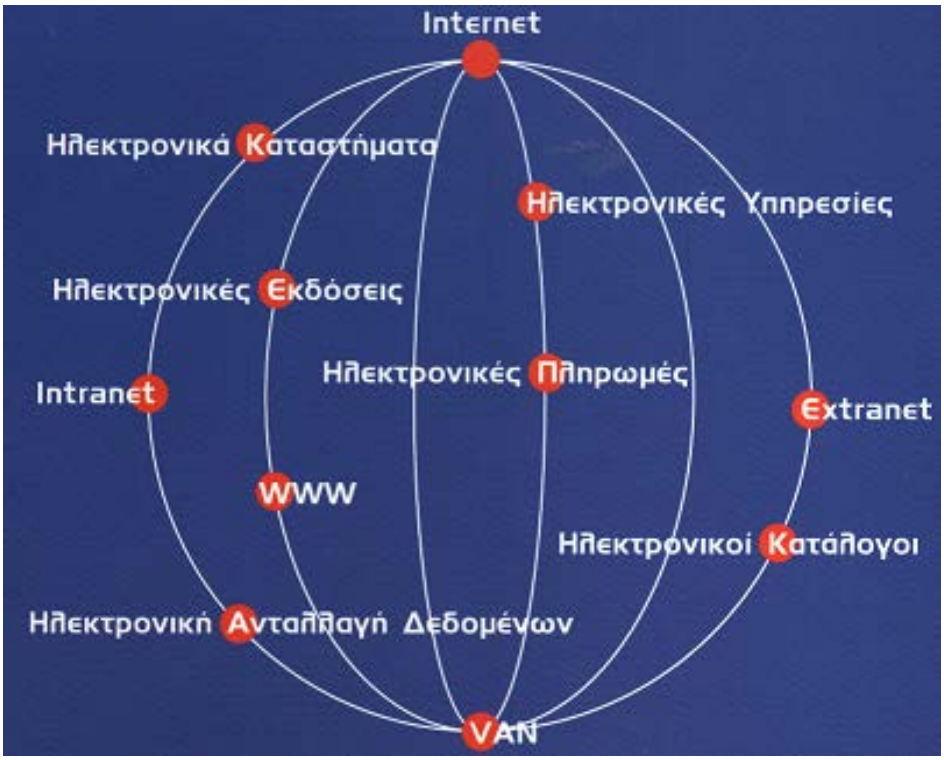
Τ.Ε.Ι. – ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΧΡΗΣΤΟΥ ΓΕΩΡΓΙΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ :

ΠΕΡΙΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ:

ΕΛΕΥΘΕΡΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ Η' ΠΕΔΙΟ ΠΑΡΑΒΑΤΙΚΗΣ ΔΡΑΣΗΣ ;



ΕΙΣΗΓΗΤΡΙΑ : ΑΛΕΞΑΝΔΡΑ ΣΤΡΑΤΗ-ΒΑΝΤΖΟΥ

ΑΡΤΑ 2005

ΠΕΡΙΕΧΟΜΕΝΑ

8. Χαρακτηριστικά Παραδείγματα Απάτης και Παραπλάνησης

ΠΡΟΛΟΓΟΣ

Ελευθερία ή Δίκτυο;

Πολλά έχουν γραφεί σχετικά με το διαδίκτυο και τις αλλαγές που θα φέρει στη ζωή μας. Ένα θέμα που συνήθως παραβλέπεται, είναι αυτό των επιδράσεων του Δικτύου στο κοινωνικό γίγνεσθαι μέσω του περιεχομένου του.

Παλιότερα τα πράγματα έμοιαζαν πιο απλά : το ίδιο το μέσο μετάδοσης μιας πληροφορίας χαρακτήριζε σε γενικές γραμμές και την ποιότητά της. Η μετάδοση πληροφοριών ήταν μια διαδικασία με μεγάλο κόστος και οι έχοντες τον έλεγχο των, σχετικά με σήμερα, λιγοστών μέσων, φρόντιζαν να τα εκμεταλλεύονται με τον καλύτερο δυνατό τρόπο για να μεταδώσουν τα μηνύματα τους.

Σήμερα αυτό απέχει πολύ από την πραγματικότητα : Η τυπογραφία έγινε μια επιτραπέζια υπόθεση και με την εξάπλωση του Δικτύου ο καθένας μπορεί να μεταδώσει ό,τι νομίζει με πρακτικά μηδαμινό κόστος και σε τεράστιο αριθμό αποδεκτών. Οι αποδέκτες των περιεχομένων του Δικτύου δεν έχουν ούτε την οργάνωση ούτε και τη δυνατότητα να ελέγξουν τα πληροφοριακά σκουπίδια και δεν αναφέρομαι μόνο στην πορνογραφία ή το σατανισμό: περισσότερο επικίνδυνα είναι τα πολιτικά και πολιτισμικά πληροφοριακά σκουπίδια, τα οποία δεν είναι άμεσα ορατά, καθώς και ο έλεγχος των συνηθειών των χρηστών του Δικτύου.

Ξεκινάνε λοιπόν οι διαμαρτυρίες από "αγανακτισμένους γονείς", εκκλησίες και άλλους και οι μητροπολίτες του σημερινού πολιτικού και τεχνολογικού status quo, αναλαμβάνουν δράση προκειμένου να μας "προστατέψουν" από "το κακό και τη διαφθορά" που υπάρχουν στο Δίκτυο κατασκευάζοντας πρότυπα.Οι ίδιες οι πολιτικές και πολιτισμικές δομές που γεννούν και υποθάλπουν φαινόμενα κοινωνικής περιθωροποίησης, διαφθοράς και φτώχειας, όπως τα ναρκωτικά, η εμπορευματοποίηση της γυναικείας (κυρίως) υπόστασης, και τα εκατομμύρια αστέγων και πεινασμένων που είναι "αναγκαία" για να "κρατηθούν οι τιμές και να λειτουργήσει η αγορά", κόπτονται να μας "προστατέψουν" από το "κακό" περιεχόμενο του Δικτύου. Σαν να μην είναι (λ.χ.) η εμπορευματοποίηση της γυναίκας το πρόβλημα αλλά η έκφραση αυτής και μέσα από το Δίκτυο. Σαν να μην είναι η κοινωνική περιθωριοποίηση, η αδιαφορία των νέων και οι μορφές με τις οποίες αυτές εκφράζονται, το πρόβλημα αλλά η δυνατότητα μετάδοσης των μορφών αυτών μέσα από το Δίκτυο. Φανταστείτε το ανάλογο την εποχή της ανάπτυξης της τηλεφωνίας: "ναι μεν το τηλέφωνο φέρνει τους ανθρώπους πιο κοντά και ο καθένας μπορεί να επικοινωνήσει με τον οποιονδήποτε αλλά ο τάδε το χρησιμοποιεί για να λέει 'κακά πράγματα' και πρέπει να βρεθεί τρόπος να μην του τηλεφωνεί κανένας..."

Αλλού είναι το πρόβλημα: το Ίντερνετ είναι ίσως το μοναδικό μέσο μαζικής επικοινωνίας που αναπτύχθηκε με αδιανόητους ρυθμούς, χωρίς όμως "αυτοί που ξέρουν και που πρέπει", να διατηρούν τον έλεγχο. Η ανάγκη να

αποδώσουν κέρδη οι τεράστιες επενδύσεις που έχουν γίνει στον τομέα των τηλεπικοινωνιών και της πληροφορικής, οδήγησε στη δημιουργία μιας τεράστιας τεχνητής ζήτησης η ικανοποίηση της οποίας, από τεχνική σκοπιά, δεν είναι δυνατό να ελεγχθεί ως προς το περιεχόμενο. Η παγκόσμια υιοθέτηση των ανοιχτών πληροφοριακών συστημάτων (τα οποία με καθυστέρηση έγιναν και τεχνικά πρότυπα) αφαίρεσαν τη δυνατότητα από λιγοστές τεράστιες εταιρείες να ελέγχουν την κατάσταση, όπως στο παρελθόν, και έβαλαν στο παιχνίδι πολλές μικρότερες εταιρείες αλλά κυρίως, επέτρεψαν στους καταναλωτές να μην είναι πουθενά υπόλογοι για τις πράξεις τους και να έχουν πολλές εναλλακτικές επιλογές.

Εδώ άλλωστε βρίσκεται και η τεράστια δυναμική του δικτύου, η οποία μπορεί τελικά να το οδηγήσει στη μια ή την άλλη κατεύθυνση. Ρυθμιστικός παράγοντας για την εξάπλωση και το περιεχόμενο αυτού, θα πρέπει να είναι η συμπεριφορά και οι παρεμβάσεις των εκατομμυρίων χρηστών του και όχι οποιοσδήποτε "πιστοποιητής καταλληλότητας περιεχομένου". Οι χρήστες έχουν την ευθύνη να εκφράσουν και να απαιτήσουν την ικανοποίηση πραγματικών και ουσιαστικών αναγκών τους μέσα από το Δίκτυο και να παύσουν να είναι παθητικοί καταναλωτές ή άλλου εύπεπτου και εκ του πονηρού σερβιρόμενου υλικού. Αυτοί είναι άλλωστε που πληρώνουν την ανάπτυξη του Δικτύου η οποία μέχρι σήμερα φαίνεται να έχει ωφελήσει περισσότερο εταιρείες και πάσης φύσεως φορείς που γνωρίζουν τι θέλουν και έχουν συγκεκριμένα κέρδη από τη βελτίωση της τηλεπικοινωνιακής υποδομής και λιγότερο τους ίδιους τους χρήστες

Η δυνατότητα άμεσης αναδρομής στην παγκόσμια συσσωρευμένη γνώση και η ενδεχομένως επακόλουθη ευαισθητοποίηση για σημαντικά ζητήματα όπως η οικολογία, η αξιοποίηση της επιστημονικής γνώσης σε όφελος του ανθρώπου, η κατανομή του πλούτου, η μελέτη της ιστορίας και των πολιτισμών, η ανάπτυξη της δημοκρατίας στις νέες συνθήκες κ.ά., αποκτούν νέα διάσταση με τη βοήθεια ενός εργαλείου σαν το Ίντερνετ. Η λέξη κλειδί στο παραπάνω είναι το "εργαλείο". Το Ίντερνετ δεν είναι αυτοσκοπός και η θεοποίησή του από τον οποιονδήποτε είτε προέρχεται εκ του πονηρού και έχει σκοπό να μεταφέρει το κόστος της ανάπτυξης στους χρήστες και τα οφέλη αυτής σε λίγους είτε είναι κοντόφθαλμη και "επιχειρηματική αρπαχτή", όπως είναι ο κάνονας στην Ελλάδα.

Το τεράστιο πρόβλημα του ελέγχου του δικτύου έχει πολλές πλευρές, μια μόνο από τις οποίες είναι η πιστοποίηση του περιεχομένου. Εξίσου αν όχι περισσότερο ανησυχητικές, είναι ορισμένες αφανείς στους απλούς χρήστες πλευρές της διαχείρισης του Δικτύου, όπως για παράδειγμα η μελέτη των "δικτυακών" συνηθειών των χρηστών. Όποιος είναι σε θέση να παρακολουθεί την κίνηση ενός χρήστη στο δίκτυο, δηλαδή το πότε και που συνδέεται, με ποιους επικοινωνεί, που "συχνάζει" περισσότερο, και, σύντομα, τι και από που αγοράζει, έχει στα χέρια του ένα πλήρες κοινωνικό προφίλ αυτού του χρήστη, το οποίο μπορεί να αναλύσει και να μελετήσει χωρίς καν να το γνωρίζει ο ενδιαφερόμενος. Υπάρχει ορατός κίνδυνος οι πάσης φύσεως διαχειριστές και πιστοποιητές στο μέλλον να έχουν στα χέρια τους υλικό για να προβλέπουν την κοινωνική συμπεριφορά και να επιδρούν εγκαίρως "διορθωτικά".

Σήμερα βλέπουμε να επιχειρείται μια παρέμβαση στο σημασιολογικό περιεχόμενο, αύριο κάποιος θα προσπαθήσει να εξασφαλίσει την μετάδοση απόρρητων πληροφοριών μέσα από το Δίκτυο, μεθαύριο κάποιος θα μας προσφέρει αποτελεσματικότερη διαχείριση, καλύτερες επιδόσεις και νέες υπηρεσίες.

1. ΣΥΝΤΟΜΗ ΑΝΑΣΚΟΠΗΣΗ ΤΟΥ INTERNET ΑΠΟ ΤΟ ΠΑΡΕΛΘΟΝ ΜΕΧΡΙ ΣΗΜΕΡΑ

1.1 Η ΙΣΤΟΡΙΑ ΤΟΥ INTERNET

Το σημερινό Internet αποτελεί εξέλιξη του **ARPANET**, ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του 60 στις ΗΠΑ.

1.1.1 Δεκαετία '60: ένα ενδιαφέρον πείραμα ξεκινά

Στα πανεπιστήμια των ΗΠΑ οι ερευνητές ξεκινούν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο **ARPANET** γεννιέται το 1969 με πόρους του προγράμματος ARPA (Advanced Research Project Agency) του Υπουργείου Άμυνας, με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς και να αποτελέσει ένα πείραμα για τη μελέτη της αξιόπιστης λειτουργίας των δικτύων. Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων (packet switching), σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή.
Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η επανασύνθεσή του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης.
Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

1.1.2 Δεκαετία '70: οι πρώτες συνδέσεις

Το 1973, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται Internetting Project (Πρόγραμμα Διαδικτύωσης) προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι που χρησιμοποιεί κάθε δίκτυο για να διακινεί τα δεδομένα του. Στόχος είναι η διασύνδεση πιθανώς ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται μια νέα τεχνική, το **Internet Protocol** (**IP**) (Πρωτόκολλο Διαδικτύωσης), από την οποία θα πάρει αργότερα το όνομά του το Internet. Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο IP μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο IP όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε τελικά οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με οποιονδήποτε άλλον.
Επίσης, σχεδιάζεται μια άλλη τεχνική για τον έλεγχο της μετάδοσης των δεδομένων, το **Transmission Control Protocol** (**TCP**) (Πρωτόκολλο Ελέγχου Μετάδοσης). Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών (FTP) και για το ηλεκτρονικό ταχυδρομείο (E-mail). Σταδιακά συνδέονται με το ARPANET

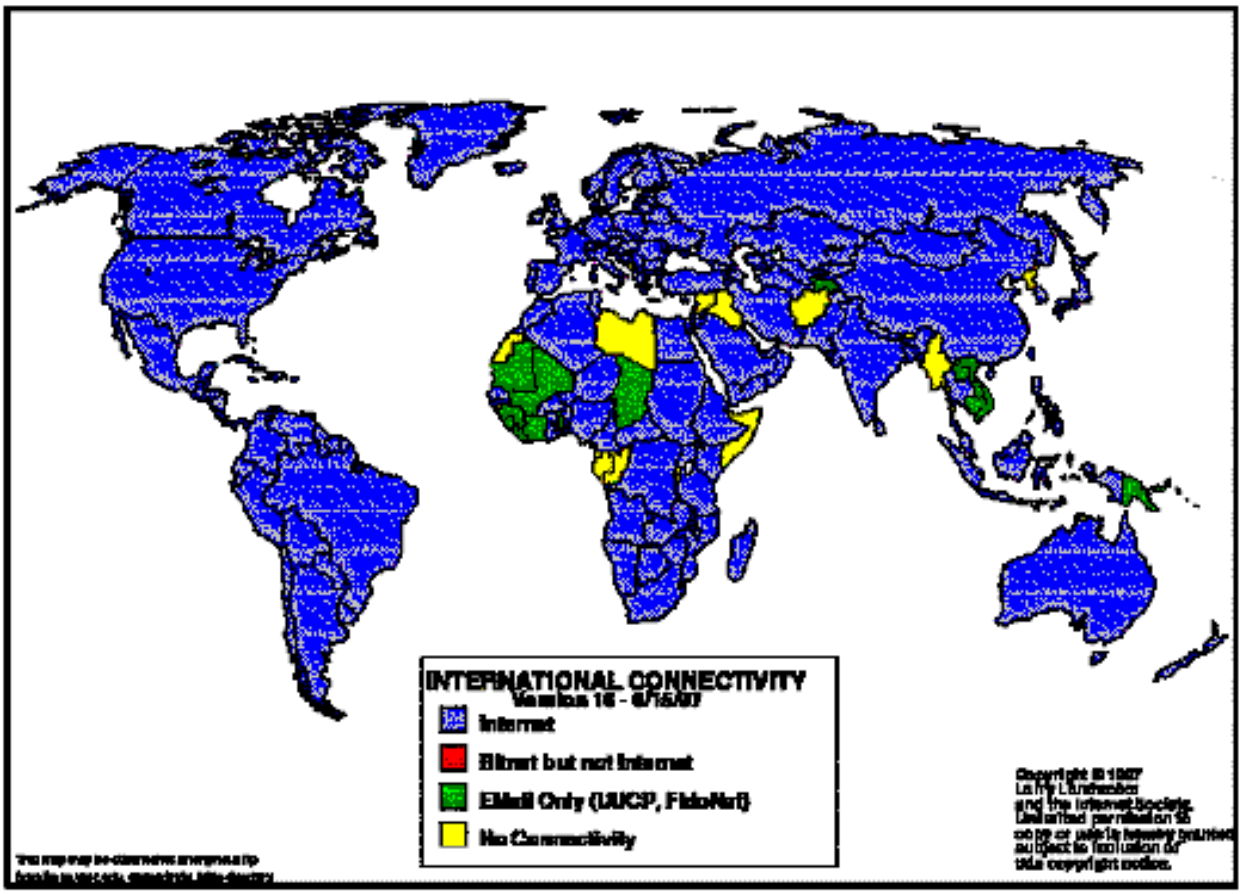
ιδρύματα από άλλες χώρες, με πρώτα το University College of London (Αγγλία) και το Royal Radar Establishment (Νορβηγία).

1.1.3 Δεκαετία '80: ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα

Το 1983, το πρωτόκολλο **TCP/IP** (δηλ. ο συνδυασμός των TCP και IP) αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος Berkeley UNIX το οποίο περιλαμβάνει το TCP/IP συντελεί στη γρήγορη εξάπλωση της διαδικτύωσης των υπολογιστών. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο ARPANET, το οποίο επιβαρύνεται πολύ και το 1983, χωρίζεται σε δύο τμήματα: στο MILNET (για στρατιωτικές επικοινωνίες) και στο νέο ARPANET (για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση).
Το 1985, το National Science Foundation (NSF) δημιουργεί ένα δικό του γρήγορο δίκτυο, το **NSFNET** χρησιμοποιώντας το πρωτόκολλο TCP/IP, προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του '80 όλο και περισσότερες χώρες συνδέονται στο NSFNET (Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α.). Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό σαν **INTERNET** και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Το 1990, το ARPANET πλέον καταργείται.

1.1.4 Δεκαετία '90: ένα παγκόσμιο δίκτυο για όλους

Όλο και περισσότερες χώρες συνδέονται στο NSFNET, μεταξύ των οποίων και η Ελλάδα το 1990.
Το 1993, το εργαστήριο CERN στην Ελβετία παρουσιάζει το **World Wide Web** (**WWW**) (Παγκόσμιο Ιστό) που αναπτύχθηκε από τον Tim Berners-Lee. Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων (multimedia) που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του Internet σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες, στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας το ποντίκι. Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του Internet προσιτή στον απλό χρήστη. Παράλληλα, εμφανίζονται στο Internet διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών Internet (Internet Service Providers - ISP) και προσφέρουν πρόσβαση στο Internet για όλους. Οποιοσδήποτε διαθέτει PC με modem μπορεί να συνδεθεί με το Internet σε τιμές που μειώνονται διαρκώς. Το 1995, το NSFNET καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα.



Εικόνα: Η κατάσταση σύνδεσης ανά χώρα, όπως είχε στις 15/6/1997. Με μοβ εμφανίζονται οι χώρες με πλήρη σύνδεση στο Internet, με πράσινο οι χώρες που διαθέτουν πρόσβαση μόνον στην υπηρεσία E-mail και με κίτρινο οι χώρες που δεν διαθέτουν κανένα είδος σύνδεσης.

Η ανακάλυψη του **WWW** σε συνδυασμό με την ευκολία απόκτησης πρόσβασης στο Internet προσέλκυσε έναν μεγάλο αριθμό καινούργιων χρηστών και έφερε την "έκρηξη" που παρακολουθήσαμε τα τελευταία χρόνια.

Σήμερα, όπως φαίνεται και από την παραπάνω εικόνα, το μεγαλύτερο μέρος του πληθυσμού της Γης ζει σε χώρες που είναι συνδεδεμένες στο Internet. Παρατηρούμε ότι καθημερινά περιοδικά και εφημερίδες εκδίδονται "on-line" και μας παραπέμπουν στις διευθύνσεις τους, επιχειρήσεις και ιδιώτες φτιάχνουν τις δικές τους σελίδες στο WWW, κλπ. Είναι προφανές ότι το Internet δεν αποτελεί πλέον ένα δίκτυο των φοιτητών και των ερευνητών αλλά ότι επεκτείνεται και επιδρά στις καθημερινές

πρακτικές όλων μας. Ήδη μιλάμε για ηλεκτρονικό εμπόριο, τηλεεργασία, τηλεκπαίδευση, τηλεϊατρική, κλπ. μέσα από το Internet.

Στην Κοινωνία της Πληροφορίας στην Ελλάδα, το ηλεκτρονικό κουτί της Πανδώρας, φαίνεται να έχει ανοίξει για τα καλά. Ακόμη και οι πιο απλές διαδικασίες, π.χ. η κουβέντα με ένα φίλο κ.λ.π. φαίνεται να έχουν αποκτήσει μια επιπλέον διάσταση, την ηλεκτρονική, στην οποία όμως, λίγοι έχουν πρόσβαση μέχρι στιγμής. Αν μέχρι «χθες», στην καθημερινότητά μας, όπως την ζούσαμε, πριν το Διαδίκτυο και τον Παγκόσμιο Ιστό, υπήρχαν οι γνωστές κοινωνικές, οικονομικές και φυλετικές ανισότητες, σήμερα, με τις νέες τεχνολογίες, προστίθεται μια νέα η οποία διαμορφώνει δύο χωριστές κοινωνίες, μέσα στην ίδια την κοινωνία : **εκείνη που το κάθε μέλος της, θα έχει τη δυνατότητα πρόσβασης στις νέες τεχνολογίες, στη νέα ηλεκτρονική πραγματικότητα και εκείνη που δεν θα έχει, δηλαδή βρισκόμαστε μπροστά στη δημιουργία του Homo Electronics. Αυτή οδηγεί πλέον καθαρά στη δημιουργία νέου τύπου διακρίσεων, μεταξύ των ανθρώπων, σε πληροφοριο-πλούσιους, που κατέχουν την πληροφορία και στους πληροφοριο-φτωχούς, που δεν την κατέχουν, δηλαδή οδηγεί σε ένα νέο είδος αναλφαβητισμού.**

Έτσι στην χαραυγή του 21^{ου} αιώνα, ο πολίτης του Διαδικτύου, αποτελεί μέρος της νέας ηλεκτρονικής πραγματικότητας. Φυσικά θα συνεχίσει να ζει στα όρια ενός κράτους.

Ο Πρόεδρος Αμερικανικής εταιρείας κατασκευής ολοκληρωμένων ηλεκτρονικών κυκλωμάτων, chips, λέει ότι **: *« Σήμερα δεν απέχουμε από το να συμπληρωθεί ο αριθμός των 1.000.000.000 διασυνδεδεμένων υπολογιστών, σε όλο τον κόσμο »*** που σημαίνει ότι σήμερα προσδιορίζεται το εύρος και η σημασία της δημιουργίας μιας νέας οντότητας, που δεν είναι άλλη από την νέα ηλεκτρονική πραγματικότητα, την νέα Ήπειρο του Διαδικτύου. Είναι η 6^{η} Ήπειρος που δημιουργείται στον πλανήτη Γη, που έννοιες όπως, σύνορα, χρονικοί και γεωγραφικοί περιορισμοί, δεν έχουν νόημα. Είναι μια ιδεατή περιοχή, που καλύπτει σχεδόν, όλο τον πλανήτη, που οι συναλλαγές θα γίνονται 24 ώρες το 24ωρο, συνεχώς, χωρίς καμία διακοπή, με μόνο απαραίτητο εφόδιο έναν υπολογιστή με διαβατήριο για το Διαδίκτυο. Κάθε πολίτης του Διαδικτύου θα μπορεί να διοχετεύει τις ιδέες και τις απόψεις του, τις οποίες θα θεωρεί σημαντικές ή λιγότερο σημαντικές στο Διαδίκτυο και έτσι γίνεται άμεσα ο αυτόματος κινητήριος μοχλός και η αξιόλογο πηγή, που θα ανανεώνει τον παγκόσμιο πλούτο γνώσεων, με απίστευτη ταχύτητα. Έτσι, ενώ **ο παραδοσιακός πολίτης (Citizen)** αντιμετωπίζει δυσκολία στην πρόσβαση και ανάκτηση πληροφοριών, που του δημιουργεί κενά στη γνώση και στη συνολική αντίληψη για την ζωή και την κοινωνία, η οποία τελικά τον οδηγεί σε κοινωνική υστέρηση, αντίθετα **ο «σύγχρονος» πολίτης του Διαδικτύου (Netizen)**, λόγω της αδυναμίας οργάνωσης, ταξινόμησης και, ως εκ τούτου, αξιοποίησης του τεράστιου όγκου της πληροφορίας, που προσφέρεται κατά τρόπο ανεξέλεγκτο, συμβάλλει στη δημιουργία μιας πληροφοριακής Βαβέλ. Στα πλαίσια αυτής, η πνευματική και νοητική σύγχυση, ως αποτέλεσμα του πληροφοριακού σοκ, θεωρείται αναπόφευκτη και, ίσως, του προκαλέσει αρνητική αντίδραση στη θέλησή του, για διαρκή μάθηση.

Παρόλα αυτά ο Κυβερνοχώρος, που είναι το Ίντερνετ, έχει τα καλά και τα κακά του , για την κοινωνία που ζούμε.

2. ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΔΙΚΑΙΟ

2.1 Εισαγωγή

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (Internet) . Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα 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 δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις. Ο συνδυασμός των δύο βασικών αλλά και διαφορετικών τρόπων σκέψεως αποτελεί "τον σταυρό του μαρτυρίου" για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και της αντιμετώπισής του.

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

Σε κάθε περίπτωση όμως ο μελετητής των σχετικών με τον κυβερνοχώρο θεμάτων θα πρέπει να καταφεύγει στα διάφορα (πολυπληθή) τεχνικά περιοδικά για τους ηλεκτρονικούς υπολογιστές, καθώς και σε δημοσιεύματα του ημερήσιου Τύπου. Αλλωστε και το ίδιο το διαδίκτυο αποτελεί πηγή αντλήσεως πληροφοριών (ίσως την σημαντικότερη), ανατρέχοντας στις ειδικές τοποθεσίες - θέσεις (Sites).

2.2 Το γενικότερο πρόβλημα της νομικής ορολογίας

Πρέπει ιδιαιτέρως να τονιστεί ότι, η διαφορετική κατανόηση - αντίληψη των ίδιων εννοιών από τον τεχνικό και νομικό αποτελεί ένα από τα σημαντικότερα προβλήματα του υπό εξέταση θέματος. Έτσι π.χ. διαφορετικά αντιλαμβάνεται την έννοια του όρου **"κυβερνοχώρος", "ασφάλεια", "χάκερ"** κλπ ο τεχνικός και διαφορετικά ο νομικός. Για τη νομική επιστήμη οι έννοιες έχουν το περιεχόμενο που ρητώς τους προσδίδει ο νόμος. Σε περίπτωση δε, που δεν υπάρχει σχετικός νόμος, ανατρέχει ο νομικός στη νομολογία, δηλαδή, στις υπάρχουσες δικαστικές αποφάσεις. Για την ύπαρξη όμως σχετικής νομολογίας, είναι απαραίτητο να έχει "φθάσει" η υπόθεση ή άλλη παρόμοια στο δικαστήριο. Σε περίπτωση που, ούτε νομολογία υπάρχει, ο νομικός ανατρέχει

στη νομική επιστήμη, προς αναζήτηση θεωρητικής τουλάχιστον λύσης του θέματος. Αυτό βέβαια δεν σημαίνει ότι, η νομική θεωρία, όπως αυτή έχει αναπτυχθεί ή αναπτύσσεται από τη (νομική) επιστήμη, γίνεται υποχρεωτικώς δεκτή στην νομική πρακτική, δηλαδή στην διερεύνηση ή την εκδίκαση των σχετικών εγκλημάτων.

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.

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

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

Στην παρούσα εργασία χρησιμοποιούνται οι σχετικοί όροι στην Ελληνική γλώσσα, για την πληρέστερη όμως κατανόησή τους χρησιμοποιείται σε παρένθεση και ο Αγγλικός όρος, όπου αυτό απαιτείται. Η ανάγκη παραθέσεως και των ξενόγλωσσων όρων προκύπτει από το γεγονός ότι, οι όροι αυτοί δεν έχουν ακόμα "δοκιμαστεί" στην Ελληνική νομική πρακτική. Έτσι για έννοιες με το ίδιο νομικό περιεχόμενο χρησιμοποιούνται στην Ελληνική γλώσσα διαφορετικοί όροι.

Σημειώνεται επίσης ότι, εκ των πραγμάτων είναι αδύνατο να αναφερθούμε στο διαδίκτυο και τη σχέση του με το ποινικό Δίκαιο, χωρίς παραπομπές στην τεχνική πλευρά των ηλεκτρονικών υπολογιστών και στην τεχνολογία γενικότερα.

2.4 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. 2867/2000 για την Οργάνωση και Λειτουργία των 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.**

2.5 Προσδιορισμός της εννοίας του εγκλήματος στον κυβερνοχώρο

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

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

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 τελεστεί σε "περιβάλλον Internet " (εννοείται βέβαια ότι απαιτείται και η χρήση computer) τότε πρόκειται για έγκλημα σχετιζόμενο με τον κυβερνοχώρο ή για έγκλημα που διαπράττεται στον κυβερνοχώρο

ή για έγκλημα που διαπράττεται με την βοήθεια του κυβερνοχώρου (Internet related crime).

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

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

2.6 Χαρακτηριστικά γνωρίσματα του εγκλήματος στον κυβερνοχώρο

- Το έγκλημα στον κυβερνοχώρο είναι γρήγορο (quick), διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
- Είναι εύκολο (easy) στην διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ συχνά δεν αφήνει ίχνη (όπως στα κοινά εγκλήματα είναι τα δακτυλικά αποτυπώματα).
- Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις, αυτή τη στιγμή είναι πιο προηγμένο (``ανεβασμένο``) και από το έγκλημα του λευκού περιλαιμίου .
- Μπορεί να διαπραχθεί χωρίς την φυσική μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, πατώντας μόνο ορισμένα πλήκτρα του υπολογιστή του.
- Δίνει τη δυνατότητα σε άτομα με ορισμένες ιδιαιτερότητες π.χ. σ΄ όσους έχουν ροπή ή τάση στην παιδοφιλία ή χρήση παιδικής πορνογραφίας (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (News groups) ή μέσα από διαδικτυακά άμεσα αναμεταδιδόμενες συζητήσεις (IRC- Internet Relay Chat).
- Οι "εγκληματίες του κυβερνοχώρου" πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα π.χ. αποστέλλουν ηλεκτρονικά μηνύματα ή επιστολές (e-mail) ανωνύμως ή /και με ψευδή στοιχεία.
- Είναι έγκλημα "χωρίς πατρίδα``, παρότι τα αποτελέσματά του μπορεί να γίνονται ταυτόχρονα αισθητά σε πολλούς τόπους.
- Κατά κανόνα είναι πολύ δύσκολο να προσδιοριστεί ο (πραγματικός) τόπος τελέσεώς του. Ακόμα όμως και αν προσδιοριστεί αυτός, είναι ακόμα πιο δύσκολο να εντοπιστεί ο δράστης.

- Η εξωτερίκευσή του μπορεί να εντοπίζεται στην Α χώρα, πλην όμως τα αποδεικτικά στοιχεία μπορεί να βρίσκονται στο άλλο άκρο της γης ή και να βρίσκονται ταυτόχρονα σε πολλούς τόπους.
- Για την διερεύνησή του απαιτείται κατά κανόνα συνεργασία δύο τουλάχιστον κρατών (δηλ. του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Περιπτώσεις που το έγκλημα στον κυβερνοχώρο (cyber-crime) περιορίζεται στα όρια ενός μόνον κράτους είναι (θεωρητικώς τουλάχιστον) ελάχιστες και σπάνιες.
- Οι παραδοσιακές (κοινές) Συμβάσεις για αμοιβαία Δικαστική Συνδρομή δεν επαρκούν, λόγω της φύσεως του αποδεικτικού υλικού, δηλαδή της ηλεκτρονικής απόδειξης (electronic evidence) που πρέπει να εντοπιστεί και να κατασχεθεί σε συνδυασμό με την ταχύτητα ενέργειας των διωκτικών Αρχών.
- Δεν υπάρχουν επαρκή στατιστικά στοιχεία, όχι μόνο στον Ελληνικό αλλά και στον Διεθνή χώρο. Ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου (cyber-crimes) καταγγέλλονται. Και αυτό για να μην αμφισβητείται η αξιοπιστία των παθόντων οι οποίοι κατά κανόνα είναι εταιρείες. Κατά συνέπεια, ο ``σκοτεινός αριθμός`` της εγκληματικότητας στον χώρο του διαδικτύου είναι ``ακόμα πιο σκοτεινός`` από ότι στον ``κοινό`` εγκληματικό χώρο.
- Η Αστυνομική διερεύνηση γενικότερα αλλά και η ανακριτική του προσέγγιση είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.
- Εξειδικευμένες γνώσεις επίσης απαιτούνται και για όσους άλλους ασχολούνται με την συγκεκριμένη μορφή εγκλήματος (Εισαγγελείς, Δικαστές, Δικηγόρους).

2.7 Σχέση εγκλήματος στον κυβερνοχώρο και εγκλήματος που τελείται με ηλεκτρονικό υπολογιστή

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

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

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

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

2.8 Σκιαγράφηση ("προφίλ ") εγκληματία του Κυβερνοχώρου

Ο "εγκληματίας του κυβερνοχώρου" διαφέρει ουσιωδώς από τον "κοινό εγκληματία". Δεν μπορεί ο καθένας να διαπράξει έγκλημα που σχετίζεται με το διαδίκτυο. **Ο δράστης πρέπει να διαθέτει ειδικές γνώσεις, τεχνική επιδεξιότητα, τεχνικά μέσα.** Χαρακτηριστικώς αναφέρεται ότι, στο έγκλημα στον κυβερνοχώρο (cyber-crime) δεν υπάρχει "Γιάννης - Αγιάννης". Υπάρχουν μόνο " Άθλιοι ". Τι σημαίνει αυτό; Ο εγκληματίας του κυβερνοχώρου (cyber-crook) δεν μπορεί να υποστηρίξει ότι ενήργησε "από ανάγκη" δηλαδή από οικονομική ανέχεια, αφού η ενέργειά του προϋποθέτει την ύπαρξη μιας αρκετά ικανής οικονομικής υποδομής (αγορά και συντήρηση υπολογιστή, αυξημένος τηλεφωνικός λογαριασμός, συνδρομή σε παροχέα πρόσβασης, εκπαίδευση σε υπολογιστές, αγορά σχετικών βιβλίων, κλπ). Δηλαδή χωρίς την κατοχή αυτή των τεχνικών και μη μέσων είναι αδύνατη η διάπραξη εγκλήματος στον κυβερνοχώρο.

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

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

β) σ΄ αυτούς που ενεργούν από οικονομικό όφελος (cracker). Στην δεύτερη ανήκουν αυτοί που δεν " εισβάλλουν " 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 Τράπεζα 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, ακόμα δε και τα εμπόδια που θα αναγνωρίζουν τα δακτυλικά αποτυπώματα ή το χρώμα του οφθαλμού. Ειδικότερα τον ανιχνευτή της ίριδος θα τον ``ξεγελούν`` με την ανάλογη κατασκευή φακών επαφής .

2.9 Σχέση ``εγκληματία του κυβερνοχώρου``(cyber - criminal) και του "εγκληματία του λευκού περιλαιμίου`` (white - collar criminal).

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

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

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

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

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

2.10 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**
- **σε εγκλήματα εναντίον περιουσιακών αγαθών .**

3. Ο δεκάλογος των δικαιωμάτων του χρήστη Internet

1. **Προσωπικό απόρρητο** - Κάθε χρήστης έχει δικαίωμα να γνωρίζει πάντοτε ποια από τα προσωπικά του στοιχεία καταγράφονται από τρίτους και για ποιο σκοπό, ενώ δικαιούται να αποφασίζει ο ίδιος για τη διαγραφή όσων από αυτά δεν είναι υποχρεωτικά από τον νόμο οποτεδήποτε θεωρήσει αναγκαίο ή επιθυμητό κάτι τέτοιο. Τέλος, κάθε χρήστης έχει δικαίωμα να ορίζει και να τροποποιεί ο ίδιος κατά την κρίση του το περιεχόμενο της έννοιας "Προσωπικά Στοιχεία".

   Η λήψη με παραπλανητικό τρόπο, η πώληση χωρίς άδεια ή ακόμη και η κλοπή προσωπικών δεδομένων γίνεται όλο και πιο συνηθισμένη. Οι χρήστες πρέπει να προστατευτούν από την παραβίαση του προσωπικού τους απορρήτου και είναι δικαίωμά τους να καθορίζουν οι ίδιοι τι θεωρούν ως προσωπικά δεδομένα και τι όχι.

2. **Εμπιστοσύνη του νομοθέτη** - Κάθε χρήστης πρέπει να θεωρείται ένοχος μόνο όταν διαπράξει μια αξιόποινη πράξη και όχι όταν διαθέτει απλώς την τεχνική δυνατότητα για μια τέτοια ενέργεια.

   Σε όλο και περισσότερες χώρες προωθείται νομοθεσία που τιμωρεί την τεχνική δυνατότητα, αδιαφορώντας για τις πραγματικές προθέσεις ή πράξεις του χρήστη. Δεν είναι δυνατόν να τιμωρούνται αθώοι μόνο και μόνο επειδή θα μπορούσαν να διαπράξουν κάτι παράνομο (π.χ. να δουν ένα πειρατικό DVD).

3. **Ισοτιμία των πράξεων εντός και εκτός δικτύου** - Οτιδήποτε επιτρέπεται στον "φυσικό" κόσμο δεν μπορεί να απαγορεύεται στον δικτυακό.

   Για παράδειγμα, όποιος έχει την οικονομική δυνατότητα μπορεί να εκδώσει μια εφημερίδα και να γράφει εκεί ό,τι θέλει χωρίς καμία λογοκρισία (οι νόμοι περί τύπου έχουν αναδρομική ισχύ) ή επίσημη αξιολόγηση. Μέσα στο δίκτυο όμως (όπου η δυνατότητα αυτή υπάρχει για όλους και όχι μόνο για λίγους πλούσιους και εύκολα ελεγχόμενους) συζητούνται διαρκώς τρόποι ελέγχου, "αξιολόγησης" και συγκεκαλυμμένης λογοκρισίας.

4. **Ισορροπημένη προάσπιση δικαιωμάτων** - Η κρατική προστασία των ιδιωτικών επιχειρηματικών συμφερόντων δεν μπορεί να είναι ισχυρότερη από την προστασία των ατομικών δικαιωμάτων του χρήστη όταν απειλούνται από αυτά τα ιδιωτικά συμφέροντα.

   Για παράδειγμα, το ΣΔΟΕ (που δημιουργήθηκε για οικονομικούς ελέγχους και συντηρείται από τον Έλληνα φορολογούμενο) χρησιμοποιείται ως μηχανισμός προστασίας των συμφερόντων των πολυεθνικών εταιρειών παραγωγής λογισμικού (ελέγχει αν οι επιχειρήσεις έχουν πληρώσει για το λογισμικό που χρησιμοποιούν). Καμία ουσιαστική προστασία όμως δεν παρέχεται στους ίδιους τους Έλληνες πολίτες από τις "αποικιοκρατικές" πρακτικές των επιχειρήσεων αυτών.

5. **Ασφάλεια και αξιοπιστία προϊόντων και υπηρεσιών** - Η σε βάθος χρόνου συντήρηση και επισκευή όσων εργαλείων χρησιμοποιεί ο χρήστης αποτελεί θεμελιώδες δικαίωμά του. Ειδικά για τα προϊόντα λογισμικού οποιαδήποτε εγκατάλειψη υποστήριξης θα πρέπει να συνοδεύεται από δημοσίευση του πηγαίου κώδικα ώστε να καθίσταται δυνατή η ανάληψη της εργασίας αυτής από τους ίδιους τους χρήστες εάν το επιθυμούν.

   Ο κατασκευαστής ενός ελαττωματικού αυτοκινήτου είναι υποχρεωμένος να το ανακαλέσει και να το επισκευάσει, αποζημιώνοντας τους πελάτες του για όσες ζημιές προκλήθηκαν από το ελάττωμα αυτό. Η ίδια υποχρέωση όμως δεν υπάρχει για τους παραγωγούς λογισμικού.

6. **Ελεύθερη χρήση ιδεών** - Κάθε χρήστης έχει το δικαίωμα να χρησιμοποιεί (ή ακόμη και να δημιουργεί) προϊόντα λογισμικού ή υπηρεσίες χωρίς να δεσμεύεται από γενικής διατύπωσης άδειες πνευματικών δικαιωμάτων που εμποδίζουν αντί να προάγουν την τεχνολογική ανάπτυξη.

   Εφαρμόζοντας καταχρηστικά την νομοθεσία περί πνευματικών δικαιωμάτων ή ακόμη και χρησιμοποιώντας ξεκάθαρα ψεύδη, πολλές εταιρείες έχουν κατοχυρώσει ως πνευματική τους ιδιοκτησία απλές και καθημερινές πρακτικές, απαγορεύοντας τη χρήση τους από τρίτους και δημιουργώντας απαράδεκτες μονοπωλιακές καταστάσεις στην αγορά πληροφορικής.

   Η αναίρεση αυτών των καταχρηστικών προνομίων μπορεί να γίνει μόνο δικαστικώς αλλά οι μικρομεσαίες επιχειρήσεις και οι ιδιώτες δεν διαθέτουν την οικονομική αντοχή για κάτι τέτοιο. Επιστρέφουμε λοιπόν στην εποχή των μεγάλων τσιφλικάδων που άλλαζαν μόνοι τους τα όρια των κτημάτων τους σε βάρος των μικρών γειτόνων τους και κανείς δεν μπορούσε να τους πειράξει.

7. **Ελεύθερη πρόσβαση** - Το περιεχόμενο του διαδικτύου δεν μπορεί να αποτελεί αντικείμενο λογοκρισίας. Οποιοσδήποτε νομικός περιορισμός πρόσβασης πρέπει να είναι σαφώς καθορισμένος και να υπάρχει η δυνατότητα ελέγχου για αποτροπή της καταχρηστικής εφαρμογής του.

   Επανειλημμένα περιστατικά στο εξωτερικό έχουν καταδείξει την τάση των "μηχανισμών ελέγχου" να λογοκρίνουν όχι μόνο αυτό που δηλώνουν στο κοινό αλλά και οτιδήποτε άλλο δεν εξυπηρετεί τα δικά τους συμφέροντα (π.χ. τις ενέργειες των ανταγωνιστών τους).

8. **Ανωνυμία** - Κάθε χρήστης πρέπει να έχει το δικαίωμα πλήρους ανώνυμης επικοινωνίας μέσω διαδικτύου αν το επιθυμεί. Οι προμηθευτές υπηρεσιών ανώνυμης πρόσβασης πρέπει να "δηλώνουν" τον ανώνυμο χαρακτήρα αυτής της επικοινωνίας (π.χ. των μηνυμάτων) ώστε οι άλλοι χρήστες του δικτύου αλλά και οι αρμόδιες υπηρεσίες (π.χ. διωκτικές αρχές) να γνωρίζουν το γεγονός και να κρίνουν ανάλογα για την αξία του σχετικού περιεχομένου.

   Η ανώνυμη φωνή ή διαμαρτυρία ενθαρρύνει την ειλικρίνεια και την ελεύθερη διατύπωση απόψεων. Ο αναγνώστης ενός ανώνυμου σχολίου μπορεί να κρίνει μόνος του ποια βαρύτητα έχει το κείμενο που διαβάζει. Δεν

χρειαζόμαστε τρίτους προστάτες που να αποφασίζουν εκείνοι για λογαριασμό μας τι είναι αξιόλογο και τι όχι.

9. **Δυνατότητα δειγματοληψίας (fair use)** - Κάθε χρήστης μπορεί να χρησιμοποιεί κατά την επικοινωνία του με άλλους χρήστες ή τις δημοσιεύσεις του μικρά αποσπάσματα έργων προστατευμένων με συγγραφικά δικαιώματα κατά τρόπο όχι διαφορετικό από την επικρατούσα πρακτική στον τύπο ("φυσικό" και διαδικτυακό).

   Δεν μπορώ να κρίνω δημόσια τις απόψεις ενός άλλου αν δεν αναφερθώ σε αυτές. Οι προσπάθειες διαφόρων οργανώσεων να απαγορεύσουν την κριτική μέσω της νομοθεσίας για τα πνευματικά δικαιώματα δεν πρέπει να γίνονται αποδεκτές. (Για παράδειγμα η Εκκλησία της Σαϊεντολογίας μηνύει τους επικριτές της υποστηρίζοντας, συχνά με επιτυχία, ότι τα όσα υποστηρίζει αποτελούν πνευματικό της δικαίωμα και κανείς δεν μπορεί κάνει οποιαδήποτε νύξη για αυτά)

10. **Νομική προστασία από απαράδεκτη πρόσβαση και χρήση πόρων** - Ο χρήστης έχει δικαίωμα να ζητήσει μέσω της νόμιμης οδού αποζημίωση για κάθε αδικαιολόγητη απασχόληση του εξοπλισμού και του χρόνου του (πρόσβαση χωρίς εξουσιοδότηση στο μηχάνημά του, spamming στο mailbox του κ.λπ.).

    Χρησιμοποιούμε το Internet για σκοπούς που εμείς επιλέγουμε. Η χωρίς την έγκρισή μας "κατάληψη" και χρήση της περιουσίας μας (π.χ. του υπολογιστή ή του χρόνου μας) από τρίτους για δικούς τους σκοπούς δεν μπορεί να γίνει αποδεκτή.

4. Η ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

4.1 Γενικές παρατηρήσεις.

Στην καθομιλουμένη γλώσσα ασφάλεια είναι η κατάσταση εκείνη, στην οποία δεν υπάρχει κίνδυνος, όπου αισθάνεται κάποιος ότι δεν απειλείται. Είναι επίσης η αποτροπή κινδύνου ή απειλής, η εξασφάλιση σιγουριάς και βεβαιότητας . Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του. Έτσι π.χ. για τον στρατιωτικό η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο απ΄ ότι για τον αστυνομικό, ο οποίος επίσης αντιλαμβάνεται την ίδια έννοια εντελώς διαφορετικά απ΄ ότι ο εργαζόμενος σε οικοδομικές εργασίες κλπ. Αλλά και στον ίδιο ευρύτερο επαγγελματικό κλάδο η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο, ανάλογα με την επιμέρους ενασχόληση του κάθε προσώπου. Έτσι π.χ. για τον στρατιωτικό που ασχολείται με τα όπλα η έννοια της ασφάλειας, δεν ταυτίζεται με αυτή που αντιλαμβάνεται ο ασχολούμενος με τους ηλεκτρονικούς υπολογιστές του ίδιου κλάδου. Ακόμα όμως και στον ίδιο στενώτερο - επιμέρους κλάδο, η οπτική γωνία θεωρήσεως του όρου ασφάλεια είναι εντελώς διαφορετική. Έτσι, π.χ. διαφορετικά αντιλαμβάνεται τον όρο "ασφάλεια" ο τεχνικός ασφαλείας δικτύων υπολογιστικών συστημάτων και διαφορετικά ο τεχνικός ασφάλειας τραπεζικών πληροφοριακών συστημάτων.

Σε κάθε περίπτωση όμως όλοι όσοι ασχολούνται με θέματα ασφαλείας, "συναντώνται" στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου αισθάνονται ασφαλείς, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν την σιγουριά και την βεβαιότητα κατά την ενάσκηση του έργου τους. Είναι ευνόητο βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα και τις επιχειρήσεις αλλά ακόμα και αυτές τις οργανωμένες πολιτείες .

4.2 Η νομική έννοια της ασφάλειας στον κυβερνοχώρο

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 λέγαμε χωρίς επιφύλαξη ότι ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικά ότι ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό .

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. Έτσι, στο 14ο κεφάλαιο του Ποινικού Κώδικα και στα άρθρα 290 επ. 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 την 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 μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια).

Συμπερασματικά 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.

4.3 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 μιλούμε 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 τεχνολογκές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειές των, 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.

4.4 Η τεχνική διάσταση του όρου ασφάλεια στο διαδίκτυο.

Από τεχνική άποψη, ασφάλεια (security) είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα.

Κλασσικό παράδειγμα ασφαλείας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με την χρήση πιστωτικής κάρτας. Σ΄ αυτήν την περίπτωση πρέπει να εξασφαλιστεί, ότι δεν είναι δυνατόν να ``συλλάβει`` (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αντιγράψει 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.

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

Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος .

Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητα των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα κάθε δε αλλαγή τους να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας .

Διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος .

4.5 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 κλπ) που αφορούν το άτομό 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, ότι 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 ``**. 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" .

Συμπερασματικά, η μυστικότητα και η ασφάλεια είναι εντελώς διαφορετικά πράγματα, δεν είναι όμως υπερβολικό να λεχθεί ότι, ασφάλεια και μυστικότητα στο διαδίκτυο αποτελούν τις δυο διαφορετικές όψεις ενός και του ίδιου νομίσματος.

4.6 Σχέση ασφάλειας και κρυπτογραφίας στο διαδίκτυο

Κρυπτογραφία (cryptography) είναι η χρήση κωδίκων για την μετατροπή δεδομένων, κατά τέτοιο τρόπο, ώστε να μπορούν να διαβαστούν μόνο από συγκεκριμένο παραλήπτη με τη χρήση ενός κλειδιού . Σκοπός της κρυπτογραφίας είναι να αποτραπεί η πρόσβαση στα δεδομένα, σε μη εξουσιοδοτημένα άτομα ιδιαίτερα κατά την διάρκεια μετάδοσής τους. Σχετικοί είναι οι όροι **" διαχείριση κινδύνων " (risk management)** και **ανάλυση κινδύνων (risk analysis)**. Είναι χαρακτηριστικό ότι οι μεγάλες εταιρείες προσλαμβάνουν ειδικώς εκπαιδευμένο προσωπικό (security administration), που καταστρώνει ειδικά σχέδια προστασίας του δικτύου της εταιρείας (system administration).

Μέχρι προσφάτως ο όρος ``κρυπτογραφία`` περιοριζόταν μόνο στον στρατιωτικό και τον διπλωματικό χώρο. Σήμερα όμως που η επικοινωνία με το ηλεκτρονικό 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 παρανόμων μηνυμάτων από οργανωμένους ή μη εγκληματίες κλπ.

Η διαδικασία της κωδικοποίησης των δεδομένων λέγεται κρυπτογράφηση (enscryption). Η κρυπτογράφηση στηρίζεται σε κλειδί (key) που πρέπει να κατέχει τόσο αυτός που στέλνει τα δεδομένα, όσο και αυτός που τα παραλαμβάνει. Αν ο παραλήπτης δεν κατέχει το κλειδί, υπάρχει κίνδυνος να γίνει υποκλοπή του κατά την μεταβίβαση (διαδρομή). Γενικώς η κρυπτογράφηση - αποκρυπτογράφηση γίνεται με την βοήθεια μιας μαθηματικής διαδικασίας.

Η διαδικασία της αποκατάστασης των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή λέγεται αποκρυπτογράφηση.

Είναι ευνόητο ότι, με την χρήση της κρυπτογραφίας αποκρύπτεται, όχι μόνον το περιεχόμενο του παράνομου υλικού που διακινείται αλλά αποφεύγεται επιπλέον και ο εντοπισμός του δράστη. Βέβαια ο εντοπισμός του δράστη μπορεί να αποφευχθεί και με την λεγομένη ``ανωνυμία στον κυβερνοχώρο``.

Από νομικής απόψεως ενδιαφέρον παρουσιάζει το ερώτημα, εάν είναι σύμφωνα με τις βασικές Αρχές του Δικαίου, η απαγόρευση χρήσεως της κρυπτογραφίας ή ο περιορισμός αυτής σε άτομα ή φορείς (π.χ. κρατικούς) που έχουν ειδική προς τούτο άδεια.

4.7 Σχέση ασφάλειας και δικαιώματος ανωνυμίας στο διαδίκτυο.

Είναι γνωστό ότι κάθε χρήστης του διαδικτύου (Internet) αφήνει στον χώρο την (ηλεκτρονική) ταυτότητά 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 είναι ευκολότερος. Μπορεί ακόμα ο χρήστης του διαδικτύου να έχει ως στοιχείο

ταυτότητος το όνομα "ανώνυμος", οπότε τυπικά φαίνεται ότι έχει όνομα. Η δυνατότητα αυτής της ανωνυμίας στο διαδίκτυο (Internet) διευκολύνει την διάπραξη παρανομιών και κάνει δύσκολο, αν όχι και αδύνατο, τον εντοπισμό του δράστη. Επιπλέον, η ανωνυμία σε συνδυασμό με την ανυπαρξία ή την δυσκολία εφαρμογής των νομικών κανόνων, κάνει τους ``ηλεκτρονικούς δράστες`` να αισθάνονται ασφαλείς κατά την διάπραξη των εγκλημάτων των.

Το ερώτημα που προκύπτει στο σημείο αυτό είναι, μήπως σε περίπτωση ψήφισης σχετικού νόμου για το διαδίκτυο, πρέπει να ποινικοποιηθεί η ανώνυμη χρήση του ή ακόμα και η παρουσία με ψευδή στοιχεία. Κάτι τέτοιο βέβαια επαφίεται στην βούληση του νομοθέτη. Αξίζει όμως να σημειωθεί ότι σχετικός νόμος που ψηφίστηκε στις Η.Π.Α και τιμωρούσε ποινικά την ανώνυμη χρήση ή την χρήση με ψεύτικο όνομα στο διαδίκτυο , κηρύχθηκε αντισυνταγματικός από τα Δικαστήρια των ΗΠΑ . Και αυτό γιατί, η ανωνυμία δεν χρησιμοποιείται στο διαδίκτυο μόνον από τους παράνομους αλλά και από όσους θέλουν να αποκρύψουν αυστηρώς προσωπικά τους (νόμιμα) στοιχεία .

5. ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΠΟΙΝΙΚΗ ΝΟΜΟΘΕΣΙΑ

5.1 Γενικές παρατηρήσεις

Το ερώτημα που προκύπτει από την σχέση διαδικτύου και ποινικής νομοθεσίας είναι αν η συμπεριφορά των χρηστών του διαδικτύου μπορεί να ρυθμιστεί με ποινικούς κανόνες δικαίου και εάν στην συνέχεια οι ποινικοί αυτοί κανόνες μπορούν να εφαρμοστούν στην πράξη. Το πρώτο αποτελεί ερώτημα του ουσιαστικού ποινικού δικαίου και το δεύτερο ερώτημα του ποινικού δικονομικού δικαίου.

Η απάντηση είναι : πάρα πολύ δύσκολα και σε πολύ περιορισμένο τομέα . Και αυτό γιατί η τεχνολογία εξελίσσεται τόσο γρήγορα, που η νομοθεσία όσο και αν προσπαθεί "ασθμαίνουσα" αδυνατεί να την προφτάσει. Επιπλέον, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο απαιτούνται εξειδικευμένες γνώσεις τόσο σε τεχνικό όσο και σε νομικό επίπεδο. Η απόκτηση των γνώσεων αυτών από νομικούς, που έχουν σχέση με την έρευνα, δίωξη και εκδίκαση των σχετικών υποθέσεων, αποτελεί ένα από τα σημαντικότερα προβλήματα κάθε πολιτείας.

Στο ποινικό πεδίο οι έννομες τάξεις έρχονται κατά κανόνα εκ των υστέρων να ρυθμίσουν νομοθετικώς τις καταστάσεις πιεζόμενες από τα πράγματα. Κλασσικό παράδειγμα στον τομέα της τεχνολογίας αποτελεί η εμφάνιση των εγκλημάτων που διαπράττονται με ηλεκτρονικούς υπολογιστές (computer crimes). Πριν από δυο δεκαετίες περίπου η "συμβατική νομοθεσία" δεν επαρκούσε για την αντιμετώπισή τους. Σήμερα όλες οι προηγμένες (τουλάχιστον) χώρες έχουν καταρτίσει σχετική νομοθεσία και προσπαθούν να αντιμετωπίσουν τα εγκλήματα που διαπράττονται με τη χρήση υπολογιστών. Στην Ελληνική έννομη τάξη ισχύει ο Ν. 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) που αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes).

Στο ίδιο σημείο με αυτό της προ δεκαπενταετίας νομοθετικής ελλείψεως βρίσκονται σήμερα οι έννομες τάξεις, όσον αφορά το θέμα του εγκλήματος στον κυβερνοχώρο (cyber crime). Πολλά από τα εγκλήματα που έχουν παρουσιαστεί στο διαδίκτυο, δεν μπορούν να αντιμετωπιστούν με την συμβατική νομοθεσία στο χώρο τουλάχιστον του ποινικού δικαίου. Σημειώνεται ότι ελάχιστα κράτη έχουν θεσπίσει μέχρι σήμερα ειδική νομοθεσία, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Στο σημείο αυτό πρέπει να τονιστεί ότι η κατάρτιση νομοθεσίας για την καταπολέμιση της εγκληματικότητας στον κυβερνοχώρο δεν αποτελεί "εσωτερική υπόθεση" κάθε κράτους χωριστά. Λόγω των ιδιαιτέρων χαρακτηριστικών των εγκλημάτων του κυβερνοχώρου απαιτείται κατάρτιση συμβάσεων στα πλαίσια Διεθνών Οργανισμών, με ιδιαίτερη έμφαση στη Δικαστική και Αστυνομική συνεργασία.

Από μη νομικούς έχει υποστηριχθεί η άποψη ότι δεν απαιτείται η κατάρτιση νέας νομοθεσίας για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο και ότι δεν υπάρχει νομικό κενό στο διαδίκτυο , διότι αναλογικά το " κοινό δίκαιο " μπορεί

να εφαρμοστεί και στον χώρο του διαδικτύου. Η άποψη βέβαια αυτή είναι εμφανώς εσφαλμένη, καθότι στον ποινικό τουλάχιστο χώρο, δεν ισχύει η αρχή της αναλογικότητας.

5.2 Διαδίκτυο και Γενικό Ποινικό Δίκαιο

Στην Ελληνική έννομη τάξη δεν υπάρχει γενικός νόμος που να αναφέρεται αποκλειστικώς σε θέματα διαδικτύου και ειδικότερα να ρυθμίζει την συμπεριφορά των χρηστών του διαδικτύου από άποψη ποινικού δικαίου.

Ο Ν. 1805/88, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα. Όταν καταρτιζόταν ο νόμος αυτός, το διαδίκτυο δεν είχε λάβει τις σημερινές του διαστάσεις και κατά συνέπεια δεν είχε γίνει αισθητή η ανάγκη καταρτίσεως ειδικότερης νομοθεσίας. Η διατύπωση όμως του νόμου αυτού έχει γίνει με τέτοιο τρόπο (συνδυασμός τεχνικών και νομικών εννοιών), που είναι εμφανής η επιθυμία του συντάκτη, να περιλάβει στο μέλλον και κάθε μορφή συμπεριφοράς, που θα δημιουργήσει η εξέλιξη της τεχνολογίας.

Ανεξάρτητα όμως από το εάν ο παραπάνω Ν. 1805/1988 επαρκεί ή όχι για την ποινική κάλυψη των θεμάτων που προκύπτουν από την ανάπτυξη της πληροφορικής , το βέβαιον είναι ότι, δεν επαρκεί να "καλύψει" τα εγκλήματα που έχουν παρουσιαστεί από την χρήση του διαδικτύου.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον Διαδικτύου (Internet), τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

5.3 Προσπάθεια νομικής αντιμετώπισης του θέματος στον Ευρωπαϊκό δικαιϊκό χώρο.

Η πρωτοπορία και στη νομική αντιμετώπιση το εγκλήματος στον κυβερνοχώρο ανήκει, όπως και η τεχνική, στις Η.Π.Α. Η Ελλάδα συνεργάζεται με τα άλλα κράτη της Ευρωπαϊκής Ένωσης, του Συμβουλίου της Ευρώπης καθώς και άλλων Διεθνών Οργανισμών για την αντιμετώπιση των σχετικών θεμάτων .

Στον Ευρωπαϊκό χώρο γίνεται προσπάθεια να ρυθμιστεί το θέμα η δε προσπάθεια αυτή βρίσκεται ακόμα σε εξέλιξη. Σχετικές προσπάθειες πάντως έχουν γίνει τόσο στα πλαίσια του Συμβουλίου της Ευρώπης όσο και στα πλαίσια της Ευρωπαϊκής Ένωσης.

5.3.1 Συμβούλιο Ευρώπης και έγκλημα στον κυβερνοχώρο.

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

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

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

Στο Συμβούλιο της Ευρώπης καταρτίζεται από το έτος 1997 Διεθνής Σύμβαση με αντικείμενο την καταπολέμηση του εγκλήματος στο Κυβερνοχώρο. Στην κατάρτιση της Σύμβαση αυτής συμμετέχει και η Ελλάδα. Σκοπός της Συμβάσεως είναι η προστασία της Κοινωνίας από το έγκλημα στον κυβερνοχώρο με την θέσπιση της κατάλληλης νομοθεσίας και την επίτευξη της ανάλογης με το θέμα Δικαστικής Συνεργασίας μεταξύ των κρατών, που θα υπογράψουν την Σύμβαση. Αρχικώς, ως χρονοδιάγραμμα για την περαίωση των εργασιών, είχε τεθεί το τέλος του έτους 1999. Επειδή όμως τα προβλήματα (νομικά και τεχνικά) που προέκυψαν κατά την συζήτηση ήταν τόσα πολλά και τόσο περίπλοκα, ζητήθηκε (και χορηγήθηκε) παράταση της προθεσμίας περαιώσεως μέχρι το τέλος του 2000. Ήδη η Σύμβαση έχει περαιωθεί και άνοιξε για υπογραφές σε ειδική τελετή που έγινε στις 22 και 23 Νοεμβρίου 2001 στην Βουδαπέστη.

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

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

α) Η παράνομη πρόσβαση (illegal access).

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

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

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

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

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

β) Η αθέμιτη παγίδευση - υποκλοπή (illegal interception)

Σύμφωνα με το άρθρο 3 της Συμβάσεως κάθε κράτος-μέλος θα πρέπει να θεσπίσει νομοθετικά και άλλα μέτρα που είναι απαραίτητα για να καθιερώσει ως ποινικό αδίκημα 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 κράτος-μέλος μπορεί να απαιτήσει ότι, το αδίκημα διαπράττεται με παράνομο σκοπό ή σε σχέση με ένα σύστημα υπολογιστών το οποίο συνδέεται με άλλο σύστημα.

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

Προστατευόμενο έννομο αγαθό είναι ``το δικαίωμα στην ιδιωτική ζωή και η ασφάλεια των τηλεπικοινωνιών στον κυβερνοχώρο`` Αποτελεί δηλαδή το άρθρο

αυτό, **το ``ηλεκτρονικό αντίστοιχο στον κυβερνοχώρο`` της παραβίασης του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας (υποκλοπή).**

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

γ) Επέμβαση σε δεδομένα (Data interference)

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

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

δ)Επέμβαση σε σύστημα (System Interference)

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

Δεδομένα υπολογιστή (computer data) είναι κάθε αναπαράσταση (representation) γεγονότων (facts), πληροφοριών (information) ή εννοιών (concepts) σε μορφή κατάλληλη για επεξεργασία σε σύστημα υπολογιστή, συμπεριλαμβανομένου προγράμματος κατάλληλου 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 ποινικό αδίκημα, σύμφωνα με την Εθνική του Νομοθεσία, όταν διαπράττεται εκ προθέσεως η

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

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

ε)Κακή χρήση συσκευών (misuse of devices)

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

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

5.3.2. Η θέση της Ευρωπαϊκής Ένωσης απέναντι στο διαδίκτυο

Η Ευρωπαϊκή Ενωση 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 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. Πριν από την έκδοση του ψηφίσματος αυτού είχαν γίνει για το θέμα διάφορες επίσημες ή ανεπίσημες για το θέμα 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.**

α)Παράνομο περιεχόμενο του Internet

Το σχετικό ψήφισμα (97/C 70/01/17-2-1997) του Συμβουλίου και των αντιπροσώπων των κυβερνήσεων των κρατών-μελών της 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 τελέσεώς τους. Θα μπορούσε εδώ να ειπωθεί ότι οι εσωτερικές νομοθεσίες από μόνες τους δεν επαρκούν και ότι απαιτούνται πολυμερείς Διεθνείς Συμβάσεις .

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

β) 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 στο Σατανισμό και στη Λατρεία του Σατανά . Για πολλούς το περιεχόμενο των sites αυτών αποτελεί κλασσική 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. Ως χαρακτηριστικό παράδειγμα επιβλαβούς περιεχομένου υλικό του διαδικτύου, θα μπορούσε κατά μία άποψη να θεωρηθεί και η περίπτωση (κατά τον Οκτώβριο του 1999) πλειοδοσίας κατά την πώληση ωαρίων εμφανίσιμων γυναικών (``μανεκέν``) σε ειδική τοποθεσία

(site). Ομοίως η περίπτωση της "ερωτικής συνεύρεσης για πρώτη φορά" (τον Αύγουστο 1998) μεταξύ δύο ``παρθένων νέων`` που όμως τελικά δεν έγινε. Είναι ευνόητο βέβαια ότι, πριν από την ματαίωση της ``παράστασης`` εκατομμύρια χρήστες από όλον τον κόσμο είχαν ``επισκεφθεί`` την αντίστοιχη τοποθεσία (site), με τεράστια οικονομικά κέρδη για τους ``διοργανωτές``. Η περίπτωση αυτή μπορεί να θεωρηθεί και ως απάτη, που διαπράττεται στο διαδίκτυο. Είναι ευνόητο όμως ότι, ουδείς βλαπτόμενος (ιδιώτης) ενδιαφέρθηκε για την υποβολή καταγγελίας προς άσκηση ποινικής διώξεως, λαμβάνοντας υπόψη την μικρή οικονομική ζημία που υπέστη ως άτομο ή την ``διαπόμπευσή`` του για τις ``διαδικτυακές του προτιμήσεις``, σε σχέση και με τα τεράστια δικαστικά έξοδα που απαιτούνται, για την κίνηση ενός τέτοιου δικαστικού αγώνα.

Σημειωτέον ότι, για την αντιμετώπιση του παρανόμου και επιβλαβούς περιεχομένου του κυβερνοχώρου έχει προταθεί -μεταξύ των 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 .

5.4 Η νομική αντιμετώπιση του "χάκερ" κατά το γενικό ποινικό δίκαιο.

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

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

Διευκρινίζεται ότι, το παραπάνω άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και

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

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

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

5.5 Νομικός ορισμός του "χάκερ".

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

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

5.6 Νομικές προϋποθέσεις για την ύπαρξη "χάκιγκ" κατά το Ελληνικό Δίκαιο

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

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

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

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

6. ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΕΙΔΙΚΟ ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ

6.1 Γενικές παρατηρήσεις

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 την σύνδεση του χρήστη με μια εταιρεία 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 την χρήση του διαδικτύου. Με άλλα λόγια το διαδίκτυο (Internet) δεν είναι τίποτα άλλο παρά μια μορφή επικοινωνίας που γίνεται με την 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 νόμος αυτός αντικατέστησε τον ισχύοντα Ν. 2246/20.10.1994 για την " Οργάνωση και Λειτουργία του Τομέα Τηλεπικοινωνιών", πλην των διατάξεών του που αφορούν την παροχή ταχυδρομικών υπηρεσιών (άρθρο 13 §12 Ν. 2867/2000) και των διατάξεων εκείνων που αναφέρονται στην σύσταση της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (άρθρ. 3§1Ν. 2867/2000).

β) Ο Ν.2774/22.12.99 για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα, σε συνδυασμό με το Ν.2472 /10.4.97 "Προστασία Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα".

γ) Ο Ν. 2225/20.7.94 για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας.

α) Ο Ν. 2867/19-12-2000 για την οργάνωση και λειτουργία τηλεπικοινωνιών και άλλες διατάξεις.

Ο νόμος αυτός ρυθμίζει κάθε είδους τηλεπικοινωνιακής 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 τηλεπικοινωνιακών δικτύων. Όπως και ο προηγούμενος Ν. 2246/1994 έτσι και αυτός προσδιορίζει όχι μόνον 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.2774/22.12.99 : Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Τηλεπικοινωνιακό Τομέα, σε συνδυασμό με το Ν.2472 /10.4.97 "Προστασία Ατόμου από την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα".

Ο Ν. 2774/22.12.1999, ο οποίος αναφέρεται στην προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, αποτελεί ειδικότερη μορφή του Ν. 2472/97, και αποτελεί υλοποίηση της οδηγίας 97/66/Ε.Κ. Δηλαδή οι προηγμένες ψηφιακές τεχνολογίες στα δημόσια τηλεπικοινωνιακά δίκτυα, δημιουργούν ειδικές απαιτήσεις στην προστασία δεδομένων προσωπικού χαρακτήρα (Βλ. Εισηγ. Έκθεση Νόμου 2774/99). **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 50 Α/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 Π.Κ., όπως αυτό προστέθηκε με το άρθρο 3 ν. 1805/88. Ο Ν. 2472/1997 προστατεύει το ίδιο το άτομο από την επεξεργασία των στοιχείων αυτών .

Χαρακτηριστικό παράδειγμα εφαρμογής του Ν. 2472/97 στο διαδίκτυο αποτελεί η διασύνδεση αρχείων .

γ) Ν. 2225/94 για την Προστασία της Ελευθερίας της Ανταπόκρισης

Ο νόμος αυτός έχει άμεση σχέση με τον κυβερνοχώρο αφού όπως ήδη αναφέρθηκε το Internet δεν είναι τίποτα άλλο παρά μια μορφή επικοινωνίας που γίνεται δια μέσου των τηλεπικοινωνιών.

Με το άρθρο 1 του Νόμου αυτού (2225/94) 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 Νόμου αυτού μπορεί να γίνει η παρακολούθηση (ανταλλαγής) e-mail π.χ.: ο Α εκβιάζει (άρθρ. 385 Π.Κ.) τον Β, στέλνοντας e-mail. Ο Β το καταγγέλλει στην Αστυνομία. Η Αστυνομία ζητά από τον Παροχέα (ISP) να παρακολουθεί την ανταλλαγή e-mail. Ο παροχέας στην περίπτωση αυτή δεν μπορεί να επικαλεσθεί το απόρρητο των επικοινωνιών.

6.2 Ειδικές ποινικές διατάξεις στον χώρο του διαδικτύου.

Τιμωρείται ποινικώς εάν διαπράττεται στον χώρο του διαδικτύου η παρακάτω συμπεριφορά:

α) Σύμφωνα με το άρθρο 11 του Ν. 2867/2000 η κατά παράβαση των άρθρων 5 (αναφέρεται στην χορήγηση γενικών αδειών τηλεπικοινωνιακών δραστηριοτήτων) και 6 (αναφέρεται στην 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 εκατομμυρίων (5.000.000) έως είκοσι εκατομμυρίων (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 Ν.2774/22.12.99 *για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα,* όποιος κατά παράβαση του νόμου αυτού χρησιμοποιεί, επεξεργάζεται, μεταδίδει, ανακοινώνει, δημοσιοποιεί δεδομένα προσωπικού χαρακτήρα συνδρομητών ή χρηστών, τα καθιστά προσιτά σε μη δικαιούμενα πρόσωπα ή επιτρέπει στα πρόσωπα αυτά να λάβουν γνώση των εν λόγω δεδομένων ή τα εκμεταλλεύεται με οποιονδήποτε τρόπο τιμωρείται με φυλάκιση και χρηματική ποινή και αν πρόκειται για ευαίσθητα δεδομένα με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) έως δέκα εκατομμυρίων (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) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

Οι διατάξεις των παραγράφων 6 έως και 14 του άρθρου 22 του Ν. 2472/1997 εφαρμόζονται και επί των πράξεων των προηγουμένων παραγράφων.

γ) Σύμφωνα με το άρθρο 22 του Ν. 2472/1997 τιμωρείται:

1. Όποιος παραλείπει να γνωστοποιήσει στην Αρχή, κατά το άρθρο 6 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) ετών και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (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 άδειας της Αρχής, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών.

3. Οποιος 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) δραχμών έως πέντε εκατομμυρίων (5.000.000) δραχμών. Όποιος προβαίνει σε διασύνδεση αρχείων χωρίς την άδεια της Αρχής, όπου αυτή απαιτείται ή κατά παράβαση των όρων της άδειας που του έχει χορηγηθεί, τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (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 με χρηματική ποινή τουλάχιστον ενός εκατομμυρίου (1.000.000) δραχμών έως πέντε εκατομμυρίων (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 δέκα 10 ετών και χρηματική ποινή τουλάχιστον δύο εκατομμυρίων (2.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

7. Αν από τις πράξεις των παρ.1 έως και 5 του παρόντος άρθρου προκλήθηκε κίνδυνος για την ελεύθερη λειτουργία του δημοκρατικού πολιτεύματος ή για την εθνική ασφάλεια, επιβάλλεται κάθειρξη και χρηματική ποινή τουλάχιστον πέντε εκατομμυρίων (5.000.000) δραχμών έως δέκα εκατομμυρίων (10.000.000) δραχμών.

6.3 Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ).

Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ) αποτελεί σημαντική Αρχή στον χώρο του διαδικτύου . Σύμφωνα με το άρθρο 3 Ν. 2867/2000 αποτελεί την Εθνική ρυθμιστική Αρχή σε θέματα τηλεπικοινωνιών. **Είναι ανεξάρτητη διοικητική Αρχή με έδρα την Αθήνα και απολαμβάνει διοικητικής και οικονομικής αυτοτέλειας.** Τα μέλη της Ε.Ε.Τ.Τ. κατά την άσκηση των καθηκόντων τους απολαύουν πλήρους προσωπικής και λειτουργικής ανεξαρτησίας. Ο Πρόεδρος, οι Αντιπρόεδροι και τα υπόλοιπα μέλη της διορίζονται με απόφαση του υπουργού Μεταφορών και Επικοινωνιών μετά από προηγούμενη επιλογή τους από τη Διάσκεψη των Προέδρων της Βουλής με την αυξημένη πλειοψηφία των τεσσάρων πέμπτων των μελών της. Ως μέλη της Ε.Ε.Τ.Τ. επιλέγονται πρόσωπα εγνωσμένου κύρους, που απολαύουν ευρείας κοινωνικής αποδοχής και διακρίνονται για την επιστημονική τους κατάρτιση και την επαγγελματική τους ικανότητα στον τεχνικό, οικονομικό ή νομικό τομέα. Κατά την εκτέλεση των καθηκόντων τους, τα μέλη της Ε.Ε.Τ.Τ. δεσμεύονται από το νόμο, έχουν δε υποχρέωση τηρήσεως, των αρχών της αντικειμενικότητας και αμεροληψίας. Ο Πρόεδρος, οι Αντιπρόεδροι και τα μέλη της Ε.Ε.Τ.Τ. υποχρεούνται στην τήρηση εμπιστευτικότητας εμπορικών πληροφοριών για τέσσερα (4) έτη μετά την εκούσια ή ακούσια αποχώρηση τους από την Ε.Ε.Τ.Τ..

6.4 Η νομική φύση του παροχέα υπηρεσιών (ISP - Internet Service provider)

Ιδιαίτερη σημασία για την ασφάλεια και την μυστικότητα του διαδικτύου έχει η συμμετοχή του παροχέα (τηλεπικοινωνιακών) υπηρεσιών. Αποτελεί μάλιστα ``κομβικό σημείο`` για τον εντοπισμό των παρανομιών και την συλλογή των αποδεικτικών στοιχείων, δεδομένου ότι, όλα τα στοιχεία (data) ``περνούν`` από τις εγκαταστάσεις του. Σύμφωνα με το άρθρο 1 παρ. 2 περίπτ. δ΄ του Ν.2246/20.10.1994 *φορείς παροχής τηλεπικοινωνιακών υπηρεσιών είναι φυσικά ή νομικά πρόσωπα τα οποία παρέχουν στο κοινό τηλεπικοινωνιακές υπηρεσίες από καθεστώς ελεύθερου ανταγωνισμού με βάση την άδεια ή δήλωση ή έγκριση.* Αποτελούν δηλαδή τηλεπικοινωνιακή επιχείρηση, για την λειτουργία της οποίας απαιτείται άδεια παροχής τηλεπικοινωνιακής υπηρεσίας. **Άδεια παροχής τηλεπικοινωνιακής υπηρεσίας είναι η ατομική διοικητική πράξη, βάσει της οποίας επιτρέπεται σε ορισμένη τηλεπικοινωνιακή επιχείρηση να παρέχει ελευθέρως και σε εμπορική βάση, καθορισμένες τηλεπικοινωνιακές υπηρεσίες, καθώς και να αναλαμβάνει κάθε αναγκαία δραστηριότητα για την ίδρυση ανάπτυξη ή επέκταση, εγκατάσταση και λειτουργία των απαιτουμένων για την εν λόγω παροχή διευκολύνσεων.** Ορισμένοι παροχείς υπηρεσιών είναι πολυεθνικές επιχειρήσεις, που παρέχουν πρόσβαση σε πολλές τοποθεσίες - θέσεις. Ο παροχέας τηλεπικοινωνιακών υπηρεσιών καλείται και φορέας παροχής υπηρεσιών (service provider) ή απλώς ``φορέας πρόσβασης`` (access provider).

Σύμφωνα με την με αριθμό ΥΑ 74.631/18.7.1995 Υπουργική απόφαση του Υπουργού Μεταφορών, που εκδόθηκε προς υλοποίησή του Ν. 2249/94 (ρυθμίζει τις προϋποθέσεις και την διαδικασία υποβολής δηλώσεως για λήψη αδείας για την

άσκηση επιχειρηματικής δραστηριότητος στον τομέα των τηλεπικοινωνιών) για την λήψη της σχετικής αδείας, 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 Αμυνα και την δημόσια ασφάλεια, ότι θα τηρεί τις διατάξεις τις σχετικές με την διασφάλιση του απορρήτου των επικοινωνιών και ότι θα αποφεύγει κάθε ενέργεια αθέμιτου ανταγωνισμού.

Ερώτημα γεννάται, 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, υποπίπτουν στην αντίληψή του και ουδέν πράττει για να σταματήσει την διάπραξή τους. Ένα δεύτερο, εξίσου σημαντικό ερώτημα είναι, το κατά πόσο μπορεί (νομοθετικώς) να υποχρεωθεί ο παροχέας να φυλλάτει τα δεδομένα που διέρχονται από τις εγκαταστάσεις του, για ένα ορισμένο χρονικό διάστημα (π.χ. 48 ώρες), προκειμένου να τα παραδώσει στις Αρχές, σε περίπτωση που του ζητηθούν. Κάτι τέτοιο βέβαια θα επιβαρύνει οικονομικώς τον παροχέα, δεδομένου ότι θα πρέπει, τουλάχιστον να διπλασιάσει τον τεχνικό εξοπλισμό του.

7. ΠΡΟΣΕΓΓΙΣΗ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΑΠΟ ΤΙΣ ΔΙΩΚΤΙΚΕΣ ΑΡΧΕΣ

7.1 Γενικές παρατηρήσεις.

Ο "παραδοσιακός" τρόπος προσεγγίσεως του εγκλήματος , δηλ. της περιγραφής του δράστη με την κατάθεση του θύματος , της συλλογής πληροφοριών από πληροφοριοδότες, της διεξαγωγής έρευνας, κατάσχεσης κλπ. δεν ισχύει στον κυβερνοχώρο. Ο **"ηλεκτρονικός δράστης ή ηλεκτρονικός εγκληματίας"** δεν θα πάρει το όπλο ούτε θα φορέσει τα γάντια και θα εισέλθει στη Τράπεζα για να τη ληστέψει ή σ΄ ένα σπίτι για να κλέψει. Αντίθετα με τους κατάλληλους κωδικούς αριθμούς, που κατά κανόνα παράνομα έχει αποκτήσει (πάλι διαπράττοντας ένα ηλεκτρονικό έγκλημα) θα δώσει εντολή για μεταφορά ενός χρηματικού ποσού από τον λογαριασμό του **"ηλεκτρονικού θύματος"** σ΄ ένα άλλο στο εξωτερικό . Και όταν το θύμα πάρει είδηση την εναντίον του ενέργεια ο δράστης ή θα έχει μεταφέρει τα χρήματα σε διάφορους άλλους λογαριασμούς για να χαθούν τα ίχνη του ή θα τα έχει "σηκώσει " και θα έχει εξαφανισθεί . 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 σ΄ 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 .**

Αλλά και στην περίπτωση εκείνη που ο παθών αντιλαμβάνεται εγκαίρως ότι έπεσε θύμα ηλεκτρονικού εγκλήματος, ερωτάται: σε ποια Αρχή θα καταγγείλει το έγκλημα αυτό; Έχει η Αρχή αυτή τις απαιτούμενες γνώσεις να ερευνήσει την αξιόποινη πράξη που της καταγγέλθηκε;

7.2 Αρμόδιες υπηρεσίες για την έρευνα του εγκλήματος στον κυβερνοχώρο

Στα λεγόμενα τεχνολογικώς αναπτυγμένα κράτη, όπου το έγκλημα στον κυβερνοχώρο ``ανθεί``, έχουν συσταθεί ειδικές υπηρεσίες για την έρευνα και καταπολέμηση του νέου αυτού εγκλήματος. Ενδεικτικώς αναφέρεται ότι στις Η.Π.Α. το F.B.I. έχει συστήσει το National Infrastructure Protection Center (NIPC), με παραρτήματα σε διάφορες πολιτείες για την έρευνα των σχετικών εγκλημάτων. Στα πλαίσια μάλιστα της ``**Ηλεκτρονικής Αστυνομίας**`` έχει συσταθεί ειδική μονάδα, που έχει ως αντικείμενο το ``σπάσιμο`` των κωδικών των ηλεκτρονικών επιστολών (e-mails), που χρησιμοποιούν οι έμποροι ναρκωτικών και τα δίκτυα παιδεραστίας . Ομοίως έχει συσταθεί ειδικό σώμα Εισαγγελέων, οι οποίοι ύστερα από κατάλληλη εκπαίδευση ασχολούνται με το έγκλημα στον κυβερνοχώρο . Παρόμοια εκπαίδευση έχει γίνει και στους Δικαστές. Στην Scotland Yard έχει συσταθεί το Computer Fraud Squad. Στον Καναδά έχει συσταθεί το the Royal Canadian Mounted Police Computer Crime Unit.

Δεκάδες συναντήσεις, συνέδρια κλπ γίνονται κάθε χρόνο από τις παραπάνω υπηρεσίες για θέματα σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Επίσης έχουν εκδοθεί δεκάδες γραπτές οδηγίες (guide lines) και

Κώδικες Πρακτικής (Code of Practice), που απευθύνονται στους δημόσιους εκείνους λειτουργούς, οι οποίοι είναι επιφορτισμένοι με την έρευνα και την καταπολέμηση των σχετικών εγκλημάτων. Ενδεικτικώς αναφέρεται ο Κώδικας Πρακτικής του Τμήματος Εμπορίου και Βιομηχανίας (DTI) της Βρετανίας (The British Code of Practice - Department of Industry).

7.3 Γενικά για τις έρευνες που έχουν σχέση με το έγκλημα στον κυβερνοχώρο

Οι δικαστικές-Αστυνομικές έρευνες που γίνονται για τον εντοπισμό εγκλημάτων στον κυβερνοχώρο, ουδεμία σχέση έχει με τις έρευνες , που μέχρι τώρα γνωρίζουμε . Στις μέχρι τώρα "παραδοσιακές" έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κλπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα έχει να ψάξει files , note pads , botes, data, κρυπτογραφημένα στοιχεία κλπ. 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 ότι στην κοινή έρευνα το αντικείμενο βρίσκεται σ΄ ένα 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 χιλιάδες τόπους τελέσεως. Γενικώς, ο αριθμός των τόπων τελέσεως εξαρτάται από την συγκεκριμένη λειτουργία του διαδικτύου (αποστολή e-mails, news groups, Internet relay chat, κλπ). Ακόμα και σε δορυφόρους (Satellite-technology) είναι δυνατό να βρίσκονται τα αποδεικτικά στοιχεία, δεδομένου ότι οι επικοινωνίες (κινητά τηλέφωνα κλπ.) γίνονται πλέον δορυφορικώς.

Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας αλλά και σε θέματα κατά τόπον αρμοδιότητας ως προς την εκδίκαση της πράξεως. Η έννοια επίσης των γεωγραφικών συνόρων είναι άγνωστη στα εγκλήματα του κυβερνοχώρου. Ειδικότερα, 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 Συνεργασίας είναι "παραχωρημένες" στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη.

7.4 Η Ελληνική Αστυνομική Πραγματικότητα

Στην Ελληνική Αστυνομία δεν υπάρχει ακόμα ειδικό Τμήμα, που να ερευνά αποκλειστικώς το έγκλημα στον κυβερνοχώρο. Το ερευνούμενο 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 την σχετική έρευνα συνδράμει με τις ειδικές της γνώσεις η Διεύθυνση Εγκληματολογικών Ερευνών (Δ.Ε.Ε.) 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 τεχνογνωσία στην εξέταση λογισμικού κατασχεθέντων ηλεκτρονικών υπολογιστών, στο ``σπάσιμο`` κωδίκων κλπ. 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 Υ.Δ.Τ. και έχει ως αρμοδιότητα την ανάπτυξη και την τεχνική υποστήριξη στον τομέα της πληροφορικής, για όλες τις υπηρεσίες της Αστυνομίας .

7.5 Συλλογή και διατήρηση των αποδεικτικών στοιχείων

Η ανακριτική τεχνική, όπως είναι η συλλογή των αποδεικτικών στοιχείων, η λήψη των μαρτυρικών καταθέσεων, η διενέργεια των ερευνών κλπ, απαιτεί διαφορετική τεχνική από εκείνη των ``κοινών`` εγκλημάτων . Κύριο χαρακτηριστικό της συλλογής και εκτίμησης των αποδεικτικών στοιχείων είναι ότι, οι νομικές γνώσεις του (προ-) ανακριτικού υπαλλήλου δεν επαρκούν για την έρευνα της υποθέσεως. Οι κατάλληλες και επαρκείς ειδικές τεχνικές γνώσεις είναι εξ ίσου σημαντικές -αν όχι και σημαντικότερες- από τις νομικές. Π.χ. η εσφαλμένη αποσύνδεση των καλωδίων του ηλεκτρονικού υπολογιστή, στον οποίο είναι ``αποθηκευμένα`` τα αποδεικτικά στοιχεία μπορεί να οδηγήσει στην εξαφάνισή (``χάσιμο``) τους. Η παρατηρητικότητα επίσης του (προ-) ανακριτικού υπαλλήλου είναι σημαντική π.χ. ο συνδυασμός αριθμών που μπορεί μεν να εμφανίζονται (εξωτερικώς) ως αριθμοί τηλεφώνων, ενδεχομένως να αποτελούν τα ``κλειδιά`` (passwords) πρόσβασης στο σύστημα ή ακόμα και τους κωδικούς αποκρυπτογράφησης, σε περίπτωση που τα στοιχεία (data) τηρούνται κρυπτογραφημένα. Μετά την συλλογή των αποδεικτικών στοιχείων σημαντική είναι η γνώση του (προ-) ανακριτικού υπαλλήλου για την διατήρησή τους. Η έκθεσή τους π.χ. σε ήλιο, υγρασία, σκόνη κλπ. ενδεχομένως να οδηγήσει στην καταστροφή τους.

7.6 Ηλεκτρονική απόδειξη

Η λεγομένη **ηλεκτρονική απόδειξη ("electronic evidence")** δεν ταυτίζεται με τα ``παραδοσιακά`` αποδεικτικά μέσα. Τα τελευταία αυτά είναι ``χειροπιαστά``, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα τα ηλεκτρονικά αποδεικτικά μέσα είναι κατά κανόνα ``μη χειροπιαστά`` μπορεί να τα κατευθύνει ή και να τα διαχειρίζεται κάποιος από μακριά, να αλλάζει την μορφή και το περιεχόμενό τους ή ακόμα και να τα εξαφανίζει με το πάτημα ενός πλήκτρου.

Παράδειγμα : ο εγκληματίας Α αποστέλλει με το ηλεκτρονικό ταχυδρομείο (e-mail) κρυπτογραφημένη επιστολή από την χώρα Χ, στον επίσης εγκληματία Β, ο οποίος διαμένει στην χώρα Ψ, αναφέροντάς του λεπτομέρειες σχετικά με την ελεγχομένη παράδοση (άρθρο 9 Ν. 1990/91) μεγάλης ποσότητος ναρκωτικών ουσιών. Η Αστυνομική Αρχή της χώρας που παρακολουθεί την περίπτωση διαπιστώνει ότι ο Β, δεν παραλαμβάνει αμέσως το ``γράμμα`` (e-mail), γιατί κατά την ώρα αποστολής - λήψεως έχει κλειστό τον ηλεκτρονικό υπολογιστή του. Ερωτάται: Σε ποιες νόμιμες ενέργειες μπορεί να προβεί η Αστυνομία προκειμένου να αποκτήσει και στη συνέχεια να χρησιμοποιήσει το ``κλειδί`` του κρυπτογραφημένου μηνύματος ; Θεωρείται το "e-mail" επιστολή τηλεγράφημα ή τηλεομοιοτυπικό έγγραφο (fax); Σε περίπτωση που αυτό (e-mail) θεωρείται ως επιστολή, πρέπει να εφαρμοστούν οι σχετικές διατάξεις περί ανοικτών επιστολών (Συνταγματική προστασία κλπ.) ή περί κλειστών επιστολών (ευκολότερη κατάσχεση κλπ.) Δικαιούται η Αστυνομία να κατάσχει το ``γράμμα`` (e-mail) στις εγκαταστάσεις του παροχέα ; Σε θετική περίπτωση δικαιούται να ανοίξει το e-mail και να το διαβάσει ; Όταν το e-mail βρίσκεται στις εγκαταστάσεις του παροχέα αποτελεί κλειστή ή ανοικτή επιστολή; Μπορεί η Αστυνομική Αρχή να υποχρεώσει τον παροχέα να της παραδώσει όλη την ηλεκτρονική αλληλογραφία μεταξύ Α και Β; Μπορεί να υποχρεωθεί ο παροχέας να φυλάττει για ορισμένο χρονικό διάστημα (και για πόσο) τα ``στοιχεία - δεδομένα`` (data) που ``περνούν`` από τις εγκαταστάσεις του; Και μόνο το παραπάνω απλό (για το διαδίκτυο) παράδειγμα αρκεί για να δώσει το μέγεθος των σημαντικών προβλημάτων που αντιμετωπίζει, αυτός που ασχολείται με την έρευνα του εγκλήματος στο διαδίκτυο.

7.7 Ηλεκτρονική Υπογραφή (digital Signature)

Χαρακτηριστική περίπτωση ηλεκτρονικής αποδείξεως αποτελεί η αξιολόγηση της ηλεκτρονικής ή ψηφιακής υπογραφής (digital Signature). **Ψηφιακή υπογραφή είναι η υπογραφή εκείνη που τίθεται στα (ηλεκτρονικά) έγγραφα, τα οποία διακινούνται δια μέσου του διαδικτύου(ή και των computers γενικότερο) από τον εκδότη του εγγράφου.** Έχει σχέση δηλ. η ψηφιακή υπογραφή με την γνησιότητα του εγγράφου και αποτελεί το αντίστοιχο της ιδιόχειρης (φυσικής) υπογραφής. Η ψηφιακή υπογραφή τίθεται σε συμφωνίες που γίνονται "εξ αποστάσεως" δηλ. οι αντισυμβαλλόμενοι βρίσκονται σε διαφορετικό τόπο. Η ψηφιακή υπογραφή είναι συνυφασμένη με την κρυπτογραφία. Βρίσκει πρακτική εφαρμογή στις Τράπεζες, στο ηλεκτρονικό εμπόριο, στις ηλεκτρονικές συναλλαγές και ειδικότερα στις συναλλαγές που γίνονται εξ αποστάσεως . Λέγοντας ηλεκτρονικό εμπόριο (**electronic commerce ή απλώς e- commerce**) εννοούμε την εμπορική

εκείνη δραστηριότητα που αναπτύσσεται δια μέσου συνδεδεμένων ηλεκτρονικών υπολογιστών (Internet).

Στο Ποινικό Δίκαιο ο Νομοθέτης προσδιορίζει την έννοια του ηλεκτρονικού εγγράφου στο άρθρο 13 περίπτ. γ΄ του Π.Κ., όπως αυτό τροποποιήθηκε με άρθρο το 2 του Ν.1805/88. Σύμφωνα λοιπόν με το άρθρο αυτό *έγγραφο είναι κάθε γραπτό που προορίζεται ή είναι πρόσφορο να αποδείξει γεγονός που έχει έννομη σημασία όπως και κάθε σημείο που προορίζεται να αποδείξει ένα τέτοιο γεγονός. Έγγραφο είναι και κάθε μέσο το οποίο χρησιμοποιείται από υπολογιστή ή περιφερειακή μνήμη υπολογιστή, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή , αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων, που δεν μπορούν να διαβιβαστούν 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.*

Σχετική με την έννοια του ηλεκτρονικού εγγράφου είναι και η διάταξη του άρθρου 444 περ. 3 Κ.Πολ.Δικ. σύμφωνα με την οποία ιδιωτικά έγγραφα θεωρούνται και φωτογραφικές ή κινηματογραφικές αναπαραστάσεις φωνοληψίες και κάθε άλλη μηχανικήαπεικόνιση.

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

8. Χαρακτηριστικά Παραδείγματα Απάτης και Παραπλάνησης

8.1 Η Περίπτωση του DirtyWorks.gr

Ο 35χρονος διαδικτυακός καλλιτέχνης και γλύπτης Δημήτρης Φωτίου αναστάτωσε την ελληνική ιντερνετική κοινότητα στις αρχές του 2005, όταν αποφάσισε να διακωμωδήσει το πάθος (ευσεβή πόθο) των Ελλήνων για διορισμό στο Δημόσιο. Ο εικαστικός δημιουργός που ασχολείται με το net art, δηλ. την τέχνη του Διαδικτύου, συνελήφθη τον Φεβρουάριο του 2005 από το Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας Αττικής και κατηγορήθηκε για απάτη σε βαθμό κακουργήματος. Το αδίκημά του ήταν ότι σχεδίασε την ιστοσελίδα http://www.dirtyworks.gr, στην οποία υποσχόταν προσλήψεις στο Δημόσιο, μετεγγραφές φοιτητών, νομιμοποίηση αυθαιρέτων και εξασφαλισμένη επιτυχία σε διαγωνισμούς του ΑΣΕΠ έναντι αμοιβής και όλα αυτά ως σχόλιο στα ρουσφέτια της εποχής μας. Το πρόβλημα που απασχόλησε την Αστυνομία ήταν βέβαια η πληρωμή των υπηρεσιών, η οποία γινόταν με πιστωτική κάρτα, αδίκημα σε βαθμό κακουργήματος. Όμως, η ιστοσελίδα ήταν έτσι σχεδιασμένη ώστε τα προσωπικά στοιχεία του χρήστη ποτέ δεν έφευγαν από τον υπολογιστή του, δεν κατέληγαν πουθενά και φυσικά δεν καταχωρούνταν ποτέ στον server του dirtyworks.gr, ώστε να μπορέσει να τα αξιοποιήσει ο οποιοσδήποτε. Υπήρχε βέβαια και μια προειδοποίηση (ψιλά γράμματα) στην κάτω δεξιά πλευρά της ιστοσελίδας, με την επισήμανση ότι όσα αναφέρονταν στην ιστοσελίδα είναι εικονικά. Έτσι, ο Δημήτρης Φωτίου αφέθηκε προσωρινά ελεύθερος με εγγύηση.

8.2 Η Περίπτωση της Amazon.gr

Το Πρωτοδικείο Σύρου έμελλε να είναι το πρώτο στην Ελλάδα που εκδίκασε υπόθεση ηλεκτρονικού εμπορίου και μάλιστα σε μια εποχή (1999) που η σχετική νομοθεσία ήταν ουσιαστικά ανύπαρκτη. Το θέμα είχε να κάνει με την πολύ γνωστή εταιρεία πώλησης βιβλίων και CD's (ηλεκτρονικό βιβλιοπωλείο) **amazon,** η οποία με έδρα το Delaware των ΗΠΑ κατοχύρωσε το όνομα χώρου (domain name) **amazon.com** και μέσω της ηλεκτρονικής διεύθυνσης www.amazon.com δεχόταν παραγγελίες απ' όλον τον κόσμο. Στην Ελλάδα, όπου η amazon δεν είχε φυσική παρουσία, εμφανίσθηκε μια άλλη εταιρεία η οποία με έδρα την Μύκονο ζήτησε και έλαβε τα domain names amazon.gr και amazon.com.gr από τον τότε αρμόδιο ελληνικό φορέα (ΙΤΕ) και ξεκίνησε να κάνει πωλήσεις βιβλίων και CD's.

Η αμερικανική εταιρεία amazon προσέφυγε στα δικαστήρια και κατέθεσε αίτηση ασφαλιστικών μέτρων τον Αύγουστο του 1999 στο Πρωτοδικείο Σύρου ζητώντας την απαγόρευση χρήσης των παραπάνω domain names θεωρώντας ότι με τη χρήση των παραπάνω ηλεκτρονικών διευθύνσεων δημιουργείται σύγχυση

στο καταναλωτικό κοινό καθώς οι αγοραστές έχουν την εντύπωση ότι παραγγέλνουν από το ελληνικό παράρτημα του διεθνούς ηλεκτρονικού βιβλιοπωλείου amazon.com. Το Δικαστήριο με την υπ' αριθμ. *637/1999* απόφασή του έκρινε ότι η ελληνική εταιρεία προσέβαλε το δικαίωμα της amazon.com στην επωνυμία και τον διακριτικό της τίτλο. Έτσι δικαίωσε την αμερικανική εταιρεία καθώς θεώρησε ότι δημιουργείται όντως σύγχυση στο καταναλωτικό κοινό δεδομένης της μεγάλης διεθνούς φήμης της, καθώς ο χρήστης που θέλει να συνδεθεί με το ελληνικό παράρτημα του διεθνούς ηλεκτρονικού βιβλιοπωλείου amazon.com, θα βρεθεί άθελά του σε μια άλλη άσχετη εταιρεία. Το δικαστήριο έκρινε ότι η ελληνική εταιρεία προσπάθησε να εκμεταλλευθεί τον διακριτικό τίτλο της amazon.com και να αυξήσει έτσι τις πωλήσεις της κατά παράβαση των χρηστών ηθών και της καλής πίστη και διέταξε την εταιρεία να σταματήσει να χρησιμοποιεί τον τίτλο amazon και να απενεργοποιήσει τα domain names amazon.gr και amazon.com.gr.

8.3 Η Περίπτωση της Εταιρείας Argos (Μεγάλη Βρετανία)

Η βρετανική εταιρεία Argos πραγματοποιεί πωλήσεις μέσω Internet αλλά ένα τραγικό λάθος των προγραμματιστών της, έφερε μια τηλεόραση των 299,99 λιρών Αγγλίας (περίπου 450 ευρώ) να φαίνεται ότι πωλείται προς 3 λίρες Αγγλίας (περίπου 4,5 ευρώ).Το πρόβλημα ήταν ότι κατά τη δημιουργία της σχετικής ιστοσελίδας έγινε στρογγυλοποίηση του ποσού στον πλησιέστερο ακέραιο αριθμό και μετά αποκοπή των 2 μηδενικών από την ακέραια ποσότητα. Μέχρι να αντιληφθούν οι υπεύθυνοι της εταιρείας το τραγικό λάθος, είχαν ήδη γίνει εκατοντάδες παραγγελίες συνολικής αξίας πάνω από 1,5 εκατομμύριο ευρώ.Η εταιρεία αποφάσισε να μην ικανοποιήσει τις παραγγελίες των πελατών της και ισχυρίσθηκε ότι δεν είχε καταρτισθεί σύμβαση μεταξύ της εταιρείας και των πελατών της, εφόσον η εταιρεία δεν επιβεβαίωσε τις παραγγελίες.

Δικηγόροι που εξέτασαν τις ιστοσελίδες της εταιρείας στο Διαδίκτυο ανέφεραν ότι δεν υπήρχε κάποια σημείωση από την εταιρεία ότι δεν φέρει ευθύνη για τυχόν λάθη αναγραφής στις τιμές των προϊόντων της. Ένας άλλος δικηγόρος ισχυρίζεται ότι αν μια εταιρεία αποδεχθεί ηλεκτρονικά μια πώληση ενός προϊόντος της, τότε μπορεί να θεωρηθεί ότι υπάρχει σύμβαση ανάμεσα στην εταιρεία (πωλητής) και τον καταναλωτή (αγοραστής).Ο πελάτης (χρήστης του Internet) που καταχώρησε στην ιστοσελίδα της Argos τον αριθμό της πιστωτικής του κάρτας και έλαβε έναν μοναδικό κωδικό παραγγελίας ως επιβεβαίωση, μπορεί να θεωρηθεί ότι έχει συνάψει σύμβαση με την εταιρεία για την πώληση του προϊόντος.

Υπάρχει βέβαια και η περίπτωση, αν η υπόθεση φθάσει στα δικαστήρια, να θεωρηθεί άκυρη η σύμβαση πώλησης αν το δικαστήριο αναγνωρίσει ότι έχει γίνει πράγματι λάθος που δεν ήταν εσκεμμένο. Στην περίπτωση αυτή θα πρέπει η εταιρεία να αποδείξει ότι έλαβε όλα τα απαραίτητα μέτρα προφύλαξης για να αποφύγει την παραπλάνηση του καταναλωτή.

8.4 Βιασμοί και κτηνοβασίες με παιδιά στο Διαδίκτυο

Υλικό παιδικής πορνογραφίας που παρουσίαζε παιδάκια ηλικίας 4 εώς 10 ετών να βιάζονται ή να αναγκάζονται να κάνουν σεξ, ακόμα και με ζώα,προωθούσε στο Internet ένα από τα μεγαλύτερα κυκλώματα παιδικής πορνογραφίας στη χώρα μας, που κατάφερε να εξαρθρώσει η Ασφάλεια Αττικής!

Περίπου είκοσι άτομα εμπλέκονται σε αυτή την ανατριχιαστική υπόθεση, ενώ όπως έγινε γνωστό από τα αποτελέσματα της έρευνας της Αστυνομίας, που κράτησε περισσότερο από 6 μήνες, η σπείρα δρούσε από τις αρχές του 2004 και σύμφωνα με αξιωματικούς της Ασφάλειας Αττικής, διακινούσαν ιδιαίτερα σκληρό υλικό παιδικής πορνογραφίας, ακόμα και φωτογραφίες με βιασμούς παιδιών. Οι έρευνες συνεχίζονται για να διαπιστωθεί αν στην υπόθεση ενέχονται και άλλα άτομα, καθώς και πόσα από τα παιδιά που αναγκάζονται να συμμετάσχουν σε ανατριχιαστική σεξουαλική δραστηριότητα με ενηλίκους κατάγονται από την Ελλάδα.

Είναι η μεγαλύτερη υπόθεση παιδικής πορνογραφίας που αποκαλύπτεται μέχρι σήμερα στη χώρα μας και η επιχείρηση για την εξιχνίασή της συνεχίζεται στην Αθήνα ,τη Λάρισα, την Ελευσίνα, τη Νάουσα, τη Θεσσαλονίκη, τη Δράμα, τη Βέροια, τις Σέρρες, καθώς και τον Αγ. Νικόλαο και τα Χανιά της Κρήτης. Τα πέντε άτομα που συνελήφθησαν ανάμεσά τους και ένας καθηγητής πανεπιστημίου οδηγήθηκαν στους κατά τόπους αρμόδιους εισαγγελείς, ενώ η έρευνα συνεχίζεται και σε άλλες χώρες μέσω διεθνούς αστυνομικής συνεργασίας

Συμπεράσματα

Η τεχνολογία, οι ηλεκτρονικοί υπολογιστές και ο κυβερνοχώρος έχουν εισέλθει για καλά στη ζωή μας. Ακόμα και στην επαγγελματική ζωή του Νομικού , η γραπτή - έντυπη δομή του Δικαίου τείνει να αντικατασταθεί από την ``ηλεκτρονική εποχή του Δικαίου ``. Όποιος αρνείται ν΄ ασχοληθεί με την σύγχρονη τεχνολογία ομοιάζει με αυτόν που, όταν ανακαλύφθηκε το αυτοκίνητο αρνιόταν ν΄ ανέβει σ΄ αυτό και προτιμούσε να πηγαίνει με το γαϊδουράκι ή στην καλύτερη περίπτωση με το άλογο .

Η προσέγγιση των νομικών θεμάτων που αφορούν τον Κυβερνοχώρο ενέχει την δυσκολία ότι προϋποθέτει όχι μόνο νομικές αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computer) και διαδικτύου (internet). Είναι πολύ δύσκολο να αντιληφθεί κάποιος τα συμβαίνοντα στο πεδίο του εγκλήματος στον κυβερνοχώρο, χωρίς την κατοχή αυτών των τεχνικών γνώσεων. Οι τεχνικές όμως γνώσεις δεν επαρκούν γα την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι για την κατανόηση των νομικών θεμάτων του διαδικτύου, ο νομικός πρέπει να διαθέτει τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις.

Το ήδη υπάρχον "νομικό οπλοστάσιο δεν επαρκεί για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Γι΄ αυτό απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών υποστάσεων εγκλημάτων, που να θέτουν όρια στην συμπεριφορά όσων χρησιμοποιούν το διαδίκτυο. Κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθεί υπόψη η ελεύθερη διακίνηση των ιδεών και οι λοιπές Συνταγματικές Αρχές, που ισχύουν στον κοινό ``Δικαιϊκό χώρο``.

Οι Εισαγγελικές, Δικαστικές, Αστυνομικές κλπ Αρχές δεν έχουν μέχρι στιγμής τις απαιτούμενες γνώσεις, για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Και αυτό είναι πολύ λογικό, αφού ουδεμία εκπαίδευση έχουν υποστεί μέχρι τώρα. Είναι βέβαιο δε ότι, εάν η πολιτεία δεν φροντίσει για την εκπαίδευσή τους στα αντίστοιχα θέματα, θα υπάρξει (στο πολύ σύντομο μέλλον) αδυναμία απονομής ορθής δικαιοσύνης σε θέματα εγκληματικότητας του κυβερνοχώρου και ηλεκτρονικής εγκληματικότητας γενικότερα. Απαραίτητη επομένως καθίσταται η άμεση εκπαίδευση όσων Αρχών (Εισαγγελικών, Δικαστικών, Αστυνομικών) ασχολούνται με θέματα διαδικτύου και ηλεκτρονικής εγκληματικότητας γενικότερα.

- **Η Τεχνολογία προχωράει πιο γρήγορα από το Δίκαιο.**

- **Το Δίκαιο αρέσκεται να βρίσκεται σε σταθερό περιβάλλον. Κάθε απότομη αλλαγή στις κοινωνικές, οικονομικές, πολιτισμικές ή τεχνολογικές συνθήκες, οι οποίες προκαλούν αναταράξεις στο περιβάλλον αυτό, θέτει το δίκαιο σε έκδηλη αμηχανία.**

- **Το τέλειο έγκλημα δεν μπορεί να γίνει πουθενά, ούτε και στο Διαδίκτυο. Τα ηλεκτρονικά αποτυπώματα (ψηφιακά ίχνη) που αφήνουν οι δράστες καθώς περιηγούνται στο Internet αποτελούν και την επικήρυξή τους. Από εκεί αρχίζει η εξιχνίαση που οδηγεί τελικά στην σύλληψή τους.**

- **Όποιος χρησιμοποιεί το Internet, θα πρέπει να γνωρίζει ότι μπορεί ένας άλλος χρήστης να εισέλθει στον υπολογιστή του και να αντιγράψει όλα τα αρχεία του ή να κάνει όποια ζημιά αυτός θέλει.**

- **Στο Internet έχουν χαθεί οι έννοιες του προσωπικού και του ιδιωτικού και ο παγκόσμιος εγκληματίας έχει εγκατασταθεί στα καλώδια του υπολογιστή που έχουμε στο σπίτι μας.**

- **Από τη στιγμή που κανείς δεν είναι σε θέση να ελέγξει το περιεχόμενό του, το Internet αποτελεί τον Παράδεισο της παρανομίας, της φάρσας και της απάτης.**

- **Κανείς δεν μπορεί να γλιτώσει τα προσωπικά δεδομένα του, όσο κι αν προσπαθήσει, από τη στιγμή που θα αποφασίσει να συνδεθεί και να περιπλανηθεί (σερφάρει) στο Internet. Σκοπός της παρακολούθησης και της καταγραφής των προσωπικών μας δεδομένων είναι η σκιαγράφηση του καταναλωτικού μας προφίλ.**

- **Αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν και από τις διωκτικές αρχές για τον εντοπισμό των κακοποιών που παρανομούν στο Internet ή επικοινωνούν μέσω του Internet.**

- **Το ηλεκτρονικό έγκλημα, δηλ. το έγκλημα που γίνεται με τη βοήθεια των υπολογιστών και κυρίως μέσω του Διαδικτύου (Internet), οργανώνεται και εξαπλώνεται ολοένα και περισσότερο καθώς οι ηλεκτρονικοί εγκληματίες βρίσκουν πρόσφορο έδαφος στο Διαδίκτυο.**

- **Το Διαδίκτυο τους δίνει τη δυνατότητα να δρουν αποτελεσματικά και να κρύβονται εύκολα.**

✹ Προτάσεις :

- **Απαραίτητη καθίσταται η θέσπιση νέων αντικειμενικών υποστάσεων εγκλημάτων, που να θέτουν όρια στην συμπεριφορά όσων χρησιμοποιούν το διαδίκτυο.**

- **Κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθεί υπόψη η ελεύθερη διακίνηση των ιδεών και οι λοιπές Συνταγματικές Αρχές, που ισχύουν στον κοινό ``Δικαιϊκό χώρο``.**

- **Απαραίτητη καθίσταται η εκπαίδευση όσων Αρχών (Εισαγγελικών, Δικαστικών, Αστυνομικών) εμπλέκονται σε θέματα διαδικτύου και ηλεκτρονικής εγκληματικότητας γενικότερα.**

ΠΗΓΕΣ – ΒΙΒΛΙΟΓΡΑΦΙΑ

www.diaplous.org/library/nomothesia.php

http://www.softlab.ece.ntua.gr

Λίλιαν Μήτρου: ΤΟ ΔΙΚΑΙΟ ΣΤΗΝ ΚΟΙΝΩΝΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ,

εκδ. 2002, ISBN 960-301-664-0

Ιωάννης Καράκωστας : ΔΙΚΑΙΟ & INTERNET Β΄ ΕΚΔΟΣΗ , εκδ. 2003,

ISBN 960-420-199-9

Άρθρο της εφημερίδας Απογευματινής, Αρ. φύλλου 16.906

Τετάρτη 19 Οκτωβρίου 2005

http://www.uth.gr/main/help/help-desk/internet/internet3.html

http://www.lawnet.gr/pages/eofn/2/cybercrime.asp

Στους γονείς μου και στον

καλό μου φίλο Κώστα

ΔΗΛΩΣΗ ΠΕΡΙ ΛΟΓΟΚΛΟΠΗΣ

Όλες οι προτάσεις οι οποίες παρουσιάζονται σ'αυτό το κείμενο και οι οποίες ανήκουν σε άλλους αναγνωρίζονται από τα εισαγωγικά και υπάρχει η σαφής δήλωση του συγγραφέα. Τα υπόλοιπα γραφόμενα είναι επινόηση του γράφοντος ο οποίος φέρει και την καθολική ευθύνη γι'αυτό το κείμενο και δηλώνω υπεύθυνα ότι δεν υπάρχει λογοκλοπή γι'αυτό το κείμενο.

Ονοματεπώνυμο: Χρήστου Γεώργιος

Υπογραφή: 

Ημερομηνία:21/11/2005