κάποιο μεσημέρι από δράστη χρήστη του Διαδικτύου με βάση τη Νέα Υόρκη κι οι Ελληνικές ειδικές διαδικτυακές δυνάμεις ασφαλείας εντοπίσουν τον δράστη, θα πρέπει οι συνάδελφοί τους στη Νέα Υόρκη, της αντίστοιχης ειδικής υπηρεσίας να είναι σε ετοιμότητα για δράση κατά τα χαράματα τοπικής ώρας Νέας Υόρκης - και το αντίστροφο.

Στις ημέρες μας το Internet που διανύουμε, τρεις διαδικτυακοί μήνες ισοδυναμούν με ένα γήινο έτος. Οι τεχνολογικές εξελίξεις είναι τόσο ραγδαίες, ώστε η επιμόρφωση των στελεχών του Ειδικού Φορέα Διαδικτυακής Ασφάλειας, πρέπει να είναι συνεχής, ενώ ο εξοπλισμός τους να χαρακτηρίζεται από τεχνολογία αιχμής.

5.2.2 Ευθύνες στον Ιδιωτικό Τομέα

Η θέσπιση των κανόνων ασφαλείας, που θα τηρούνται από το διαδικτυακό κοινό και από τους διαχειριστές των online συστημάτων αποτελεί ευθύνη της πολιτείας, αλλά εξίσου ευθύνη και του ιδιωτικού τομέα. Για παράδειγμα, μία γαλακτοβιομηχανία μπορεί στα χάρτινα κουτιά του γάλατος να ενημερώσει τα παιδιά για το Διαδίκτυο, πολύ αμεσότερα από την ίδια τη Πολιτεία ή και τον ίδιο τον γονέα, που ενδεχομένως να μην έχει τις γνώσεις ως προς τούτο.

Στις προσπάθειες καταπολέμησης της παιδικής πορνογραφίας στο Διαδίκτυο[16] ήταν η ιδιωτική πρωτοβουλία, που προσπάθησε αρχικά και μερικώς κατάφερε να δημιουργήσει δικτυακές παρουσιάσεις με συμβουλές προς τους γονείς και τα παιδιά κι ειδικά προγράμματα ελέγχου ή φιλτραρίσματος της περιήγησης των ανηλίκων στο Διαδίκτυο.

Αποτελεί καθήκον των επιχειρήσεων να ασχοληθούν με την ασφάλεια στο Διαδίκτυο και όχι μόνο να προσφέρουν λύσεις σε προβληματικές καταστάσεις, που προκύπτουν από τη χρήση αυτού, αλλά επίσης να εντοπίζουν τις προβληματικές αυτές καταστάσεις, να τις αναφέρουν στον παραπάνω δημόσιο φορέα, που αναφέρθηκε και να υποστηρίζουν ή να συμμετέχουν στις προσπάθειες ενημέρωσης του κοινού. Ούτως ή άλλως το κοινό πρέπει να εμπιστευτεί αρχικά το Διαδίκτυο, για να μπορέσει συνακόλουθα να λειτουργήσει το ηλεκτρονικό εμπόριο, που θα αποφέρει κέρδος στον ιδιωτικό τομέα, που με τη σειρά του θα ενισχύσει τις προσπάθειες για την εγγύηση ασφάλειας των συναλλαγών στο δίκτυο.

Σε συνδυασμό με τα κίνητρα, που η Πολιτεία θα παράσχει στον ιδιωτικό τομέα, το μέλημα του ιδιωτικού φορέα πρέπει να είναι η δημιουργία μίας διαδικτυακής άμυνας με τη δημιουργία:

- Ειδικού διαδικτυακού τόπου για την ενημέρωση των καταναλωτών με τη παροχή πολλαπλών δυνατοτήτων αλληλεπίδρασης με το διαδικτυακό κοινό (chats, mailing lists, forums, talk-back, feedback, live help).
- Ειδικών μηχανισμών για την αναφορά των διαδικτυακών εγκλημάτων σε ζωντανό χρόνο και την αυτόματη κι άμεση ενημέρωση όλων των σχετικών αρχών κι υπηρεσιών.

---

[16]. Εγχειρίδιο της Europol που αφορά τη Νομοθεσία για την παιδική πορνογραφία στα κράτη μέλη Νοέμβριος 2000.

- Ειδικών forums ενημέρωσης κι εκπαίδευσης του διαδικτυακού κοινού και βοήθειας των θυμάτων.
- Ειδικών σεμιναρίων για την ασφάλεια στο Διαδίκτυο, από όλους τους επαγγελματικούς φορείς, ώστε να αναλυθούν και ειδικότερα θέματα, που θα προβληματίζουν τους συγκεκριμένους επαγγελματίες, που θα συμμετάσχουν.

Όλα τα παραπάνω με την αντίστοιχη off line υποστήριξη από τα Μέσα Μαζικής Ενημέρωσης.

5.2.3 Ευθύνες Μέσων Μαζικής Ενημέρωσης (Μ.Μ.Ε.)

Τα Μέσα Μαζικής Ενημέρωσης είναι αυτά, που θα υποστηρίξουν off line όλες τις παραπάνω προσπάθειες, αντλώντας την ενημέρωση από αυτές και δημιουργώντας αντίστοιχα κανάλια επικοινωνίας με το κοινό, παρουσιάζοντας τις προσπάθειες της Πολιτείας και του ιδιωτικού τομέα, καλλιεργώντας τη νέα κυβερνο-ηθική (διαδικτυακής συνείδησης) και τους κανόνες αποδεκτών κανόνων ασφαλείας στη συνείδηση του κοινού και προωθώντας τη δημιουργία εθελοντικών διαδικτυακών σχημάτων, που με της σειρά τους θα τροφοδοτήσουν τον αρμόδιο φορέα και τα ειδικά τμήματα διαδικτυακής ασφαλείας με νέα στοιχεία.

5.2.4 Ευθύνες Εθελοντών

Οι εθελοντές στο Διαδίκτυο είναι αυτοί, που μαζί με την Πολιτεία και τον ιδιωτικό τομέα θα υποστηρίξουν τη δημιουργία διαδικτυακής συνείδησης κατά του διαδικτυακού εγκλήματος.

- Διακίνηση ψηφιακών εγχειριδίων, που θα παρέχουν συμβουλές και θα προτείνουν τρόπους για την ασφαλή χρήση του Διαδικτύου και θα ενημερώνουν το κοινό για τα "σημάδια", που προδίδουν στην οθόνη τους, ότι η σύνδεση τους δεν είναι ασφαλής.
- Δημιουργία δικτυακών ενημερωτικών τόπων με τη μορφή της μεταξύ τους "αλυσίδας" (rings), ώστε ο επισκέπτης να οδηγείται από τη μία παρουσίαση στην επόμενη και να αποκτά σφαιρικές γνώσεις ταυτόχρονα με την εμπιστοσύνη, που απαιτείται για να μπορέσει να δράσει ως καταναλωτής στο Διαδίκτυο.

- Δημιουργία συνδέσμων (Links) των δικτυακών τόπων τους με τους δικτυακούς τόπους, που θα δέχονται και θα δημοσιεύουν αναφορές για τις σκοτεινές σελίδες που υπάρχουν στο Διαδίκτυο με ό,τι νεότερο ισχύει στο Διαδίκτυο.

5.2.5 Ευθύνες Γονέων

Η ενημέρωση για την ασφαλή χρήση του Διαδικτύου, πρέπει να ξεκινά από τη παιδική ηλικία και να συνεχίζεται μέχρις ότου ο/η έφηβος να μπορεί είτε να διασφαλίζει μόνος του πλέον την ατομική ασφάλεια του ή να γνωρίζει πώς θα βοηθηθεί ή πώς αναφέρει την εγκληματική δραστηριότητα, που θα συναντήσει στο Διαδίκτυο.

Οι γονείς πρέπει :

- Να μάθουν στα παιδιά τους, ότι δεν είναι ασφαλές να παρέχουν αναγνωρίσιμα της ταυτότητας τους ή της ταυτότητας των γονέων τους στοιχεία οπουδήποτε στο Διαδίκτυο, αλλά ειδικότερα στα κανάλια συζήτησης (IRC chat), στις ομάδες συζητήσεων (USENET) και σε κανάλια συζητήσεων στον Παγκόσμιο Ιστό (bulletin boards).
- Να ΜΗΝ δημοσιεύουν στο Διαδίκτυο ή διακινούν μέσω ηλεκτρονικής αλληλογραφίας φωτογραφίες των παιδιών τους.
- Να μην επιτρέπουν στα παιδιά τους να συναντώνται με άτομα που γνώρισαν στο Διαδίκτυο κι αν λάβει χώρα τέτοιο ραντεβού να είναι πάντα με τη παρουσία των γονέων και πάντα σε δημόσιο χώρο.
- Να μην απαντούν ούτε οι ίδιοι, ούτε τα παιδιά τους σε μηνύματα που έχουν αποσταλεί από αγνώστους, ή που έχουν προσβλητικό ή πορνογραφικό ή εξυβριστικό ή απειλητικό περιεχόμενο.
- Να ενθαρρύνουν τα παιδιά και να συζητούν μαζί τους για ό,τι κι αν συναντήσουν στο Διαδίκτυο, αφού το Διαδίκτυο για τα παιδιά είναι ο Κόσμος των Θαυμάτων τους.
- Να έχουν οπτική πρόσβαση στην οθόνη του υπολογιστή, που χρησιμοποιεί το παιδί κι ο υπολογιστής αυτός να είναι στο σαλόνι ή το καθιστικό κι όχι στο υπνοδωμάτιο του παιδιού.
- Να προσδιορίσουν επιτρεπόμενα όρια πρόσβασης στον υπολογιστή και στο Διαδίκτυο σε συγκεκριμένες ημέρες και ώρες.

5.3 Προτάσεις

Σύμφωνα με την ανάλυση της παραπάνω έρευνας προκύπτουν οι ακόλουθες προτάσεις:

1. Ανταλλαγή πληροφοριών για δικτυοπειρατίες ανάμεσα σε δημόσιο - ιδιωτικό τομέα.

2. Να διευρυνθούν οι συζητήσεις για ανταλλαγή πληροφοριών σε επίπεδο βιομηχανικού τομέα.

3. Να ζητήσουμε πληροφορίες από τις ΗΠΑ για το Εθνικό Κέντρο Προστασίας Υποδομών που διαθέτουν.

4. Να συνδράμουμε στη συλλογή και ανταλλαγή RISK DATA.

5. Να βελτιωθούν οι επαφές ανάμεσα στις αναρμόδιες υπηρεσίες και Υπουργεία που ασχολούνται με τον τομέα ασφάλεια.

6. Να γίνουν σεμινάρια για την επιμόρφωση - εκπαίδευση των στελεχών των επιχειρήσεων - υπουργείων για θέματα κυβερονοασφάλειας κ.α.

7. Να συσταθεί ειδικός κόμβος για κυβερνοαπειλές - κυβερνοσυναγερμούς, δηλαδή κάποιος κυβερνοδιοικητής για την καλύτερη παρακολούθηση των θεμάτων.

8. Να συσταθεί Δύναμη Ταχείας Αντίδρασης των συναρμοδίων φορέων για την ασφάλεια στον κυβερνοχώρο.

9. Να υπάρξει πνεύμα συνεργασίας και από νομικής πλευράς.

10. Να δοθούν απ' ευθείας οικονομικά κίνητρα στα Πανεπιστήμια για να αναπτύξουν CURRICULA (σημειώματα) πληροφοριών ασφαλείας.

ΕΠΙΛΟΓΟΣ

Οι ανάγκες της επιβολής του νόμου και της τάξης στο Διαδίκτυο, καθώς και οι προκλήσεις που κρύβει το Internet πρέπει να αναγνωριστούν ως ύψιστης σημασίας. Σήμερα, οι επιβολές κατά της εθνικής κυριαρχίας κι η ακεραιτότητα του Κράτους και της ασφάλειας των πολιτών του, μεταφράζονται σε συνδυασμούς ψηφίων 0 και 1 και αποτελούν διακινήσεις "πακέτων" δεδομένων μεταξύ διαδικτυωμένων υπολογιστών.

Η αξία του Internet ως μέσο επικοινωνίας ή φορέα πληροφόρησης είναι αδιαμφισβήτητη κι οι υπηρεσίες, που προσφέρει, αναντικατάστατες. Η άρνηση του Διαδικτύου ή η αποχή από τη χρήση του δεν αποτελούν λύσεις, ενώ, όπως αποδεικνύεται, το "Λευκό και Άγιο Διαδίκτυο" είναι μία ουτοπία.

Οι ανάγκες αντιμετώπισης του διαδικτυακού εγκλήματος κι οι προκλήσεις, που παρουσιάζονται σε όλα τα επίπεδα, δεν πρέπει να αντιμετωπιστούν από τους αρμόδιους φορείς επιπόλαια ή μόνο σε θεωρητικό επίπεδο ή έστω ως ζήτημα, που πρέπει να τους απασχολήσει "αύριο" ή "κάποτε". Πολύ σύντομα τα όργανα της τάξης θα αντιμετωπίζουν, καθημερινά, ηλεκτρονικά μηνύματα, που θα προειδοποιούν για τρομοκρατικές ενέργειες ή για τοποθέτηση βομβών και θα είναι αναγκαία η λήψη άμμεσων κι υπεύθυνων αποφάσεων σε κάποια δευτερόλεπτα. Σε άλλες περιπτώσεις οι καταστάσεις δεν θα είναι τόσο απλές. Τι θα γίνει για παράδειγμα αν ένας εισβολέας κάνει χρήση δικτυακών κυκλωμάτων ανά τον κόσμο για να επιτεθεί στους υπολογιστές μιας ελληνικής εταιρίας και να υποκλέψει τους αριθμούς των πιστωτικών καρτών των πελατών της; Ποια θα είναι η αντιμετώπιση του δράστη σε επίπεδο δίωξης την στιγμή που η κοινή γνώμη και τα θύματα θα απαιτούν άμμεση απονομή της δικαιοσύνης;

Η επιθυμία του Δόκτωρα Τζέκυλ να σκιαγραφήσει τον εγκληματία, τον μετάλλαξε σε Μίστερ Χάϊντ. Και οι δύο είναι αξιομνημόνευτοι ως χαρακτήρες. Μερικές φορές είναι αναγκαία μία επίσκεψη στην Κόλαση για την καλύτερη γνωριμία με τον Παράδεισο. Ούτως ή άλλως και οι δύο καταστάσεις, υπάρχουν ως ζευγάρι στη συνείδηση πολλών πιστών, που είτε ως Χριστιανοί, είτε ως Μουσουλμάνοι, Βουδιστές ή Ινδοϊστές προσπαθούν να εξισορροπήσουν μεταξύ αυτών, μεταξύ του καλού και του κακού, παραμένοντας όμως πιστοί και συνεχίζοντας τον αγώνα τους, μέχρι τέλους, με πίστη στην αξία της ζωής.

ΠΑΡΑΡΤΗΜΑ: 1

Νομοθεσία Σχετικά με το Internet

Νόμοι

Ν. 2867/2000 ("Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις")	Ν. 2246/1994 ("Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών")	Ν. 2251/1994 ("Προστασία του Καταναλωτή")
Ν. 2672/1998 ("Διακίνηση εγγράφων με ηλεκτρονικά μέσα")	Ν. 2472/1997 ("Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα")	Ν. 2121/1993 ("Πνευματική Ιδιοκτησία")
Ν. 3193/2003 ("Κανόνες Ηλεκτρονικής Τιμολόγησης")	Ν. 3115/2003 ("Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών")	

Προεδρικά Διατάγματα

ΠΔ. 269/1997 (Διάρθρωση ΕΕΤΤ)	ΠΔ. 150/2001 ("Προσαρμογή στην Οδηγία 99/93/ΕΚ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές")	ΠΔ. 342/2002 ("Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο") & ΠΔ.343/2002 ("Συνδρομητικές υπηρεσίες)
ΠΔ. 156 & ΠΔ.157/1999	ΠΔ. 165/1999	ΠΔ. 181/1999
ΠΔ. 131/2003 (Οδηγία για το Ηλεκτρονικό Εμπόριο)	ΠΔ.47/2005 (Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών)	

Οδηγίες της Ευρωπαϊκής Ένωσης

Οδηγία ΕΟΚ 90/387/1990	Οδηγία ΕΟΚ 90/388/1990	Οδηγία 1999/93/ΕΚ
Οδηγία 98/34/1998	Οδηγία 98/48/1998	Οδηγία 96/9/ΕΟΚ/1996 (Νομική Προστασία των Βάσεων Δεδομένων)

Κανονισμοί της Ε.Ε.Τ.Τ.

ΕΕΤΤ - Κανονισμός 207/6/2001 - Διαχείρισης και Εκχώρησης Αριθμών του ΕΣΑ	ΕΕΤΤ - Κανονισμός 248/71/2002 - Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής	ΕΕΤΤ - Κανονισμός 69452/95 - Εσωτερικής Λειτουργίας
ΕΕΤΤ - Κανονισμός 206/2/2001 - Εθνικό Σχέδιο Αριθμοδότησης	ΕΕΤΤ - Κανονισμός 268/73/2002 - Διαχείρισης και Εκχώρησης Ονομάτων Χώρου (Domain Names) με κατάληξη .gr	

Κανονισμοί της Α.Δ.Α.Ε.

ΑΔΑΕ - Κανονισμός Εσωτερικής Λειτουργίας	ΑΔΑΕ - Κανονισμοί για την Διασφάλιση του Απορρήτου	

Υπουργικές Αποφάσεις - Εγκύκλιοι

ΥΑ 76994/1998	ΥΑ - 60266/1996 (Κανονισμός Οικονομικής Διαχείρισης ΕΕΤΤ)	Εγκύκλιος ΔΙΑΔΠ/Α1/2523/1999 ("περί διακίνησης εγγράφων με ηλεκτρονικά μέσα")
Εγκύκλιος ΔΙΑΔΠ/Α1/3753/2001 ("περί ηλεκτρονικής διοίκησης")	Εγκύκλιος ΔΙΑΔΠ/Α1/8249/2001 ("περί αρχειοθέτησης μηνυμάτων ηλεκτρονικού ταχυδρομείου")	ΥΑ 68141/1995 (Κώδικας Δεοντολογίας Άσκησης Τηλεπικοινωνιακών Δραστηριοτήτων)

Χρήσιμοι Δικτυακοί Τόποι

Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
Διεύθυνση Απλούστευσης Διαδικασιών και Παραγωγικότητας
Επιτροπή Ανταγωνισμού
Τειρεσίας Α.Ε.
Νομοθεσία Υπουργείου Μεταφορών και Επικοινωνιών

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική βιβλιογραφία

- Αγαλλοπούλου, Π., **«Βασικές έννοιες Αστικού Δικαίου»**, (2003)
- Αγγελή, Ι (1991) **«Έγκλημα στον Κυβερνοχώρο & Ελληνικό Δίκαιο»**, ΠοινΔικ 12/2001(ΕΤΟΣ 4ο)
- Αυγουστιανάκη, Μ **«Προστασία του ατόμου από την επεξεργασία προσωπικών δεδομένων»**,. , ΔτΑ,(2001)
- Δωρή, Φ **«Νομικές Μελέτες»**, (2003).
- Ιγγλεζάκη, Ι (2000) **«Οι νομικές ρυθμίσεις για τις ψηφιακές υπογραφές»**, Η Οδηγία 1999/93/ΕΚ και οι εθνικές νομοθεσίες, ΕπισκΕΔ Γ (2000).
- Καράκωστα, Γ «**Δίκαιο και Ιντερνετ**»,
- Μήτρου, Λ., «**Η αρχή προστασίας προσωπικών δεδομένων**» (1999)
- Εγχειρίδιο της Europol που αφορά τη Νομοθεσία για την παιδική πορνογραφία στα κράτη μέλη – Νοέμβριος 2000.
- Σύμβαση για την καταπολέμηση του εγκλήματος στον Κυβερνοχώρο του Συμβουλίου της Ευρώπης – 23-11-2001.
- Συμπεράσματα συνεδριάσεων εμπειρογνωμόνων σε θέματα Πληροφορικής Τεχνολογίας στα πλαίσια της Europol.
- Συνέδριο «**Ασφάλεια στον κυβερνοχώρο και δικτυοπειρατεία "Hacking"**» 30 & 31-10-2001, συνδιοργάνωση από το Γενικό Επιτελείο Στρατού & Εθνικό & Καποδιστριακό Πανεπιστήμιο Αθηνών.

Ξενόγλωσση βιβλιογραφία

- «**Digital Evidence and Computer Crime**» – Eoghan Casey – Αμερικανική Έκδοση 2000.
- Edwards, L., « **Defamation and the Internet**»
- «**Hacking Exposed, Network Security Secrets & Solutions**» – Ioel Scambray, Stuart McClure, George Klurtz – Αμερικάνικη έκδοση 2001.
- Kohl, U., «The **rule of law, jurisdiction and the Internet, International**

Journal of Law and Information Technology»

- Lloyd, I., «**Information Techonology Law**» (1997)
- «**Secrets of a Super Hacker – The Knightmare**» - Αμερικανική Έκδοση 1994.